



## **3Com Switch 4800G Family** Command Reference Guide

Switch 4800G 24-Port

Switch 4800G 48-Port

Switch 4800G PWR 24-Port

Switch 4800G PWR 48-Port

Switch 4800G 24-Port SFP

Product Version:  
Release 2202  
Manual Version:  
6W100-20090120  
[www.3com.com](http://www.3com.com)

**3Com Corporation**  
350 Campus Drive, Marlborough,  
MA, USA 01752 3064



Copyright © 2009, 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

## **UNITED STATES GOVERNMENT LEGEND**

*If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:*

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com and the 3Com logo are registered trademarks of 3Com Corporation.

All other company and product names may be trademarks of the respective companies with which they are associated.

## **ENVIRONMENTAL STATEMENT**

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

### **End of Life Statement**

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

### **Regulated Materials Statement**

3Com products do not contain any hazardous or ozone-depleting material.

### **Environmental Statement about the Documentation**

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

# About This Manual

## Organization

3Com Switch 4800G Family Command Reference Guide is organized as follows:

Volume	Features			
00-Command Index	Command Index			
01-Access Volume	Ethernet Interface	Link Aggregation	Port Isolation	Service Loopback Group
	DLDP	LLDP	Smart Link	Monitor Link
	VLAN	GVRP	QinQ	BPDU Tunneling
	VLAN Mapping	Ethernet OAM	Connectivity Fault Detection	MSTP
	RRPP	Port Mirroring		
02-IP Services Volume	IP Addressing	ARP	DHCP	DNS
	IP Performance Optimization	UDP Helper	URPF	IPv6 Basics
	Tunneling	sFlow		
03-IP Routing Volume	IP Routing Table Display	Static Routing	RIP	OSPF
	IS-IS	BGP	IPv6 Static Routing	RIPng
	OSPFv3	IPv6 IS-IS	IPv6 BGP	Route Policy
	BFD	MCE		
04-Multicast Volume	Multicast Routing and Forwarding	IGMP	PIM	MSDP
	MBGP	IGMP Snooping	Multicast VLAN	IPv6 Multicast Routing and Forwarding
	MLD	IPv6 PIM	IPv6 MBGP	MLD Snooping
	IPv6 Multicast VLAN			
05-QoS Volume	QoS	User Profile		
06-Security Volume	AAA	802.1X	HABP	MAC Authentication
	Portal	Port Security	IP Source Guard	SSH2.0
	PKI	SSL	Public Key	ACL

Volume	Features			
07-System Volume	Login	Basic System Configuration	Device Management	File System Management
	HTTP	SNMP	RMON	MAC Address Table Management
	System Maintaining and Debugging	Information Center	PoE	Track
	NQA	NTP	VRRP	Hotfix
	Cluster Management	IRF Stack	IPC	

## Conventions

The manual uses the following conventions:

### Command conventions

Convention	Description
<b>Boldface</b>	The keywords of a command line are in <b>Boldface</b> .
<i>italic</i>	Command arguments are in <i>italic</i> .
[ ]	Items (keywords or arguments) in square brackets [ ] are optional.
{ x   y   ... }	Alternative items are grouped in braces and separated by vertical bars. One is selected.
[ x   y   ... ]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.
{ x   y   ... }*	Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected.
[ x   y   ... ]*	Optional alternative items are grouped in square brackets and separated by vertical bars. Many or none can be selected.
&<1-n>	The argument(s) before the ampersand (&) sign can be entered 1 to n times.
#	A line starting with the # sign is comments.

### GUI conventions

Convention	Description
< >	Button names are inside angle brackets. For example, click <OK>.
[ ]	Window names, menu items, data table and field names are inside square brackets. For example, pop up the [New User] window.
/	Multi-level menus are separated by forward slashes. For example, [File/Create/Folder].

## Symbols

Convention	Description
 <b>Warning</b>	Means reader be extremely careful. Improper operation may cause bodily injury.
 <b>Caution</b>	Means reader be careful. Improper operation may cause data loss or damage to equipment.
 <b>Note</b>	Means a complementary description.

## Related Documentation

In addition to this manual, each 3com Switch 4800G documentation set includes the following:

Manual	Description
3Com Switch 4800G Family Configuration Guide	Describe how to configure your 4800G Switch using the supported protocols and CLI commands.
3Com Switch 4800G Family Getting Started Guide	This guide provides all the information you need to install and use the 3Com Switch 4800G Family.

## Obtaining Documentation

You can access the most up-to-date 3Com product documentation on the World Wide Web at this URL:  
<http://www.3com.com>.

# Appendix A Command Index

---

The command index includes all the commands in the *Command Manual*, which are arranged alphabetically.

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)

## A

abr-summary (OSPF area view)	IP Routing Volume-04-OSPF	1-1
abr-summary (OSPFv3 area view)	IP Routing Volume-09-OSPFv3	1-1
access-limit	Security Volume-01-AAA	1-1
access-limit enable	Security Volume-01-AAA	1-1
accounting	QoS Volume-01-QoS	1-6
accounting default	Security Volume-01-AAA	1-2
accounting lan-access	Security Volume-01-AAA	1-3
accounting login	Security Volume-01-AAA	1-4
accounting optional	Security Volume-01-AAA	1-5
accounting portal	Security Volume-01-AAA	1-6
acl	Security Volume-12-ACL	1-5
acl	System Volume-01-Login	2-1
acl copy	Security Volume-12-ACL	1-6
acl ipv6	Security Volume-12-ACL	1-20
acl ipv6 copy	Security Volume-12-ACL	1-21
acl ipv6 name	Security Volume-12-ACL	1-22
acl name	Security Volume-12-ACL	1-7
activation-key	System Volume-01-Login	1-1
active region-configuration	Access Volume-16-MSTP	1-1
add-member	System Volume-17-Cluster Management	1-14
administrator-address	System Volume-17-Cluster Management	1-15
advantage-factor	System Volume-13-NQA	1-1

aggregate	IP Routing Volume-06-BGP	1-1
aggregate (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-1
aggregate (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-1
aggregate (MBGP family view)	IP Multicast Volume-05-MBGP	1-1
apply as-path	IP Routing Volume-12-Route Policy	1-1
apply comm-list delete	IP Routing Volume-12-Route Policy	1-2
apply community	IP Routing Volume-12-Route Policy	1-2
apply cost	IP Routing Volume-12-Route Policy	1-3
apply cost-type	IP Routing Volume-12-Route Policy	1-4
apply extcommunity	IP Routing Volume-12-Route Policy	1-5
apply ip-address next-hop	IP Routing Volume-12-Route Policy	1-21
apply ipv6 next-hop	IP Routing Volume-12-Route Policy	1-26
apply isis	IP Routing Volume-12-Route Policy	1-5
apply local-preference	IP Routing Volume-12-Route Policy	1-6
apply origin	IP Routing Volume-12-Route Policy	1-7
apply poe-profile	System Volume-11-PoE	1-1
apply poe-profile interface	System Volume-11-PoE	1-2
apply preference	IP Routing Volume-12-Route Policy	1-8
apply preferred-value	IP Routing Volume-12-Route Policy	1-8
apply tag	IP Routing Volume-12-Route Policy	1-9
area (OSPF view)	IP Routing Volume-04-OSPF	1-2
area (OSPFv3 view)	IP Routing Volume-09-OSPFv3	1-2
area-authentication-mode	IP Routing Volume-05-IS-IS	1-1
arp anti-attack active-ack enable	IP Services Volume-02-ARP	3-3
arp anti-attack source-mac	IP Services Volume-02-ARP	3-4
arp anti-attack source-mac aging-time	IP Services Volume-02-ARP	3-5
arp anti-attack source-mac exclude-mac	IP Services Volume-02-ARP	3-6
arp anti-attack source-mac threshold	IP Services Volume-02-ARP	3-6
arp anti-attack valid-ack enable	IP Services Volume-02-ARP	3-8
arp check enable	IP Services Volume-02-ARP	1-1
arp detection enable	IP Services Volume-02-ARP	3-9

arp detection mode	IP Services Volume-02-ARP	3-10
arp detection static-bind	IP Services Volume-02-ARP	3-11
arp detection trust	IP Services Volume-02-ARP	3-11
arp detection validate	IP Services Volume-02-ARP	3-12
arp max-learning-num	IP Services Volume-02-ARP	1-1
arp rate-limit	IP Services Volume-02-ARP	3-8
arp resolving-route enable	IP Services Volume-02-ARP	3-3
arp source-suppression enable	IP Services Volume-02-ARP	3-1
arp source-suppression limit	IP Services Volume-02-ARP	3-1
arp static	IP Services Volume-02-ARP	1-2
arp timer aging	IP Services Volume-02-ARP	1-3
asbr-summary	IP Routing Volume-04-OSPF	1-2
ascii	System Volume-04-File System Management	2-6
attribute	Security Volume-09-PKI	1-1
authentication default	Security Volume-01-AAA	1-7
authentication lan-access	Security Volume-01-AAA	1-8
authentication login	Security Volume-01-AAA	1-8
authentication portal	Security Volume-01-AAA	1-9
authentication-mode	IP Routing Volume-04-OSPF	1-3
authentication-mode	System Volume-01-Login	1-2
authorization command	Security Volume-01-AAA	1-10
authorization default	Security Volume-01-AAA	1-11
authorization lan-access	Security Volume-01-AAA	1-12
authorization login	Security Volume-01-AAA	1-13
authorization portal	Security Volume-01-AAA	1-14
authorization-attribute	Security Volume-01-AAA	1-15
auto-build	System Volume-17-Cluster Management	1-16
auto-cost enable	IP Routing Volume-05-IS-IS	1-2
auto-execute command	System Volume-01-Login	1-3
auto-rp enable	IP Multicast Volume-03-PIM	1-1

# B

backup startup-configuration	System Volume-04-File System Management	1-15
balance (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-2
balance (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-2
balance (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-2
balance (MBGP family view)	IP Multicast Volume-05-MBGP	1-2
bandwidth-reference	IP Routing Volume-09-OSPFv3	1-2
bandwidth-reference (IS-IS view)	IP Routing Volume-05-IS-IS	1-3
bandwidth-reference (OSPF view)	IP Routing Volume-04-OSPF	1-4
bestroute as-path-neglect (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-3
bestroute as-path-neglect (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-3
bestroute as-path-neglect (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-3
bestroute as-path-neglect (MBGP family view)	IP Multicast Volume-05-MBGP	1-3
bestroute compare-med (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-4
bestroute compare-med (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-3
bestroute compare-med (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-3
bestroute compare-med (MBGP family view)	IP Multicast Volume-05-MBGP	1-4
bestroute med-confederation (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-5
bestroute med-confederation (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-4
bestroute med-confederation (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-4
bestroute med-confederation (MBGP family view)	IP Multicast Volume-05-MBGP	1-4
bfd authentication-mode	IP Routing Volume-13-BFD	1-1
bfd detect-multiplier	IP Routing Volume-13-BFD	1-2
bfd echo-source-ip	IP Routing Volume-13-BFD	1-3
bfd min-echo-receive-interval	IP Routing Volume-13-BFD	1-3

bfd min-receive-interval	IP Routing Volume-13-BFD	1-4
bfd min-transmit-interval	IP Routing Volume-13-BFD	1-5
bfd session init-mode	IP Routing Volume-13-BFD	1-5
bgp	IP Routing Volume-06-BGP	1-5
bims-server	IP Services Volume-03-DHCP	1-1
binary	System Volume-04-File System Management	2-7
bind-attribute	Security Volume-01-AAA	1-17
black-list add-mac	System Volume-17-Cluster Management	1-17
black-list delete-mac	System Volume-17-Cluster Management	1-18
bootfile-name	IP Services Volume-03-DHCP	1-2
boot-loader file	System Volume-03-Device Management	1-1
bootrom	System Volume-03-Device Management	1-2
bootrom-update security-check enable	System Volume-03-Device Management	1-4
bpdu-tunnel dot1q stp	Access Volume-12-BPDU Tunneling	1-1
bpdu-tunnel tunnel-dmac	Access Volume-12-BPDU Tunneling	1-2
broadcast-suppression	Access Volume-01-Ethernet Interface	1-1
bsr-policy (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-1
bsr-policy (PIM view)	IP Multicast Volume-03-PIM	1-2
build	System Volume-17-Cluster Management	1-18
bye	Security Volume-08-SSH2.0	1-16
bye	System Volume-04-File System Management	2-7
<b>C</b>		
ca identifier	Security Volume-09-PKI	1-2
cache-sa-enable	IP Multicast Volume-04-MSDP	1-1
car	QoS Volume-01-QoS	1-6

c-bsr (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-2
c-bsr (PIM view)	IP Multicast Volume-03-PIM	1-2
c-bsr admin-scope	IP Multicast Volume-03-PIM	1-3
c-bsr global	IP Multicast Volume-03-PIM	1-4
c-bsr group	IP Multicast Volume-03-PIM	1-4
c-bsr hash-length (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-2
c-bsr hash-length (PIM view)	IP Multicast Volume-03-PIM	1-5
c-bsr holdtime (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-3
c-bsr holdtime (PIM view)	IP Multicast Volume-03-PIM	1-6
c-bsr interval (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-4
c-bsr interval (PIM view)	IP Multicast Volume-03-PIM	1-6
c-bsr priority (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-5
c-bsr priority (PIM view)	IP Multicast Volume-03-PIM	1-7
cd	Security Volume-08-SSH2.0	1-16
cd	System Volume-04-File System Management	1-1
cd	System Volume-04-File System Management	2-8
cdup	Security Volume-08-SSH2.0	1-17
cdup	System Volume-04-File System Management	2-8
certificate request entity	Security Volume-09-PKI	1-3
certificate request from	Security Volume-09-PKI	1-3
certificate request mode	Security Volume-09-PKI	1-4
certificate request polling	Security Volume-09-PKI	1-5
certificate request url	Security Volume-09-PKI	1-5
cfd cc enable	Access Volume-15-Connectivity Fault Detection	1-1
cfd cc interval	Access Volume-15-Connectivity Fault Detection	1-1
cfd enable	Access Volume-15-Connectivity Fault Detection	1-2
cfd linktrace	Access Volume-15-Connectivity Fault Detection	1-3

cfid linktrace auto-detection	Access Volume-15-Connectivity Fault Detection	1-4
cfid loopback	Access Volume-15-Connectivity Fault Detection	1-5
cfid ma	Access Volume-15-Connectivity Fault Detection	1-6
cfid md	Access Volume-15-Connectivity Fault Detection	1-7
cfid mep	Access Volume-15-Connectivity Fault Detection	1-7
cfid mep enable	Access Volume-15-Connectivity Fault Detection	1-8
cfid mip-rule	Access Volume-15-Connectivity Fault Detection	1-9
cfid remote-mep	Access Volume-15-Connectivity Fault Detection	1-10
cfid service-instance	Access Volume-15-Connectivity Fault Detection	1-11
check region-configuration	Access Volume-16-MSTP	1-1
checkzero	IP Routing Volume-03-RIP	1-1
checkzero	IP Routing Volume-08-RIPng	1-1
ciphersuite	Security Volume-10-SSL	1-1
circuit-cost	IP Routing Volume-05-IS-IS	1-3
classifier behavior	QoS Volume-01-QoS	1-17
client-verify enable	Security Volume-10-SSL	1-2
clock datetime	System Volume-02-Basic System Configuration	1-1
clock summer-time one-off	System Volume-02-Basic System Configuration	1-1
clock summer-time repeating	System Volume-02-Basic System Configuration	1-2
clock timezone	System Volume-02-Basic System Configuration	1-4
close	System Volume-04-File System Management	2-9
close-mode wait	Security Volume-10-SSL	1-2

cluster	System Volume-17-Cluster Management	1-19
cluster enable	System Volume-17-Cluster Management	1-20
cluster switch-to	System Volume-17-Cluster Management	1-21
cluster-local-user	System Volume-17-Cluster Management	1-21
cluster-mac	System Volume-17-Cluster Management	1-22
cluster-mac syn-interval	System Volume-17-Cluster Management	1-23
cluster-snmp-agent community	System Volume-17-Cluster Management	1-23
cluster-snmp-agent group v3	System Volume-17-Cluster Management	1-24
cluster-snmp-agent mib-view included	System Volume-17-Cluster Management	1-25
cluster-snmp-agent usm-user v3	System Volume-17-Cluster Management	1-26
codec-type	System Volume-13-NQA	1-1
command-privilege level	System Volume-02-Basic System Configuration	1-5
common-name	Security Volume-09-PKI	1-6
compare-different-as-med (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-6
compare-different-as-med (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-5
compare-different-as-med (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-5
compare-different-as-med (MBGP family view)	IP Multicast Volume-05-MBGP	1-5
confederation id	IP Routing Volume-06-BGP	1-7
confederation nonstandard	IP Routing Volume-06-BGP	1-8
confederation peer-as	IP Routing Volume-06-BGP	1-8
control-vlan	Access Volume-17-RRPP	1-1

copy	System Volume-04-File System Management	1-2
copyright-info enable	System Volume-02-Basic System Configuration	1-6
cost-style	IP Routing Volume-05-IS-IS	1-4
country	Security Volume-09-PKI	1-7
crl check	Security Volume-09-PKI	1-7
crl update-period	Security Volume-09-PKI	1-8
crl url	Security Volume-09-PKI	1-8
c-rp (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-5
c-rp (PIM view)	IP Multicast Volume-03-PIM	1-8
c-rp advertisement-interval (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-6
c-rp advertisement-interval (PIM view)	IP Multicast Volume-03-PIM	1-9
c-rp holdtime (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-7
c-rp holdtime (PIM view)	IP Multicast Volume-03-PIM	1-10
crp-policy (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-8
crp-policy (PIM view)	IP Multicast Volume-03-PIM	1-10
cut connection	Security Volume-01-AAA	1-18
<b>D</b>		
dampening (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-9
dampening (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-6
dampening (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-6
dampening (MBGP family view)	IP Multicast Volume-05-MBGP	1-6
databits	System Volume-01-Login	1-4
data-fill	System Volume-13-NQA	1-2
data-flow-format (HWTACACS scheme view)	Security Volume-01-AAA	3-1
data-flow-format (RADIUS scheme view)	Security Volume-01-AAA	2-1
data-size	System Volume-13-NQA	1-3
debugging	System Volume-04-File System Management	2-10
debugging	System Volume-09-System Maintaining and Debugging	1-8

default	IP Routing Volume-04-OSPF	1-5
default cost	IP Routing Volume-09-OSPFv3	1-3
default cost (RIP view)	IP Routing Volume-03-RIP	1-2
default cost (RIPng view)	IP Routing Volume-08-RIPng	1-2
default ipv4-unicast	IP Routing Volume-06-BGP	1-10
default local-preference (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-11
default local-preference (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-7
default local-preference (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-7
default local-preference (MBGP family view)	IP Multicast Volume-05-MBGP	1-6
default med (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-12
default med (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-7
default med (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-7
default med (MBGP family view)	IP Multicast Volume-05-MBGP	1-7
default-cost (OSPF area view)	IP Routing Volume-04-OSPF	1-5
default-cost (OSPFv3 area view)	IP Routing Volume-09-OSPFv3	1-4
default-route	IP Routing Volume-03-RIP	1-2
default-route imported (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-13
default-route imported (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-8
default-route imported (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-8
default-route imported (MBGP family view)	IP Multicast Volume-05-MBGP	1-8
default-route-advertise	IP Routing Volume-09-OSPFv3	1-4
default-route-advertise (IS-IS view)	IP Routing Volume-05-IS-IS	1-5
default-route-advertise (OSPF view)	IP Routing Volume-04-OSPF	1-6
delete	Security Volume-08-SSH2.0	1-18
delete	System Volume-04-File System Management	1-3
delete	System Volume-04-File System Management	2-11
delete ipv6 static-routes all	IP Routing Volume-07-IPv6 Static Routing	1-1

delete static-routes all	IP Routing Volume-02-Static Routing	1-1
delete-member	System Volume-17-Cluster Management	1-27
description	Access Volume-01-Ethernet Interface	1-2
description	Access Volume-02-Link Aggregation	1-1
description	Access Volume-09-VLAN	1-1
description	IP Routing Volume-14-MCE	1-1
description (any NQA test type view)	System Volume-13-NQA	1-4
description (for IPv4)	Security Volume-12-ACL	1-8
description (for IPv6)	Security Volume-12-ACL	1-22
description (OSPF/OSPF area view)	IP Routing Volume-04-OSPF	1-7
destination	IP Services Volume-09-Tunneling	1-1
destination ip	System Volume-13-NQA	1-5
destination port	System Volume-13-NQA	1-5
dhcp enable	IP Services Volume-03-DHCP	1-2
dhcp relay address-check	IP Services Volume-03-DHCP	2-1
dhcp relay information circuit-id format-type	IP Services Volume-03-DHCP	2-2
dhcp relay information circuit-id string	IP Services Volume-03-DHCP	2-2
dhcp relay information enable	IP Services Volume-03-DHCP	2-3
dhcp relay information format	IP Services Volume-03-DHCP	2-4
dhcp relay information remote-id format-type	IP Services Volume-03-DHCP	2-5
dhcp relay information remote-id string	IP Services Volume-03-DHCP	2-6
dhcp relay information strategy	IP Services Volume-03-DHCP	2-7
dhcp relay release ip	IP Services Volume-03-DHCP	2-7
dhcp relay security static	IP Services Volume-03-DHCP	2-8
dhcp relay security tracker	IP Services Volume-03-DHCP	2-9
dhcp relay server-detect	IP Services Volume-03-DHCP	2-9
dhcp relay server-group	IP Services Volume-03-DHCP	2-10
dhcp relay server-select	IP Services Volume-03-DHCP	2-11
dhcp select relay	IP Services Volume-03-DHCP	2-12
dhcp select server global-pool	IP Services Volume-03-DHCP	1-4
dhcp server apply ip-pool	IP Services Volume-03-DHCP	1-3

dhcp server detect	IP Services Volume-03-DHCP	1-5
dhcp server forbidden-ip	IP Services Volume-03-DHCP	1-5
dhcp server ip-pool	IP Services Volume-03-DHCP	1-6
dhcp server ping packets	IP Services Volume-03-DHCP	1-7
dhcp server ping timeout	IP Services Volume-03-DHCP	1-7
dhcp server relay information enable	IP Services Volume-03-DHCP	1-8
dhcp-snooping	IP Services Volume-03-DHCP	4-1
dhcp-snooping information circuit-id format-type	IP Services Volume-03-DHCP	4-2
dhcp-snooping information circuit-id string	IP Services Volume-03-DHCP	4-2
dhcp-snooping information enable	IP Services Volume-03-DHCP	4-3
dhcp-snooping information format	IP Services Volume-03-DHCP	4-4
dhcp-snooping information remote-id format-type	IP Services Volume-03-DHCP	4-5
dhcp-snooping information remote-id string	IP Services Volume-03-DHCP	4-6
dhcp-snooping information strategy	IP Services Volume-03-DHCP	4-7
dhcp-snooping trust	IP Services Volume-03-DHCP	4-7
dir	Security Volume-08-SSH2.0	1-18
dir	System Volume-04-File System Management	1-4
dir	System Volume-04-File System Management	2-11
disconnect	System Volume-04-File System Management	2-13
display acl	Security Volume-12-ACL	1-9
display acl ipv6	Security Volume-12-ACL	1-23
display acl resource	Security Volume-12-ACL	1-1
display arp	IP Services Volume-02-ARP	1-4
display arp anti-attack source-mac	IP Services Volume-02-ARP	3-7
display arp detection	IP Services Volume-02-ARP	3-13
display arp detection statistics	IP Services Volume-02-ARP	3-13
display arp <i>ip-address</i>	IP Services Volume-02-ARP	1-5
display arp source-suppression	IP Services Volume-02-ARP	3-2
display arp timer aging	IP Services Volume-02-ARP	1-6

display arp vpn-instance	IP Services Volume-02-ARP	1-6
display bfd debugging-switches	IP Routing Volume-13-BFD	1-6
display bfd interface	IP Routing Volume-13-BFD	1-7
display bfd paf	IP Routing Volume-13-BFD	1-8
display bfd session	IP Routing Volume-13-BFD	1-9
display bgp group	IP Routing Volume-06-BGP	1-13
display bgp ipv6 group	IP Routing Volume-11-IPv6 BGP	1-9
display bgp ipv6 multicast group	IP Multicast Volume-11-IPv6 MBGP	1-12
display bgp ipv6 multicast network	IP Multicast Volume-11-IPv6 MBGP	1-13
display bgp ipv6 multicast paths	IP Multicast Volume-11-IPv6 MBGP	1-14
display bgp ipv6 multicast peer	IP Multicast Volume-11-IPv6 MBGP	1-15
display bgp ipv6 multicast routing-table	IP Multicast Volume-11-IPv6 MBGP	1-16
display bgp ipv6 multicast routing-table as-path-acl	IP Multicast Volume-11-IPv6 MBGP	1-18
display bgp ipv6 multicast routing-table community	IP Multicast Volume-11-IPv6 MBGP	1-19
display bgp ipv6 multicast routing-table community-list	IP Multicast Volume-11-IPv6 MBGP	1-20
display bgp ipv6 multicast routing-table dampened	IP Multicast Volume-11-IPv6 MBGP	1-20
display bgp ipv6 multicast routing-table dampening parameter	IP Multicast Volume-11-IPv6 MBGP	1-21
display bgp ipv6 multicast routing-table different-origin-as	IP Multicast Volume-11-IPv6 MBGP	1-22
display bgp ipv6 multicast routing-table flap-info	IP Multicast Volume-11-IPv6 MBGP	1-23
display bgp ipv6 multicast routing-table peer	IP Multicast Volume-11-IPv6 MBGP	1-24
display bgp ipv6 multicast routing-table regular-expression	IP Multicast Volume-11-IPv6 MBGP	1-25
display bgp ipv6 multicast routing-table statistic	IP Multicast Volume-11-IPv6 MBGP	1-26
display bgp ipv6 network	IP Routing Volume-11-IPv6 BGP	1-10
display bgp ipv6 paths	IP Routing Volume-11-IPv6 BGP	1-11
display bgp ipv6 peer	IP Routing Volume-11-IPv6 BGP	1-12
display bgp ipv6 routing-table	IP Routing Volume-11-IPv6 BGP	1-13
display bgp ipv6 routing-table as-path-acl	IP Routing Volume-11-IPv6 BGP	1-15
display bgp ipv6 routing-table community	IP Routing Volume-11-IPv6 BGP	1-16
display bgp ipv6 routing-table community-list	IP Routing Volume-11-IPv6 BGP	1-17

display bgp ipv6 routing-table dampened	IP Routing Volume-11-IPv6 BGP	1-17
display bgp ipv6 routing-table dampening parameter	IP Routing Volume-11-IPv6 BGP	1-18
display bgp ipv6 routing-table different-origin-as	IP Routing Volume-11-IPv6 BGP	1-19
display bgp ipv6 routing-table flap-info	IP Routing Volume-11-IPv6 BGP	1-20
display bgp ipv6 routing-table peer	IP Routing Volume-11-IPv6 BGP	1-21
display bgp ipv6 routing-table regular-expression	IP Routing Volume-11-IPv6 BGP	1-22
display bgp ipv6 routing-table statistic	IP Routing Volume-11-IPv6 BGP	1-23
display bgp multicast group	IP Multicast Volume-05-MBGP	1-12
display bgp multicast network	IP Multicast Volume-05-MBGP	1-14
display bgp multicast paths	IP Multicast Volume-05-MBGP	1-15
display bgp multicast peer	IP Multicast Volume-05-MBGP	1-16
display bgp multicast routing-table	IP Multicast Volume-05-MBGP	1-18
display bgp multicast routing-table as-path-acl	IP Multicast Volume-05-MBGP	1-19
display bgp multicast routing-table cidr	IP Multicast Volume-05-MBGP	1-20
display bgp multicast routing-table community	IP Multicast Volume-05-MBGP	1-21
display bgp multicast routing-table community-list	IP Multicast Volume-05-MBGP	1-22
display bgp multicast routing-table dampened	IP Multicast Volume-05-MBGP	1-23
display bgp multicast routing-table dampening parameter	IP Multicast Volume-05-MBGP	1-23
display bgp multicast routing-table different-origin-as	IP Multicast Volume-05-MBGP	1-24
display bgp multicast routing-table flap-info	IP Multicast Volume-05-MBGP	1-25
display bgp multicast routing-table peer	IP Multicast Volume-05-MBGP	1-26
display bgp multicast routing-table regular-expression	IP Multicast Volume-05-MBGP	1-27
display bgp multicast routing-table statistic	IP Multicast Volume-05-MBGP	1-28
display bgp network	IP Routing Volume-06-BGP	1-15
display bgp paths	IP Routing Volume-06-BGP	1-16
display bgp peer	IP Routing Volume-06-BGP	1-17
display bgp routing-table	IP Routing Volume-06-BGP	1-19
display bgp routing-table as-path-acl	IP Routing Volume-06-BGP	1-20
display bgp routing-table cidr	IP Routing Volume-06-BGP	1-21
display bgp routing-table community	IP Routing Volume-06-BGP	1-22

display bgp routing-table community-list	IP Routing Volume-06-BGP	1-23
display bgp routing-table dampened	IP Routing Volume-06-BGP	1-23
display bgp routing-table dampening parameter	IP Routing Volume-06-BGP	1-24
display bgp routing-table different-origin-as	IP Routing Volume-06-BGP	1-25
display bgp routing-table flap-info	IP Routing Volume-06-BGP	1-26
display bgp routing-table label	IP Routing Volume-06-BGP	1-27
display bgp routing-table peer	IP Routing Volume-06-BGP	1-28
display bgp routing-table regular-expression	IP Routing Volume-06-BGP	1-29
display bgp routing-table statistic	IP Routing Volume-06-BGP	1-29
display bgp vpnv4 vpn-instance group	IP Routing Volume-14-MCE	1-1
display bgp vpnv4 vpn-instance network	IP Routing Volume-14-MCE	1-3
display bgp vpnv4 vpn-instance paths	IP Routing Volume-14-MCE	1-4
display bgp vpnv4 vpn-instance peer	IP Routing Volume-14-MCE	1-5
display bgp vpnv4 vpn-instance routing-table	IP Routing Volume-14-MCE	1-7
display boot-loader	System Volume-03-Device Management	1-4
display bootp client	IP Services Volume-03-DHCP	5-1
display brief interface	Access Volume-01-Ethernet Interface	1-3
display cfd linktrace-reply	Access Volume-15-Connectivity Fault Detection	1-12
display cfd linktrace-reply auto-detection	Access Volume-15-Connectivity Fault Detection	1-13
display cfd ma	Access Volume-15-Connectivity Fault Detection	1-14
display cfd md	Access Volume-15-Connectivity Fault Detection	1-15
display cfd mep	Access Volume-15-Connectivity Fault Detection	1-16
display cfd mp	Access Volume-15-Connectivity Fault Detection	1-18
display cfd remote-mep	Access Volume-15-Connectivity Fault Detection	1-20
display cfd service-instance	Access Volume-15-Connectivity Fault Detection	1-21

display cfd status	Access Volume-15-Connectivity Fault Detection	1-22
display channel	System Volume-10-Information Center	1-1
display clipboard	System Volume-02-Basic System Configuration	1-7
display clock	System Volume-02-Basic System Configuration	1-8
display cluster	System Volume-17-Cluster Management	1-28
display cluster base-topology	System Volume-17-Cluster Management	1-29
display cluster black-list	System Volume-17-Cluster Management	1-31
display cluster candidates	System Volume-17-Cluster Management	1-32
display cluster current-topology	System Volume-17-Cluster Management	1-33
display cluster members	System Volume-17-Cluster Management	1-35
display connection	Security Volume-01-AAA	1-19
display cpu-usage	System Volume-03-Device Management	1-5
display cpu-usage history	System Volume-03-Device Management	1-7
display current-configuration	System Volume-02-Basic System Configuration	1-8
display debugging	System Volume-09-System Maintaining and Debugging	1-9
display default-configuration	System Volume-02-Basic System Configuration	1-10
display device	System Volume-03-Device Management	1-10
display device manuinfo	System Volume-03-Device Management	1-11
display dhcp client	IP Services Volume-03-DHCP	3-1
display dhcp relay	IP Services Volume-03-DHCP	2-12

display dhcp relay information	IP Services Volume-03-DHCP	2-13
display dhcp relay security	IP Services Volume-03-DHCP	2-14
display dhcp relay security statistics	IP Services Volume-03-DHCP	2-15
display dhcp relay security tracker	IP Services Volume-03-DHCP	2-16
display dhcp relay server-group	IP Services Volume-03-DHCP	2-16
display dhcp relay statistics	IP Services Volume-03-DHCP	2-17
display dhcp server conflict	IP Services Volume-03-DHCP	1-9
display dhcp server expired	IP Services Volume-03-DHCP	1-9
display dhcp server forbidden-ip	IP Services Volume-03-DHCP	1-11
display dhcp server free-ip	IP Services Volume-03-DHCP	1-10
display dhcp server ip-in-use	IP Services Volume-03-DHCP	1-12
display dhcp server statistics	IP Services Volume-03-DHCP	1-13
display dhcp server tree	IP Services Volume-03-DHCP	1-14
display dhcp-snooping	IP Services Volume-03-DHCP	4-8
display dhcp-snooping information	IP Services Volume-03-DHCP	4-9
display dhcp-snooping packet statistics	IP Services Volume-03-DHCP	4-10
display dhcp-snooping trust	IP Services Volume-03-DHCP	4-11
display diagnostic-information	System Volume-02-Basic System Configuration	1-10
display dldp	Access Volume-05-DLDP	1-1
display dldp statistics	Access Volume-05-DLDP	1-3
display dns domain	IP Services Volume-04-DNS	1-1
display dns dynamic-host	IP Services Volume-04-DNS	1-2
display dns ipv6 dynamic-host	IP Services Volume-08-IPv6 Basics	1-1
display dns ipv6 server	IP Services Volume-08-IPv6 Basics	1-2
display dns server	IP Services Volume-04-DNS	1-3
display domain	Security Volume-01-AAA	1-20
display dot1x	Security Volume-02-802.1X	1-1
display environment	System Volume-03-Device Management	1-12
display fan	System Volume-03-Device Management	1-13

display fib	IP Services Volume-05-IP Performance Optimization	1-1
display fib <i>ip-address</i>	IP Services Volume-05-IP Performance Optimization	1-3
display ftp client configuration	System Volume-04-File System Management	2-13
display ftp-server	System Volume-04-File System Management	2-1
display ftp-user	System Volume-04-File System Management	2-2
display garp statistics	Access Volume-10-GVRP	1-1
display garp timer	Access Volume-10-GVRP	1-2
display gvrp local-vlan interface	Access Volume-10-GVRP	1-3
display gvrp state	Access Volume-10-GVRP	1-3
display gvrp statistics	Access Volume-10-GVRP	1-4
display gvrp status	Access Volume-10-GVRP	1-5
display gvrp vlan-operation interface	Access Volume-10-GVRP	1-5
display habp	Security Volume-03-HABP	1-1
display habp table	Security Volume-03-HABP	1-1
display habp traffic	Security Volume-03-HABP	1-2
display history-command	System Volume-02-Basic System Configuration	1-11
display hotkey	System Volume-02-Basic System Configuration	1-12
display hwtacacs	Security Volume-01-AAA	3-1
display icmp statistics	IP Services Volume-05-IP Performance Optimization	1-4
display igmp group	IP Multicast Volume-02-IGMP	1-1
display igmp group port-info	IP Multicast Volume-02-IGMP	1-2
display igmp interface	IP Multicast Volume-02-IGMP	1-4
display igmp proxying group	IP Multicast Volume-02-IGMP	1-6
display igmp routing-table	IP Multicast Volume-02-IGMP	1-7
display igmp ssm-mapping	IP Multicast Volume-02-IGMP	1-9
display igmp ssm-mapping group	IP Multicast Volume-02-IGMP	1-10

display igmp-snooping group	IP Multicast Volume-06-IGMP Snooping	1-1
display igmp-snooping statistics	IP Multicast Volume-06-IGMP Snooping	1-2
display info-center	System Volume-10-Information Center	1-2
display interface	Access Volume-01-Ethernet Interface	1-6
display interface tunnel	IP Services Volume-09-Tunneling	1-2
display interface vlan-interface	Access Volume-09-VLAN	1-2
display ip as-path	IP Routing Volume-12-Route Policy	1-10
display ip check source	Security Volume-07-IP Source Guard	1-1
display ip community-list	IP Routing Volume-12-Route Policy	1-10
display ip extcommunity-list	IP Routing Volume-12-Route Policy	1-11
display ip host	IP Services Volume-04-DNS	1-4
display ip http	System Volume-05-HTTP	1-1
display ip https	System Volume-05-HTTP	2-1
display ip interface	IP Services Volume-01-IP Addressing	1-1
display ip interface brief	IP Services Volume-01-IP Addressing	1-3
display ip ip-prefix	IP Routing Volume-12-Route Policy	1-22
display ip ipv6-prefix	IP Routing Volume-12-Route Policy	1-27
display ip multicast routing-table	IP Multicast Volume-05-MBGP	1-9
display ip multicast routing-table <i>ip-address</i>	IP Multicast Volume-05-MBGP	1-11
display ip routing-table	IP Routing Volume-01-IP Routing Table Display	1-1
display ip routing-table acl	IP Routing Volume-01-IP Routing Table Display	1-4
display ip routing-table <i>ip-address</i>	IP Routing Volume-01-IP Routing Table Display	1-7
display ip routing-table ip-prefix	IP Routing Volume-01-IP Routing Table Display	1-9
display ip routing-table protocol	IP Routing Volume-01-IP Routing Table Display	1-10
display ip routing-table statistics	IP Routing Volume-01-IP Routing Table Display	1-11

display ip routing-table vpn-instance	IP Routing Volume-14-MCE	1-10
display ip socket	IP Services Volume-05-IP Performance Optimization	1-5
display ip statistics	IP Services Volume-05-IP Performance Optimization	1-8
display ip vpn-instance	IP Routing Volume-14-MCE	1-11
display ipc channel	System Volume-19-IPC	1-1
display ipc link	System Volume-19-IPC	1-2
display ipc multicast-group	System Volume-19-IPC	1-3
display ipc node	System Volume-19-IPC	1-4
display ipc packet	System Volume-19-IPC	1-4
display ipc performance	System Volume-19-IPC	1-5
display ipc queue	System Volume-19-IPC	1-7
display ip-subnet-vlan interface	Access Volume-09-VLAN	1-28
display ip-subnet-vlan vlan	Access Volume-09-VLAN	1-29
display ipv6 fib	IP Services Volume-08-IPv6 Basics	1-3
display ipv6 host	IP Services Volume-08-IPv6 Basics	1-4
display ipv6 interface	IP Services Volume-08-IPv6 Basics	1-5
display ipv6 interface tunnel	IP Services Volume-09-Tunneling	1-3
display ipv6 multicast routing-table	IP Multicast Volume-11-IPv6 MBGP	1-9
display ipv6 multicast routing-table <i>ipv6-address prefix-length</i>	IP Multicast Volume-11-IPv6 MBGP	1-11
display ipv6 neighbors	IP Services Volume-08-IPv6 Basics	1-9
display ipv6 neighbors count	IP Services Volume-08-IPv6 Basics	1-10
display ipv6 pathmtu	IP Services Volume-08-IPv6 Basics	1-11
display ipv6 routing-table	IP Routing Volume-01-IP Routing Table Display	1-12
display ipv6 routing-table acl	IP Routing Volume-01-IP Routing Table Display	1-13
display ipv6 routing-table <i>ipv6-address</i>	IP Routing Volume-01-IP Routing Table Display	1-14
display ipv6 routing-table <i>ipv6-address1 ipv6-address2</i>	IP Routing Volume-01-IP Routing Table Display	1-15

display ipv6 routing-table ipv6-prefix	IP Routing Volume-01-IP Routing Table Display	1-16
display ipv6 routing-table protocol	IP Routing Volume-01-IP Routing Table Display	1-17
display ipv6 routing-table statistics	IP Routing Volume-01-IP Routing Table Display	1-18
display ipv6 routing-table verbose	IP Routing Volume-01-IP Routing Table Display	1-19
display ipv6 socket	IP Services Volume-08-IPv6 Basics	1-12
display ipv6 statistics	IP Services Volume-08-IPv6 Basics	1-14
display irf	System Volume-18-IRF Stack	1-1
display irf configuration	System Volume-18-IRF Stack	1-2
display irf topology	System Volume-18-IRF Stack	1-3
display isis brief	IP Routing Volume-05-IS-IS	1-6
display isis debug-switches	IP Routing Volume-05-IS-IS	1-7
display isis graceful-restart status	IP Routing Volume-05-IS-IS	1-8
display isis interface	IP Routing Volume-05-IS-IS	1-9
display isis license	IP Routing Volume-05-IS-IS	1-11
display isis lsdb	IP Routing Volume-05-IS-IS	1-13
display isis mesh-group	IP Routing Volume-05-IS-IS	1-15
display isis name-table	IP Routing Volume-05-IS-IS	1-16
display isis peer	IP Routing Volume-05-IS-IS	1-17
display isis route	IP Routing Volume-05-IS-IS	1-20
display isis route ipv6	IP Routing Volume-10-IPv6 IS-IS	1-1
display isis spf-log	IP Routing Volume-05-IS-IS	1-23
display isis statistics	IP Routing Volume-05-IS-IS	1-24
display isolate-user-vlan	Access Volume-09-VLAN	2-1
display lacp system-id	Access Volume-02-Link Aggregation	1-2
display link-aggregation load-sharing mode	Access Volume-02-Link Aggregation	1-2
display link-aggregation member-port	Access Volume-02-Link Aggregation	1-3
display link-aggregation summary	Access Volume-02-Link Aggregation	1-6
display link-aggregation verbose	Access Volume-02-Link Aggregation	1-7
display lldp local-information	Access Volume-06-LLDP	1-1

display lldp neighbor-information	Access Volume-06-LLDP	1-5
display lldp statistics	Access Volume-06-LLDP	1-10
display lldp status	Access Volume-06-LLDP	1-12
display lldp tlv-config	Access Volume-06-LLDP	1-14
display local-proxy-arp	IP Services Volume-02-ARP	2-1
display local-user	Security Volume-01-AAA	1-21
display logbuffer	System Volume-10-Information Center	1-4
display logbuffer summary	System Volume-10-Information Center	1-6
display loopback-detection	Access Volume-01-Ethernet Interface	1-8
display mac-address	System Volume-08-MAC Address Table Management	1-1
display mac-address aging-time	System Volume-08-MAC Address Table Management	1-2
display mac-authentication	Security Volume-04-MAC Authentication	1-1
display mac-vlan	Access Volume-09-VLAN	1-18
display mac-vlan interface	Access Volume-09-VLAN	1-20
display memory	System Volume-03-Device Management	1-13
display mib-style	System Volume-06-SNMP	2-1
display mirroring-group	Access Volume-18-Port Mirroring	1-1
display mld group	IP Multicast Volume-09-MLD	1-1
display mld group port-info	IP Multicast Volume-09-MLD	1-2
display mld interface	IP Multicast Volume-09-MLD	1-4
display mld proxying group	IP Multicast Volume-09-MLD	1-6
display mld routing-table	IP Multicast Volume-09-MLD	1-7
display mld ssm-mapping	IP Multicast Volume-09-MLD	1-8
display mld ssm-mapping group	IP Multicast Volume-09-MLD	1-9
display mld-snooping group	IP Multicast Volume-12-MLD Snooping	1-1
display mld-snooping statistics	IP Multicast Volume-12-MLD Snooping	1-2

display monitor-link group	Access Volume-08-Monitor Link	1-1
display msdp brief	IP Multicast Volume-04-MSDP	1-2
display msdp peer-status	IP Multicast Volume-04-MSDP	1-3
display msdp sa-cache	IP Multicast Volume-04-MSDP	1-5
display msdp sa-count	IP Multicast Volume-04-MSDP	1-6
display multicast boundary	IP Multicast Volume-01-Multicast Routing and Forwarding	1-1
display multicast forwarding-table	IP Multicast Volume-01-Multicast Routing and Forwarding	1-2
display multicast ipv6 boundary	IP Multicast Volume-08-IPv6 Multicast Routing and Forwarding	1-1
display multicast ipv6 forwarding-table	IP Multicast Volume-08-IPv6 Multicast Routing and Forwarding	1-2
display multicast ipv6 routing-table	IP Multicast Volume-08-IPv6 Multicast Routing and Forwarding	1-4
display multicast ipv6 rpf-info	IP Multicast Volume-08-IPv6 Multicast Routing and Forwarding	1-6
display multicast routing-table	IP Multicast Volume-01-Multicast Routing and Forwarding	1-4
display multicast routing-table static	IP Multicast Volume-01-Multicast Routing and Forwarding	1-6
display multicast rpf-info	IP Multicast Volume-01-Multicast Routing and Forwarding	1-7
display multicast-vlan	IP Multicast Volume-07-Multicast VLAN	1-1
display multicast-vlan ipv6	IP Multicast Volume-13-IPv6 Multicast VLAN	1-1
display ndp	System Volume-17-Cluster Management	1-1
display nqa history	System Volume-13-NQA	1-6
display nqa result	System Volume-13-NQA	1-7
display nqa server status	System Volume-13-NQA	1-38
display nqa statistics	System Volume-13-NQA	1-11
display ntdp	System Volume-17-Cluster Management	1-7

display ntdp device-list	System Volume-17-Cluster Management	1-8
display ntdp single-device mac-address	System Volume-17-Cluster Management	1-10
display ntp-service sessions	System Volume-14-NTP	1-1
display ntp-service status	System Volume-14-NTP	1-2
display ntp-service trace	System Volume-14-NTP	1-4
display oam	Access Volume-14-Ethernet OAM	1-1
display oam configuration	Access Volume-14-Ethernet OAM	1-4
display oam critical-event	Access Volume-14-Ethernet OAM	1-6
display oam link-event	Access Volume-14-Ethernet OAM	1-7
display ospf abr-asbr	IP Routing Volume-04-OSPF	1-8
display ospf asbr-summary	IP Routing Volume-04-OSPF	1-9
display ospf brief	IP Routing Volume-04-OSPF	1-10
display ospf cumulative	IP Routing Volume-04-OSPF	1-13
display ospf error	IP Routing Volume-04-OSPF	1-15
display ospf interface	IP Routing Volume-04-OSPF	1-16
display ospf lsdb	IP Routing Volume-04-OSPF	1-18
display ospf nexthop	IP Routing Volume-04-OSPF	1-20
display ospf peer	IP Routing Volume-04-OSPF	1-21
display ospf peer statistics	IP Routing Volume-04-OSPF	1-24
display ospf request-queue	IP Routing Volume-04-OSPF	1-25
display ospf retrans-queue	IP Routing Volume-04-OSPF	1-26
display ospf routing	IP Routing Volume-04-OSPF	1-27
display ospf sham-link	IP Routing Volume-04-OSPF	1-28
display ospf vlink	IP Routing Volume-04-OSPF	1-29
display ospfv3	IP Routing Volume-09-OSPFv3	1-5
display ospfv3 graceful-restart status	IP Routing Volume-09-OSPFv3	1-7
display ospfv3 interface	IP Routing Volume-09-OSPFv3	1-8
display ospfv3 lsdb	IP Routing Volume-09-OSPFv3	1-9
display ospfv3 lsdb statistic	IP Routing Volume-09-OSPFv3	1-12
display ospfv3 next-hop	IP Routing Volume-09-OSPFv3	1-13

display ospfv3 peer	IP Routing Volume-09-OSPFv3	1-13
display ospfv3 peer statistic	IP Routing Volume-09-OSPFv3	1-15
display ospfv3 request-list	IP Routing Volume-09-OSPFv3	1-16
display ospfv3 retrans-list	IP Routing Volume-09-OSPFv3	1-18
display ospfv3 routing	IP Routing Volume-09-OSPFv3	1-19
display ospfv3 statistics	IP Routing Volume-09-OSPFv3	1-21
display ospfv3 topology	IP Routing Volume-09-OSPFv3	1-22
display ospfv3 vlink	IP Routing Volume-09-OSPFv3	1-23
display packet-drop interface	Access Volume-01-Ethernet Interface	1-9
display packet-drop summary	Access Volume-01-Ethernet Interface	1-10
display patch information	System Volume-16-Hotfix	1-1
display pim bsr-info	IP Multicast Volume-03-PIM	1-11
display pim claimed-route	IP Multicast Volume-03-PIM	1-13
display pim control-message counters	IP Multicast Volume-03-PIM	1-14
display pim grafts	IP Multicast Volume-03-PIM	1-16
display pim interface	IP Multicast Volume-03-PIM	1-16
display pim ipv6 bsr-info	IP Multicast Volume-10-IPv6 PIM	1-9
display pim ipv6 claimed-route	IP Multicast Volume-10-IPv6 PIM	1-10
display pim ipv6 control-message counters	IP Multicast Volume-10-IPv6 PIM	1-11
display pim ipv6 grafts	IP Multicast Volume-10-IPv6 PIM	1-13
display pim ipv6 interface	IP Multicast Volume-10-IPv6 PIM	1-14
display pim ipv6 join-prune	IP Multicast Volume-10-IPv6 PIM	1-16
display pim ipv6 neighbor	IP Multicast Volume-10-IPv6 PIM	1-17
display pim ipv6 routing-table	IP Multicast Volume-10-IPv6 PIM	1-18
display pim ipv6 rp-info	IP Multicast Volume-10-IPv6 PIM	1-20
display pim join-prune	IP Multicast Volume-03-PIM	1-18
display pim neighbor	IP Multicast Volume-03-PIM	1-20
display pim routing-table	IP Multicast Volume-03-PIM	1-21
display pim rp-info	IP Multicast Volume-03-PIM	1-23
display pki certificate	Security Volume-09-PKI	1-9
display pki certificate access-control-policy	Security Volume-09-PKI	1-11

display pki certificate attribute-group	Security Volume-09-PKI	1-11
display pki crl domain	Security Volume-09-PKI	1-12
display poe device	System Volume-11-PoE	1-2
display poe interface	System Volume-11-PoE	1-3
display poe interface power	System Volume-11-PoE	1-6
display poe pse	System Volume-11-PoE	1-8
display poe pse interface	System Volume-11-PoE	1-9
display poe pse interface power	System Volume-11-PoE	1-10
display poe-profile	System Volume-11-PoE	1-11
display poe-profile interface	System Volume-11-PoE	1-14
display port	Access Volume-09-VLAN	1-9
display port combo	Access Volume-01-Ethernet Interface	1-11
display portal acl	Security Volume-05-Portal	1-1
display portal connection statistics	Security Volume-05-Portal	1-3
display portal free-rule	Security Volume-05-Portal	1-6
display portal interface	Security Volume-05-Portal	1-7
display portal server	Security Volume-05-Portal	1-8
display portal server statistics	Security Volume-05-Portal	1-9
display portal tcp-cheat statistics	Security Volume-05-Portal	1-11
display portal user	Security Volume-05-Portal	1-12
display port-group manual	Access Volume-01-Ethernet Interface	1-12
display port-isolate group	Access Volume-03-Port Isolation	1-1
display port-security	Security Volume-06-Port Security	1-1
display port-security mac-address block	Security Volume-06-Port Security	1-3
display port-security mac-address security	Security Volume-06-Port Security	1-4
display power	System Volume-03-Device Management	1-14
display protocol-vlan interface	Access Volume-09-VLAN	1-22
display protocol-vlan vlan	Access Volume-09-VLAN	1-23
display proxy-arp	IP Services Volume-02-ARP	2-1
display public-key local public	Security Volume-11-Public Key	1-1
display public-key peer	Security Volume-11-Public Key	1-2

display qos gts interface	QoS Volume-01-QoS	3-1
display qos lr interface	QoS Volume-01-QoS	3-2
display qos map-table	QoS Volume-01-QoS	2-1
display qos policy	QoS Volume-01-QoS	1-18
display qos policy global	QoS Volume-01-QoS	1-19
display qos policy interface	QoS Volume-01-QoS	1-20
display qos sp interface	QoS Volume-01-QoS	4-1
display qos trust interface	QoS Volume-01-QoS	2-4
display qos vlan-policy	QoS Volume-01-QoS	1-21
display qos wfq interface	QoS Volume-01-QoS	4-1
display qos wred interface	QoS Volume-01-QoS	5-1
display qos wred table	QoS Volume-01-QoS	5-1
display qos wrr interface	QoS Volume-01-QoS	4-2
display radius scheme	Security Volume-01-AAA	2-2
display radius statistics	Security Volume-01-AAA	2-4
display reboot-type	System Volume-03-Device Management	1-15
display rip	IP Routing Volume-03-RIP	1-3
display rip database	IP Routing Volume-03-RIP	1-5
display rip interface	IP Routing Volume-03-RIP	1-6
display rip route	IP Routing Volume-03-RIP	1-7
display ripng	IP Routing Volume-08-RIPng	1-2
display ripng database	IP Routing Volume-08-RIPng	1-3
display ripng interface	IP Routing Volume-08-RIPng	1-4
display ripng route	IP Routing Volume-08-RIPng	1-6
display rmon alarm	System Volume-07-RMON	1-1
display rmon event	System Volume-07-RMON	1-2
display rmon eventlog	System Volume-07-RMON	1-3
display rmon history	System Volume-07-RMON	1-4
display rmon prialarm	System Volume-07-RMON	1-7
display rmon statistics	System Volume-07-RMON	1-8
display route-policy	IP Routing Volume-12-Route Policy	1-11

display router id	IP Routing Volume-01-IP Routing Table Display	1-20
display rps	System Volume-03-Device Management	1-15
display rrpp brief	Access Volume-17-RRPP	1-2
display rrpp ring-group	Access Volume-17-RRPP	1-3
display rrpp statistics	Access Volume-17-RRPP	1-4
display rrpp verbose	Access Volume-17-RRPP	1-7
display saved-configuration	System Volume-04-File System Management	1-16
display schedule job	System Volume-03-Device Management	1-16
display schedule reboot	System Volume-03-Device Management	1-17
display service-loopback group	Access Volume-04-Service Loopback Group	1-1
display sflow	IP Services Volume-10-sFlow	1-1
display sftp client source	Security Volume-08-SSH2.0	1-19
display smart-link flush	Access Volume-07-Smart Link	1-1
display smart-link group	Access Volume-07-Smart Link	1-2
display snmp-agent community	System Volume-06-SNMP	1-1
display snmp-agent group	System Volume-06-SNMP	1-2
display snmp-agent local-engineid	System Volume-06-SNMP	1-3
display snmp-agent mib-view	System Volume-06-SNMP	1-4
display snmp-agent statistics	System Volume-06-SNMP	1-5
display snmp-agent sys-info	System Volume-06-SNMP	1-7
display snmp-agent trap queue	System Volume-06-SNMP	1-8
display snmp-agent trap-list	System Volume-06-SNMP	1-8
display snmp-agent usm-user	System Volume-06-SNMP	1-9
display ssh client source	Security Volume-08-SSH2.0	1-8
display ssh server	Security Volume-08-SSH2.0	1-1
display ssh server-info	Security Volume-08-SSH2.0	1-9
display ssh user-information	Security Volume-08-SSH2.0	1-2

display ssl client-policy	Security Volume-10-SSL	1-3
display ssl server-policy	Security Volume-10-SSL	1-4
display startup	System Volume-04-File System Management	1-18
display stop-accounting-buffer	Security Volume-01-AAA	2-7
display stop-accounting-buffer	Security Volume-01-AAA	3-4
display storm-constrain	Access Volume-01-Ethernet Interface	1-13
display stp	Access Volume-16-MSTP	1-2
display stp abnormal-port	Access Volume-16-MSTP	1-6
display stp down-port	Access Volume-16-MSTP	1-7
display stp history	Access Volume-16-MSTP	1-8
display stp region-configuration	Access Volume-16-MSTP	1-9
display stp root	Access Volume-16-MSTP	1-10
display stp tc	Access Volume-16-MSTP	1-11
display switchover state	System Volume-18-IRF Stack	1-5
display system-failure	System Volume-03-Device Management	1-17
display tcp ipv6 statistics	IP Services Volume-08-IPv6 Basics	1-17
display tcp ipv6 status	IP Services Volume-08-IPv6 Basics	1-19
display tcp statistics	IP Services Volume-05-IP Performance Optimization	1-10
display tcp status	IP Services Volume-05-IP Performance Optimization	1-12
display telnet client configuration	System Volume-01-Login	1-5
display tftp client configuration	System Volume-04-File System Management	3-1
display this	System Volume-02-Basic System Configuration	1-13
display time-range	Security Volume-12-ACL	1-2
display track	System Volume-12-Track	1-1
display traffic behavior	QoS Volume-01-QoS	1-8
display traffic classifier	QoS Volume-01-QoS	1-1
display transceiver	System Volume-03-Device Management	1-22

display transceiver alarm	System Volume-03-Device Management	1-18
display transceiver diagnosis	System Volume-03-Device Management	1-21
display transceiver manuinfo	System Volume-03-Device Management	1-23
display trapbuffer	System Volume-10-Information Center	1-7
display udp ipv6 statistics	IP Services Volume-08-IPv6 Basics	1-20
display udp statistics	IP Services Volume-05-IP Performance Optimization	1-13
display udp-helper server	IP Services Volume-06-UDP Helper	1-1
display user-bind	Security Volume-07-IP Source Guard	1-2
display user-group	Security Volume-01-AAA	1-23
display user-interface	System Volume-01-Login	1-5
display user-profile	QoS Volume-02-User Profile	1-1
display users	System Volume-01-Login	1-7
display version	System Volume-02-Basic System Configuration	1-14
display vlan	Access Volume-09-VLAN	1-3
display voice vlan oui	Access Volume-09-VLAN	3-1
display voice vlan state	Access Volume-09-VLAN	3-2
display vrrp	System Volume-15-VRRP	1-1
display vrrp ipv6	System Volume-15-VRRP	1-14
display vrrp ipv6 statistics	System Volume-15-VRRP	1-16
display vrrp statistics	System Volume-15-VRRP	1-3
display web users	System Volume-01-Login	1-8
dldp authentication-mode	Access Volume-05-DLDP	1-4
dldp delaydown-timer	Access Volume-05-DLDP	1-5
dldp enable	Access Volume-05-DLDP	1-5
dldp interval	Access Volume-05-DLDP	1-6
dldp reset	Access Volume-05-DLDP	1-7
dldp unidirectional-shutdown	Access Volume-05-DLDP	1-8

dldp work-mode	Access Volume-05-DLDP	1-8
dns domain	IP Services Volume-04-DNS	1-4
dns proxy enable	IP Services Volume-04-DNS	1-5
dns resolve	IP Services Volume-04-DNS	1-6
dns server	IP Services Volume-04-DNS	1-6
dns server ipv6	IP Services Volume-08-IPv6 Basics	1-21
dns-list	IP Services Volume-03-DHCP	1-16
domain	Security Volume-01-AAA	1-24
domain default enable	Security Volume-01-AAA	1-25
domain ring	Access Volume-17-RRPP	1-9
domain-authentication-mode	IP Routing Volume-05-IS-IS	1-25
domain-id	IP Routing Volume-14-MCE	1-12
domain-name	IP Services Volume-03-DHCP	1-16
dot1x	Security Volume-02-802.1X	1-4
dot1x authentication-method	Security Volume-02-802.1X	1-5
dot1x free-ip	Security Volume-02-802.1X	2-1
dot1x guest-vlan	Security Volume-02-802.1X	1-6
dot1x handshake	Security Volume-02-802.1X	1-7
dot1x mandatory-domain	Security Volume-02-802.1X	1-8
dot1x max-user	Security Volume-02-802.1X	1-9
dot1x multicast-trigger	Security Volume-02-802.1X	1-10
dot1x port-control	Security Volume-02-802.1X	1-10
dot1x port-method	Security Volume-02-802.1X	1-11
dot1x quiet-period	Security Volume-02-802.1X	1-12
dot1x retry	Security Volume-02-802.1X	1-13
dot1x timer	Security Volume-02-802.1X	1-14
dot1x timer ead-timeout	Security Volume-02-802.1X	2-2
dot1x url	Security Volume-02-802.1X	2-2
duplex	Access Volume-01-Ethernet Interface	1-14

## E

ebgp-interface-sensitive	IP Routing Volume-06-BGP	1-30
--------------------------	--------------------------	------

embedded-rp	IP Multicast Volume-10-IPv6 PIM	1-21
enable link-local-signaling	IP Routing Volume-04-OSPF	1-30
enable log	IP Routing Volume-04-OSPF	1-31
enable log updown	System Volume-10-Information Center	1-8
enable out-of-band-resynchronization	IP Routing Volume-04-OSPF	1-32
enable snmp trap updown	Access Volume-02-Link Aggregation	1-9
enable snmp trap updown	System Volume-06-SNMP	1-10
encap-data-enable	IP Multicast Volume-04-MSDP	1-7
escape-key	System Volume-01-Login	1-9
execute	System Volume-04-File System Management	1-5
exit	Security Volume-08-SSH2.0	1-20
expiration-date	Security Volume-01-AAA	1-25
expired	IP Services Volume-03-DHCP	1-17
export route-policy	IP Routing Volume-14-MCE	1-13
ext-community-type	IP Routing Volume-14-MCE	1-13

## F

fast-leave (IGMP view)	IP Multicast Volume-02-IGMP	1-11
fast-leave (IGMP-Snooping view)	IP Multicast Volume-06-IGMP Snooping	1-3
fast-leave (MLD view)	IP Multicast Volume-09-MLD	1-10
fast-leave (MLD-Snooping view)	IP Multicast Volume-12-MLD Snooping	1-3
file prompt	System Volume-04-File System Management	1-6
filename	System Volume-13-NQA	1-16
filter	IP Routing Volume-04-OSPF	1-32
filter	QoS Volume-01-QoS	1-9
filter-policy export	IP Routing Volume-08-RIPng	1-7
filter-policy export	IP Routing Volume-14-MCE	1-14
filter-policy export (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-31

filter-policy export (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-23
filter-policy export (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-26
filter-policy export (IS-IS view)	IP Routing Volume-05-IS-IS	1-27
filter-policy export (MBGP family view)	IP Multicast Volume-05-MBGP	1-28
filter-policy export (OSPF view)	IP Routing Volume-04-OSPF	1-33
filter-policy export (OSPFv3 view)	IP Routing Volume-09-OSPFv3	1-24
filter-policy export (RIP view)	IP Routing Volume-03-RIP	1-9
filter-policy import	IP Routing Volume-14-MCE	1-15
filter-policy import (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-32
filter-policy import (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-24
filter-policy import (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-27
filter-policy import (IS-IS view)	IP Routing Volume-05-IS-IS	1-27
filter-policy import (MBGP Family view)	IP Multicast Volume-05-MBGP	1-29
filter-policy import (OSPF view)	IP Routing Volume-04-OSPF	1-34
filter-policy import (OSPFv3 view)	IP Routing Volume-09-OSPFv3	1-25
filter-policy import (RIP view)	IP Routing Volume-03-RIP	1-10
filter-policy import (RIPng view)	IP Routing Volume-08-RIPng	1-7
fixdisk	System Volume-04-File System Management	1-7
flash-flood	IP Routing Volume-05-IS-IS	1-28
flow-control	Access Volume-01-Ethernet Interface	1-15
flow-control	System Volume-01-Login	1-10
flow-interval	Access Volume-01-Ethernet Interface	1-16
flush enable	Access Volume-07-Smart Link	1-3
forbidden-ip	IP Services Volume-03-DHCP	1-18
format	System Volume-04-File System Management	1-7
fqdn	Security Volume-09-PKI	1-14
free ftp user	System Volume-04-File System Management	2-3
free user-interface	System Volume-01-Login	1-11
free web-users	System Volume-01-Login	2-2

frequency	System Volume-13-NQA	1-16
ftp	System Volume-04-File System Management	2-14
ftp client source	System Volume-04-File System Management	2-15
ftp ipv6	System Volume-04-File System Management	2-16
ftp server acl	System Volume-04-File System Management	2-3
ftp server enable	System Volume-04-File System Management	2-4
ftp timeout	System Volume-04-File System Management	2-4
ftp update	System Volume-04-File System Management	2-5
ftp-server	System Volume-17-Cluster Management	1-38

## G

garp timer hold	Access Volume-10-GVRP	1-6
garp timer join	Access Volume-10-GVRP	1-6
garp timer leave	Access Volume-10-GVRP	1-7
garp timer leaveall	Access Volume-10-GVRP	1-8
gateway-list	IP Services Volume-03-DHCP	1-19
get	Security Volume-08-SSH2.0	1-20
get	System Volume-04-File System Management	2-17
graceful-restart (BGP view)	IP Routing Volume-06-BGP	1-32
graceful-restart (IS-IS view)	IP Routing Volume-05-IS-IS	1-29
graceful-restart (OSPF view)	IP Routing Volume-04-OSPF	1-35
graceful-restart enable	IP Routing Volume-09-OSPFv3	1-26
graceful-restart help	IP Routing Volume-04-OSPF	1-36
graceful-restart helper enable	IP Routing Volume-09-OSPFv3	1-27
graceful-restart helper strict-lsa-checking	IP Routing Volume-09-OSPFv3	1-27
graceful-restart interval	IP Routing Volume-09-OSPFv3	1-28

graceful-restart interval (IS-IS view)	IP Routing Volume-05-IS-IS	1-30
graceful-restart interval (OSPF view)	IP Routing Volume-04-OSPF	1-37
graceful-restart suppress-sa	IP Routing Volume-05-IS-IS	1-30
graceful-restart timer restart	IP Routing Volume-06-BGP	1-33
graceful-restart timer wait-for-rib	IP Routing Volume-06-BGP	1-34
gratuitous-arp-learning enable	IP Services Volume-02-ARP	1-9
gratuitous-arp-sending enable	IP Services Volume-02-ARP	1-8
group	Security Volume-01-AAA	1-26
group (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-34
group (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-25
group-member	Access Volume-01-Ethernet Interface	1-16
group-policy (IGMP-Snooping view)	IP Multicast Volume-06-IGMP Snooping	1-4
group-policy (MLD-Snooping view)	IP Multicast Volume-12-MLD Snooping	1-4
gvrp	Access Volume-10-GVRP	1-9
gvrp registration	Access Volume-10-GVRP	1-9

## H

habp enable	Security Volume-03-HABP	1-3
habp server vlan	Security Volume-03-HABP	1-4
habp timer	Security Volume-03-HABP	1-4
handshake timeout	Security Volume-10-SSL	1-5
header	System Volume-02-Basic System Configuration	1-14
hello-option dr-priority (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-22
hello-option dr-priority (PIM view)	IP Multicast Volume-03-PIM	1-25
hello-option holdtime (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-23
hello-option holdtime (PIM view)	IP Multicast Volume-03-PIM	1-25
hello-option lan-delay (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-24
hello-option lan-delay (PIM view)	IP Multicast Volume-03-PIM	1-26
hello-option neighbor-tracking (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-24
hello-option neighbor-tracking (PIM view)	IP Multicast Volume-03-PIM	1-26

hello-option override-interval (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-25
hello-option override-interval (PIM view)	IP Multicast Volume-03-PIM	1-27
help	Security Volume-08-SSH2.0	1-21
history-command max-size	System Volume-01-Login	1-11
history-records	System Volume-13-NQA	1-17
holdtime	System Volume-17-Cluster Management	1-39
holdtime assert (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-26
holdtime assert (PIM view)	IP Multicast Volume-03-PIM	1-28
holdtime join-prune (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-26
holdtime join-prune (PIM view)	IP Multicast Volume-03-PIM	1-28
host-advertise	IP Routing Volume-04-OSPF	1-37
host-aging-time (IGMP-Snooping view)	IP Multicast Volume-06-IGMP Snooping	1-5
host-aging-time (MLD-Snooping view)	IP Multicast Volume-12-MLD Snooping	1-5
host-route	IP Routing Volume-03-RIP	1-11
hotkey	System Volume-02-Basic System Configuration	1-16
http-version	System Volume-13-NQA	1-18
hwtaacs nas-ip	Security Volume-01-AAA	3-4
hwtaacs scheme	Security Volume-01-AAA	3-5
<b>I</b>		
idle-cut enable	Security Volume-01-AAA	1-27
idle-timeout	System Volume-01-Login	1-12
if-match	QoS Volume-01-QoS	1-2
if-match acl	IP Routing Volume-12-Route Policy	1-22
if-match as-path	IP Routing Volume-12-Route Policy	1-12
if-match community	IP Routing Volume-12-Route Policy	1-13
if-match cost	IP Routing Volume-12-Route Policy	1-14
if-match extcommunity	IP Routing Volume-12-Route Policy	1-14
if-match interface	IP Routing Volume-12-Route Policy	1-15

if-match ip	IP Routing Volume-12-Route Policy	1-23
if-match ip-prefix	IP Routing Volume-12-Route Policy	1-24
if-match ipv6	IP Routing Volume-12-Route Policy	1-28
if-match route-type	IP Routing Volume-12-Route Policy	1-16
if-match tag	IP Routing Volume-12-Route Policy	1-17
igmp	IP Multicast Volume-02-IGMP	1-12
igmp enable	IP Multicast Volume-02-IGMP	1-13
igmp group-limit	IP Multicast Volume-02-IGMP	1-13
igmp group-policy	IP Multicast Volume-02-IGMP	1-14
igmp last-member-query-interval	IP Multicast Volume-02-IGMP	1-15
igmp max-response-time	IP Multicast Volume-02-IGMP	1-16
Igmp proxying enable	IP Multicast Volume-02-IGMP	1-16
Igmp proxying forwarding	IP Multicast Volume-02-IGMP	1-17
igmp require-router-alert	IP Multicast Volume-02-IGMP	1-18
igmp robust-count	IP Multicast Volume-02-IGMP	1-18
igmp send-router-alert	IP Multicast Volume-02-IGMP	1-19
igmp ssm-mapping enable	IP Multicast Volume-02-IGMP	1-20
igmp startup-query-count	IP Multicast Volume-02-IGMP	1-20
igmp startup-query-interval	IP Multicast Volume-02-IGMP	1-21
igmp static-group	IP Multicast Volume-02-IGMP	1-22
igmp timer other-querier-present	IP Multicast Volume-02-IGMP	1-23
igmp timer query	IP Multicast Volume-02-IGMP	1-24
igmp version	IP Multicast Volume-02-IGMP	1-24
igmp-snooping	IP Multicast Volume-06-IGMP Snooping	1-6
igmp-snooping drop-unknown	IP Multicast Volume-06-IGMP Snooping	1-6
igmp-snooping enable	IP Multicast Volume-06-IGMP Snooping	1-7
igmp-snooping fast-leave	IP Multicast Volume-06-IGMP Snooping	1-8
igmp-snooping general-query source-ip	IP Multicast Volume-06-IGMP Snooping	1-9

igmp-snooping group-limit	IP Multicast Volume-06-IGMP Snooping	1-9
igmp-snooping group-policy	IP Multicast Volume-06-IGMP Snooping	1-10
igmp-snooping host-aging-time	IP Multicast Volume-06-IGMP Snooping	1-12
igmp-snooping host-join	IP Multicast Volume-06-IGMP Snooping	1-12
igmp-snooping last-member-query-interval	IP Multicast Volume-06-IGMP Snooping	1-13
igmp-snooping max-response-time	IP Multicast Volume-06-IGMP Snooping	1-14
igmp-snooping overflow-replace	IP Multicast Volume-06-IGMP Snooping	1-15
igmp-snooping querier	IP Multicast Volume-06-IGMP Snooping	1-16
igmp-snooping query-interval	IP Multicast Volume-06-IGMP Snooping	1-16
igmp-snooping router-aging-time	IP Multicast Volume-06-IGMP Snooping	1-17
igmp-snooping source-deny	IP Multicast Volume-06-IGMP Snooping	1-18
igmp-snooping special-query source-ip	IP Multicast Volume-06-IGMP Snooping	1-18
igmp-snooping static-group	IP Multicast Volume-06-IGMP Snooping	1-19
igmp-snooping static-router-port	IP Multicast Volume-06-IGMP Snooping	1-20
igmp-snooping version	IP Multicast Volume-06-IGMP Snooping	1-21
import	QoS Volume-01-QoS	2-2
import route-policy	IP Routing Volume-14-MCE	1-16
import-route	IP Routing Volume-08-RIPng	1-8
import-route (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-35
import-route (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-25
import-route (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-28

import-route (IS-IS view)	IP Routing Volume-05-IS-IS	1-31
import-route (MBGP family view)	IP Multicast Volume-05-MBGP	1-30
import-route (OSPF view)	IP Routing Volume-04-OSPF	1-38
import-route (OSPFv3 view)	IP Routing Volume-09-OSPFv3	1-28
import-route (RIP view)	IP Routing Volume-03-RIP	1-11
import-route isis level-2 into level-1	IP Routing Volume-05-IS-IS	1-32
import-route limit (IS-IS view)	IP Routing Volume-05-IS-IS	1-33
import-source	IP Multicast Volume-04-MSDP	1-8
info-center channel name	System Volume-10-Information Center	1-9
info-center console channel	System Volume-10-Information Center	1-9
info-center enable	System Volume-10-Information Center	1-10
info-center logbuffer	System Volume-10-Information Center	1-11
info-center loghost	System Volume-10-Information Center	1-11
info-center loghost source	System Volume-10-Information Center	1-12
info-center monitor channel	System Volume-10-Information Center	1-13
info-center snmp channel	System Volume-10-Information Center	1-14
info-center source	System Volume-10-Information Center	1-15
info-center synchronous	System Volume-10-Information Center	1-17
info-center timestamp	System Volume-10-Information Center	1-19
info-center timestamp loghost	System Volume-10-Information Center	1-20
info-center trapbuffer	System Volume-10-Information Center	1-20
instance	Access Volume-16-MSTP	1-12
interface	Access Volume-01-Ethernet Interface	1-17

interface bridge-aggregation	Access Volume-02-Link Aggregation	1-10
interface tunnel	IP Services Volume-09-Tunneling	1-7
interface vlan-interface	Access Volume-09-VLAN	1-4
ip (PKI entity view)	Security Volume-09-PKI	1-14
ip address	Access Volume-09-VLAN	1-5
ip address	IP Services Volume-01-IP Addressing	1-4
ip address bootp-alloc	IP Services Volume-03-DHCP	5-2
ip address dhcp-alloc	IP Services Volume-03-DHCP	3-3
ip as-path	IP Routing Volume-12-Route Policy	1-17
ip binding vpn-instance	IP Routing Volume-04-OSPF	1-39
ip binding vpn-instance	IP Routing Volume-14-MCE	1-16
ip check source	Security Volume-07-IP Source Guard	1-3
ip community-list	IP Routing Volume-12-Route Policy	1-18
ip extcommunity-list	IP Routing Volume-12-Route Policy	1-19
ip forward-broadcast (interface view)	IP Services Volume-05-IP Performance Optimization	1-14
ip forward-broadcast (system view)	IP Services Volume-05-IP Performance Optimization	1-15
ip host	IP Services Volume-04-DNS	1-7
ip http acl	System Volume-01-Login	2-2
ip http acl	System Volume-05-HTTP	1-2
ip http enable	System Volume-01-Login	1-13
ip http enable	System Volume-05-HTTP	1-2
ip http port	System Volume-05-HTTP	1-3
ip https acl	System Volume-05-HTTP	2-2
ip https certificate access-control-policy	System Volume-05-HTTP	2-2
ip https enable	System Volume-05-HTTP	2-3
ip https port	System Volume-05-HTTP	2-4
ip https ssl-server-policy	System Volume-05-HTTP	2-4
ip ip-prefix	IP Routing Volume-12-Route Policy	1-24
ip ipv6-prefix	IP Routing Volume-12-Route Policy	1-28

ip redirects enable	IP Services Volume-05-IP Performance Optimization	1-15
ip route-static	IP Routing Volume-02-Static Routing	1-2
ip route-static default-preference	IP Routing Volume-02-Static Routing	1-4
ip rpf-route-static	IP Multicast Volume-01-Multicast Routing and Forwarding	1-8
ip ttl-expires enable	IP Services Volume-05-IP Performance Optimization	1-16
ip unreachable enable	IP Services Volume-05-IP Performance Optimization	1-16
ip urpf strict	IP Services Volume-07-URPF	1-1
ip vpn-instance	IP Routing Volume-14-MCE	1-17
ipc performance enable	System Volume-19-IPC	1-8
ip-pool	System Volume-17-Cluster Management	1-40
ip-subnet-vlan	Access Volume-09-VLAN	1-30
ipv4-family multicast	IP Multicast Volume-05-MBGP	1-31
ipv4-family vpn-instance	IP Routing Volume-14-MCE	1-18
ipv6	IP Services Volume-08-IPv6 Basics	1-22
ipv6 address	IP Services Volume-08-IPv6 Basics	1-22
ipv6 address auto link-local	IP Services Volume-08-IPv6 Basics	1-23
ipv6 address eui-64	IP Services Volume-08-IPv6 Basics	1-24
ipv6 address link-local	IP Services Volume-08-IPv6 Basics	1-25
ipv6 default-route-advertise	IP Routing Volume-10-IPv6 IS-IS	1-3
ipv6 enable	IP Routing Volume-10-IPv6 IS-IS	1-4
ipv6 filter-policy export	IP Routing Volume-10-IPv6 IS-IS	1-5
ipv6 filter-policy import	IP Routing Volume-10-IPv6 IS-IS	1-6
ipv6 hoplimit-expires enable	IP Services Volume-08-IPv6 Basics	1-26
ipv6 host	IP Services Volume-08-IPv6 Basics	1-26
ipv6 icmp-error	IP Services Volume-08-IPv6 Basics	1-27
ipv6 icmpv6 multicast-echo-reply enable	IP Services Volume-08-IPv6 Basics	1-28
ipv6 import-route	IP Routing Volume-10-IPv6 IS-IS	1-6
ipv6 import-route isisv6 level-2 into level-1	IP Routing Volume-10-IPv6 IS-IS	1-8

ipv6 import-route limit	IP Routing Volume-10-IPv6 IS-IS	1-8
ipv6 maximum load-balancing	IP Routing Volume-10-IPv6 IS-IS	1-9
ipv6 nd autoconfig managed-address-flag	IP Services Volume-08-IPv6 Basics	1-28
ipv6 nd autoconfig other-flag	IP Services Volume-08-IPv6 Basics	1-29
ipv6 nd dad attempts	IP Services Volume-08-IPv6 Basics	1-29
ipv6 nd hop-limit	IP Services Volume-08-IPv6 Basics	1-30
ipv6 nd ns retrans-timer	IP Services Volume-08-IPv6 Basics	1-31
ipv6 nd nud reachable-time	IP Services Volume-08-IPv6 Basics	1-31
ipv6 nd ra halt	IP Services Volume-08-IPv6 Basics	1-32
ipv6 nd ra interval	IP Services Volume-08-IPv6 Basics	1-33
ipv6 nd ra prefix	IP Services Volume-08-IPv6 Basics	1-33
ipv6 nd ra router-lifetime	IP Services Volume-08-IPv6 Basics	1-34
ipv6 neighbor	IP Services Volume-08-IPv6 Basics	1-35
ipv6 neighbors max-learning-num	IP Services Volume-08-IPv6 Basics	1-36
ipv6 pathmtu	IP Services Volume-08-IPv6 Basics	1-36
ipv6 pathmtu age	IP Services Volume-08-IPv6 Basics	1-37
ipv6 preference	IP Routing Volume-10-IPv6 IS-IS	1-10
ipv6 route-static	IP Routing Volume-07-IPv6 Static Routing	1-2
ipv6 summary	IP Routing Volume-10-IPv6 IS-IS	1-10
ipv6-family	IP Routing Volume-11-IPv6 BGP	1-26
ipv6-family multicast	IP Multicast Volume-11-IPv6 MBGP	1-28
irf auto-update enable	System Volume-18-IRF Stack	1-6
irf link-delay	System Volume-18-IRF Stack	1-7
irf mac-address persistent	System Volume-18-IRF Stack	1-8
irf member irf-port	System Volume-18-IRF Stack	1-11
irf member priority	System Volume-18-IRF Stack	1-9
irf member renumber	System Volume-18-IRF Stack	1-10
irf switch-to	System Volume-18-IRF Stack	1-12
isis	IP Routing Volume-05-IS-IS	1-34
isis authentication-mode	IP Routing Volume-05-IS-IS	1-34
isis bfd enable	IP Routing Volume-13-BFD	1-11

isis circuit-level	IP Routing Volume-05-IS-IS	1-36
isis circuit-type p2p	IP Routing Volume-05-IS-IS	1-36
isis cost	IP Routing Volume-05-IS-IS	1-37
isis dis-name	IP Routing Volume-05-IS-IS	1-38
isis dis-priority	IP Routing Volume-05-IS-IS	1-39
isis enable	IP Routing Volume-05-IS-IS	1-40
isis ipv6 enable	IP Routing Volume-10-IPv6 IS-IS	1-11
isis mesh-group	IP Routing Volume-05-IS-IS	1-41
isis mib-binding	IP Routing Volume-05-IS-IS	1-42
isis silent	IP Routing Volume-05-IS-IS	1-42
isis small-hello	IP Routing Volume-05-IS-IS	1-43
isis timer csnp	IP Routing Volume-05-IS-IS	1-44
isis timer hello	IP Routing Volume-05-IS-IS	1-44
isis timer holding-multiplier	IP Routing Volume-05-IS-IS	1-45
isis timer lsp	IP Routing Volume-05-IS-IS	1-46
isis timer retransmit	IP Routing Volume-05-IS-IS	1-47
is-level	IP Routing Volume-05-IS-IS	1-48
is-name	IP Routing Volume-05-IS-IS	1-49
is-name map	IP Routing Volume-05-IS-IS	1-49
isolate-user-vlan	Access Volume-09-VLAN	2-2
isolate-user-vlan enable	Access Volume-09-VLAN	2-4
is-snmp-traps enable	IP Routing Volume-05-IS-IS	1-50

## J

jp-pkt-size (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-27
jp-pkt-size (PIM view)	IP Multicast Volume-03-PIM	1-29
jp-queue-size (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-27
jp-queue-size (PIM view)	IP Multicast Volume-03-PIM	1-30
jumboframe enable	Access Volume-01-Ethernet Interface	1-17

## K

key (HWTACACS scheme view)	Security Volume-01-AAA	3-6
----------------------------	------------------------	-----

key (RADIUS scheme view)	Security Volume-01-AAA	2-7
<b>L</b>		
lACP port-priority	Access Volume-02-Link Aggregation	1-11
lACP system-priority	Access Volume-02-Link Aggregation	1-11
last-listener-query-interval (MLD view)	IP Multicast Volume-09-MLD	1-11
last-listener-query-interval (MLD-Snooping view)	IP Multicast Volume-12-MLD Snooping	1-6
last-member-query-interval (IGMP view)	IP Multicast Volume-02-IGMP	1-25
last-member-query-interval (IGMP-Snooping view)	IP Multicast Volume-06-IGMP Snooping	1-22
lcd	System Volume-04-File System Management	2-18
ldap-server	Security Volume-09-PKI	1-15
link-aggregation load-sharing mode	Access Volume-02-Link Aggregation	1-12
link-aggregation mode	Access Volume-02-Link Aggregation	1-13
link-delay	Access Volume-01-Ethernet Interface	1-18
lldp admin-status	Access Volume-06-LLDP	1-15
lldp check-change-interval	Access Volume-06-LLDP	1-16
lldp compliance admin-status cdp	Access Volume-06-LLDP	1-17
lldp compliance cdp	Access Volume-06-LLDP	1-17
lldp enable	Access Volume-06-LLDP	1-18
lldp encapsulation snap	Access Volume-06-LLDP	1-19
lldp fast-count	Access Volume-06-LLDP	1-20
lldp hold-multiplier	Access Volume-06-LLDP	1-20
lldp management-address-format string	Access Volume-06-LLDP	1-21
lldp management-address-tlv	Access Volume-06-LLDP	1-22
lldp notification remote-change enable	Access Volume-06-LLDP	1-22
lldp timer notification-interval	Access Volume-06-LLDP	1-23
lldp timer reinit-delay	Access Volume-06-LLDP	1-23
lldp timer tx-delay	Access Volume-06-LLDP	1-24
lldp timer tx-interval	Access Volume-06-LLDP	1-25
lldp tlv-enable	Access Volume-06-LLDP	1-25

locality	Security Volume-09-PKI	1-16
local-proxy-arp enable	IP Services Volume-02-ARP	2-2
local-user	Security Volume-01-AAA	1-27
local-user password-display-mode	Security Volume-01-AAA	1-28
lock	System Volume-01-Login	1-13
logging-host	System Volume-17-Cluster Management	1-40
log-peer-change	IP Routing Volume-04-OSPF	1-40
log-peer-change	IP Routing Volume-06-BGP	1-36
log-peer-change	IP Routing Volume-09-OSPFv3	1-29
log-peer-change (IS-IS view)	IP Routing Volume-05-IS-IS	1-51
loopback	Access Volume-01-Ethernet Interface	1-19
loopback-detection control enable	Access Volume-01-Ethernet Interface	1-20
loopback-detection enable	Access Volume-01-Ethernet Interface	1-21
loopback-detection interval-time	Access Volume-01-Ethernet Interface	1-22
loopback-detection per-vlan enable	Access Volume-01-Ethernet Interface	1-22
ls	Security Volume-08-SSH2.0	1-21
ls	System Volume-04-File System Management	2-18
lsa-arrival-interval	IP Routing Volume-04-OSPF	1-41
lsa-generation-interval	IP Routing Volume-04-OSPF	1-41
lsdb-overflow-limit	IP Routing Volume-04-OSPF	1-42
lsp-fragments-extend	IP Routing Volume-05-IS-IS	1-51
lsp-length originate	IP Routing Volume-05-IS-IS	1-52
lsp-length receive	IP Routing Volume-05-IS-IS	1-53

## M

mac-address (Interface view)	System Volume-08-MAC Address Table Management	1-3
mac-address (system view)	System Volume-08-MAC Address Table Management	1-4
mac-address information enable (Ethernet interface view)	System Volume-08-MAC Address Table Management	2-1

mac-address information enable (system view)	System Volume-08-MAC Address Table Management	2-2
mac-address information interval	System Volume-08-MAC Address Table Management	2-2
mac-address information mode	System Volume-08-MAC Address Table Management	2-3
mac-address information queue-length	System Volume-08-MAC Address Table Management	2-4
mac-address mac-learning disable	System Volume-08-MAC Address Table Management	1-5
mac-address max-mac-count (Interface view)	System Volume-08-MAC Address Table Management	1-6
mac-address timer	System Volume-08-MAC Address Table Management	1-7
mac-authentication	Security Volume-04-MAC Authentication	1-3
mac-authentication domain	Security Volume-04-MAC Authentication	1-4
mac-authentication timer	Security Volume-04-MAC Authentication	1-4
mac-authentication user-name-format	Security Volume-04-MAC Authentication	1-5
mac-vlan enable	Access Volume-09-VLAN	1-20
mac-vlan mac-address	Access Volume-09-VLAN	1-21
management-vlan	System Volume-17-Cluster Management	1-41
management-vlan synchronization enable	System Volume-17-Cluster Management	1-42
maximum load-balancing (IS-IS view)	IP Routing Volume-05-IS-IS	1-53
maximum load-balancing (OSPF view)	IP Routing Volume-04-OSPF	1-43
maximum load-balancing (OSPFv3 view)	IP Routing Volume-09-OSPFv3	1-30
maximum load-balancing (RIP view)	IP Routing Volume-03-RIP	1-13
maximum load-balancing (RIPng view)	IP Routing Volume-08-RIPng	1-9
maximum-routes	IP Routing Volume-04-OSPF	1-43
max-response-time (IGMP view)	IP Multicast Volume-02-IGMP	1-25

max-response-time (IGMP-Snooping view)	IP Multicast Volume-06-IGMP Snooping	1-22
max-response-time (MLD view)	IP Multicast Volume-09-MLD	1-12
max-response-time (MLD-Snooping view)	IP Multicast Volume-12-MLD Snooping	1-6
mdi	Access Volume-01-Ethernet Interface	1-23
mib-style	System Volume-06-SNMP	2-1
mirroring-group	Access Volume-18-Port Mirroring	1-2
mirroring-group mirroring-port	Access Volume-18-Port Mirroring	1-3
mirroring-group monitor-egress	Access Volume-18-Port Mirroring	1-4
mirroring-group monitor-port	Access Volume-18-Port Mirroring	1-5
mirroring-group remote-probe vlan	Access Volume-18-Port Mirroring	1-6
mirroring-port	Access Volume-18-Port Mirroring	1-7
mirror-to	QoS Volume-01-QoS	6-1
mkdir	Security Volume-08-SSH2.0	1-22
mkdir	System Volume-04-File System Management	1-8
mkdir	System Volume-04-File System Management	2-20
mld	IP Multicast Volume-09-MLD	1-13
mld enable	IP Multicast Volume-09-MLD	1-13
mld group-limit	IP Multicast Volume-09-MLD	1-14
mld group-policy	IP Multicast Volume-09-MLD	1-15
mld last-listener-query-interval	IP Multicast Volume-09-MLD	1-16
mld max-response-time	IP Multicast Volume-09-MLD	1-16
mld proxying enable	IP Multicast Volume-09-MLD	1-18
mld proxying forwarding	IP Multicast Volume-09-MLD	1-18
mld require-router-alert	IP Multicast Volume-09-MLD	1-17
mld robust-count	IP Multicast Volume-09-MLD	1-19
mld send-router-alert	IP Multicast Volume-09-MLD	1-20
mld ssm-mapping enable	IP Multicast Volume-09-MLD	1-20
mld startup-query-count	IP Multicast Volume-09-MLD	1-21
mld startup-query-interval	IP Multicast Volume-09-MLD	1-22

mld static-group	IP Multicast Volume-09-MLD	1-23
mld timer other-querier-present	IP Multicast Volume-09-MLD	1-24
mld timer query	IP Multicast Volume-09-MLD	1-24
mld version	IP Multicast Volume-09-MLD	1-25
mld-snooping	IP Multicast Volume-12-MLD Snooping	1-7
mld-snooping drop-unknown	IP Multicast Volume-12-MLD Snooping	1-8
mld-snooping enable	IP Multicast Volume-12-MLD Snooping	1-8
mld-snooping fast-leave	IP Multicast Volume-12-MLD Snooping	1-9
mld-snooping general-query source-ip	IP Multicast Volume-12-MLD Snooping	1-10
mld-snooping group-limit	IP Multicast Volume-12-MLD Snooping	1-11
mld-snooping group-policy	IP Multicast Volume-12-MLD Snooping	1-12
mld-snooping host-aging-time	IP Multicast Volume-12-MLD Snooping	1-13
mld-snooping host-join	IP Multicast Volume-12-MLD Snooping	1-13
mld-snooping last-listener-query-interval	IP Multicast Volume-12-MLD Snooping	1-15
mld-snooping max-response-time	IP Multicast Volume-12-MLD Snooping	1-15
mld-snooping overflow-replace	IP Multicast Volume-12-MLD Snooping	1-16
mld-snooping querier	IP Multicast Volume-12-MLD Snooping	1-17
mld-snooping query-interval	IP Multicast Volume-12-MLD Snooping	1-17
mld-snooping router-aging-time	IP Multicast Volume-12-MLD Snooping	1-18
mld-snooping source-deny	IP Multicast Volume-12-MLD Snooping	1-19

mld-snooping special-query source-ip	IP Multicast Volume-12-MLD Snooping	1-19
mld-snooping static-group	IP Multicast Volume-12-MLD Snooping	1-20
mld-snooping static-router-port	IP Multicast Volume-12-MLD Snooping	1-21
mld-snooping version	IP Multicast Volume-12-MLD Snooping	1-22
monitor-link group	Access Volume-08-Monitor Link	1-2
monitor-port	Access Volume-18-Port Mirroring	1-8
more	System Volume-04-File System Management	1-9
move	System Volume-04-File System Management	1-10
msdp	IP Multicast Volume-04-MSDP	1-9
mtracert	IP Multicast Volume-01-Multicast Routing and Forwarding	1-9
multicast boundary	IP Multicast Volume-01-Multicast Routing and Forwarding	1-11
multicast forwarding-table downstream-limit	IP Multicast Volume-01-Multicast Routing and Forwarding	1-12
multicast forwarding-table route-limit	IP Multicast Volume-01-Multicast Routing and Forwarding	1-13
multicast ipv6 boundary	IP Multicast Volume-08-IPv6 Multicast Routing and Forwarding	1-7
multicast ipv6 forwarding-table downstream-limit	IP Multicast Volume-08-IPv6 Multicast Routing and Forwarding	1-8
multicast ipv6 forwarding-table route-limit	IP Multicast Volume-08-IPv6 Multicast Routing and Forwarding	1-8
multicast ipv6 load-splitting	IP Multicast Volume-08-IPv6 Multicast Routing and Forwarding	1-9
multicast ipv6 longest-match	IP Multicast Volume-08-IPv6 Multicast Routing and Forwarding	1-10
multicast ipv6 routing-enable	IP Multicast Volume-08-IPv6 Multicast Routing and Forwarding	1-10
multicast load-splitting	IP Multicast Volume-01-Multicast Routing and Forwarding	1-13

multicast longest-match	IP Multicast Volume-01-Multicast Routing and Forwarding	1-14
multicast routing-enable	IP Multicast Volume-01-Multicast Routing and Forwarding	1-14
multicast-suppression	Access Volume-01-Ethernet Interface	1-24
multicast-vlan	IP Multicast Volume-07-Multicast VLAN	1-2
multicast-vlan ipv6	IP Multicast Volume-13-IPv6 Multicast VLAN	1-2

## N

name	Access Volume-09-VLAN	1-6
nas-ip (HWTACACS scheme view)	Security Volume-01-AAA	3-6
nas-ip (RADIUS scheme view)	Security Volume-01-AAA	2-8
nbns-list	IP Services Volume-03-DHCP	1-19
ndp enable	System Volume-17-Cluster Management	1-4
ndp timer aging	System Volume-17-Cluster Management	1-5
ndp timer hello	System Volume-17-Cluster Management	1-6
nest	QoS Volume-01-QoS	1-9
netbios-type	IP Services Volume-03-DHCP	1-20
network	IP Services Volume-03-DHCP	1-21
network	IP Routing Volume-03-RIP	1-13
network (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-37
network (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-27
network (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-29
network (MBGP family view)	IP Multicast Volume-05-MBGP	1-31
network (OSPF area view)	IP Routing Volume-04-OSPF	1-44
network ip range	IP Services Volume-03-DHCP	1-21
network mask	IP Services Volume-03-DHCP	1-22
network short-cut (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-38
network-entity	IP Routing Volume-05-IS-IS	1-54

next-hop	System Volume-13-NQA	1-18
nm-interface vlan-interface	System Volume-17-Cluster Management	1-43
nqa	System Volume-13-NQA	1-19
nqa agent enable	System Volume-13-NQA	1-19
nqa agent max-concurrent	System Volume-13-NQA	1-20
nqa schedule	System Volume-13-NQA	1-21
nqa server enable	System Volume-13-NQA	1-39
nqa server tcp-connect	System Volume-13-NQA	1-40
nqa server udp-echo	System Volume-13-NQA	1-41
nssa	IP Routing Volume-04-OSPF	1-45
ntdp enable	System Volume-17-Cluster Management	1-11
ntdp explore	System Volume-17-Cluster Management	1-11
ntdp hop	System Volume-17-Cluster Management	1-12
ntdp timer	System Volume-17-Cluster Management	1-12
ntdp timer hop-delay	System Volume-17-Cluster Management	1-13
ntdp timer port-delay	System Volume-17-Cluster Management	1-14
ntp-service access	System Volume-14-NTP	1-5
ntp-service authentication enable	System Volume-14-NTP	1-6
ntp-service authentication-keyid	System Volume-14-NTP	1-7
ntp-service broadcast-client	System Volume-14-NTP	1-8
ntp-service broadcast-server	System Volume-14-NTP	1-8
ntp-service in-interface disable	System Volume-14-NTP	1-9
ntp-service max-dynamic-sessions	System Volume-14-NTP	1-9
ntp-service multicast-client	System Volume-14-NTP	1-10
ntp-service multicast-server	System Volume-14-NTP	1-11
ntp-service reliable authentication-keyid	System Volume-14-NTP	1-12
ntp-service source-interface	System Volume-14-NTP	1-12

ntp-service unicast-peer	System Volume-14-NTP	1-13
ntp-service unicast-server	System Volume-14-NTP	1-14
<b>O</b>		
oam enable	Access Volume-14-Ethernet OAM	1-8
oam errored-frame period	Access Volume-14-Ethernet OAM	1-9
oam errored-frame threshold	Access Volume-14-Ethernet OAM	1-10
oam errored-frame-period period	Access Volume-14-Ethernet OAM	1-10
oam errored-frame-period threshold	Access Volume-14-Ethernet OAM	1-11
oam errored-frame-seconds period	Access Volume-14-Ethernet OAM	1-12
oam errored-frame-seconds threshold	Access Volume-14-Ethernet OAM	1-12
oam errored-symbol period	Access Volume-14-Ethernet OAM	1-13
oam errored-symbol threshold	Access Volume-14-Ethernet OAM	1-13
oam loopback	Access Volume-14-Ethernet OAM	1-14
oam mode	Access Volume-14-Ethernet OAM	1-15
opaque-capability enable	IP Routing Volume-04-OSPF	1-46
open	System Volume-04-File System Management	2-20
open ipv6	System Volume-04-File System Management	2-21
operation (FTP test type view)	System Volume-13-NQA	1-22
operation (HTTP test type view)	System Volume-13-NQA	1-22
operation interface	System Volume-13-NQA	1-23
option	IP Services Volume-03-DHCP	1-23
organization	Security Volume-09-PKI	1-16
organization-unit	Security Volume-09-PKI	1-17
originating-rp	IP Multicast Volume-04-MSDP	1-10
ospf	IP Routing Volume-04-OSPF	1-46
ospf authentication-mode	IP Routing Volume-04-OSPF	1-47
ospf bfd enable	IP Routing Volume-13-BFD	1-12
ospf cost	IP Routing Volume-04-OSPF	1-49
ospf dr-priority	IP Routing Volume-04-OSPF	1-49

ospf mib-binding	IP Routing Volume-04-OSPF	1-50
ospf mtu-enable	IP Routing Volume-04-OSPF	1-51
ospf network-type	IP Routing Volume-04-OSPF	1-51
ospf packet-process prioritized-treatment	IP Routing Volume-04-OSPF	1-52
ospf timer dead	IP Routing Volume-04-OSPF	1-53
ospf timer hello	IP Routing Volume-04-OSPF	1-54
ospf timer poll	IP Routing Volume-04-OSPF	1-55
ospf timer retransmit	IP Routing Volume-04-OSPF	1-55
ospf trans-delay	IP Routing Volume-04-OSPF	1-56
ospfv3	IP Routing Volume-09-OSPFv3	1-31
ospfv3 area	IP Routing Volume-09-OSPFv3	1-31
ospfv3 cost	IP Routing Volume-09-OSPFv3	1-32
ospfv3 dr-priority	IP Routing Volume-09-OSPFv3	1-33
ospfv3 mtu-ignore	IP Routing Volume-09-OSPFv3	1-33
ospfv3 network-type	IP Routing Volume-09-OSPFv3	1-34
ospfv3 peer	IP Routing Volume-09-OSPFv3	1-35
ospfv3 timer dead	IP Routing Volume-09-OSPFv3	1-35
ospfv3 timer hello	IP Routing Volume-09-OSPFv3	1-36
ospfv3 timer poll	IP Routing Volume-09-OSPFv3	1-38
ospfv3 timer retransmit	IP Routing Volume-09-OSPFv3	1-37
ospfv3 trans-delay	IP Routing Volume-09-OSPFv3	1-38
output-delay	IP Routing Volume-03-RIP	1-14
overflow-replace (IGMP-Snooping view)	IP Multicast Volume-06-IGMP Snooping	1-23
overflow-replace (MLD-Snooping view)	IP Multicast Volume-12-MLD Snooping	1-23

## P

parity	System Volume-01-Login	1-14
passive	System Volume-04-File System Management	2-22
password	Security Volume-01-AAA	1-29
password (FTP test type view)	System Volume-13-NQA	1-24

patch active	System Volume-16-Hotfix	1-2
patch deactivate	System Volume-16-Hotfix	1-2
patch delete	System Volume-16-Hotfix	1-3
patch install	System Volume-16-Hotfix	1-4
patch load	System Volume-16-Hotfix	1-5
patch location	System Volume-16-Hotfix	1-5
patch run	System Volume-16-Hotfix	1-6
peer	IP Routing Volume-03-RIP	1-15
peer	IP Routing Volume-04-OSPF	1-57
peer advertise-community (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-39
peer advertise-community (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-27
peer advertise-community (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-30
peer advertise-community (MBGP family view)	IP Multicast Volume-05-MBGP	1-32
peer advertise-ext-community (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-39
peer advertise-ext-community (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-28
peer advertise-ext-community (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-31
peer advertise-ext-community (MBGP family view)	IP Multicast Volume-05-MBGP	1-33
peer allow-as-loop	IP Routing Volume-14-MCE	1-18
peer allow-as-loop (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-40
peer allow-as-loop (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-29
peer allow-as-loop (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-31
peer allow-as-loop (MBGP family view)	IP Multicast Volume-05-MBGP	1-34
peer as-number (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-41
peer as-number (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-30
peer as-path-acl (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-42
peer as-path-acl (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-30
peer as-path-acl (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-32

peer as-path-acl (MBGP family view)	IP Multicast Volume-05-MBGP	1-34
peer capability-advertise conventional	IP Routing Volume-06-BGP	1-43
peer capability-advertise route-refresh	IP Routing Volume-06-BGP	1-44
peer capability-advertise route-refresh	IP Routing Volume-11-IPv6 BGP	1-31
peer connect-interface	IP Multicast Volume-04-MSDP	1-10
peer connect-interface (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-44
peer connect-interface (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-32
peer default-route-advertise	IP Routing Volume-11-IPv6 BGP	1-33
peer default-route-advertise (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-45
peer default-route-advertise (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-33
peer default-route-advertise (MBGP family view)	IP Multicast Volume-05-MBGP	1-35
peer description	IP Multicast Volume-04-MSDP	1-11
peer description (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-46
peer description (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-33
peer ebgp-max-hop (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-47
peer ebgp-max-hop (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-34
peer enable (BGP view)	IP Routing Volume-06-BGP	1-48
peer enable (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-34
peer enable (MBGP family view)	IP Multicast Volume-05-MBGP	1-36
peer fake-as (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-48
peer fake-as (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-35
peer filter-policy (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-49
peer filter-policy (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-35
peer filter-policy (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-35
peer filter-policy (MBGP family view)	IP Multicast Volume-05-MBGP	1-37
peer group	IP Routing Volume-14-MCE	1-19
peer group (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-50
peer group (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-36
peer group (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-35

peer group (MBGP family view)	IP Multicast Volume-05-MBGP	1-37
peer ignore (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-51
peer ignore (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-37
peer <i>ip-address</i> bfd	IP Routing Volume-13-BFD	1-12
peer ip-prefix	IP Routing Volume-06-BGP	1-52
peer ip-prefix (MBGP family view)	IP Multicast Volume-05-MBGP	1-38
peer ipv6-prefix	IP Routing Volume-11-IPv6 BGP	1-38
peer ipv6-prefix (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-36
peer keep-all-routes (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-53
peer keep-all-routes (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-38
peer keep-all-routes (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-37
peer keep-all-routes (MBGP family view)	IP Multicast Volume-05-MBGP	1-39
peer log-change (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-53
peer log-change (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-39
peer mesh-group	IP Multicast Volume-04-MSDP	1-12
peer minimum-ttl	IP Multicast Volume-04-MSDP	1-12
peer next-hop-local (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-54
peer next-hop-local (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-40
peer next-hop-local (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-38
peer next-hop-local (MBGP family view)	IP Multicast Volume-05-MBGP	1-40
peer password	IP Routing Volume-06-BGP	1-55
peer preferred-value (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-56
peer preferred-value (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-40
peer preferred-value (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-39
peer preferred-value (MBGP family view)	IP Multicast Volume-05-MBGP	1-40
peer public-as-only (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-57
peer public-as-only (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-41
peer public-as-only (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-40
peer public-as-only (MBGP family view)	IP Multicast Volume-05-MBGP	1-41

peer reflect-client (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-58
peer reflect-client (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-42
peer reflect-client (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-40
peer reflect-client (MBGP family view)	IP Multicast Volume-05-MBGP	1-42
peer request-sa-enable	IP Multicast Volume-04-MSDP	1-13
peer route-limit (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-59
peer route-limit (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-43
peer route-limit (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-41
peer route-limit (MBGP family view)	IP Multicast Volume-05-MBGP	1-43
peer route-policy (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-60
peer route-policy (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-44
peer route-policy (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-42
peer route-policy (MBGP family view)	IP Multicast Volume-05-MBGP	1-44
peer route-update-interval (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-61
peer route-update-interval (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-45
peer sa-cache-maximum	IP Multicast Volume-04-MSDP	1-14
peer sa-policy	IP Multicast Volume-04-MSDP	1-15
peer sa-request-policy	IP Multicast Volume-04-MSDP	1-15
peer substitute-as (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-61
peer substitute-as (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-45
peer timer (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-62
peer timer (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-46
peer-public-key end	Security Volume-11-Public Key	1-3
pim	IP Multicast Volume-03-PIM	1-30
pim bsr-boundary	IP Multicast Volume-03-PIM	1-31
pim dm	IP Multicast Volume-03-PIM	1-32
pim hello-option dr-priority	IP Multicast Volume-03-PIM	1-32
pim hello-option holdtime	IP Multicast Volume-03-PIM	1-33
pim hello-option lan-delay	IP Multicast Volume-03-PIM	1-34
pim hello-option neighbor-tracking	IP Multicast Volume-03-PIM	1-34

pim hello-option override-interval	IP Multicast Volume-03-PIM	1-35
pim holdtime assert	IP Multicast Volume-03-PIM	1-36
pim holdtime join-prune	IP Multicast Volume-03-PIM	1-36
pim ipv6	IP Multicast Volume-10-IPv6 PIM	1-28
pim ipv6 bsr-boundary	IP Multicast Volume-10-IPv6 PIM	1-29
pim ipv6 dm	IP Multicast Volume-10-IPv6 PIM	1-29
pim ipv6 hello-option dr-priority	IP Multicast Volume-10-IPv6 PIM	1-30
pim ipv6 hello-option holdtime	IP Multicast Volume-10-IPv6 PIM	1-31
pim ipv6 hello-option lan-delay	IP Multicast Volume-10-IPv6 PIM	1-31
pim ipv6 hello-option neighbor-tracking	IP Multicast Volume-10-IPv6 PIM	1-32
pim ipv6 hello-option override-interval	IP Multicast Volume-10-IPv6 PIM	1-33
pim ipv6 holdtime assert	IP Multicast Volume-10-IPv6 PIM	1-33
pim ipv6 holdtime join-prune	IP Multicast Volume-10-IPv6 PIM	1-34
pim ipv6 neighbor-policy	IP Multicast Volume-10-IPv6 PIM	1-35
pim ipv6 require-genid	IP Multicast Volume-10-IPv6 PIM	1-35
pim ipv6 sm	IP Multicast Volume-10-IPv6 PIM	1-36
pim ipv6 state-refresh-capable	IP Multicast Volume-10-IPv6 PIM	1-37
pim ipv6 timer graft-retry	IP Multicast Volume-10-IPv6 PIM	1-37
pim ipv6 timer hello	IP Multicast Volume-10-IPv6 PIM	1-38
pim ipv6 timer join-prune	IP Multicast Volume-10-IPv6 PIM	1-38
pim ipv6 triggered-hello-delay	IP Multicast Volume-10-IPv6 PIM	1-39
pim neighbor-policy	IP Multicast Volume-03-PIM	1-37
pim require-genid	IP Multicast Volume-03-PIM	1-38
pim sm	IP Multicast Volume-03-PIM	1-38
pim state-refresh-capable	IP Multicast Volume-03-PIM	1-39
pim timer graft-retry	IP Multicast Volume-03-PIM	1-39
pim timer hello	IP Multicast Volume-03-PIM	1-40
pim timer join-prune	IP Multicast Volume-03-PIM	1-41
pim triggered-hello-delay	IP Multicast Volume-03-PIM	1-41
ping	System Volume-09-System Maintaining and Debugging	1-1

ping ipv6	System Volume-09-System Maintaining and Debugging	1-4
pki certificate access-control-policy	Security Volume-09-PKI	1-17
pki certificate attribute-group	Security Volume-09-PKI	1-18
pki delete-certificate	Security Volume-09-PKI	1-19
pki domain	Security Volume-09-PKI	1-19
pki entity	Security Volume-09-PKI	1-20
pki import-certificate	Security Volume-09-PKI	1-21
pki request-certificate domain	Security Volume-09-PKI	1-21
pki retrieval-certificate	Security Volume-09-PKI	1-22
pki retrieval-crl domain	Security Volume-09-PKI	1-23
pki validate-certificate	Security Volume-09-PKI	1-23
pki-domain	Security Volume-10-SSL	1-6
poe disconnect	System Volume-11-PoE	1-15
poe enable	System Volume-11-PoE	1-15
poe legacy enable	System Volume-11-PoE	1-16
poe max-power	System Volume-11-PoE	1-17
poe mode	System Volume-11-PoE	1-17
poe pd-description	System Volume-11-PoE	1-18
poe pd-policy priority	System Volume-11-PoE	1-19
poe priority	System Volume-11-PoE	1-19
poe update	System Volume-11-PoE	1-20
poe utilization-threshold	System Volume-11-PoE	1-21
poe-profile	System Volume-11-PoE	1-22
port	Access Volume-07-Smart Link	1-4
port	Access Volume-08-Monitor Link	1-2
port	Access Volume-09-VLAN	1-10
port (IPv6 multicast VLAN view)	IP Multicast Volume-13-IPv6 Multicast VLAN	1-3
port (multicast VLAN view)	IP Multicast Volume-07-Multicast VLAN	1-3
port access vlan	Access Volume-09-VLAN	1-10

port hybrid ip-subnet-vlan vlan	Access Volume-09-VLAN	1-31
port hybrid protocol-vlan	Access Volume-09-VLAN	1-24
port hybrid pvid vlan	Access Volume-09-VLAN	1-11
port hybrid vlan	Access Volume-09-VLAN	1-13
port link-aggregation group	Access Volume-02-Link Aggregation	1-14
port link-type	Access Volume-09-VLAN	1-14
port monitor-link group	Access Volume-08-Monitor Link	1-3
port multicast-vlan	IP Multicast Volume-07-Multicast VLAN	1-3
port multicast-vlan ipv6	IP Multicast Volume-13-IPv6 Multicast VLAN	1-3
port service-loopback group	Access Volume-04-Service Loopback Group	1-2
port smart-link group	Access Volume-07-Smart Link	1-4
port trunk permit vlan	Access Volume-09-VLAN	1-15
port trunk pvid vlan	Access Volume-09-VLAN	1-17
portal auth-network	Security Volume-05-Portal	1-13
portal delete-user	Security Volume-05-Portal	1-14
portal domain	Security Volume-05-Portal	1-14
portal free-rule	Security Volume-05-Portal	1-15
portal server	Security Volume-05-Portal	1-16
portal server method	Security Volume-05-Portal	1-17
port-group manual	Access Volume-01-Ethernet Interface	1-25
port-isolate enable	Access Volume-03-Port Isolation	1-2
port-security authorization ignore	Security Volume-06-Port Security	1-6
port-security enable	Security Volume-06-Port Security	1-7
port-security intrusion-mode	Security Volume-06-Port Security	1-8
port-security mac-address security	Security Volume-06-Port Security	1-9
port-security max-mac-count	Security Volume-06-Port Security	1-10
port-security ntk-mode	Security Volume-06-Port Security	1-11
port-security oui	Security Volume-06-Port Security	1-12
port-security port-mode	Security Volume-06-Port Security	1-13

port-security timer disableport	Security Volume-06-Port Security	1-14
port-security trap	Security Volume-06-Port Security	1-15
preemption delay	Access Volume-07-Smart Link	1-5
preemption mode	Access Volume-07-Smart Link	1-6
prefer-cipher	Security Volume-10-SSL	1-6
preference	IP Routing Volume-03-RIP	1-15
preference	IP Routing Volume-04-OSPF	1-58
preference	IP Routing Volume-08-RIPng	1-10
preference	IP Routing Volume-09-OSPFv3	1-39
preference (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-63
preference (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-47
preference (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-43
preference (IS-IS view)	IP Routing Volume-05-IS-IS	1-55
preference (MBGP family view)	IP Multicast Volume-05-MBGP	1-45
primary accounting (HWTACACS scheme view)	Security Volume-01-AAA	3-7
primary accounting (RADIUS scheme view)	Security Volume-01-AAA	2-9
primary authentication (HWTACACS scheme view)	Security Volume-01-AAA	3-8
primary authentication (RADIUS scheme view)	Security Volume-01-AAA	2-10
primary authorization	Security Volume-01-AAA	3-9
probe count	System Volume-13-NQA	1-24
probe packet-interval	System Volume-13-NQA	1-25
probe packet-number	System Volume-13-NQA	1-26
probe packet-timeout	System Volume-13-NQA	1-26
probe timeout	System Volume-13-NQA	1-27
probe-interval (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-40
probe-interval (PIM view)	IP Multicast Volume-03-PIM	1-42
protected-vlan	Access Volume-07-Smart Link	1-7
protected-vlan	Access Volume-17-RRPP	1-10
protocol inbound	System Volume-01-Login	1-15
protocol-vlan	Access Volume-09-VLAN	1-26
proxy-arp enable	IP Services Volume-02-ARP	2-2

public-key local create	Security Volume-11-Public Key	1-5
public-key local destroy	Security Volume-11-Public Key	1-6
public-key local export dsa	Security Volume-11-Public Key	1-7
public-key local export rsa	Security Volume-11-Public Key	1-8
public-key peer	Security Volume-11-Public Key	1-9
public-key peer import sshkey	Security Volume-11-Public Key	1-10
public-key-code begin	Security Volume-11-Public Key	1-4
public-key-code end	Security Volume-11-Public Key	1-4
put	Security Volume-08-SSH2.0	1-22
put	System Volume-04-File System Management	2-22
pwd	Security Volume-08-SSH2.0	1-23
pwd	System Volume-04-File System Management	1-10
pwd	System Volume-04-File System Management	2-23

## Q

qinq enable	Access Volume-11-QinQ	1-2
qinq enable downlink	Access Volume-13-VLAN Mapping	1-1
qinq enable uplink	Access Volume-13-VLAN Mapping	1-2
qinq ethernet-type	Access Volume-11-QinQ	1-3
qinq vid	Access Volume-11-QinQ	1-4
qos apply policy	QoS Volume-01-QoS	1-23
qos apply policy global	QoS Volume-01-QoS	1-24
qos bandwidth queue	QoS Volume-01-QoS	4-4
qos gts	QoS Volume-01-QoS	3-2
qos lr outbound	QoS Volume-01-QoS	3-3
qos map-table	QoS Volume-01-QoS	2-2
qos policy	QoS Volume-01-QoS	1-25
qos priority	QoS Volume-01-QoS	2-3
qos sp	QoS Volume-01-QoS	4-4
qos trust	QoS Volume-01-QoS	2-5

qos vlan-policy	QoS Volume-01-QoS	1-26
qos wfq	QoS Volume-01-QoS	4-5
qos wfq weight	QoS Volume-01-QoS	4-6
qos wred apply	QoS Volume-01-QoS	5-2
qos wred queue table	QoS Volume-01-QoS	5-3
qos wrr	QoS Volume-01-QoS	4-6
qos wrr group	QoS Volume-01-QoS	4-7
queue	QoS Volume-01-QoS	5-4
quit	Security Volume-08-SSH2.0	1-24
quit	System Volume-02-Basic System Configuration	1-18
quit	System Volume-04-File System Management	2-24

## R

radius client	Security Volume-01-AAA	2-11
radius nas-ip	Security Volume-01-AAA	2-12
radius scheme	Security Volume-01-AAA	2-13
radius trap	Security Volume-01-AAA	2-13
raw-vlan-id inbound	Access Volume-11-QinQ	1-1
reaction	System Volume-13-NQA	1-28
reaction trap	System Volume-13-NQA	1-29
reboot	System Volume-03-Device Management	1-24
reboot member	System Volume-17-Cluster Management	1-43
redirect	QoS Volume-01-QoS	1-10
reflect between-clients (BGP view)	IP Routing Volume-06-BGP	1-64
reflect between-clients (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-48
reflect between-clients (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-44
reflect between-clients (MBGP family view)	IP Multicast Volume-05-MBGP	1-45
reflector cluster-id (BGP view)	IP Routing Volume-06-BGP	1-65

reflector cluster-id (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-48
reflector cluster-id (IPv6 MBGP address family view)	IP Multicast Volume-11-IPv6 MBGP	1-45
reflector cluster-id (MBGP family view)	IP Multicast Volume-05-MBGP	1-46
refresh bgp ipv4 multicast	IP Multicast Volume-05-MBGP	1-47
refresh bgp	IP Routing Volume-06-BGP	1-65
refresh bgp ipv6	IP Routing Volume-11-IPv6 BGP	1-49
refresh bgp ipv6 multicast	IP Multicast Volume-11-IPv6 MBGP	1-45
refresh bgp vpn-instance	IP Routing Volume-14-MCE	1-20
region-name	Access Volume-16-MSTP	1-12
register-policy (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-40
register-policy (PIM view)	IP Multicast Volume-03-PIM	1-42
register-suppression-timeout (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-41
register-suppression-timeout (PIM view)	IP Multicast Volume-03-PIM	1-43
register-whole-checksum (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-42
register-whole-checksum (PIM view)	IP Multicast Volume-03-PIM	1-44
remark customer-vlan-id	QoS Volume-01-QoS	1-11
remark dot1p	QoS Volume-01-QoS	1-12
remark drop-precedence	QoS Volume-01-QoS	1-12
remark dscp	QoS Volume-01-QoS	1-13
remark ip-precedence	QoS Volume-01-QoS	1-14
remark local-precedence	QoS Volume-01-QoS	1-15
remark service-vlan-id	QoS Volume-01-QoS	1-15
remotehelp	System Volume-04-File System Management	2-24
remove	Security Volume-08-SSH2.0	1-24
rename	Security Volume-08-SSH2.0	1-25
rename	System Volume-04-File System Management	1-11
report-aggregation (IGMP-Snooping view)	IP Multicast Volume-06-IGMP Snooping	1-24
report-aggregation (MLD-Snooping view)	IP Multicast Volume-12-MLD Snooping	1-24
require-router-alert (IGMP view)	IP Multicast Volume-02-IGMP	1-26

require-router-alert (MLD view)	IP Multicast Volume-09-MLD	1-26
reset acl counter	Security Volume-12-ACL	1-10
reset acl ipv6 counter	Security Volume-12-ACL	1-24
reset arp	IP Services Volume-02-ARP	1-7
reset arp detection statistics	IP Services Volume-02-ARP	3-14
reset bfd session statistics	IP Routing Volume-13-BFD	1-13
reset bgp	IP Routing Volume-06-BGP	1-66
reset bgp dampening	IP Routing Volume-06-BGP	1-67
reset bgp flap-info	IP Routing Volume-06-BGP	1-67
reset bgp ipv4 all	IP Routing Volume-06-BGP	1-68
reset bgp ipv4 multicast	IP Multicast Volume-05-MBGP	1-48
reset bgp ipv4 multicast dampening	IP Multicast Volume-05-MBGP	1-48
reset bgp ipv4 multicast flap-info	IP Multicast Volume-05-MBGP	1-49
reset bgp ipv6	IP Routing Volume-11-IPv6 BGP	1-50
reset bgp ipv6 dampening	IP Routing Volume-11-IPv6 BGP	1-50
reset bgp ipv6 flap-info	IP Routing Volume-11-IPv6 BGP	1-51
reset bgp ipv6 multicast	IP Multicast Volume-11-IPv6 MBGP	1-46
reset bgp ipv6 multicast dampening	IP Multicast Volume-11-IPv6 MBGP	1-47
reset bgp ipv6 multicast flap-info	IP Multicast Volume-11-IPv6 MBGP	1-47
reset bgp vpn-instance	IP Routing Volume-14-MCE	1-20
reset bgp vpn-instance dampening	IP Routing Volume-14-MCE	1-21
reset bgp vpn-instance flap-info	IP Routing Volume-14-MCE	1-22
reset counters interface	Access Volume-01-Ethernet Interface	1-26
reset dhcp relay statistics	IP Services Volume-03-DHCP	2-19
reset dhcp server conflict	IP Services Volume-03-DHCP	1-24
reset dhcp server ip-in-use	IP Services Volume-03-DHCP	1-24
reset dhcp server statistics	IP Services Volume-03-DHCP	1-25
reset dhcp-snooping	IP Services Volume-03-DHCP	4-12
reset dhcp-snooping packet statistics	IP Services Volume-03-DHCP	4-12
reset dldp statistics	Access Volume-05-DLDP	1-9
reset dns dynamic-host	IP Services Volume-04-DNS	1-7

reset dns ipv6 dynamic-host	IP Services Volume-08-IPv6 Basics	1-38
reset dot1x statistics	Security Volume-02-802.1X	1-15
reset garp statistics	Access Volume-10-GVRP	1-10
reset hwtacacs statistics	Security Volume-01-AAA	3-10
reset igmp group	IP Multicast Volume-02-IGMP	1-27
reset igmp group port-info	IP Multicast Volume-02-IGMP	1-28
reset igmp ssm-mapping group	IP Multicast Volume-02-IGMP	1-28
reset igmp-snooping group	IP Multicast Volume-06-IGMP Snooping	1-24
reset igmp-snooping statistics	IP Multicast Volume-06-IGMP Snooping	1-25
reset ip ip-prefix	IP Routing Volume-12-Route Policy	1-26
reset ip ipv6-prefix	IP Routing Volume-12-Route Policy	1-30
reset ip routing-table statistics protocol	IP Routing Volume-01-IP Routing Table Display	1-21
reset ip statistics	IP Services Volume-05-IP Performance Optimization	1-17
reset ipc performance	System Volume-19-IPC	1-9
reset ipv6 neighbors	IP Services Volume-08-IPv6 Basics	1-38
reset ipv6 pathmtu	IP Services Volume-08-IPv6 Basics	1-39
reset ipv6 routing-table statistics	IP Routing Volume-01-IP Routing Table Display	1-22
reset ipv6 statistics	IP Services Volume-08-IPv6 Basics	1-39
reset isis all	IP Routing Volume-05-IS-IS	1-55
reset isis peer	IP Routing Volume-05-IS-IS	1-56
reset lacp statistics	Access Volume-02-Link Aggregation	1-14
reset logbuffer	System Volume-10-Information Center	1-21
reset mac-authentication statistics	Security Volume-04-MAC Authentication	1-6
reset mld group	IP Multicast Volume-09-MLD	1-26
reset mld group port-info	IP Multicast Volume-09-MLD	1-27
reset mld ssm-mapping group	IP Multicast Volume-09-MLD	1-28

reset mld-snooping group	IP Multicast Volume-12-MLD Snooping	1-24
reset mld-snooping statistics	IP Multicast Volume-12-MLD Snooping	1-25
reset msdp peer	IP Multicast Volume-04-MSDP	1-16
reset msdp sa-cache	IP Multicast Volume-04-MSDP	1-17
reset msdp statistics	IP Multicast Volume-04-MSDP	1-17
reset multicast forwarding-table	IP Multicast Volume-01-Multicast Routing and Forwarding	1-15
reset multicast ipv6 forwarding-table	IP Multicast Volume-08-IPv6 Multicast Routing and Forwarding	1-11
reset multicast ipv6 routing-table	IP Multicast Volume-08-IPv6 Multicast Routing and Forwarding	1-12
reset multicast routing-table	IP Multicast Volume-01-Multicast Routing and Forwarding	1-16
reset ndp statistics	System Volume-17-Cluster Management	1-6
reset oam	Access Volume-14-Ethernet OAM	1-15
reset ospf counters	IP Routing Volume-04-OSPF	1-59
reset ospf process	IP Routing Volume-04-OSPF	1-59
reset ospf redistribution	IP Routing Volume-04-OSPF	1-60
reset packet-drop interface	Access Volume-01-Ethernet Interface	1-26
reset pim control-message counters	IP Multicast Volume-03-PIM	1-44
reset pim ipv6 control-message counters	IP Multicast Volume-10-IPv6 PIM	1-42
reset portal connection statistics	Security Volume-05-Portal	1-18
reset portal server statistics	Security Volume-05-Portal	1-19
reset portal tcp-cheat statistics	Security Volume-05-Portal	1-19
reset qos policy global	QoS Volume-01-QoS	1-27
reset qos vlan-policy	QoS Volume-01-QoS	1-27
reset radius statistics	Security Volume-01-AAA	2-14
reset recycle-bin	System Volume-04-File System Management	1-11
reset rip statistics	IP Routing Volume-03-RIP	1-16
reset rrp statistics	Access Volume-17-RRPP	1-11

reset saved-configuration	System Volume-04-File System Management	1-19
reset smart-link statistics	Access Volume-07-Smart Link	1-8
reset stop-accounting-buffer	Security Volume-01-AAA	2-15
reset stop-accounting-buffer	Security Volume-01-AAA	3-10
reset stp	Access Volume-16-MSTP	1-13
reset tcp ipv6 statistics	IP Services Volume-08-IPv6 Basics	1-40
reset tcp statistics	IP Services Volume-05-IP Performance Optimization	1-17
reset trapbuffer	System Volume-10-Information Center	1-22
reset udp ipv6 statistics	IP Services Volume-08-IPv6 Basics	1-40
reset udp statistics	IP Services Volume-05-IP Performance Optimization	1-18
reset udp-helper packet	IP Services Volume-06-UDP Helper	1-1
reset unused porttag	System Volume-03-Device Management	1-25
reset vrrp ipv6 statistics	System Volume-15-VRRP	1-18
reset vrrp statistics	System Volume-15-VRRP	1-5
restore startup-configuration	System Volume-04-File System Management	1-20
retry	Security Volume-01-AAA	2-16
retry realtime-accounting	Security Volume-01-AAA	2-16
retry stop-accounting (HWTACACS scheme view)	Security Volume-01-AAA	3-11
retry stop-accounting (RADIUS scheme view)	Security Volume-01-AAA	2-17
return	System Volume-02-Basic System Configuration	1-18
revision-level	Access Volume-16-MSTP	1-14
rfc1583 compatible	IP Routing Volume-04-OSPF	1-60
ring	Access Volume-17-RRPP	1-12
ring enable	Access Volume-17-RRPP	1-14
rip	IP Routing Volume-03-RIP	1-16
rip authentication-mode	IP Routing Volume-03-RIP	1-17
rip bfd enable	IP Routing Volume-13-BFD	1-14

rip default-route	IP Routing Volume-03-RIP	1-18
rip input	IP Routing Volume-03-RIP	1-19
rip metricin	IP Routing Volume-03-RIP	1-20
rip metricout	IP Routing Volume-03-RIP	1-21
rip mib-binding	IP Routing Volume-03-RIP	1-21
rip output	IP Routing Volume-03-RIP	1-22
rip poison-reverse	IP Routing Volume-03-RIP	1-23
rip split-horizon	IP Routing Volume-03-RIP	1-23
rip summary-address	IP Routing Volume-03-RIP	1-24
rip version	IP Routing Volume-03-RIP	1-25
ripng	IP Routing Volume-08-RIPng	1-10
ripng default-route	IP Routing Volume-08-RIPng	1-11
ripng enable	IP Routing Volume-08-RIPng	1-12
ripng metricin	IP Routing Volume-08-RIPng	1-12
ripng metricout	IP Routing Volume-08-RIPng	1-13
ripng poison-reverse	IP Routing Volume-08-RIPng	1-14
ripng split-horizon	IP Routing Volume-08-RIPng	1-14
ripng summary-address	IP Routing Volume-08-RIPng	1-15
rmdir	Security Volume-08-SSH2.0	1-25
rmdir	System Volume-04-File System Management	1-14
rmdir	System Volume-04-File System Management	2-26
rmon alarm	System Volume-07-RMON	1-10
rmon event	System Volume-07-RMON	1-12
rmon history	System Volume-07-RMON	1-13
rmon prialarm	System Volume-07-RMON	1-14
rmon statistics	System Volume-07-RMON	1-16
robust-count (IGMP view)	IP Multicast Volume-02-IGMP	1-29
robust-count (MLD view)	IP Multicast Volume-09-MLD	1-29
root-certificate fingerprint	Security Volume-09-PKI	1-24
route-distinguisher	IP Routing Volume-14-MCE	1-22

route-option bypass-route	System Volume-13-NQA	1-29
route-policy	IP Routing Volume-12-Route Policy	1-20
router id	IP Routing Volume-01-IP Routing Table Display	1-20
router-aging-time (IGMP-Snooping view)	IP Multicast Volume-06-IGMP Snooping	1-25
router-aging-time (MLD-Snooping view)	IP Multicast Volume-12-MLD Snooping	1-25
router-id	IP Routing Volume-06-BGP	1-68
router-id	IP Routing Volume-09-OSPFv3	1-40
router-id	IP Routing Volume-11-IPv6 BGP	1-52
route-tag	IP Routing Volume-04-OSPF	1-61
routing-table limit	IP Routing Volume-14-MCE	1-23
rrpp domain	Access Volume-17-RRPP	1-15
rrpp enable	Access Volume-17-RRPP	1-16
rrpp ring-group	Access Volume-17-RRPP	1-16
rule (access control policy view)	Security Volume-09-PKI	1-25
rule (advanced IPv4 ACL view)	Security Volume-12-ACL	1-12
rule (advanced IPv6 ACL view)	Security Volume-12-ACL	1-26
rule (basic IPv4 ACL view)	Security Volume-12-ACL	1-10
rule (basic IPv6 ACL view)	Security Volume-12-ACL	1-25
rule (Ethernet frame header ACL view)	Security Volume-12-ACL	1-16
rule comment (for IPv4)	Security Volume-12-ACL	1-18
rule comment (for IPv6)	Security Volume-12-ACL	1-30

## S

save	System Volume-04-File System Management	1-21
schedule job	System Volume-03-Device Management	1-26
schedule reboot at	System Volume-03-Device Management	1-27
schedule reboot delay	System Volume-03-Device Management	1-29

screen-length	System Volume-01-Login	1-16
screen-length disable	System Volume-02-Basic System Configuration	1-19
secondary accounting (HWTACACS scheme view)	Security Volume-01-AAA	3-12
secondary accounting (RADIUS scheme view)	Security Volume-01-AAA	2-18
secondary authentication (HWTACACS scheme view)	Security Volume-01-AAA	3-12
secondary authentication (RADIUS scheme view)	Security Volume-01-AAA	2-19
secondary authorization	Security Volume-01-AAA	3-13
security-policy-server	Security Volume-01-AAA	2-20
self-service-url enable	Security Volume-01-AAA	1-30
send	System Volume-01-Login	1-16
send-router-alert (IGMP view)	IP Multicast Volume-02-IGMP	1-30
send-router-alert (MLD view)	IP Multicast Volume-09-MLD	1-29
server-type	Security Volume-01-AAA	2-21
service-loopback group	Access Volume-04-Service Loopback Group	1-2
service-loopback-group	IP Services Volume-09-Tunneling	1-7
service-type	Security Volume-01-AAA	1-31
session	Security Volume-10-SSL	1-7
set authentication password	System Volume-01-Login	1-17
set-overload	IP Routing Volume-05-IS-IS	1-57
sflow agent ip	IP Services Volume-10-sFlow	1-2
sflow collector ip	IP Services Volume-10-sFlow	1-3
sflow enable	IP Services Volume-10-sFlow	1-3
sflow interval	IP Services Volume-10-sFlow	1-4
sflow sampling-mode	IP Services Volume-10-sFlow	1-5
sflow sampling-rate	IP Services Volume-10-sFlow	1-5
sftp	Security Volume-08-SSH2.0	1-26
sftp client ipv6 source	Security Volume-08-SSH2.0	1-27
sftp client source	Security Volume-08-SSH2.0	1-27
sftp ipv6	Security Volume-08-SSH2.0	1-28

sftp server enable	Security Volume-08-SSH2.0	1-15
sftp server idle-timeout	Security Volume-08-SSH2.0	1-15
sham-link	IP Routing Volume-04-OSPF	1-62
shell	System Volume-01-Login	1-18
shutdown	Access Volume-01-Ethernet Interface	1-27
shutdown	Access Volume-02-Link Aggregation	1-15
shutdown	Access Volume-09-VLAN	1-7
shutdown (MSDP View)	IP Multicast Volume-04-MSDP	1-18
shutdown-interval	System Volume-03-Device Management	1-30
silent-interface (OSPF view)	IP Routing Volume-04-OSPF	1-63
silent-interface (RIP view)	IP Routing Volume-03-RIP	1-26
silent-interface(OSPFv3 view)	IP Routing Volume-09-OSPFv3	1-40
slave auto-update config	System Volume-04-File System Management	1-23
smart-link flush enable	Access Volume-07-Smart Link	1-8
smart-link group	Access Volume-07-Smart Link	1-9
snmp-agent	System Volume-06-SNMP	1-11
snmp-agent calculate-password	System Volume-06-SNMP	1-12
snmp-agent community	System Volume-06-SNMP	1-13
snmp-agent group	System Volume-06-SNMP	1-15
snmp-agent local-engineid	System Volume-06-SNMP	1-16
snmp-agent log	System Volume-06-SNMP	1-17
snmp-agent mib-view	System Volume-06-SNMP	1-18
snmp-agent packet max-size	System Volume-06-SNMP	1-19
snmp-agent sys-info	System Volume-06-SNMP	1-19
snmp-agent target-host	System Volume-06-SNMP	1-21
snmp-agent trap enable	System Volume-06-SNMP	1-22
snmp-agent trap enable bfd	IP Routing Volume-13-BFD	1-15
snmp-agent trap enable ospf	IP Routing Volume-04-OSPF	1-64
snmp-agent trap if-mib link extended	System Volume-06-SNMP	1-24
snmp-agent trap life	System Volume-06-SNMP	1-25

snmp-agent trap queue-size	System Volume-06-SNMP	1-25
snmp-agent trap source	System Volume-06-SNMP	1-26
snmp-agent usm-user { v1   v2c }	System Volume-06-SNMP	1-27
snmp-agent usm-user v3	System Volume-06-SNMP	1-28
snmp-host	System Volume-17-Cluster Management	1-44
source	IP Services Volume-09-Tunneling	1-8
source interface	System Volume-13-NQA	1-30
source ip	System Volume-13-NQA	1-31
source port	System Volume-13-NQA	1-32
source-deny (IGMP-Snooping view)	IP Multicast Volume-06-IGMP Snooping	1-26
source-deny (MLD-Snooping view)	IP Multicast Volume-12-MLD Snooping	1-26
source-lifetime (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-43
source-lifetime (PIM view)	IP Multicast Volume-03-PIM	1-45
source-policy (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-43
source-policy (PIM view)	IP Multicast Volume-03-PIM	1-45
speed	Access Volume-01-Ethernet Interface	1-28
speed	System Volume-01-Login	1-19
spf timers	IP Routing Volume-09-OSPFv3	1-41
spf-schedule-interval	IP Routing Volume-04-OSPF	1-65
spt-switch-threshold (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-44
spt-switch-threshold (PIM view)	IP Multicast Volume-03-PIM	1-46
ssh client authentication server	Security Volume-08-SSH2.0	1-10
ssh client first-time enable	Security Volume-08-SSH2.0	1-10
ssh client ipv6 source	Security Volume-08-SSH2.0	1-11
ssh client source	Security Volume-08-SSH2.0	1-12
ssh server authentication-retries	Security Volume-08-SSH2.0	1-3
ssh server authentication-timeout	Security Volume-08-SSH2.0	1-4
ssh server compatible-ssh1x enable	Security Volume-08-SSH2.0	1-5
ssh server enable	Security Volume-08-SSH2.0	1-5

ssh server rekey-interval	Security Volume-08-SSH2.0	1-6
ssh user	Security Volume-08-SSH2.0	1-7
ssh2	Security Volume-08-SSH2.0	1-12
ssh2 ipv6	Security Volume-08-SSH2.0	1-14
ssl client-policy	Security Volume-10-SSL	1-8
ssl server-policy	Security Volume-10-SSL	1-9
ssm-mapping (IGMP view)	IP Multicast Volume-02-IGMP	1-30
ssm-mapping (MLD view)	IP Multicast Volume-09-MLD	1-30
ssm-policy (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-45
ssm-policy (PIM view)	IP Multicast Volume-03-PIM	1-47
startup bootrom-access enable	System Volume-03-Device Management	1-31
startup saved-configuration	System Volume-04-File System Management	1-23
startup-query-count (IGMP view)	IP Multicast Volume-02-IGMP	1-31
startup-query-count (MLD view)	IP Multicast Volume-09-MLD	1-31
startup-query-interval (IGMP view)	IP Multicast Volume-02-IGMP	1-32
startup-query-interval (MLD view)	IP Multicast Volume-09-MLD	1-31
state	Security Volume-01-AAA	1-32
state	Security Volume-01-AAA	2-22
state	Security Volume-09-PKI	1-25
state-refresh-hoplimit	IP Multicast Volume-10-IPv6 PIM	1-46
state-refresh-interval (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-47
state-refresh-interval (PIM view)	IP Multicast Volume-03-PIM	1-48
state-refresh-rate-limit (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-47
state-refresh-rate-limit (PIM view)	IP Multicast Volume-03-PIM	1-49
state-refresh-ttl	IP Multicast Volume-03-PIM	1-49
static-bind client-identifier	IP Services Volume-03-DHCP	1-25
static-bind ip-address	IP Services Volume-03-DHCP	1-26
static-bind mac-address	IP Services Volume-03-DHCP	1-27
static-rp (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-48
static-rp (PIM view)	IP Multicast Volume-03-PIM	1-50

static-rpf-peer	IP Multicast Volume-04-MSDP	1-18
statistics hold-time	System Volume-13-NQA	1-32
statistics interval	System Volume-13-NQA	1-34
statistics max-group	System Volume-13-NQA	1-33
step (for IPv4)	Security Volume-12-ACL	1-19
step (for IPv6)	Security Volume-12-ACL	1-31
stop-accounting-buffer enable (HWTACACS scheme view)	Security Volume-01-AAA	3-14
stop-accounting-buffer enable (RADIUS scheme view)	Security Volume-01-AAA	2-23
stopbits	System Volume-01-Login	1-20
storm-constrain	Access Volume-01-Ethernet Interface	1-29
storm-constrain control	Access Volume-01-Ethernet Interface	1-30
storm-constrain enable log	Access Volume-01-Ethernet Interface	1-31
storm-constrain enable trap	Access Volume-01-Ethernet Interface	1-32
storm-constrain interval	Access Volume-01-Ethernet Interface	1-32
stp bpdu-protection	Access Volume-16-MSTP	1-14
stp bridge-diameter	Access Volume-16-MSTP	1-15
stp compliance	Access Volume-16-MSTP	1-16
stp config-digest-snooping	Access Volume-16-MSTP	1-17
stp cost	Access Volume-16-MSTP	1-18
stp edged-port	Access Volume-16-MSTP	1-19
stp enable	Access Volume-16-MSTP	1-20
stp loop-protection	Access Volume-16-MSTP	1-21
stp max-hops	Access Volume-16-MSTP	1-21
stp mcheck	Access Volume-16-MSTP	1-22
stp mode	Access Volume-16-MSTP	1-23
stp no-agreement-check	Access Volume-16-MSTP	1-24
stp pathcost-standard	Access Volume-16-MSTP	1-24
stp point-to-point	Access Volume-16-MSTP	1-26
stp port priority	Access Volume-16-MSTP	1-27
stp port-log	Access Volume-16-MSTP	1-28

stp priority	Access Volume-16-MSTP	1-28
stp region-configuration	Access Volume-16-MSTP	1-29
stp root primary	Access Volume-16-MSTP	1-30
stp root secondary	Access Volume-16-MSTP	1-31
stp root-protection	Access Volume-16-MSTP	1-31
stp tc-protection	Access Volume-16-MSTP	1-32
stp tc-protection threshold	Access Volume-16-MSTP	1-33
stp timer forward-delay	Access Volume-16-MSTP	1-33
stp timer hello	Access Volume-16-MSTP	1-34
stp timer max-age	Access Volume-16-MSTP	1-35
stp timer-factor	Access Volume-16-MSTP	1-36
stp transmit-limit	Access Volume-16-MSTP	1-37
stub (OSPF area view)	IP Routing Volume-04-OSPF	1-66
stub (OSPFv3 area view)	IP Routing Volume-09-OSPFv3	1-42
stub-router	IP Routing Volume-04-OSPF	1-67
subvlan (IPv6 multicast VLAN view)	IP Multicast Volume-13-IPv6 Multicast VLAN	1-4
subvlan (multicast VLAN view)	IP Multicast Volume-07-Multicast VLAN	1-4
summary	IP Routing Volume-03-RIP	1-26
summary (IS-IS view)	IP Routing Volume-05-IS-IS	1-58
summary automatic	IP Routing Volume-06-BGP	1-69
summary automatic (MBGP family view)	IP Multicast Volume-05-MBGP	1-49
super	System Volume-02-Basic System Configuration	1-19
super password	System Volume-02-Basic System Configuration	1-20
synchronization (BGP view)	IP Routing Volume-06-BGP	1-70
synchronization (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-52
sysname	System Volume-01-Login	1-21
sysname	System Volume-02-Basic System Configuration	1-21

system-failure	System Volume-03-Device Management	1-32
system-view	System Volume-02-Basic System Configuration	1-22
<b>T</b>		
tcp ipv6 timer fin-timeout	IP Services Volume-08-IPv6 Basics	1-41
tcp ipv6 timer syn-timeout	IP Services Volume-08-IPv6 Basics	1-41
tcp ipv6 window	IP Services Volume-08-IPv6 Basics	1-42
tcp timer fin-timeout	IP Services Volume-05-IP Performance Optimization	1-18
tcp timer syn-timeout	IP Services Volume-05-IP Performance Optimization	1-19
tcp window	IP Services Volume-05-IP Performance Optimization	1-20
telnet	System Volume-01-Login	1-21
telnet client source	System Volume-01-Login	1-23
telnet ipv6	System Volume-01-Login	1-22
telnet server enable	System Volume-01-Login	1-24
terminal debugging	System Volume-10-Information Center	1-22
terminal logging	System Volume-10-Information Center	1-23
terminal monitor	System Volume-10-Information Center	1-24
terminal trapping	System Volume-10-Information Center	1-24
terminal type	System Volume-01-Login	1-24
tftp	System Volume-04-File System Management	3-2
tftp client source	System Volume-04-File System Management	3-4
tftp ipv6	System Volume-04-File System Management	3-5
tftp-server	System Volume-17-Cluster Management	1-44

fttp-server acl	System Volume-04-File System Management	3-1
fttp-server domain-name	IP Services Volume-03-DHCP	1-28
fttp-server ip-address	IP Services Volume-03-DHCP	1-29
timer	Access Volume-17-RRPP	1-17
timer	System Volume-17-Cluster Management	1-45
timer (BGP/BGP-VPN instance view)	IP Routing Volume-06-BGP	1-71
timer (IPv6 address family view)	IP Routing Volume-11-IPv6 BGP	1-53
timer hello (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-49
timer hello (PIM view)	IP Multicast Volume-03-PIM	1-51
timer join-prune (IPv6 PIM view)	IP Multicast Volume-10-IPv6 PIM	1-49
timer join-prune (PIM view)	IP Multicast Volume-03-PIM	1-51
timer lsp-generation	IP Routing Volume-05-IS-IS	1-59
timer lsp-max-age	IP Routing Volume-05-IS-IS	1-60
timer lsp-refresh	IP Routing Volume-05-IS-IS	1-61
timer other-querier-present (IGMP view)	IP Multicast Volume-02-IGMP	1-33
timer other-querier-present (MLD view)	IP Multicast Volume-09-MLD	1-32
timer query (IGMP view)	IP Multicast Volume-02-IGMP	1-33
timer query (MLD view)	IP Multicast Volume-09-MLD	1-33
timer quiet (HWTACACS scheme view)	Security Volume-01-AAA	3-15
timer quiet (RADIUS scheme view)	Security Volume-01-AAA	2-23
timer realtime-accounting (HWTACACS scheme view)	Security Volume-01-AAA	3-16
timer realtime-accounting (RADIUS scheme view)	Security Volume-01-AAA	2-24
timer response-timeout (HWTACACS scheme view)	Security Volume-01-AAA	3-17
timer response-timeout (RADIUS scheme view)	Security Volume-01-AAA	2-25
timer retry	IP Multicast Volume-04-MSDP	1-19
timer spf	IP Routing Volume-05-IS-IS	1-61
time-range	Security Volume-12-ACL	1-3
timers	IP Routing Volume-03-RIP	1-27
timers	IP Routing Volume-08-RIPng	1-16

topology accept	System Volume-17-Cluster Management	1-46
topology restore-from	System Volume-17-Cluster Management	1-47
topology save-to	System Volume-17-Cluster Management	1-47
tos	System Volume-13-NQA	1-34
tracert	System Volume-09-System Maintaining and Debugging	1-6
tracert ipv6	System Volume-09-System Maintaining and Debugging	1-7
track bfd echo	System Volume-12-Track	1-2
track nqa	System Volume-12-Track	1-3
traffic behavior	QoS Volume-01-QoS	1-16
traffic classifier	QoS Volume-01-QoS	1-5
transmit-pacing	IP Routing Volume-04-OSPF	1-67
ttl	System Volume-13-NQA	1-35
tunnel-protocol	IP Services Volume-09-Tunneling	1-9
type	System Volume-13-NQA	1-36

## U

udp-helper enable	IP Services Volume-06-UDP Helper	1-2
udp-helper port	IP Services Volume-06-UDP Helper	1-2
udp-helper server	IP Services Volume-06-UDP Helper	1-3
undelete	System Volume-04-File System Management	1-14
unicast-suppression	Access Volume-01-Ethernet Interface	1-33
url	System Volume-13-NQA	1-36
user	System Volume-04-File System Management	2-27
user privilege level	System Volume-01-Login	1-26
user-bind	Security Volume-07-IP Source Guard	1-4
user-group	Security Volume-01-AAA	1-32
user-interface	System Volume-01-Login	1-25

username (FTP test type view)	System Volume-13-NQA	1-37
user-name-format (HWTACACS scheme view)	Security Volume-01-AAA	3-17
user-name-format (RADIUS scheme view)	Security Volume-01-AAA	2-26
user-profile	QoS Volume-02-User Profile	1-3
user-profile enable	QoS Volume-02-User Profile	1-2

## V

validate-source-address	IP Routing Volume-03-RIP	1-28
verbose	System Volume-04-File System Management	2-28
version	IP Routing Volume-03-RIP	1-29
version	Security Volume-10-SSL	1-9
version (IGMP view)	IP Multicast Volume-02-IGMP	1-34
version (MLD view)	IP Multicast Volume-09-MLD	1-34
virtual-cable-test	Access Volume-01-Ethernet Interface	1-34
virtual-system	IP Routing Volume-05-IS-IS	1-63
vlan	Access Volume-09-VLAN	1-7
vlan precedence	Access Volume-09-VLAN	1-22
vlan-mapping modulo	Access Volume-16-MSTP	1-38
vlink-peer (OSPF area view)	IP Routing Volume-04-OSPF	1-68
vlink-peer (OSPFv3 area view)	IP Routing Volume-09-OSPFv3	1-42
voice vlan aging	Access Volume-09-VLAN	3-3
voice vlan enable	Access Volume-09-VLAN	3-4
voice vlan mac-address	Access Volume-09-VLAN	3-4
voice vlan mode auto	Access Volume-09-VLAN	3-6
voice vlan security enable	Access Volume-09-VLAN	3-6
voice-config	IP Services Volume-03-DHCP	1-29
vpn-instance (ICMP echo test type view)	System Volume-13-NQA	1-38
vpn-instance-capability simple	IP Routing Volume-14-MCE	1-24
vpn-target	IP Routing Volume-14-MCE	1-24
vrrp ipv6 method	System Volume-15-VRRP	1-18
vrrp ipv6 vrid authentication-mode	System Volume-15-VRRP	1-19

vrrp ipv6 vrid preempt-mode	System Volume-15-VRRP	1-20
vrrp ipv6 vrid priority	System Volume-15-VRRP	1-21
vrrp ipv6 vrid timer advertise	System Volume-15-VRRP	1-22
vrrp ipv6 vrid track interface	System Volume-15-VRRP	1-23
vrrp ipv6 vrid virtual-ip	System Volume-15-VRRP	1-24
vrrp method	System Volume-15-VRRP	1-6
vrrp un-check ttl	System Volume-15-VRRP	1-6
vrrp vrid authentication-mode	System Volume-15-VRRP	1-7
vrrp vrid preempt-mode	System Volume-15-VRRP	1-8
vrrp vrid priority	System Volume-15-VRRP	1-9
vrrp vrid timer advertise	System Volume-15-VRRP	1-10
vrrp vrid track	System Volume-15-VRRP	1-11
vrrp vrid track interface	System Volume-15-VRRP	1-12
vrrp vrid virtual-ip	System Volume-15-VRRP	1-13

W

X

Y

Z

# Access Volume Organization

---

## Manual Version

6W100-20090120

## Product Version

Release 2202

## Organization

The Access Volume is organized as follows:

Features	Description
Ethernet Interface	<p>This document introduces the commands for:</p> <ul style="list-style-type: none"><li>• Basic Ethernet Interface Configuration</li><li>• Combo Port Configuration</li><li>• Configuring Flow Control on an Ethernet Interface</li><li>• Configuring the Suppression Time of Physical-Link-State Change on an Ethernet Interface</li><li>• Configuring Loopback Testing on an Ethernet Interface</li><li>• Configuring a Port Group</li><li>• Configuring Storm Suppression</li><li>• Setting the Interval for Collecting Ethernet Interface Statistics</li><li>• Enabling Forwarding of Jumbo Frames</li><li>• Enabling Loopback Detection on an Ethernet Interface</li><li>• Configuring the MDI Mode for an Ethernet Interface</li><li>• Testing the Cable on an Ethernet Interface</li><li>• Configuring the Storm Constrain Function on an Ethernet Interface</li></ul>
Link aggregation	<p>Link aggregation aggregates multiple physical Ethernet ports into one logical link. This document introduces the commands for:</p> <ul style="list-style-type: none"><li>• Configuring a Static Aggregation Group</li><li>• Configuring a Dynamic Aggregation Group</li><li>• Configuring an Aggregate Interface</li><li>• Configuring a Load Sharing Mode for Load-Sharing Link Aggregation Groups</li></ul>
Port Isolation	<p>The port isolation feature allows you to isolate different ports within the same VLAN. This document introduces the commands for configuring the Isolation Group</p>
Service Loopback Group	<p>To increase service redirecting throughput, you can bundle multiple service loopback ports into a logical link, called a service loopback group. This document introduces the commands for configuring a Service Loopback Group</p>

Features	Description
DLDP	<p>In the use of fibers, link errors, namely unidirectional links, are likely to occur. DLDP is designed to detect such errors. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• Enabling DLDP</li> <li>• Setting DLDP Mode</li> <li>• Setting the Interval for Sending Advertisement Packets</li> <li>• Setting the DelayDown Timer</li> <li>• Setting the Port Shutdown Mode</li> <li>• Configuring DLDP Authentication</li> <li>• Resetting DLDP State</li> </ul>
LLDP	<p>LLDP enables a device to maintain and manage its own and its immediate neighbor's device information, based on which the network management system detects and determines the conditions of the communications links. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• Performing Basic LLDP Configuration</li> <li>• Configuring the Encapsulation Format for LLDPDUs</li> <li>• Configuring the Encapsulation Format of the Management Address</li> <li>• Configuring CDP Compatibility</li> <li>• Configuring LLDP Trapping</li> </ul>
Smart Link	<p>Smart Link is a solution for active-standby link redundancy backup and rapid transition in dual-uplink networking. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• Configuring a Smart Link Device</li> <li>• Configuring an Associated Device</li> </ul>
Monitor Link	<p>Monitor link is a port collaboration function used to enable a device to be aware of the up/down state change of the ports on an indirectly connected link. This document introduces the commands for configuring Monitor Link</p>
VLAN	<p>Using the VLAN technology, you can partition a LAN into multiple logical LANs. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• Types of VLAN</li> <li>• Isolate-user-vlan configuration</li> <li>• Configuration of Voice VLAN</li> </ul>
GVRP	<p>GVRP is a GARP application. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• GVRP configuration</li> <li>• GARP Timers configuration</li> </ul>
QinQ	<p>As defined in IEEE802.1Q, 12 bits are used to identify a VLAN ID, so a device can support a maximum of 4094 VLANs. The QinQ feature extends the VLAN space by allowing Ethernet frames to travel across the service provider network with double VLAN tags. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• Configuring basic QinQ</li> <li>• Configuring Selective QinQ</li> <li>• Configuring the TPID Value in VLAN Tags</li> </ul>

Features	Description
BPDU Tunnel	<p>BPDU tunneling enables transparently transmission of customer network BPDU frames over the service provider network. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• Configuring BPDU Transparent Transmission</li> <li>• Configuring Destination Multicast MAC Address for BPDU Tunnel Frames</li> </ul>
VLAN Mapping	<p>The VLAN mapping feature maps CVLAN tags to SVLAN tags. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• Configuring One-to-One VLAN Mapping</li> <li>• Configuring Many-to-One VLAN Mapping</li> <li>• Configuring Two-to-Two VLAN Mapping</li> </ul>
Ethernet OAM	<p>Ethernet OAM is a tool monitoring Layer-2 link status. It helps network administrators manage their networks effectively. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• Configuring Basic Ethernet OAM Functions</li> <li>• Configuring Link Monitoring</li> <li>• Enabling OAM Loopback Testing</li> </ul>
Connectivity Fault Detection	<p>Connectivity fault detection is an end-to-end, per-VLAN link-layer OAM mechanism for link connectivity detection, fault verification, and fault location. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• Configuring CC on MEPs</li> <li>• Configuring LB on MEPs</li> <li>• Configuring LT on MEPs</li> </ul>
MSTP	<p>MSTP is used to eliminate loops in a LAN. It is compatible with STP and RSTP. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• Configuring the Root Bridge</li> <li>• Configuring Leaf Nodes</li> <li>• Performing mCheck</li> <li>• Configuring Digest Snooping</li> <li>• Configuring No Agreement Check</li> <li>• Configuring Protection Functions</li> </ul>
RRPP	<p>RRPP is a link layer protocol designed for Ethernet rings. RRPP can prevent broadcast storms caused by data loops when an Ethernet ring is healthy, and rapidly restore the communication paths between the nodes after a link is disconnected on the ring. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• Configuring Master Node</li> <li>• Configuring Transit Node</li> <li>• Configuring Edge Node</li> <li>• Configuring Assistant Edge Node</li> <li>• Configuring Ring Group</li> </ul>
Port Mirroring	<p>Port mirroring copies packets passing through a port to another port connected with a monitoring device for packet analysis to help implement network monitoring and troubleshooting. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• Local port mirroring configuration</li> <li>• Remote port mirroring configuration</li> </ul>

# Table of Contents

<b>1 Ethernet Interface Configuration Commands</b>	<b>1-1</b>
General Ethernet Interface Configuration Commands	1-1
broadcast-suppression	1-1
description	1-2
display brief interface	1-3
display interface	1-6
display loopback-detection	1-8
display packet-drop interface	1-9
display packet-drop summary	1-10
display port combo	1-11
display port-group manual	1-12
display storm-constrain	1-13
duplex	1-14
flow-control	1-15
flow-interval	1-16
group-member	1-16
interface	1-17
jumboframe enable	1-17
link-delay	1-18
loopback	1-19
loopback-detection control enable	1-20
loopback-detection enable	1-21
loopback-detection interval-time	1-22
loopback-detection per-vlan enable	1-22
mdi	1-23
multicast-suppression	1-24
port-group manual	1-25
reset counters interface	1-26
reset packet-drop interface	1-26
shutdown	1-27
speed	1-28
storm-constrain	1-29
storm-constrain control	1-30
storm-constrain enable log	1-31
storm-constrain enable trap	1-32
storm-constrain interval	1-32
unicast-suppression	1-33
virtual-cable-test	1-34

# 1 Ethernet Interface Configuration Commands

---

## General Ethernet Interface Configuration Commands

### **broadcast-suppression**

#### **Syntax**

**broadcast-suppression** { *ratio* | **pps** *max-pps* }

**undo broadcast-suppression**

#### **View**

Ethernet interface view, port group view

#### **Default Level**

2: System level

#### **Parameters**

*ratio*: Maximum percentage of broadcast traffic to the total transmission capability of an Ethernet interface. The smaller the ratio, the less broadcast traffic is allowed to pass through the interface. this argument ranges from 1 to 100.

**pps** *max-pps*: Specifies the maximum number of broadcast packets that can be forwarded on an Ethernet interface per second (in pps, representing packets per second).

- For a Gigabit port, the value range is 1 to 1488100.
- For a 10-Gigabit port, the value range is 1 to 1488100.

Note that:

- When a suppression granularity larger than 1 is specified on the device, the value of the **pps** keyword should be no smaller than and an integral multiple of the granularity. The broadcast suppression threshold value configured through this keyword on an Ethernet interface may not be the one that actually takes effect. To display the actual broadcast suppression threshold value on an Ethernet interface, you can use the **display interface** command.
- When no suppression granularity is specified or the suppression granularity is set to 1, the value of the **pps** keyword should be no smaller than 1, and the broadcast suppression threshold value is the one that actually takes effect on the Ethernet interface.

#### **Description**

Use the **broadcast-suppression** command to set a broadcast traffic threshold on one or multiple Ethernet ports.

Use the **undo broadcast-suppression** command to restore the default.

By default, all broadcast traffic is allowed to pass through an Ethernet interface, that is, broadcast traffic is not suppressed.

If you execute this command in Ethernet interface view, the configuration takes effect only on the current interface. If you execute this command in port-group view, the configuration takes effect on all the ports in the port group.

When broadcast traffic exceeds the broadcast traffic threshold, the system begins to discard broadcast packets until the broadcast traffic drops below the threshold to ensure operation of network services.



#### Note

- If you set different suppression ratios in Ethernet interface view or port-group view for multiple times, the latest configuration takes effect.
  - Do not use the **broadcast-suppression** command along with the **storm-constrain** command. Otherwise, the broadcast storm suppression ratio configured may get invalid.
- 

## Examples

# For Ethernet interface GigabitEthernet 1/0/1, allow broadcast traffic equivalent to 20% of the total transmission capability of GigabitEthernet 1/0/1 to pass.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] broadcast-suppression 20
```

# For all the ports of the manual port group named **group1**, allow broadcast traffic equivalent to 20% of the total transmission capability of each port to pass and suppress excessive broadcast packets.

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group manual group1] group-member GigabitEthernet 1/0/2
[Sysname-port-group manual group1] group-member GigabitEthernet 1/0/3
[Sysname-port-group manual group1] broadcast-suppression 20
```

## description

### Syntax

**description** *text*

**undo description**

### View

Ethernet interface view

### Default Level

2: System level

### Parameters

*text*: Description of an Ethernet interface, a string of 1 to 80 characters. Currently, the device supports the following types of characters or symbols: standard English characters (numbers and case-sensitive

letters), special English characters, spaces, and other characters or symbols that conform to the Unicode standard.

---



- A port description can be the mixture of English characters and other Unicode characters. The mixed description cannot exceed the specified length.
  - To use a type of Unicode characters or symbols in a port description, you need to install the corresponding Input Method Editor (IME) and log in to the device through remote login software that supports this character type.
  - Each Unicode character or symbol (non-English characters) takes the space of two regular characters. When the length of a description string reaches or exceeds the maximum line width on the terminal software, the software starts a new line, possibly breaking a Unicode character into two. As a result, garbled characters may be displayed at the end of a line.
- 

## Description

Use the **description** command to set the description string of the current interface.

Use the **undo description** command to restore the default.

By default, the description of an interface is the interface name followed by the “interface” string, **GigabitEthernet1/0/1 Interface** for example.

Related commands: **display interface**.

## Examples

# Configure the description string of interface GigabitEthernet 1/0/1 as **lanswitch-interface**.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] description lanswitch-interface
```

## display brief interface

### Syntax

```
display brief interface [ interface-type [ interface-number ] ] [ | { begin | exclude | include } regular-expression ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*interface-type*: Type of a specified interface.

*interface-number*: Number of a specified interface.

|: Uses a regular expression to filter output information. For detailed description on regular expression, refer to *Basic System Configuration* in the *System Volume*.

**begin**: Displays the line that matches the regular expression and all the subsequent lines.

**exclude**: Displays the lines that do not match the regular expression.

**include**: Displays the lines that match the regular expression.

*regular-expression*: Regular expression, a string of 1 to 256 characters. Note that this argument is case-sensitive.

## Description

Use the **display brief interface** command to display brief interface information.

- If neither interface type nor interface number is specified, all interface information will be displayed.
- If only interface type is specified, then only information of this particular type of interface will be displayed.
- If both interface type and interface number are specified, then only information of the specified interface will be displayed.

Related commands: **interface**.

## Examples

# Display the brief information of interfaces.

```
<Sysname> display brief interface
```

The brief information of interface(s) under route mode:

Interface	Link	Protocol-link	Protocol type	Main IP
Loop1	UP	UP(spoofing)	LOOP	2.2.2.1
NULL0	UP	UP(spoofing)	NULL	--
Vlan1	UP	UP	ETHERNET	192.168.0.153
Vlan10	DOWN	DOWN	ETHERNET	1.1.1.1
Vlan100	ADM DOWN	DOWN	ETHERNET	--

The brief information of interface(s) under bridge mode:

Interface	Link	Speed	Duplex	Link-type	PVID
BAGG1	DOWN	auto	auto	access	1
GE1/0/1	DOWN	auto	auto	access	1
GE1/0/2	DOWN	auto	auto	access	1
GE1/0/3	DOWN	auto	auto	access	1
GE1/0/4	UP	1G(a)	full(a)	access	1
GE1/0/5	DOWN	auto	auto	access	1
GE1/0/6	DOWN	auto	auto	access	1
GE1/0/7	DOWN	auto	auto	access	1
GE1/0/8	DOWN	auto	auto	access	1
GE1/0/9	DOWN	auto	auto	access	1
GE1/0/10	DOWN	auto	auto	access	1
GE1/0/11	DOWN	auto	auto	trunk	1
GE1/0/12	DOWN	auto	auto	trunk	1

# Display the information of interfaces beginning with the string "spoo".

```
<Sysname> display brief interface | begin spoo
```

The brief information of interface(s) under route mode:

Interface	Link	Protocol-link	Protocol type	Main IP
Loop0	UP	UP(spoofing)	LOOP	5.5.5.5
NULL0	UP	UP(spoofing)	NULL	--
Vlan999	UP	UP	ETHERNET	10.1.1.1

# Display the brief information of all UP interfaces.

<Sysname> display brief interface | include UP

The brief information of interface(s) under route mode:

Interface	Link	Protocol-link	Protocol type	Main IP
Loop0	UP	UP(spoofing)	LOOP	5.5.5.5
NULL0	UP	UP(spoofing)	NULL	--
Vlan999	UP	UP	ETHERNET	10.1.1.1

The brief information of interface(s) under bridge mode:

Interface	Link	Speed	Duplex	Link-type	PVID
GE1/0/7	UP	100M(a)	full(a)	trunk	303
GE1/0/9	UP	100M(a)	full(a)	access	999

# Display the brief information of all interfaces excluding Ethernet interfaces.

<Sysname> display brief interface | exclude GE

The brief information of interface(s) under route mode:

Interface	Link	Protocol-link	Protocol type	Main IP
Loop1	UP	UP(spoofing)	LOOP	2.2.2.1
NULL0	UP	UP(spoofing)	NULL	--
Vlan1	UP	UP	ETHERNET	192.168.0.153
Vlan10	DOWN	DOWN	ETHERNET	1.1.1.1
Vlan100	ADM DOWN	DOWN	ETHERNET	--

The brief information of interface(s) under bridge mode:

Interface	Link	Speed	Duplex	Link-type	PVID
BAGG1	DOWN	auto	auto	access	1

**Table 1-1 display brief interface command output description**

Field	Description
The brief information of interface(s) under route mode:	Brief information of interface(s) in route mode
Interface	Abbreviated interface name
Link	Interface physical link state, which can be up or down
Protocol-link	Interface protocol link state, which can be up or down
Protocol type	Interface protocol type
Main IP	Main IP
The brief information of interface(s) under bridge mode:	Brief information of interface(s) in bridge mode
Speed	Interface rate, in bps

Field	Description
Duplex	Duplex mode, which can be half (half duplex), full (full duplex), or auto (auto-negotiation).
PVID	Default VLAN ID

## display interface

### Syntax

**display interface** [ *interface-type* [ *interface-number* ] ]

### View

Any view

### Default Level

1: Monitor level

### Parameters

*interface-type*: Type of a specified interface.

*interface-number*: Number of a specified interface.

### Description

Use the **display interface** command to display the current state of a specified interface and related information.

- If neither interface type nor interface number is specified, all interface information will be displayed.
- If only interface type is specified, then only information of this particular type of interface will be displayed.
- If both interface type and interface number are specified, then only information of the specified interface will be displayed.

Related commands: **interface**.

### Examples

# Display the current state of interface GigabitEthernet 1/0/1 and related information.

```
<Sysname> display interface GigabitEthernet 1/0/1
GigabitEthernet1/0/1 current state: DOWN
  IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-e200-8048
  Description: GigabitEthernet1/0/1 Interface
  Loopback is not set
  Media type is twisted pair, port hardware type is 100_BASE_TX
  Unknown-speed mode, unknown-duplex mode
  Link speed type is autonegotiation, link duplex type is autonegotiation
  Flow-control is not enabled
  The Maximum Frame Length is 9022
  Broadcast MAX-ratio: 100%
  Unicast MAX-ratio: 100%
  Multicast MAX-ratio: 100%
```

```

Allow jumbo frame to pass
PVID: 100
Mdi type: auto
Port link-type: access
  Tagged VLAN ID : none
  Untagged VLAN ID : 100
Port priority: 0
Peak value of input: 96132560 bytes/sec, at 2007-10-26 07:05:06
Peak value of output: 0 bytes/sec, at 2000-04-26 12:00:12
Last 300 seconds input: 6 packets/sec 678 bytes/sec 20%
Last 300 seconds output: 1 packets/sec 179 bytes/sec 17%
Input (total): 61745144 packets, 12152212250 bytes
  - unicasts, 47519150 broadcasts, 12121681 multicasts
Input (normal): 61745144 packets, - bytes
  205227373 unicasts, 47519150 broadcasts, 12121681 multicasts
Input: 0 input errors, 0 runts, 0 giants, 0 throttles
  0 CRC, 0 frame, - overruns, 0 aborts
  - ignored, - parity errors
Output (total): 1395522 packets, 183608303 bytes
  - unicasts, 13 broadcasts, 1273860 multicasts, 0 pauses
Output (normal): 1395522 packets, - bytes
  0 unicasts, 13 broadcasts, 1273860 multicasts, 0 pauses
Output: 0 output errors, - underruns, 1 buffer failures
  0 aborts, 0 deferred, 0 collisions, 0 late collisions
  0 lost carrier, - no carrier

```

**Table 1-2 display interface command output description**

Field	Description
GigabitEthernet1/0/1 current state	Current physical link state of the Ethernet interface
IP Packet Frame Type	Frame type of the Ethernet interface
Hardware address	Hardware address
Description	Description of the interface
Loopback is not set	Loopback is not configured.
Unknown-speed mode	Unknown-speed mode, in which mode speed is negotiated between the current host and the peer.
unknown-duplex mode	Unknown-duplex mode, in which mode speed is negotiated between the current host and the peer.
Link speed type is autonegotiation	Link speed type is autonegotiation.
link duplex type is autonegotiation	Link duplex type is autonegotiation.
Flow-control is not enabled	Flow-control is not enabled.
The Maximum Frame Length	The maximum frame length allowed on an interface
Broadcast-suppression ratio (%)	Broadcast storm suppression ratio (the maximum ratio of allowed number of broadcast packets to overall traffic through an interface)

Field	Description
Unicast MAX-ratio	Unicast storm suppression ratio (the maximum ratio of allowed number of unknown unicast packets to overall traffic over an interface)
Multicast MAX-ratio	Multicast storm suppression ratio (the maximum ratio of allowed number of multicast packets to overall traffic through an interface)
Allow jumbo frame to pass	Allow jumbo frame to pass through
PVID	Default VLAN ID
Mdi type	Cable type
Port link-type	Interface link type, which could be access, trunk, and hybrid.
Tagged VLAN ID	VLANs whose packets are sent through the port with VLAN tag kept
Untagged VLAN ID	VLANs whose packets are sent through the port with VLAN tag stripped off
Peak value of input	Peak value of inbound traffic, in bytes/sec.
Peak time of input	Time of peak inbound traffic
Peak value of output	Peak value of outbound traffic, in bytes/sec.
Peak time of output	Time of peak outbound traffic
Last 300 seconds input:	Average input rate over the last 300 seconds, among which: <ul style="list-style-type: none"> <li>• <b>packets/sec</b> indicates the average input rate in terms of the average number of the packets received per second.</li> <li>• <b>bytes/sec</b> indicates the average input rate in terms of the average number of bytes received per second.</li> <li>• <b>x%</b> indicates the percentage of the average input rate to the total bandwidth, where - indicates that the rate is greater than the maximum value that can be displayed.</li> </ul>
Last 300 seconds output:	Average output rate over the last 300 seconds, among which: <ul style="list-style-type: none"> <li>• <b>packets/sec</b> indicates the average output rate in terms of the average number of the packets output per second.</li> <li>• <b>bytes/sec</b> indicates the average output rate in terms of the average number of bytes output per second.</li> <li>• <b>x%</b> indicates the percentage of the average output rate to the total bandwidth, where "-" indicates that the rate is greater than the maximum value that can be displayed.</li> </ul>
Input (total): Input (normal): Input: Output (total): Output (normal): Output:	Error statistics on the interface inbound and outbound packets, where "-" indicates that the corresponding entry is not supported.

## display loopback-detection

### Syntax

display loopback-detection

## View

Any view

## Default Level

1: Monitor level

## Parameters

None

## Description

Use the **display loopback-detection** command to display loopback detection information on a port.

If loopback detection is already enabled, this command will also display the detection interval and information on the ports currently detected with a loopback.

## Examples

# Display loopback detection information on a port.

```
<Sysname> display loopback-detection
Loopback-detection is running
Detection interval time is 30 seconds
No port is detected with loopback
```

**Table 1-3** display loopback-detection command output description

Field	Description
Loopback-detection is running	Loopback-detection is running.
Detection interval time is 30 seconds	Detection interval is 30 seconds.
No port is detected with loopback	No port is currently being detected with a loopback.

## display packet-drop interface

### Syntax

```
display packet-drop interface [ interface-type [ interface-number ] ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*interface-type*: Type of a specified interface.

*interface-number*: Number of a specified interface.

## Description

Use the **display packet-drop interface** command to display information about dropped packets on an interface or multiple interfaces.

- If you do not specify an interface type or interface number, this command displays information about dropped packets on all the interfaces on the device.
- If you specify an interface type only, this command displays information about dropped packets on the specified type of interfaces.
- If you specify both the interface type and interface number, this command displays information about dropped packets on the specified interface.

## Examples

# Display information about dropped packets on GigabitEthernet 1/0/1.

```
<Sysname> display packet-drop interface GigabitEthernet 1/0/1
GigabitEthernet1/0/1:
Packets dropped by GBP full or insufficient bandwidth: 301
Packets dropped by FFP: 261
Packets dropped by STP non-forwarding state: 321
Packets dropped by Rate-limit: 143
Packets dropped by broadcast-suppression: 301
Packets dropped by unicast-suppression: 215
Packets dropped by multicast-suppression: 241
Packets dropped by transmit egress aging: 246
```

## display packet-drop summary

### Syntax

```
display packet-drop summary
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display packet-drop summary** command to display information about dropped packets on all interfaces.

## Examples

# Display information about dropped packets on all interfaces.

```
<Sysname> display packet-drop summary
All interfaces:
Packets dropped by GBP full or insufficient bandwidth: 301
```

Packets dropped by FFP: 261  
Packets dropped by STP non-forwarding state: 321  
Packets dropped by Rate-limit: 143  
Packets dropped by broadcast-suppression: 301  
Packets dropped by unicast-suppression: 215  
Packets dropped by multicast-suppression: 241  
Packets dropped by transmit egress aging: 246

### display packet-drop summary command output description

Field	Description
Packets dropped by GBP full or insufficient bandwidth	Packets that are dropped because the buffer is used up or the bandwidth is insufficient
Packets dropped by FFP	Packets that are filtered out
Packets dropped by STP non-forwarding state	Packets that are dropped because STP is in the non-forwarding state
Packets dropped by Rate-limit	Packets that are dropped due to the rate limit set on the device
Packets dropped by broadcast-suppression	Packets that are dropped due to broadcast suppression configured on interfaces
Packets dropped by unicast-suppression	Packets that are dropped due to unicast suppression configured on interfaces
Packets dropped by multicast-suppression	Packets that are dropped due to multicast suppression configured on interfaces
Packets dropped by transmit egress aging	Outbound packets that are timed out

## display port combo

### Syntax

```
display port combo
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display port combo** command to display the Combo ports of a device and the corresponding optical ports and electrical ports.

### Examples

```
# Display the Combo ports of the device and the corresponding optical ports and electrical ports.
```

```
<Sysname> display port combo
```

Combo-group	Active	Inactive
1	GigabitEthernet1/0/25	GigabitEthernet1/0/22
2	GigabitEthernet1/0/26	GigabitEthernet1/0/24
3	GigabitEthernet1/0/27	GigabitEthernet1/0/21
4	GigabitEthernet1/0/28	GigabitEthernet1/0/23

**Table 1-4 display port combo** command output description

Field	Description
Combo-group	Combo ports of the device, represented by Combo port number, which is generated by the system.
Active	Ports of the Combo ports that are active
Inactive	Ports of the Combo ports that are inactive

As for the optical port and the electrical port of a Combo port, the one with the smaller port number is active by default. You can determine whether a port is an optical port or an electrical port by checking the “Media type is” field of the **display interface** command.

## display port-group manual

### Syntax

```
display port-group manual [ all | name port-group-name ]
```

### View

Any view

### Default Level

2: System level

### Parameters

**all**: Specifies all the manual port groups.

**name *port-group-name***: Specifies the name of a manual port group, a string of 1 to 32 characters.

### Description

Use the **display port-group manual** command to display the information about a manual port group or all the manual port groups.

- If you provide the *port-group-name* argument, this command displays the details for a specified manual port group, including its name and the Ethernet interface ports included.
- If you provide the **all** keyword, this command displays the details for all manual port groups, including their names and the Ethernet interface ports included.
- Absence of parameters indicates that the names of all the port groups will be displayed.

### Examples

# Display the names of all the port groups.

```
<Sysname> display port-group manual
```

The following manual port group exist(s):

```
group1                                group2
```

# Display details of all the manual port groups.

```
<Sysname> display port-group manual all
```

Member of group1:

```
GigabitEthernet1/0/3      GigabitEthernet1/0/4      GigabitEthernet1/0/5
GigabitEthernet1/0/6      GigabitEthernet1/0/7      GigabitEthernet1/0/8
```

Member of group2:

None

**Table 1-5 display port-group manual command output description**

Field	Description
Member of group	Member of the manual port group

## display storm-constrain

### Syntax

```
display storm-constrain [ broadcast | multicast ] [ interface interface-type interface-number ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**broadcast:** Displays the information about storm constrain for broadcast packets.

**multicast:** Displays the information about storm constrain for multicast packets.

**interface *interface-type interface-number*:** Specifies an interface by its type and number.

### Description

Use the **display storm-constrain** command to display the information about storm constrain.

If you provide no argument or keyword, this command displays the information about storm constrain for all types of packets on all the interfaces.

### Examples

# Display the information about storm constrain for all types of packets on all the interfaces.

```
<Sysname> display storm-constrain
```

Abbreviation: BC - broadcast; MC - multicast; UC - unicast

Flow Statistic Interval: 10(second)

```
PortName      Type LowerLimit UpperLimit CtrMode  Status  Trap  Log  SwiNum Unit
-----
GE1/0/2       BC    1           2         N/A     normal  on   on   0     kbps
GE1/0/2       MC    1           5         N/A     normal  on   on   0     ratio
```

**Table 1-6 display storm-constrain** command output description

Field	Description
Flow Statistic Interval	Interval for generating storm constrain statistics
PortName	Abbreviated port name
Type	Type of the packets for which storm constrain function is enabled, which can be broadcast (for broadcast packets), and multicast (for multicast packets).
LowerLimit	Lower threshold (in pps, Kbps or percentage)
UpperLimit	Upper threshold (in pps, Kbps or percentage)
CtrMode	Action to be taken when the upper threshold is reached, which can be block, shutdown, and N/A.
Status	Interface state, which can be normal (indicating the interface operates properly), control (indicating the interface is blocked or shut down).
Trap	State of trap messages sending. "on" indicates trap message sending is enabled; "off" indicates trap message sending is disabled.
Log	State of log sending. "on" indicates log sending is enabled; "off" indicates log sending is disabled.
SwiNum	Number of the forwarding state switching. This field is numbered modulo 65,535.

## duplex

### Syntax

```
duplex { auto | full | half }  
undo duplex
```

### View

Ethernet interface view

### Default Level

2: System level

### Parameters

**auto**: Indicates that the interface is in auto-negotiation state.

**full**: Indicates that the interface is in full-duplex state.

**half**: Indicates that the interface is in half-duplex state. The optical interface of a Combo port does not support the **half** keyword.

### Description

Use the **duplex** command to configure the duplex mode for an Ethernet interface.

Use the **undo duplex** command to restore the duplex mode for an Ethernet interface to the default.

By default, the duplex mode for an Ethernet interface is **auto**.

Related commands: **speed**.

---



10-Gigabit Ethernet ports do not support this command.

---

## Examples

# Configure the interface GigabitEthernet 1/0/1 to work in full-duplex mode.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] duplex full
```

## flow-control

### Syntax

**flow-control**

**undo flow-control**

### View

Ethernet interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **flow-control** command to enable flow control on an Ethernet interface.

Use the **undo flow-control** command to disable flow control on an Ethernet interface.

By default, flow control on an Ethernet interface is disabled.



The flow control function takes effect on the local Ethernet interface only when it is enabled on both the local and peer devices.

---

## Examples

# Enable flow control on interface GigabitEthernet1/0/1.

```
<Sysname> system-view
```

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] flow-control
```

## flow-interval

### Syntax

**flow-interval** *interval*

**undo flow-interval**

### View

Ethernet interface view

### Default Level

2: System level

### Parameters

*interval*: Interval at which the interface collects statistics. It ranges from 5 to 300 seconds and must be a multiple of 5. The default value is 300 seconds.

### Description

Use the **flow-interval** command to configure the time interval for collecting interface statistics.

Use the **undo flow-interval** command to restore the default interval.

### Examples

# Set the time interval for collecting interface statistics to 100 seconds.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] flow-interval 100
```

## group-member

### Syntax

**group-member** *interface-list*

**undo group-member** *interface-list*

### View

Port group view

### Default Level

2: System level

### Parameters

*interface-list*: Ethernet interface list, in the form of *interface-type interface-number* [ **to** *interface-type interface-number* ] &<1-10>, where &<1-10> indicates that you can specify up to 10 port or port ranges.

## Description

Use the **group-member** command to assign an Ethernet interface or a list of Ethernet interfaces to the manual port group.

Use the **undo group-member** command to remove an Ethernet interface or a list of Ethernet interfaces from the manual port group.

By default, there is no Ethernet interface in a manual port group.

## Examples

```
# Add interface GigabitEthernet 1/0/1 to the manual port group named group1.
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group-manual-group1] group-member GigabitEthernet 1/0/1
```

## interface

### Syntax

```
interface interface-type interface-number
```

### View

System view

### Default Level

2: System level

### Parameters

*interface-type interface-number*: Interface type and interface number.

## Description

Use the **interface** command to enter interface view.

## Examples

```
# Enter GigabitEthernet 1/0/1 interface view
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1]
```

## jumboframe enable

### Syntax

```
jumboframe enable
```

```
undo jumboframe enable
```

### View

Ethernet interface view, port group view

## Default Level

2: System level

## Parameters

.None

## Description

Use the **jumboframe enable** command to allow jumbo frames with the specified length to pass through an Ethernet interface.

Use the **undo jumboframe enable** command to prevent jumbo frames from passing through an Ethernet interface.

By default, the device allows frames no larger than 9216 bytes to pass through an Ethernet interface.

You can configure length of jumbo frames on a port (in Ethernet interface view, port-group view) to allow them to pass through Ethernet interfaces.

- Execution of this command under Ethernet interface view will only apply the configurations to the current Ethernet interface.
- Execution of this command under port group view will apply the configurations to the Ethernet interface(s) in the port group.

## Examples

# Enable jumbo frames to pass through all the Ethernet interfaces in the manual port group named **group1**.

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group manual group1] group-member GigabitEthernet 1/0/1
[Sysname-port-group manual group1] jumboframe enable
```

# Enable jumbo frames to pass through GigabitEthernet1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] jumboframe enable
```

## link-delay

### Syntax

**link-delay** *delay-time*

**undo link-delay**

### View

Ethernet interface view

## Default Level

2: System level

## Parameters

*delay-time*: Up/down suppression time for the physical connection of an Ethernet interface (in seconds).

in the range 2 to 10.

## Description

Use the **link-delay** command to configure the suppression time of physical-link-state changes on an Ethernet Interface.

Use the **undo link-delay** command to restore the default suppression time.

By default, the physical-link-state change suppression time is not configured.

## Examples

# Set the up/down suppression time of the physical connection of an Ethernet interface to 8 seconds.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] link-delay 8
```

## loopback

### Syntax

**loopback** { **external** | **internal** }

**undo loopback**

### View

Ethernet interface view

### Default Level

2: System level

### Parameters

**external**: Enables external loopback testing on an Ethernet interface.

**internal**: Enables internal loopback testing on an Ethernet interface.

## Description

Use the **loopback** command to enable Ethernet interface loopback testing.

Use the **undo loopback** command to disable Ethernet interface loopback testing.

By default, Ethernet interface loopback testing is disabled.



### Note

- Ethernet interface loopback testing should be enabled while testing certain functionalities, such as during the initial identification of any network failure.
  - While enabled, Ethernet interface loopback testing will work in full-duplex mode. The interface will return to its original state upon completion of the loopback testing.
-

## Examples

```
# Enable loopback testing on GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] loopback internal
```

## loopback-detection control enable

### Syntax

```
loopback-detection control enable
undo loopback-detection control enable
```

### View

Ethernet interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **loopback-detection control enable** command to enable loopback detection for a Trunk port or Hybrid port.

Use the **undo loopback-detection control enable** command to restore the default.

By default, loopback detection for a Trunk port or Hybrid port is disabled.

- When the loopback detection is enabled, if a port has been detected with loopback, it will be shut down. A Trap message will be sent to the terminal and the corresponding MAC address forwarding entries will be deleted.
- When the loopback detection is disabled, if a port has been detected with loopback, a Trap message will be sent to the terminal. The port is still working properly.

Note that this command is inapplicable to an Access port as its loopback detection is enabled by default.

## Examples

```
# Enable loopback detection for the trunk port GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] loopback-detection enable
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] loopback-detection enable
[Sysname-GigabitEthernet1/0/1] loopback-detection control enable
```

## loopback-detection enable

### Syntax

```
loopback-detection enable
undo loopback-detection enable
```

### View

System view, Ethernet interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **loopback-detection enable** command to enable loopback detection globally or on a specified port.

Use the **undo loopback-detection enable** command to disable loopback detection globally or on a specified port.

By default, loopback detection is disabled for an Access, Trunk, or Hybrid port.

- If an Access port has been detected with loopback, it will be shut down. A Trap message will be sent to the terminal and the corresponding MAC address.
- If a Trunk port or Hybrid port has been detected with loopback, a Trunk message will be sent to the terminal. They will be shut down if the loopback testing function is enabled on them. In addition, a Trap message will be sent to the terminal and the corresponding MAC address forwarding entries will be deleted.

Related commands: **loopback-detection control enable**.



### Caution

- Loopback detection on a given port is enabled only after the **loopback-detection enable** command has been configured in both system view and interface view of the port.
  - Loopback detection on all ports will be disabled after the configuration of the **undo loopback-detection enable** command in system view.
- 

### Examples

```
# Enable loopback detection on the interface GigabitEthernet 1/0/1.
```

```
<Sysname> system-view
[Sysname] loopback-detection enable
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] loopback-detection enable
```

## loopback-detection interval-time

### Syntax

```
loopback-detection interval-time time  
undo loopback-detection interval-time
```

### View

System view

### Default Level

2: System level

### Parameters

*time*: Time interval for performing port loopback detection, in the range 5 to 300 (in seconds).

### Description

Use the **loopback-detection interval-time** command to configure time interval for performing port loopback detection.

Use the **undo loopback-detection interval-time** command to restore the default time interval for port loopback detection, which is 30 seconds.

Related commands: **display loopback-detection**.

### Examples

```
# Set the time interval for performing port loopback detection to 10 seconds.
```

```
<Sysname> system-view  
[Sysname] loopback-detection interval-time 10
```

## loopback-detection per-vlan enable

### Syntax

```
loopback-detection per-vlan enable  
undo loopback-detection per-vlan enable
```

### View

Ethernet interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **loopback-detection per-vlan enable** command to enable loopback detection in all VLANs with Trunk ports or Hybrid ports.

Use the **undo loopback-detection per-vlan enable** command to enable loopback detection in the default VLAN with Trunk ports or Hybrid ports.

By default, loopback detection is only enabled in the default VLAN(s) with Trunk ports or Hybrid ports.

Note that the **loopback-detection per-vlan enable** command is not applicable to Access ports.

## Examples

# Enable loopback detection in all the VLANs to which the Hybrid port GigabitEthernet 1/1 belongs.

```
<Sysname> system-view
[Sysname] loopback-detection enable
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] loopback-detection enable
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] loopback-detection per-vlan enable
```

## mdi

### Syntax

**mdi** { **across** | **auto** | **normal** }

**undo mdi**

### View

Ethernet interface view

### Default Level

2: System level

### Parameters

**across**: Specifies the MDI mode as **across**.

**auto**: Specifies the MDI mode as **auto**.

**normal**: Specifies the MDI mode as **normal**.

### Description

Use the **mdi** command to configure the MDI mode for an Ethernet interface.

Use the **undo mdi** command to restore the system default.

By default, the MDI mode of an Ethernet interface is **auto**, that is, the Ethernet interface determines the physical pin roles (transmit or receive) through negotiation.



#### Note

The command is not applicable to Combo ports operating as optical interfaces or 10-Gigabit Ethernet ports.

---

## Examples

```
# Set the MDI mode of GigabitEthernet 1/0/1 to across.
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mdi across
```

## multicast-suppression

### Syntax

```
multicast-suppression { ratio | pps max-pps }
undo multicast-suppression
```

### View

Ethernet interface view, port group view

### Default Level

2: System level

### Parameters

*ratio*: Maximum percentage of multicast traffic to the total transmission capability of an Ethernet interface, in the range 1 to 100. The smaller the ratio is, the less multicast traffic is allowed to pass through the interface.

**pps** *max-pps*: Specifies the maximum number of multicast packets allowed on an Ethernet interface per second (in pps, representing packets per second).

- For a Gigabit port, the value range is 1 to 1488100.
- For a 10-Gigabit port, the value range is 1 to 14881000.

Note that:

- When a suppression granularity larger than 1 is specified on the device, the value of the **pps** keyword should be no smaller than and an integral multiple of the granularity. The multicast suppression threshold value configured through this keyword on an Ethernet interface may not be the one that actually takes effect. To display the actual multicast suppression threshold value on an Ethernet interface, you can use the **display interface** command.
- When no suppression granularity is specified or the suppression granularity is set to 1, the value of the **pps** keyword should be no smaller than 1, and the multicast suppression threshold value is the one that actually takes effect on the Ethernet interface.

### Description

Use the **multicast-suppression** command to configure multicast storm suppression ratio on an interface.

Use the **undo multicast-suppression** command to restore the default multicast suppression ratio.

By default, all multicast traffic is allowed to go through an Ethernet interface, that is, multicast traffic is not suppressed.

If you execute this command in Ethernet interface view, the configurations take effect only on the current interface. If you execute this command in port-group view, the configurations take effect on all ports in the port group.

Note that when multicast traffic exceeds the maximum value configured, the system will discard the extra packets so that the multicast traffic ratio can drop below the limit to ensure that the network functions properly.



#### Note

- If you set different suppression ratios in Ethernet interface view or port-group view for multiple times, the latest configuration takes effect.
  - Do not use the **multicast-suppression** command along with the **storm-constrain** command. Otherwise, the multicast storm suppression ratio configured may get invalid.
- 

## Examples

# For Ethernet interface GigabitEthernet 1/0/1, allow multicast traffic equivalent to 20% of the total transmission capability of GigabitEthernet 1/0/1 to pass.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] multicast-suppression 20
```

# For all the ports of the manual port group **group1**, allow multicast traffic equivalent to 20% of the total transmission capability of each port to pass.

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group manual group1] group-member GigabitEthernet 1/0/2
[Sysname-port-group manual group1] group-member GigabitEthernet 1/0/3
[Sysname-port-group manual group1] multicast-suppression 20
```

## port-group manual

### Syntax

```
port-group manual port-group-name
undo port-group manual port-group-name
```

### View

System view

### Default Level

2: System level

### Parameters

*port-group-name*: Specifies name of a manual port group, a string of 1 to 32 characters.

### Description

Use the **port-group manual** command to create a manual port group and enter manual port group view.

Use the **undo port-group manual** command to remove a manual port group.

By default, no manual port group is created.

## Examples

```
# Create a manual port group named group1.
```

```
<Sysname> system-view  
[Sysname] port-group manual group1  
[Sysname-port-group-manual-group1]
```

## reset counters interface

### Syntax

```
reset counters interface [ interface-type [ interface-number ] ]
```

### View

User view

### Default Level

2: System level

### Parameters

*interface-type*: Interface type.

*interface-number*: Interface number.

### Description

Use the **reset counters interface** command to clear the statistics of an interface.

Before sampling network traffic within a specific period of time on an interface, you need to clear the existing statistics.

- If neither interface type nor interface number is specified, this command clears the statistics of all the interfaces.
- If only the interface type is specified, this command clears the statistics of the interfaces that are of the interface type specified.
- If both the interface type and interface number are specified, this command clears the statistics of the specified interface.

## Examples

```
# Clear the statistics of GigabitEthernet 1/0/1.
```

```
<Sysname> reset counters interface GigabitEthernet 1/0/1
```

## reset packet-drop interface

### Syntax

```
reset packet-drop interface [ interface-type [ interface-number ] ]
```

### View

Any view

## Default Level

2: System level

## Parameters

*interface-type*: Type of a specified interface.

*interface-number*: Number of a specified interface.

## Description

Use the **reset packet-drop interface** command to clear statistics of dropped packets on an interface or multiple interfaces. Sometimes when you want to collect the statistics of dropped packets on an interface, you need to clear the old statistics on the interface first.

- If you do not specify an interface type or interface number, this command clears statistics of dropped packets on all the interfaces on the device.
- If you specify an interface type only, this command clears statistics of dropped packets on the specified type of interfaces.
- If you specify both the interface type and interface number, this command clears statistics of dropped packets on the specified interface.

## Examples

# Clear statistics of dropped packets on GigabitEthernet 1/0/1.

```
<Sysname> reset packet-drop interface GigabitEthernet 1/0/1
```

# Clear statistics of dropped packets on all interfaces.

```
<Sysname> reset packet-drop interface
```

## shutdown

### Syntax

**shutdown**

**undo shutdown**

### View

Ethernet interface view

## Default Level

2: System level

## Parameters

None

## Description

Use the **shutdown** command to shut down an Ethernet interface.

Use the **undo shutdown** command to bring up an Ethernet interface.

By default, an Ethernet interface is in the up state.

In certain circumstances, modification to the interface parameters does not immediately take effect, and therefore, you need to shut down the relative interface to make the modification work.

Note that in case of a Combo port, only one interface (either the optical port or the electrical port) is active at a time. That is, once the optical port is active (after you execute the **undo shutdown** command), the electrical port will be inactive automatically, and vice versa.

## Examples

```
# Shut down interface GigabitEthernet 1/0/1.
```

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] shutdown
```

```
# Bring up interface GigabitEthernet 1/0/1.
```

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo shutdown
```

## speed

### Syntax

```
speed { 10 | 100 | 1000 | auto }
```

```
undo speed
```

### View

Ethernet interface view

### Default Level

2: System level

### Parameters

**10**: Specifies the interface rate as 10 Mbps. The optical interface of a Combo port does not support the **10** keyword.

**100**: Specifies the interface rate as 100 Mbps. The optical interface of a Combo port does not support the **100** keyword.

**1000**: Specifies the interface rate as 1,000 Mbps.

**auto**: Specifies to determine the interface rate through auto-negotiation.

### Description

Use the **speed** command to configure Ethernet interface data rate.

Use the **undo speed** command to restore Ethernet interface data rate.

Related commands: **duplex**, **speed auto**.



## Note

10-Gigabit Ethernet ports do not support this command.

---

## Examples

```
# Configure the interface rate as 100 Mbps for interface GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] speed 100
```

## storm-constrain

### Syntax

```
storm-constrain { broadcast | multicast } { pps | kbps | ratio } max-values min-values
undo storm-constrain { all | broadcast | multicast }
```

### View

Ethernet interface view

### Default Level

2: System level

### Parameters

**all**: Disables the storm constrain function for all types of packets (that is, multicast packets, and broadcast packets).

**broadcast**: Enables/Disables the storm constrain function for broadcast packets.

**multicast**: Enables/Disables the storm constrain function for multicast packets.

**pps**: Specifies the storm constrain threshold in terms of number of packets.

**kbps**: Specifies the storm constrain threshold in terms of number of kilobytes.

**ratio**: Specifies the storm constrain threshold in terms of percentages of the received packets to the whole transmission capacity.

*max-values*: Upper threshold to be set, in pps, kbps, or percentages.

When the threshold is set in pps:

- For a Gigabit port, the value range is 1 to 1488100.
- For a 10-Gigabit port, the value range is 1 to 14881000.

When the threshold is set in kbps:

- For a Gigabit port, the value range is 1 to 1000000.
- For a 10-Gigabit port, the value range is 1 to 10000000.

When the threshold is set in percentages, that is, keyword **ratio** is used, the value range is 1 to 100.

*min-values*: Lower threshold to be set, in pps, kbps, or percentages.

- For lower threshold to be set, in pps, this value ranges from 1 to *max-values*.

- For lower threshold to be set, in kbps, this value ranges from 1 to *max-values*.
- For lower threshold to be set, in percentages, this value ranges from 1 to *max-values*.

## Description

Use the **storm-constrain** command to enable the storm constrain function for specific type of packets and set the upper and lower thresholds.

Use the **undo storm-constrain** command to disable the storm constrain function for specific type of packets.

By default, the storm constrain function is not enabled.



### Note

- Do not use the **storm-constrain** command along with the **unicast-suppression** command, the **multicast-suppression** command, or the **broadcast-suppression** command. Otherwise, traffics may be suppressed in an unpredictable way.
  - An upper threshold cannot be less than the corresponding lower threshold. Besides, do not configure the two thresholds as the same value.
- 

## Examples

# Enable the storm constrain function for broadcast packets on GigabitEthernet 1/0/1, setting the upper and lower threshold to 2000 kbps and 1500 kbps.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] storm-constrain broadcast kbps 2000 1500
```

# Enable the storm constrain function for multicast packets on GigabitEthernet1/0/3 in terms of percentages of the received multicast packets to the port's total transmission capacity, setting the upper and lower threshold to 80% and 15%.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/3
[Sysname-GigabitEthernet1/0/3] storm-constrain multicast ratio 80 15
```

## storm-constrain control

### Syntax

**storm-constrain control { block | shutdown }**

**undo storm-constrain control**

### View

Ethernet interface view

### Default Level

2: System level

## Parameters

**block:** Blocks the traffic of a specific type on a port when the traffic detected exceeds the upper threshold.

**shutdown:** Shuts down a port when a type of traffic exceeds the corresponding upper threshold. A port shut down by the storm constrain function stops forwarding all types of packets.

## Description

Use the **storm-constrain control** command to set the action to be taken when a type of traffic exceeds the corresponding upper threshold.

Use the **undo storm-constrain control** command to restore the default.

By default, no action is taken when a type of traffic exceeds the corresponding threshold.

## Examples

# Configure to block interface GigabitEthernet 1/0/1 when a type of traffic reaching it exceeds the corresponding upper threshold.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] storm-constrain control block
```

## storm-constrain enable log

### Syntax

**storm-constrain enable log**

**undo storm-constrain enable log**

### View

Ethernet interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **storm-constrain enable log** command to enable log sending. With log sending enabled, the system sends log when traffic reaching a port exceeds the corresponding threshold or the traffic drops down below the lower threshold after exceeding the upper threshold.

Use the **undo storm-constrain enable log** command to disable log sending.

By default, log sending is enabled.

### Examples

# Disable log sending for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] undo storm-constrain enable log
```

## storm-constrain enable trap

### Syntax

```
storm-constrain enable trap  
undo storm-constrain enable trap
```

### View

Ethernet interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **storm-constrain enable trap** command to enable trap message sending. With trap message sending enabled, the system sends trap messages when traffic reaching a port exceeds the corresponding threshold or the traffic drops down below the lower threshold after exceeding the upper threshold.

Use the **undo storm-constrain enable trap** command to disable trap message sending.

By default, trap message sending is enabled.

### Examples

# Disable trap message sending for GigabitEthernet 1/0/1.

```
<Sysname> system-view  
[Sysname] interface GigabitEthernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] undo storm-constrain enable trap
```

## storm-constrain interval

### Syntax

```
storm-constrain interval seconds  
undo storm-constrain interval
```

### View

System view

### Default Level

2: System level

### Parameters

*seconds*: Interval for generating traffic statistics, in the range 1 to 300 (in seconds).

## Description

Use the **storm-constrain interval** command to set the interval for generating traffic statistics.

Use the **undo storm-constrain interval** command to restore the default.

By default, the interval for generating traffic statistics is 10 seconds.

---



### Note

- The interval set by the **storm-constrain interval** command is specifically for the storm constrain function. It is different from that set by the **flow-interval** command.
  - For network stability consideration, configure the interval for generating traffic statistics to a value that is not shorter than the default.
- 

## Examples

```
# Set the interval for generating traffic statistics to 60 seconds.
```

```
<Sysname> system-view  
[Sysname] storm-constrain interval 60
```

## unicast-suppression

### Syntax

```
unicast-suppression { ratio | pps max-pps }
```

```
undo unicast-suppression
```

### View

Ethernet interface view, port group view

### Default Level

2: System level

### Parameters

**ratio**: Maximum percentage of unicast traffic to the total transmission capability of an Ethernet interface, in the range of 1 to 100. The smaller the ratio is, the less unicast traffic is allowed through the interface.

**pps** *max-pps*: Specifies the maximum number of unknown unicast packets passing through an Ethernet interface per second (in pps, representing packets per second).

- For a Gigabit port, the value range is 1 to 1488100;
- For a 10-Gigabit port, the value range is 1 to 14881000.

Note that:

- When a suppression granularity larger than 1 is specified on the device, the value of the **pps** keyword should be no smaller than and an integral multiple of the granularity. The unicast suppression threshold value configured through this keyword on an Ethernet interface may not be the one that actually takes effect. To display the actual unicast suppression threshold value on an Ethernet interface, you can use the **display interface** command.

- When no suppression granularity is specified or the suppression granularity is set to 1, the value of the **pps** keyword should be no smaller than 1, and the unicast suppression threshold value is the one that actually takes effect on the Ethernet interface.

## Description

Use the **unicast-suppression** command to configure a unicast storm suppression ratio.

Use the **undo unicast-suppression** command to restore the default unicast suppression ratio.

By default, all unicast traffic is allowed to go through an Ethernet interface, that is, unicast traffic is not suppressed.

If you execute this command in Ethernet interface view, the configurations take effect only on the current interface. If you execute this command in port-group view, the configurations take effect on all ports in the port group

Note that when unicast traffic exceeds the maximum value configured, the system will discard the extra packets so that the unknown unicast traffic ratio can drop below the limit to ensure that the network functions properly.



### Note

- If you set different suppression ratios in Ethernet interface view or port-group view repeatedly, the latest configuration takes effect.
  - Do not use the **unicast-suppression** command along with the **storm-constrain** command. Otherwise, the unicast storm suppression ratio configured may get invalid.
- 

## Examples

# For Ethernet interface GigabitEthernet 1/0/1, allow unknown unicast traffic equivalent to 20% of the total transmission capability of the interface to pass and suppress the excessive unknown unicast packets.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] unicast-suppression 20
```

# For all the ports of the manual port group **group1**, allow unknown unicast traffic equivalent to 20% of the total transmission capability of each port to pass and suppress excessive unknown unicast packets.

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group manual group1] group-member GigabitEthernet 1/0/5
[Sysname-port-group manual group1] group-member GigabitEthernet 1/0/6
[Sysname-port-group manual group1] unicast-suppression 20
```

## virtual-cable-test

### Syntax

**virtual-cable-test**

## View

Ethernet interface view

## Default Level

2: System level

## Parameters

None

## Description

Use the **virtual-cable-test** command to test the cable connected to the Ethernet interface once and to display the testing result. The tested items include:

Note that:

- When the cable is functioning properly, the cable length in the test result represents the total cable length;
- When the cable is not functioning properly, the cable length in the test result represents the length from the current interface to the failed position.



### Note

- 10-Gigabit ports and Combo ports operating as optical interfaces do not support this command.
  - A link in the up state goes down and then up automatically if you execute this command on one of the Ethernet interfaces forming the link.
  - The test result is for your information only. The maximum error in the tested cable length is 5 m. A hyphen "-" indicates that the corresponding test item is not supported.
- 

## Examples

```
# Enable the virtual cable test for the interface GigabitEthernet 1/0/1.
```

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] virtual-cable-test
Cable status: normal, 1 metres
Pair Impedance mismatch: -
Pair skew: - ns
Pair swap: -
Pair polarity: -
Insertion loss: - db
Return loss: - db
Near-end crosstalk: - db
```

# Table of Contents

<b>1 Link Aggregation Configuration Commands</b> .....	<b>1-1</b>
Link Aggregation Configuration Commands .....	1-1
description .....	1-1
display lacp system-id .....	1-2
display link-aggregation load-sharing mode.....	1-2
display link-aggregation member-port .....	1-3
display link-aggregation summary.....	1-6
display link-aggregation verbose.....	1-7
enable snmp trap updown .....	1-9
interface bridge-aggregation .....	1-10
lacp port-priority.....	1-11
lacp system-priority.....	1-11
link-aggregation load-sharing mode .....	1-12
link-aggregation mode .....	1-13
port link-aggregation group .....	1-14
reset lacp statistics .....	1-14
shutdown .....	1-15

# 1 Link Aggregation Configuration Commands

---

## Link Aggregation Configuration Commands

### description

#### Syntax

```
description text  
undo description
```

#### View

Layer-2 aggregate interface view

#### Default Level

2: System level

#### Parameters

*text*: Description of an Ethernet interface, a string of 1 to 80 characters. Currently, the device supports the following types of characters or symbols: standard English characters (numbers and case-sensitive letters), special English characters, spaces, and other characters or symbols that conform to the Unicode standard.



#### Note

- A port description can be the mixture of English characters and other Unicode characters. The mixed description cannot exceed the specified length.
  - To use a type of Unicode characters or symbols in a port description, you need to install the corresponding Input Method Editor (IME) and log in to the device through remote login software that supports this character type.
  - Each Unicode character or symbol (non-English characters) takes the space of two regular characters. When the length of a description string reaches or exceeds the maximum line width on the terminal software, the software starts a new line, possibly breaking a Unicode character into two. As a result, garbled characters may be displayed at the end of a line.
- 

#### Description

Use the **description** command to set the description of the current interface.

Use the **undo description** command to restore the default.

By default, the description of an interface is *interface-name* **Interface**, such as **Bridge-Aggregation1 Interface**.

## Examples

```
# Set the description of interface Bridge-aggregation 1 to link-aggregation interface.  
<Sysname> system-view  
[Sysname] interface bridge-aggregation 1  
[Sysname-Bridge-Aggregation1] description link-aggregation interface
```

## display lacp system-id

### Syntax

```
display lacp system-id
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display lacp system-id** command to display the system ID of the local system (that is, the actor). The ID comprises the system LACP priority and the system MAC address.

## Examples

```
# Display the local system ID.  
<Sysname> display lacp system-id  
Actor System ID: 0x8000, 000f-e200-0100
```

**Table 1-1 display lacp system-id command output description**

Field	Description
Actor System ID	The local system ID, which comprises the LACP system priority and the system MAC address.

## display link-aggregation load-sharing mode

### Syntax

```
display link-aggregation load-sharing mode
```

### View

Any view

### Default Level

1: Monitor level

## Parameters

None

## Description

Use the **display link-aggregation load-sharing mode** command to display load sharing mode for link aggregation groups.

## Examples

# Display the default global link aggregation load sharing mode.

```
<Sysname> display link-aggregation load-sharing mode
```

```
Link-Aggregation Load-Sharing Mode:
```

```
Layer 2 traffic: destination-mac address, source-mac address
```

```
Layer 3 traffic: destination-ip address, source-ip address
```

# Display the configured global link aggregation load sharing mode.

```
<Sysname> display link-aggregation load-sharing mode
```

```
Link-Aggregation Load-Sharing Mode:
```

```
destination-mac address, source-mac address
```

**Table 1-2** display link-aggregation load-sharing mode command output description

Field	Description
Link-Aggregation Load-Sharing Mode	Displays the global link aggregation load sharing mode. <ul style="list-style-type: none"><li>• By default, the link aggregation load sharing modes for Layer-2 traffic, and Layer-3 traffic displayed.</li><li>• If you have configured a global load sharing mode, the configured mode is displayed.</li></ul>
Layer 2 traffic: destination-mac address, source-mac address	The default load sharing mode for Layer-2 traffic. In this sample output, it is based on source MAC address and destination MAC address.
Layer 3 traffic: destination-ip address, source-ip address	The default load sharing mode for Layer-3 traffic. In this sample output, it is based on source IP address and destination IP address.
destination-mac address, source-mac address	The user-configured link aggregation load sharing mode. In this sample output, it is based on source MAC address and destination MAC address.

## display link-aggregation member-port

### Syntax

```
display link-aggregation member-port [ interface-type interface-number [ to interface-type interface-number ] ]
```

### View

Any view

## Default Level

1: Monitor level

## Parameters

*interface-type interface-number*: Port type and port number.

**to**: Specifies an interface range in the form of *interface-type interface-number to interface-type interface-number*, where the start interface number must be smaller than the end interface number.

Note that both the start interface and the end interface are inclusive.

## Description

Use the **display link-aggregation member-port** command to display the detailed link aggregation information of the specified interface(s) or all interfaces if no interface is specified.

For an interface in a static aggregation group, only its port number and operational key are displayed, because it is not aware of the information of the partner.

## Examples

# Display the detailed link aggregation information of GigabitEthernet 1/0/1, which is in a static aggregation group.

```
<Sysname> display link-aggregation member-port GigabitEthernet 1/0/1
```

```
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,  
       D -- Synchronization, E -- Collecting, F -- Distributing,  
       G -- Defaulted, H -- Expired
```

```
GigabitEthernet1/0/1:
```

```
Aggregation Interface: Bridge-Aggregation1
```

```
Port Number: 1
```

```
Oper-Key: 1
```

# Display the detailed link aggregation information of GigabitEthernet 1/0/2, which is in a dynamic aggregation group.

```
<Sysname> display link-aggregation member-port GigabitEthernet 1/0/2
```

```
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,  
       D -- Synchronization, E -- Collecting, F -- Distributing,  
       G -- Defaulted, H -- Expired
```

```
GigabitEthernet1/0/2:
```

```
Aggregation Interface: Bridge-Aggregation10
```

```
Local:
```

```
Port Number: 2
```

```
Port Priority: 32768
```

```
Oper-Key: 2
```

```
Flag: {ACDEF}
```

```
Remote:
```

```
System ID: 0x8000, 000f-e267-6c6a
```

```
Port Number: 26
```

```

Port Priority: 32768
Oper-Key: 2
Flag: {ACDEF}
Received LACP Packets: 5 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 7 packet(s)

```

**Table 1-3** display link-aggregation member-port command output description

Field	Description
Flags	<p>One-octet LACP state flags field. From the least to the most significant bit, they are represented by A through H as follows:</p> <ul style="list-style-type: none"> <li>• A indicates whether LACP is enabled. 1 for enabled and 0 for disabled.</li> <li>• B indicates the timeout control value. 1 for short timeout, and 0 for long timeout.</li> <li>• C indicates whether the link is considered as aggregatable by the sending system. 1 for true, and 0 for false.</li> <li>• D indicates whether the link is considered as synchronized by the sending system. 1 for true, and 0 for false.</li> <li>• E indicates whether the sending system considers that collection of incoming frames is enabled on the link. 1 for true and 0 for false.</li> <li>• F indicates whether the sending system considers that distribution of outgoing frames is enabled on the link. 1 for true and 0 for false.</li> <li>• G indicates whether the receive state machine of the sending system is using default operational partner information. 1 for true and 0 for false.</li> <li>• H indicates whether the receive state machine of the sending system is in the expired state. 1 for true and 0 for false.</li> </ul> <p>If a flag bit is set to 1, the corresponding English letter that otherwise is not output is displayed.</p>
Aggregation Interface	Aggregate interface to which the port belongs
Local: Port Number Port Priority Oper-key Flag	Information about the local end: <ul style="list-style-type: none"> <li>• Port Number: Number of the port.</li> <li>• Port Priority: LACP priority of the port.</li> <li>• Oper-key: Operational key</li> <li>• Flag: LACP protocol state flag.</li> </ul>
Remote: System ID Port Number Port Priority Oper-key Flag	Information about the remote end: <ul style="list-style-type: none"> <li>• System ID: System ID of the remote end.</li> <li>• Port Number: Number of the port.</li> <li>• Port Priority: LACP priority of the port.</li> <li>• Oper-key: Operational key</li> <li>• Flag: LACP protocol state flag.</li> </ul>
Received LACP Packets	Number of LACP packets received
Illegal	Number of illegal packets
Sent LACP Packets	Number of LACP packets sent

## display link-aggregation summary

### Syntax

**display link-aggregation summary**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display link-aggregation summary** command to display the summary information of all aggregation groups.

You may find out that information about the remote system for a static link aggregation group is either replaced by **none** or not displayed at all. This is normal because this type of aggregation group is not aware of its partner.

### Examples

# Display the summary information of all aggregation groups.

```
<Sysname> display link-aggregation summary
```

```
Aggregation Interface Type:
```

```
BAGG -- Bridge-Aggregation, RAGG -- Route-Aggregation
```

```
Aggregation Mode: S -- Static, D -- Dynamic
```

```
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
```

```
Actor System ID: 0x8000, 000f-e267-6c6a
```

AGG Interface	AGG Mode	Partner ID	Select Ports	Unselect Ports	Share Type
BAGG1	S	none	1	0	Shar
BAGG10	D	0x8000, 000f-e267-6c6a	2	0	Shar

**Table 1-4** display link-aggregation summary command output description

Field	Description
Aggregation Interface Type	Aggregate interface type: <ul style="list-style-type: none"><li>• BAGG for a Layer-2 aggregate interface</li><li>• RAGG for a Layer-3 aggregate interface</li></ul>
Aggregation Mode	Aggregation group type: <ul style="list-style-type: none"><li>• S for static link aggregation</li><li>• D for dynamic aggregation</li></ul>

Field	Description
Loadsharing Type	Loadsharing type: <ul style="list-style-type: none"> <li>• Shar for load sharing</li> <li>• NonS for non-load sharing</li> </ul>
Actor System ID	Local system ID
AGG Interface	Abbreviated name of the aggregate interface
AGG Mode	Aggregation group type
Partner ID	System ID of the partner
Select Ports	The number of selected ports
Unselect Ports	The number of unselected ports
Share Type	Load sharing type

## display link-aggregation verbose

### Syntax

```
display link-aggregation verbose [ bridge-aggregation [ interface-number ] ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**bridge-aggregation:** Displays detailed information about the Layer-2 aggregate groups corresponding to Layer-2 aggregate interfaces.

*interface-number.* Aggregate interface number. Note that the aggregate interface you specify must already exist.

### Description

Use the **display link-aggregation verbose** command to display detailed information about the aggregation groups corresponding to the aggregate interfaces.

To display the information of a specific Layer-2 aggregate group, use the **display link-aggregation verbose bridge-aggregation interface-number** command.

To display the information of all Layer-2 aggregate groups, use the **display link-aggregation verbose bridge-aggregation** command.

To display the information of all aggregate groups, use the **display link-aggregation verbose** command.

### Examples

# Display the detailed information of the aggregation group corresponding to Layer-2 aggregate interface **Bridge-aggregation 10**.

<Sysname> display link-aggregation verbose bridge-aggregation 10

Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing

Port Status: S -- Selected, U -- Unselected

Flags: A -- LACP\_Activity, B -- LACP\_Timeout, C -- Aggregation,  
D -- Synchronization, E -- Collecting, F -- Distributing,  
G -- Defaulted, H -- Expired

Aggregation Interface: Bridge-Aggregation10

Aggregation Mode: Dynamic

Loadsharing Type: Shar

System ID: 0x8000, 000f-e267-6c6a

Local:

Port	Status	Priority	Oper-Key	Flag
GE1/0/6	S	32768	2	{ACDEF}
GE1/0/12	S	32768	2	{ACDEF}

Remote:

Actor	Partner	Priority	Oper-Key	SystemID	Flag
GE1/0/6	32	32768	2	0x8000, 000f-e267-6c6a	{ACDEF}
GE1/0/12	26	32768	2	0x8000, 000f-e267-6c6a	{ACDEF}

**Table 1-5** display link-aggregation verbose command output description

Field	Description
Loadsharing Type	Loadsharing type: <ul style="list-style-type: none"> <li>• Shar for load sharing</li> <li>• NonS for non-load sharing</li> </ul>
Port Status	Port state: Selected or unselected.
Flags	<p>One-octet LACP state flags field. From the least to the most significant bit, they are represented by A through H as follows:</p> <ul style="list-style-type: none"> <li>• A indicates whether LACP is enabled. 1 for enabled and 0 for disabled.</li> <li>• B indicates the timeout control value. 1 for short timeout, and 0 for long timeout.</li> <li>• C indicates whether the link is considered as aggregatable by the sending system. 1 for true, and 0 for false.</li> <li>• D indicates whether the link is considered as synchronized by the sending system. 1 for true, and 0 for false.</li> <li>• E indicates whether the sending system considers that collection of incoming frames is enabled on the link. 1 for true and 0 for false.</li> <li>• F indicates whether the sending system considers that distribution of outgoing frames is enabled on the link. 1 for true and 0 for false.</li> <li>• G indicates whether the receive state machine of the sending system is using default operational partner information. 1 for true and 0 for false.</li> <li>• H indicates whether the receive state machine of the sending system is in the expired state. 1 for true and 0 for false.</li> </ul> <p>If a flag bit is set to 1, the corresponding English letter that otherwise is not output is displayed.</p>
Aggregation Interface	Name of the aggregate interface
Aggregation Mode	Type of the aggregation group: Static for static aggregation, and Dynamic for dynamic aggregation.
System ID	Local system ID
Local: Port Status Priority Oper-Key Flag	Other information of the local end, including the member ports, port state, port LACP priority, operational key, and LACP protocol state flags.
Remote: Actor Partner Priority Oper-Key SystemID Flag	Detailed information about the remote end, including the corresponding local port, port ID, port LACP priority, operational key, system ID, and LACP protocol state flags

## enable snmp trap updown

### Syntax

**enable snmp trap updown**

**undo enable snmp trap updown**

### View

Layer-2 aggregate interface view

## Default Level

2: System level

## Parameters

None

## Description

Use the **enable snmp trap updown** command to enable linkUp/linkDown trap generation for the current aggregate interface.

Use the **undo enable snmp trap updown** command to disable linkUp/linkDown trap generation for the current aggregate interface.

By default, linkUp/linkDown trap generation is enabled for an aggregate interface.

Note that for an aggregate interface to generate linkUp/linkDown traps when its link state changes, you must also enable linkUp/linkDown trap generation globally with the **snmp-agent trap enable [ standard [ linkdown | linkup ] \* ]** command.

Refer to *SNMP Commands* in the *System Volume* for information about the **snmp-agent trap enable** command.

## Examples

```
# Enable linkUp/linkDown trap generation on interface Bridge-aggregation 1.
```

```
<Sysname> system-view  
[Sysname] snmp-agent trap enable  
[Sysname] interface bridge-aggregation 1  
[Sysname-Bridge-Aggregation1] enable snmp trap updown
```

## interface bridge-aggregation

### Syntax

```
interface bridge-aggregation interface-number  
undo interface bridge-aggregation interface-number
```

### View

System view

## Default Level

2: System level

## Parameters

*interface-number*: Layer-2 aggregate interface number. The value range is 1 to 128

## Description

Use the **interface bridge-aggregation** command to create a Layer-2 aggregate interface and enter the Layer-2 aggregate interface view.

Use the **undo interface bridge-aggregation** command to remove a Layer-2 aggregate interface.

Upon creation of a Layer-2 aggregate interface, a Layer-2 aggregation group numbered the same is created automatically. Removing the Layer-2 aggregate interface also removes the Layer-2 aggregation group. At the same time, the member ports of the aggregation group, if any, leave the aggregation group.

## Examples

```
# Create Layer-2 aggregate interface Bridge-aggregation 1.
```

```
<Sysname> system-view  
[Sysname] interface bridge-aggregation 1  
[Sysname-Bridge-Aggregation1]
```

## lACP port-priority

### Syntax

```
lACP port-priority port-priority
```

```
undo lACP port-priority
```

### View

Ethernet interface view

### Default Level

2: System level

### Parameters

*port-priority*: LACP port priority, in the range of 0 to 65535.

### Description

Use the **lACP port-priority** command to set the LACP priority of a port.

Use the **undo lACP port-priority** command to restore the default.

The default LACP priority of a port is 32768.

## Examples

```
# Set the LACP priority of GigabitEthernet 1/0/1 to 64.
```

```
<Sysname> system-view  
[Sysname] interface GigabitEthernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] lACP port-priority 64
```

## lACP system-priority

### Syntax

```
lACP system-priority system-priority
```

```
undo lACP system-priority
```

### View

System view

## Default Level

2: System level

## Parameters

*system-priority*: LACP priority of the local system, in the range of 0 to 65535.

## Description

Use the **lacp system-priority** command to set the LACP priority of the local system.

Use the **undo lacp port-priority** command to restore the default.

By default, the system LACP priority is 32768.

## Examples

```
# Set the system LACP priority to 64.
```

```
<Sysname> system-view  
[Sysname] lacp system-priority 64
```

## link-aggregation load-sharing mode

### Syntax

```
link-aggregation load-sharing mode { destination-ip | destination-mac | destination-port |  
ingress-port | source-ip | source-mac | source-port } *
```

```
undo link-aggregation load-sharing mode
```

### View

System view

## Default Level

2: System level

## Parameters

**destination-ip**: Specifies to perform load sharing in link aggregation groups based on destination IP address.

**destination-mac**: Specifies to perform load sharing in load-sharing link aggregation groups based on destination MAC address.

**destination-port**: Specifies to perform load sharing in load-sharing link aggregation groups based on destination port.

**ingress-port**: Specifies to perform load sharing in load-sharing link aggregation groups based on ingress port.

**source-ip**: Specifies to perform load sharing in load-sharing link aggregation groups based on source IP address.

**source-mac**: Specifies to perform load sharing in load-sharing link aggregation groups based on source MAC address.

**source-port**: Specifies to perform load sharing in load-sharing link aggregation groups based on source port.

## Description

Use the **link-aggregation load-sharing mode** command to configure the link aggregation load sharing mode.

Use the **undo link-aggregation load-sharing mode** command to restore the default.

By default, link aggregation load sharing for Layer-2 packets is performed based on source MAC addresses and destination MAC addresses, and that for Layer-3 packets is performed based on source IP addresses and destination IP addresses.

Note that:

- The load sharing mode you configured overwrites rather than adds to the old one, if any. Therefore, to change the load sharing mode from source port based to source and destination ports based for example, you must configure the **link-aggregation load-sharing mode destination-port source-port** to overwrite the **link-aggregation load-sharing mode destination-port** command rather than configure the **link-aggregation load-sharing mode source-port** command.
- Currently, the hash keys for a switch are source IP addresses, destination IP addresses, source MAC addresses, destination MAC addresses, source ports, destination ports, or the combination of these fields carried in packets (excluding the combination of MAC addresses with IP addresses, source ports, or destination ports). The **ingress-port** parameter can only be used as a hash key when combined with a MAC address, not when combined with an IP address, source port, or destination port. The parameter alone cannot be used as a hash key either. In case an unsupported load sharing mode is configured, you will be prompted of the error.

## Examples

```
# Configure the link aggregation load sharing mode as destination MAC-based.
```

```
<Sysname> system-view  
[Sysname] link-aggregation load-sharing mode destination-mac
```

## link-aggregation mode

### Syntax

```
link-aggregation mode dynamic
```

```
undo link-aggregation mode
```

### View

```
Layer-2 aggregate interface view
```

### Default Level

```
2: System level
```

### Parameters

```
None
```

### Description

Use the **link-aggregation mode dynamic** command to configure an aggregation group to work in dynamic aggregation mode.

Use the **undo link-aggregation mode** command to restore the default.

By default, an aggregation group works in static aggregation mode.

If there is any member port in an aggregation group, you cannot modify the aggregation mode of the aggregation group.

## Examples

# Configure the aggregation group of **Bridge-aggregation 1** to work in dynamic aggregation mode.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation mode dynamic
```

## port link-aggregation group

### Syntax

```
port link-aggregation group number
undo port link-aggregation group
```

### View

Ethernet interface view

### Default Level

2: System level

### Parameters

*number*: Aggregate group number. The value range is 1 to 128.

### Description

Use the **port link-aggregation group** command to assign the current Ethernet interface to the specified aggregation group.

Use the **port link-aggregation group** command to remove the current Ethernet interface from the specified aggregation group.

Note that

- If the Ethernet interface is a Layer-2 interface, you must assign it to a Layer-2 aggregation group.
- An Ethernet interface can belong to only one aggregation group.

## Examples

# Assign GigabitEthernet 1/0/1 to aggregation group 22.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-aggregation group 22
```

## reset lacp statistics

### Syntax

```
reset lacp statistics [ interface interface-type interface-number [ to interface-type interface-number ] ]
```

## View

User view

## Default Level

1: Monitor level

## Parameters

*interface-type interface-number*: Interface type and interface number.

**to**: Specifies an interface range in the form of *interface-type interface-number to interface-type interface-number*, where the start interface number must be smaller than the end interface number. Note that both the start interface and the end interface are inclusive.

## Description

Use the **reset lacp statistics** command to clear the LACP statistics for the specified interface(s) or all interfaces if no interface is specified.

Related commands: **display link-aggregation member-port**.

## Examples

# Clear the LACP statistics for all Ethernet ports.

```
<Sysname> reset lacp statistics
```

## shutdown

### Syntax

**shutdown**

**undo shutdown**

### View

Layer-2 aggregate interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **shutdown** command to shut down the current aggregate interface/subinterface.

Use the **undo shutdown** command to bring up the current aggregate interface/subinterface.

By default, aggregate interfaces are enabled.

### Examples

# Shut down aggregate interface **Bridge-Aggregation 1**.

```
<Sysname> system-view
```

```
[Sysname] interface bridge-aggregation 1  
[Sysname-Bridge-Aggregation1] shutdown
```

# Table of Contents

<b>1 Port Isolation Configuration Commands .....</b>	<b>1-1</b>
Port Isolation Configuration Commands .....	1-1
display port-isolate group .....	1-1
port-isolate enable .....	1-2

# 1 Port Isolation Configuration Commands

---

## Port Isolation Configuration Commands

### display port-isolate group

#### Syntax

**display port-isolate group**

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

None

#### Description

Use the **display port-isolate group** command to display information about the default isolation group (isolation group 1).

#### Examples

# On a single-isolation-group device, display information about the isolation group.

```
<Sysname> display port-isolate group
Port-isolate group information:
Uplink port support: NO
Group ID: 1
Group members:
    GigabitEthernet1/0/1
```

**Table 1-1** display port-isolate group command output description

Field	Description
Port-isolate group information	Display the information of a port-isolation group
Uplink port support	Indicates whether the uplink port is supported.
Group ID	Isolation group number
Group members	Isolated ports in the isolation group

## port-isolate enable

### Syntax

```
port-isolate enable
undo port-isolate enable
```

### View

Ethernet interface view, Layer-2 aggregate interface view, port group view

### Default Level

2: System level

### Parameters

None

### Description

Use the **port-isolate enable** command to add a port in Ethernet interface view or a group of ports in port group view to an isolation group as isolated ports.

Use the **undo port-isolate enable** command to remove the port or ports from the isolation group.

- In Ethernet interface view, the configuration applies to the current port.
- In port group view, the configuration applies to all ports in the port group.
- In Layer-2 aggregate interface view, the configuration applies to the Layer-2 aggregate interface and all its member ports. After you make the configuration, the system starts applying the configuration to the aggregate interface and its aggregation member ports. If the system fails to do that on the aggregate interface, it stops applying the configuration to the aggregation member ports. If it fails to do that on an aggregation member port, it simply skips the port and moves to the next port. For detailed information about Layer-2 aggregate interfaces, refer to *Link Aggregation Configuration* in the *Access Volume*.



#### Note

The member port of a service loopback group cannot be assigned to an isolation group and vice versa.

---

### Examples

# On a single-isolation-group device, assign ports GigabitEthernet 1/1 and GigabitEthernet 1/2 to the isolation group.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-isolate enable
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port-isolate enable
```

# On a single-isolation-group device, assign all the ports within port group **aa** to the isolation group.

```
<Sysname> system-view
[Sysname] port-group manual aa
[Sysname-port-group-manual-aa] group-member GigabitEthernet 1/0/1
[Sysname-port-group-manual-aa] group-member GigabitEthernet 1/0/2
[Sysname-port-group-manual-aa] group-member GigabitEthernet 1/0/3
[Sysname-port-group-manual-aa] group-member GigabitEthernet 1/0/4
[Sysname-port-group-manual-aa] port-isolate enable
```

**# Assign Layer-2 aggregate interface Bridge-aggregation 1 and its member ports to the isolation group on a single-isolation-group device.**

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] quit
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-aggregation group 1
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port link-aggregation group 1
[Sysname-GigabitEthernet1/0/2] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port-isolate enable
rt-isolate uplink-port group 2
```

# Table of Contents

<b>1 Service Loopback Group Configuration Commands</b> .....	<b>1-1</b>
Service Loopback Group Configuration Commands .....	1-1
display service-loopback group .....	1-1
port service-loopback group .....	1-2
service-loopback group .....	1-2

# 1 Service Loopback Group Configuration

## Commands

---



### Caution

The SFP+ subcards and GE subcards of the 3Com Switch 4800G do not support service loopback groups.

---

## Service Loopback Group Configuration Commands

### display service-loopback group

#### Syntax

```
display service-loopback group [ number ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

*number*: ID of the service loopback group to be displayed. The range of the *number* argument is 1 to 1,024.

#### Description

Use the **display service-loopback group** command to display information of the specified service loopback group. If no service loopback group is specified, information of all service loopback groups is displayed.

#### Examples

```
# Display information of service loopback group 5.
```

```
<Sysname> display service-loopback group 5
```

```
Service Group ID:      5          Quote Number: 0
```

```
Service Type: tunnel
```

```
Member
```

```
Status
```

---

GE1/0/1	Selected
GE1/0/2	Selected

**Table 1-1** display service-loopback group command output description

Field	Description
Service Group ID	Service loopback group ID
Quote Number	Reference count of the service loopback group
Service Type	Service type of the service loopback group
Member	Member ports of the service loopback group
Status	Port state, which can be selected or unselected

## port service-loopback group

### Syntax

```
port service-loopback group number
undo port service-loopback group
```

### View

Ethernet interface view

### Default Level

2: System level

### Parameters

*number*: Service loopback group ID. The range of the *number* argument is 1 to 1,024.

### Description

Use the **port service-loopback group** command to assign the Ethernet interface to the specified service loopback group.

Use the **undo port service-loopback group** command to remove the Ethernet interface from the specified service loopback group.

Note that you cannot remove the last member port of a referenced service loopback group.

### Examples

```
# Assign Ethernet interface GigabitEthernet 1/0/1 to service loopback group 5.
```

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port service-loopback group 5
```

## service-loopback group

### Syntax

```
service-loopback group number type tunnel
```

**undo service-loopback group** *number*

## View

System view

## Default Level

2: System level

## Parameters

*number*: Service loopback group ID. The range of the *number* argument is 1 to 1,024.

**type**: Specifies the service type of a service loopback group.

**tunnel**: Specifies the service type of a service loopback group as Tunnel.

## Description

Use the **service-loopback group** command to create a service loopback group or change the service type of an existing service loopback group.

Use the **undo service-loopback group** command to remove a service loopback group.

Note that:

- A service loopback group can be referenced by other features after its creation. Only after being referenced can a service loopback group process service traffic. A service loopback group can be referenced by multiple features at the same time.
- You can change the service type of an existing service loopback group. For the change to be successful, you must ensure that the service group has not been referenced; the attributes of all member ports (if any) are not conflicting with the target service type; and no service loopback group has been created for the target service type, because only one service loopback group is allowed for a service type.
- You can remove any service loopback group except the referenced ones.

## Examples

# Configure service loopback group 5 to support the tunnel service.

```
<Sysname> system-view
```

```
[Sysname] service-loopback group 5 type tunnel
```

# Table of Contents

<b>1 DLDP Configuration Commands</b> .....	<b>1-1</b>
DLDP Configuration Commands.....	1-1
display dldp.....	1-1
display dldp statistics.....	1-3
dldp authentication-mode .....	1-4
dldp delaydown-timer .....	1-5
dldp enable .....	1-5
dldp interval .....	1-6
dldp reset.....	1-7
dldp unidirectional-shutdown.....	1-8
dldp work-mode .....	1-8
reset dldp statistics.....	1-9

# 1 DLDP Configuration Commands

---

## DLDP Configuration Commands

### display dldp

#### Syntax

```
display dldp [ interface-type interface-number ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

*interface-type interface-number*: Port type and port number.

#### Description

Use the **display dldp** command to display the DLDP configuration of a port.

If you do not provide the *interface-type* or *interface-number* arguments, this command displays the DLDP configuration of all the DLDP-enabled ports.

#### Examples

# Display the DLDP configuration of all the DLDP-enabled ports.

```
<Sysname> display dldp
DLDP global status : enable
DLDP interval : 5s
DLDP work-mode : enhance
DLDP authentication-mode : simple, password is 123
DLDP unidirectional-shutdown : auto
DLDP delaydown-timer : 2s
The number of enabled ports is 2.
```

```
Interface GigabitEthernet1/0/50
DLDP port state : advertisement
DLDP link state : up
The neighbor number of the port is 1.
Neighbor mac address : 0000-0000-0100
Neighbor port index : 79
Neighbor state : two way
Neighbor aged time : 13
```

```

Interface GigabitEthernet1/0/51
  DLDP port state : advertisement
  DLDP link state : up
  The neighbor number of the port is 1.
    Neighbor mac address : 0000-0000-1100
    Neighbor port index : 81
    Neighbor state : two way
    Neighbor aged time : 12

```

**# Display the DLDP configuration of GigabitEthernet1/0/50.**

```

<Sysname> display dldp gigabitethernet 1/0/50
Interface GigabitEthernet1/0/50
  DLDP port state : advertisement
  DLDP link state : up
  The neighbor number of the port is 1.
    Neighbor mac address : 0000-0000-0100
    Neighbor port index : 79
    Neighbor state : two way
    Neighbor aged time : 13

```

**Table 1-1 display dldp command output description**

Field	Description
DLDP global status	Global DLDP state ( <b>enable</b> or <b>disable</b> )
DLDP interval	Interval for sending Advertisement packets (in seconds)
DLDP work-mode	DLDP mode ( <b>enhance</b> or <b>normal</b> )
DLDP authentication-mode	DLDP authentication mode ( <b>none</b> , <b>simple</b> , or <b>md5</b> )
password	Password for DLDP authentication
DLDP unidirectional-shutdown	Port shutdown mode ( <b>auto</b> or <b>manual</b> )
DLDP delaydown-timer	Setting of the DelayDown timer
The number of enabled ports	Number of the DLDP-enabled ports
Interface	Index of a DLDP-enabled port
DLDP port state	DLDP state on a port ( <b>initial</b> , <b>inactive</b> , <b>active</b> , <b>advertisement</b> , <b>probe</b> , <b>disable</b> , or <b>delaydown</b> )
DLDP link state	Port state ( <b>up</b> or <b>down</b> )
The neighbor number of the port	Number of the neighbors of a port
Neighbor mac address	MAC address of a neighbor
Neighbor port index	Neighbor port index
Neighbor state	Neighbor state ( <b>unknown</b> , <b>one way</b> , or <b>two way</b> )
Neighbor aged time	Neighbor aging time

## display dldp statistics

### Syntax

```
display dldp statistics [ interface-type interface-number ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*interface-type interface-number*: Port type and port number.

### Description

Use the **display dldp statistics** command to display the statistics on the DLDP packets passing through a port.

If you do not provide the *interface-type* or *interface-number* argument, this command displays the statistics on the DLDP packets passing through all the DLDP-enabled ports.

### Examples

# Display the statistics on the DLDP packets passing through all the DLDP-enabled ports.

```
<Sysname> display dldp statistics
Interface GigabitEthernet1/0/50
  Packets sent : 6
  Packets received : 5
  Invalid packets received : 2
  Loop packets received : 0
  Authentication failed packets received : 0
  Valid packets received : 3
```

```
Interface GigabitEthernet1/0/51
  Packets sent : 7
  Packets received : 7
  Invalid packets received : 3
  Loop packets received : 0
  Authentication failed packets received : 0
  Valid packets received : 4
```

# Display the statistics on the DLDP packets passing through GigabitEthernet1/0/50.

```
<Sysname> display dldp statistics gigabitethernet1/0/50
Interface GigabitEthernet1/0/50
  Packets sent : 6
  Packets received : 5
  Invalid packets received : 2
  Loop packets received : 0
  Authentication failed packets received : 0
  Valid packets received : 3
```

**Table 1-2 display dldp statistics** command output description

Field	Description
Interface	Port index
Packets sent	Total number of DLDP packets sent
Packets received	Total number of DLDP packets received
Invalid packets received	Number of the invalid packets received
Loop packets received	Number of the loopback packets received
Authentication failed packets received	Number of the received packets that failed to pass the authentication
Valid packets received	Number of the valid packets received

## dldp authentication-mode

### Syntax

```
dldp authentication-mode { md5 md5-password | none | simple simple-password }  
undo dldp authentication-mode
```

### View

System view

### Default Level

2: System level

### Parameters

**md5** *md5-password*: Specifies to perform MD5 authentication and sets the password. The *md5-password* argument is the password, a string of 1 to 16 characters or a 24-bit string. The former indicates a plain text password and the latter indicates a cipher text password. Note that this argument is case-sensitive.

**None**: Specifies not to perform authentication.

**simple** *simple-password*: Specifies to perform plain text authentication and sets the password. The *simple-password* argument is the password, a case-sensitive string of 1 to 16 characters.

### Description

Use the **dldp authentication-mode** command to configure DLDP authentication.

Use the **undo dldp authentication-mode** command to restore the default.

By default, DLDP authentication is not performed.

To enable DLDP to operate properly, make sure the DLDP authentication modes and the passwords of the both sides of a link are the same.

### Examples

```
# Configure to perform plain text authentication, setting the password as abc (assuming that Device A and Device B are connected by the DLDP link).
```

- Configuration on Device A

```
<DeviceA> system-view  
[DeviceA] dldp authentication-mode simple abc
```

- Configuration on Device B

```
<DeviceB> system-view  
[DeviceB] dldp authentication-mode simple abc
```

## dldp delaydown-timer

### Syntax

```
dldp delaydown-timer time  
undo dldp delaydown-timer
```

### View

System view

### Default Level

2: System level

### Parameters

*Time*: Setting of the DelayDown timer, in the range 1 to 5 (in seconds).

### Description

Use the **dldp delaydown-timer** command to set the DelayDown timer.

Use the **undo dldp delaydown-timer** command to restore the default.

By default, the setting of the DelayDown timer is 1 second.

Note that these two commands apply to all the DLDP-enabled ports.

### Examples

# Set the DelayDown timer to 2 seconds.

```
<Sysname> system-view  
[Sysname] dldp delaydown-timer 2
```

## dldp enable

### Syntax

```
dldp enable  
undo dldp enable
```

### View

System view, Ethernet port view, port group view

### Default Level

2: System level

## Parameters

None

## Description

Use the **lldp enable** command to enable LLDP.

Use the **undo lldp enable** command to disable LLDP.

When executed in system view, these two commands enables/disables LLDP globally; when executed in Ethernet port view, these two commands enables/disables LLDP on the current port; when executed in port group view, these two commands enables/disables LLDP on all the ports in the port group.

By default, LLDP is disabled globally or on a port.



### Note

- These two commands are applicable to Layer 2 Ethernet ports, including optical ports and electrical ports.
  - LLDP can take effect only when it is enabled both globally and on a port.
- 

## Examples

# Enable LLDP globally.

```
<Sysname> system-view
[Sysname] lldp enable
```

# Enable LLDP on GigabitEthernet1/0/50.

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/50
[Sysname-GigabitEthernet1/0/50] lldp enable
```

# Enable LLDP for all the ports in port group 1.

```
<Sysname> system-view
[Sysname] port-group manual 1
[Sysname-port-group-manual-1] group-member gigabitethernet1/0/50 to gigabitethernet1/0/52
[Sysname-port-group-manual-1] lldp enable
```

## lldp interval

### Syntax

**lldp interval** *time*

**undo lldp interval**

### View

System view

### Default Level

2: System level

## Parameters

*time*: Interval for sending Advertisement packets, in the range 1 to 100 (in seconds).

## Description

Use the **dldp interval** command to set the interval for sending Advertisement packets.

Use the **undo dldp interval** command to restore the default.

By default, the interval for sending Advertisement packets is 5 seconds.

Note that:

- These two commands apply to all the DLDP-enabled ports.
- Set the interval for sending Advertisement packets to a value not longer than one-third of the STP convergence time. If the interval is too long, STP loops may occur before unidirectional links are torn down; if the interval is too short, network traffic may increase in vain due to excessive Advertisement packets.

## Examples

```
# Set the interval for sending Advertisement packets to 20 seconds.
```

```
<Sysname> system-view  
[Sysname] dldp interval 20
```

## dldp reset

### Syntax

```
dldp reset
```

### View

System view, Ethernet port view, port group view

### Default Level

2: System level

### Parameters

None

### Description

Use the **dldp reset** command to reset DLDP state for ports shut down by DLDP to enable them to perform unidirectional link detect.

When executed in system view, this command applies to all the ports shut down by DLDP; when executed in Ethernet port view, this command applies to the current port; when executed in port group view, this command applies to all the ports in the port group shut down by DLDP.

Related commands: **dldp enable**, **dldp unidirectional-shutdown**.

## Examples

```
# Reset DLDP state for all the ports shut down by DLDP.
```

```
<Sysname> system-view  
[Sysname] dldp reset
```

# Reset DLDLP state for GigabitEthernet1/0/50 (assuming that GigabitEthernet1/0/50 is shut down by DLDLP).

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/50
[Sysname-GigabitEthernet1/0/50] dldp reset
```

# Reset DLDLP state for all the ports in port group 1 shut down by DLDLP.

```
<Sysname> system-view
[Sysname] port-group manual 1
[Sysname-port-group-manual-1] group-member gigabitethernet1/0/50 to gigabitethernet1/0/52
[Sysname-port-group-manual-1] dldp reset
```

## dldp unidirectional-shutdown

### Syntax

```
dldp unidirectional-shutdown { auto | manual }
undo dldp unidirectional-shutdown
```

### View

System view

### Default Level

2: System level

### Parameters

**auto**: Sets the port shutdown mode as auto mode, where, when a unidirectional link is detected, the port involved is shut down by DLDLP.

**manual**: Sets the port shutdown mode as manual mode, where, when a unidirectional link is detected, DLDLP prompts you to shut down the involved port instead of doing so automatically.

### Description

Use the **dldp unidirectional-shutdown** command to set the port shutdown mode.

Use the **undo dldp unidirectional-shutdown** command to restore the default.

By default, the port shutdown mode is auto mode.

Related commands: **dldp work-mode**.

### Examples

# Set the port shutdown mode as auto mode.

```
<Sysname> system-view
[Sysname] dldp unidirectional-shutdown auto
```

## dldp work-mode

### Syntax

```
dldp work-mode { enhance | normal }
undo dldp work-mode
```

## View

System view

## Default Level

2: System level

## Parameters

**enhance:** Specifies the enhanced DLDP mode. When a device operates in this mode and a neighbor entry it maintains expires, the device detects the neighbor before removing the neighbor entry.

**normal:** Specifies the normal DLDP mode. When a device operates in this mode and a neighbor entry it maintains expires, the device removes the neighbor entry directly.

## Description

Use the **dldp work-mode** command to set the DLDP mode.

Use the **undo dldp work-mode** command to restore the default DLDP mode.

By default, a device operates in normal DLDP mode.

Note that:

- In normal DLDP mode, only fiber cross-connected unidirectional links can be detected.
- In enhanced DLDP mode, two types of unidirectional links can be detected. One is fiber cross-connected links. The other refers to fiber pairs with one fiber not connected or disconnected.



### Note

The support for these two commands varies with device models.

---

## Examples

# Configure the device to operate in enhanced DLDP mode.

```
<Sysname> system-view  
[Sysname] dldp work-mode enhance
```

## reset dldp statistics

### Syntax

```
reset dldp statistics [ interface-type interface-number ]
```

### View

User view

### Default Level

1: Monitor level

## Parameters

*interface-type interface-number*: Port type and port number.

## Description

Use the **reset dldp statistics** command to clear the statistics on DLDP packets passing through a port.

If you do not provide the *interface-type* or *interface-number* argument, this command clears the statistics on the DLDP packets passing through all the DLDP-enabled ports.

## Examples

# Clear the statistics on the DLDP packets passing through all the DLDP-enabled ports.

```
<Sysname> reset dldp statistics
```

# Table of Contents

<b>1 LLDP Configuration Commands</b> .....	<b>1-1</b>
LLDP Configuration Commands .....	1-1
display lldp local-information .....	1-1
display lldp neighbor-information .....	1-5
display lldp statistics .....	1-10
display lldp status .....	1-12
display lldp tlv-config .....	1-14
lldp admin-status .....	1-15
lldp check-change-interval .....	1-16
lldp compliance admin-status cdp .....	1-17
lldp compliance cdp .....	1-17
lldp enable .....	1-18
lldp encapsulation snap .....	1-19
lldp fast-count .....	1-20
lldp hold-multiplier .....	1-20
lldp management-address-format string .....	1-21
lldp management-address-tlv .....	1-22
lldp notification remote-change enable .....	1-22
lldp timer notification-interval .....	1-23
lldp timer reinit-delay .....	1-23
lldp timer tx-delay .....	1-24
lldp timer tx-interval .....	1-25
lldp tlv-enable .....	1-25

# 1 LLDP Configuration Commands

---

## LLDP Configuration Commands

### display lldp local-information

#### Syntax

```
display lldp local-information [ global | interface interface-type interface-number ]
```

#### View

Any view

#### Default level

1: Monitor level

#### Parameters

**global**: Displays the global LLDP information.

**interface** *interface-type interface-number*: Specifies a port by its type and number.

#### Description

Use the **display lldp local-information** command to display the global LLDP information or the information contained in the LLDP TLVs to be sent to neighboring devices through a port.

If no keyword or argument is specified, this command displays all the LLDP information to be sent, including the global LLDP information and the LLDP information about the LLDP-enabled ports.

#### Examples

```
# Display all the LLDP information to be sent.
```

```
<Sysname> display lldp local-information
Global LLDP local-information:
  Chassis ID          : 00e0-fc00-5600
  System name        : Sysname
  System description  : Sysname 4800G
  System capabilities supported : Bridge,Router
  System capabilities enabled   : Bridge,Router

MED information
Device class: Connectivity device

(MED inventory information of master board)
HardwareRev          : REV.A
FirmwareRev          : 109
SoftwareRev          : 5.20 Alpha 2101
```

```

SerialNum          : NONE
Manufacturer name  : 3Com
Model name         : Swich
Asset tracking identifier : Unknown
LLDP local-information of port 1[GigabitEthernet1/0/1]:
  Port ID subtype  : Interface name
  Port ID          : GigabitEthernet1/0/1
  Port description : GigabitEthernet1/0/1 Interface

  Management address type      : ipv4
  Management address           : 192.168.102.11
  Management address interface type : IfIndex
  Management address interface ID : 54
  Management address OID       : 0

  Port VLAN ID(PVID): 1

  Port and protocol VLAN ID(PPVID) : 1
  Port and protocol VLAN supported : Yes
  Port and protocol VLAN enabled   : No

  VLAN name of VLAN 1: VLAN 0001

  Auto-negotiation supported : Yes
  Auto-negotiation enabled   : Yes
  OperMau                    : speed(1000)/duplex(Full)

  Power port class           : PSE
  PSE power supported        : Yes
  PSE power enabled          : No
  PSE pairs control ability  : No
  Power pairs                 : Signal
  Port power classification   : Class 0

  Link aggregation supported  : Yes
  Link aggregation enabled    : No
  Aggregation port ID        : 0

  Maximum frame Size: 1536

  MED information
  Media policy type           : Unknown
  Unknown Policy              : Yes
  VLAN tagged                 : No
  Media policy VlanID         : 0
  Media policy L2 priority    : 0

```

```

Media policy Dscp          : 0

PoE PSE power source      : Primary
Port PSE Priority         : Low
Port Available power value: 15.4(w)

```

**Table 1-1** display lldp local-information command output description

Field	Description
Global LLDP local-information	The global LLDP information
Chassis ID	Device MAC address
System name	System name of the device
System description	System description
System capabilities supported	Supported capabilities, which can be: <ul style="list-style-type: none"> <li>• Bridge, indicating switching</li> <li>• Router, indicating routing</li> </ul>
System capabilities enabled	Currently enabled capabilities, which can be: <ul style="list-style-type: none"> <li>• Bridge, indicating switching is currently enabled.</li> <li>• Router, indicating routing is currently enabled.</li> </ul>
PoE device type	PoE device type
MED information	MED information
Device class	MED device type, which can be: <ul style="list-style-type: none"> <li>• Connectivity device, indicating an intermediate device.</li> <li>• Class I, indicating a normal terminal device. All terminal devices that are LLDP-enabled are of this type.</li> <li>• Class II, indicating a media terminal device. A device of this type is media-capable. That is, besides the capabilities of a normal terminal device, it also supports media stream.</li> <li>• Class III, indicating a communication terminal device. A device of this type supports IP communication systems of end user. A device of this type supports all the capabilities of a normal terminal device and a media terminal device and can be used directly by end users.</li> </ul>
(MED inventory information of master board)	MED inventory information of the master board
HardwareRev	Hardware version
FirmwareRev	Firmware version
SoftwareRev	Software version
SerialNum	Serial number
Manufacturer name	Device manufacturer
Model name	Device model
Asset tracking identifier	Asset tracking ID
LLDP local-information of port number [ <i>interface-type interface-number</i> ]	LLDP information about a port
Port ID subtype	Port ID type
Port ID	Port ID

Field	Description
Port description	Port description
Management address type	Management address type
Management address	Management address
Management address interface type	Type of the interface identified by the management address
Management address interface ID	ID of the interface identified by the management address
Management address OID	Management address object ID
Port VLAN ID(PVID)	Port VLAN ID
Port and protocol VLAN ID(PPVID)	Port protocol VLAN ID
Port and protocol VLAN supported	Indicates whether protocol VLAN is supported on the port.
Port and protocol VLAN enabled	Indicates whether protocol VLAN is enabled on the port.
VLAN name of VLAN ID	Name of the VLAN identified by the VLAN ID
Auto-negotiation supported	Indicates whether auto-negotiation is supported on the port.
Auto-negotiation enabled	State of auto-negotiation
OperMau	Current speed and duplex state of the port
PoE supported	Indicates whether or not PoE is supported on this device.
Power port class	PoE device type, which can be : <ul style="list-style-type: none"> <li>• PSE, indicating a power supply device</li> <li>• PD, indicating a powered device</li> </ul>
PSE power supported	Indicates whether or not the device can operate as a PSE.
PSE power enabled	Indicates whether or not the device is operating as a PSE.
PSE pairs control ability	Indicates whether or not the PSE-PD pair control is available.
Power pairs	PoE mode, which can be <b>Signal</b> or <b>Spare</b> .
Port power classification	Port power classification of the PD, which can be: <ul style="list-style-type: none"> <li>• Class0</li> <li>• Class1</li> <li>• Class2</li> <li>• Class3</li> <li>• Class4</li> </ul>
Link aggregation supported	Indicates whether or not link aggregation is supported.
Link aggregation enabled	Indicates whether or not link aggregation is enabled.
Aggregation port ID	Aggregation group ID, which is 0 if link aggregation is not enabled.
Maximum frame Size	Maximum frame size supported
MED information	MED LLDP information

Field	Description
Media policy type	Media policy type, which can be: <ul style="list-style-type: none"> <li>• unknown</li> <li>• voice</li> <li>• voiceSignaling</li> <li>• guestVoice</li> <li>• guestVoiceSignaling</li> <li>• softPhoneVoice</li> <li>• videoconferencing</li> <li>• streamingVideo</li> <li>• videoSignaling</li> </ul>
Unknown Policy	Indicates whether or not the media policy is unknown.
VLAN tagged	Indicates whether packets of the voice VLAN are tagged.
Media Policy VlanID	ID of the voice VLAN
Media Policy L2 priority	Layer 2 priority
Media Policy Dscp	DSCP precedence
Location format	Location format, which can be: <ul style="list-style-type: none"> <li>• Invalid, indicating the format of the location information is invalid.</li> <li>• Coordinate-based LCI, indicating the location information is coordinate-based.</li> <li>• Civic Address LCI, indicating normal address information.</li> <li>• ECS ELIN, indicating telephone number for urgencies.</li> </ul>
Location Information	Location information
PoE PSE power source	PSE type, which can be: <ul style="list-style-type: none"> <li>• Primary, indicating a primary power supply</li> <li>• Backup, indicating a backup power supply</li> </ul>
Port PSE Priority	Port PSE priority, which can be : <ul style="list-style-type: none"> <li>• Unknown</li> <li>• Critical</li> <li>• High</li> <li>• Low</li> </ul>
Port Available power value	PoE power

## display lldp neighbor-information

### Syntax

```
display lldp neighbor-information [ interface interface-type interface-number ] [ brief ]
```

### View

Any view

### Default level

1: Monitor level

## Parameters

**interface** *interface-type interface-number*: Specifies a port by its type and number.

**brief**: Displays the LLDP information in brief.

## Description

Use the **display lldp neighbor-information** command to display the LLDP information about the neighboring devices received through a port.

With no keyword/argument specified, this command displays the LLDP information received through all the ports.

## Examples

# Display the LLDP information received through all the ports.

```
<Sysname> display lldp neighbor-information
LLDP neighbor-information of port 1[GigabitEthernet1/0/1]:
  Neighbor index      : 1
  Update time        : 0 days,0 hours,1 minutes,1 seconds
  Chassis type       : MAC address
  Chassis ID         : 000f-0055-0002
  Port ID type       : Interface name
  Port ID            : GigabitEthernet1/0/1
  Port description   : GigabitEthernet1/0/1 Interface
  System name        : Sysname
  System description : Sysname 4800G
  System capabilities supported : Bridge,Router
  System capabilities enabled   : Bridge,Router

  Management address type      : ipv4
  Management address           : 127.0.0.1
  Management address interface type : IfIndex
  Management address interface ID : Unknown
  Management address OID       : 0

  Port VLAN ID(PVID): 1

  Port and protocol VLAN ID(PPVID) : 1
  Port and protocol VLAN supported : Yes
  Port and protocol VLAN enabled   : No

  VLAN name of VLAN 1: VLAN 0001

  Auto-negotiation supported : Yes
  Auto-negotiation enabled   : Yes
  OperMau                    : speed(1000)/duplex(Full)

  Power port class           : PD
  PSE power supported        : No
```

PSE power enabled : No  
PSE pairs control ability : No  
Power pairs : Signal  
Port power classification : Class 0

Link aggregation supported : Yes  
Link aggregation enabled : No  
Aggregation port ID : 0

Maximum frame Size: 1536

LLDP neighbor-information of port 2[GigabitEthernet1/0/2]:

Neighbor index : 1  
Update time : 0 days,0 hours,1 minutes,1 seconds  
Chassis type : MAC address  
Chassis ID : 000f-0055-0002  
Port ID type : Interface name  
Port ID : GigabitEthernet1/0/2  
Port description : GigabitEthernet1/0/2 Interface  
System name : Sysname  
System description : Sysname 4800G  
System capabilities supported : Bridge,Router  
System capabilities enabled : Bridge,Router

Management address type : ipv4  
Management address : 127.0.0.1  
Management address interface type : IfIndex  
Management address interface ID : Unknown  
Management address OID : 0

Port VLAN ID(PVID): 1

Port and protocol VLAN ID(PPVID) : 1  
Port and protocol VLAN supported : Yes  
Port and protocol VLAN enabled : No

VLAN name of VLAN 1: VLAN 0001

Auto-negotiation supported : Yes  
Auto-negotiation enabled : Yes  
OperMau : speed(1000)/duplex(Full)

Power port class : PD  
PSE power supported : No  
PSE power enabled : No  
PSE pairs control ability : No  
Power pairs : Signal

Port power classification : Class 0

Link aggregation supported : Yes

Link aggregation enabled : No

Aggregation port ID : 0

Maximum frame Size: 1536

**Table 1-2** display lldp neighbor-information command output description

Field	Description
LLDP neighbor-information of Port number [ <i>interface-type interface number</i> ]	LLDP information received through a specific port
Neighbor index	Neighbor index
Update time	Time when the LLDP information about a neighboring device is latest updated.
Chassis type	Chassis information, which can be: <ul style="list-style-type: none"><li>• Chassis component</li><li>• Interface alias</li><li>• Port component</li><li>• MAC address</li><li>• Network address</li><li>• Interface name</li><li>• Locally assigned (indicating the local configuration)</li></ul>
Chassis ID	Value of chassis type
Port ID type	Port information, which can be: <ul style="list-style-type: none"><li>• Interface alias</li><li>• Port component</li><li>• MAC address</li><li>• Network Address</li><li>• Interface name</li><li>• Agent circuit ID</li><li>• Locally assigned (indicating the local configuration)</li></ul>
Port ID	Value of port ID type
Port description	Port description
System name	System name of the neighboring device
System description	System description of the neighboring device
System capabilities supported	Capabilities supported on the neighboring device, which can be: <ul style="list-style-type: none"><li>• Bridge, indicating switching</li><li>• Router, indicating routing</li></ul>
System capabilities enabled	Capabilities currently enabled on the neighboring device, which can be: <ul style="list-style-type: none"><li>• Bridge, indicating switching is currently enabled.</li><li>• Router, indicating routing is currently enabled.</li></ul>
Management address type	Management address type
Management address	Management address

Field	Description
Management address interface type	Type of the interface identified by the management address
Management address interface ID	Management address interface ID
Management address OID	Management address object ID
Port VLAN ID	Port VLAN ID
Port and protocol VLAN ID(PPVID)	Port protocol VLAN ID
Port and protocol VLAN supported	Indicates whether protocol VLAN is supported.
Port and protocol VLAN enabled	Indicates whether protocol VLAN is enabled.
VLAN name of VLAN 1	Name of the port VLAN
Auto-negotiation supported	Indicates whether auto-negotiation is supported.
Auto-negotiation enabled	State of auto-negotiation
OperMau	Current speed and duplex state
Power port class	PoE device type, which can be: <ul style="list-style-type: none"> <li>• PSE, indicating a power supply device.</li> <li>• PD, indicating a powered device.</li> </ul>
PSE power supported	Indicates whether or not the device can operate as a PSE.
PSE power enabled	Indicates whether or not the device is operating as a PSE.
PSE pairs control ability	Indicates whether or not the PSE-PD pair control is available.
Power pairs	PoE mode, which can be <b>Signal</b> or <b>Spare</b> .
Port power classification	Port power classification of the PD, which can be the following: <ul style="list-style-type: none"> <li>• Class0</li> <li>• Class1</li> <li>• Class2</li> <li>• Class3</li> <li>• Class4</li> </ul>
Link aggregation supported	Indicates whether or not link aggregation is supported.
Link aggregation enabled	Indicates whether or not link aggregation is enabled.
Aggregation port ID	Aggregation group ID, which is 0 if link aggregation is not enabled.
Maximum frame Size	Maximum frame size supported
Location format	Location information format, which can be: <ul style="list-style-type: none"> <li>• Invalid, indicating the format of the location information is invalid.</li> <li>• Coordinate-based LCI, indicating the location information is coordinate-based.</li> <li>• Civic Address LCI, indicating normal address information.</li> <li>• ECS ELIN, indicating a telephone for urgencies.</li> </ul>
Location Information	Location information
PoE PSE power source	PSE type, which can be: <ul style="list-style-type: none"> <li>• Primary, indicating a primary power supply</li> <li>• Backup, indicating a backup power supply</li> </ul>
PoE service type	PoE service type

Field	Description
Port PSE Priority	Port PSE priority, which can be: <ul style="list-style-type: none"> <li>• Unknown</li> <li>• Critical</li> <li>• High</li> <li>• Low</li> </ul>
Available power value	PoE power
Unknown basic TLV	Unknown basic TLV
TLV type	Unknown basic TLV type
TLV information	Information contained in the unknown basic TLV type
Unknown organizationally-defined TLV	Unknown organization-defined TLV
TLV OUI	OUI of the unknown organization-defined TLV
TLV subtype	Unknown organization-defined TLV subtype
Index	Unknown organization index
TLV information	Information contained in unknown organization-defined TLV

## display lldp statistics

### Syntax

**display lldp statistics** [ **global** | **interface** *interface-type interface-number* ]

### View

Any view

### Default level

1: Monitor level

### Parameters

**global**: Displays the global LLDP statistics.

**interface** *interface-type interface-number*: Specifies a port by its type and number.

### Description

Use the **display lldp statistics** command to display the global LLDP statistics or the LLDP statistics of a port.

If no keyword/argument is specified, this command displays all the LLDP statistics.

### Examples

# Display all the LLDP statistics.

```
<Sysname> display lldp statistics
```

```
LLDP statistics global Information :
```

```
LLDP neighbor information last change time : 0 days, 0 hours, 4 minutes, 40 seconds
```

```
The number of LLDP neighbor information inserted : 1
```

```

The number of LLDP neighbor information deleted      : 1
The number of LLDP neighbor information dropped      : 0
The number of LLDP neighbor information aged out    : 1

```

LLDP statistics Information of port 1 [GigabitEthernet1/0/1]:

```

The number of LLDP frames transmitted              : 0
The number of LLDP frames received                 : 0
The number of LLDP frames discarded                 : 0
The number of LLDP error frames                    : 0
The number of LLDP TLVs discarded                  : 0
The number of LLDP TLVs unrecognized               : 0
The number of LLDP neighbor information aged out    : 0
The number of CDP frames transmitted                : 0
The number of CDP frames received                  : 0
The number of CDP frames discarded                 : 0
The number of CDP error frames                     : 0

```

**Table 1-3 display lldp statistics** command output description

Field	Description
LLDP statistics global information	Global LLDP statistics
LLDP neighbor information last change time	Time the neighbor information is latest updated
The number of LLDP neighbor information inserted	Number of times of adding neighbor information
The number of LLDP neighbor information deleted	Number of times of removing neighbor information
The number of LLDP neighbor information dropped	Number of times of dropping neighbor information due to lack of available memory space
The number of LLDP neighbor information aged out	Number of the neighbor information entries that have aged out
LLDP statistics Information of port number [ <i>interface-type interface-number</i> ]	LLDP statistics of a port
The number of LLDP frames transmitted	Total number of the LLDP frames transmitted through the port
The number of LLDP frames received	Total number of the LLDP frames received through the port
The number of LLDP frames discarded	Total number of the LLDP frames dropped on the port
The number of LLDP error frames	Total number of the LLDP error frames received through the port
The number of LLDP TLVs discarded	Total number of the LLDP TLVs dropped on the port
The number of LLDP TLVs unrecognized	Total number of the LLDP TLVs that cannot be recognized on the port
The number of LLDP neighbor information aged out	Number of the LLDP neighbor information entries that have aged out on the port
The number of CDP frames transmitted	Total number of the CDP frames transmitted on the port

Field	Description
The number of CDP frames received	Total number of the CDP frames received on the port
The number of CDP frames discarded	Total number of the CDP frames dropped on the port
The number of CDP error frames	Total number of the CDP error frames received on the port

## display lldp status

### Syntax

**display lldp status** [ **interface** *interface-type interface-number* ]

### View

Any view

### Default level

1: Monitor level

### Parameters

**interface** *interface-type interface-number*: Specifies a port by its type and number.

### Description

Use the **display lldp status** command to display the LLDP status of a port.

If no port is specified, this command displays the LLDP status of all the ports.

### Examples

# Display the LLDP status of all the ports.

```
<Sysname> display lldp status
Global status of LLDP: Enable
The current number of LLDP neighbors: 0
The current number of CDP neighbors: 0
LLDP neighbor information last changed time : 0 days, 0 hours, 4 minutes, 40 seconds
Transmit interval           : 30s
Hold multiplier             : 4
Reinit delay                : 2s
Transmit delay              : 2s
Trap interval               : 5s
Fast start times            : 3

Port 1 [GigabitEthernet1/0/1] :
Port status of LLDP         : Enable
Admin status                 : Tx_Rx
Trap flag                    : No
Roll time                    : 0s

Number of neighbors         : 5
```

```

Number of MED neighbors      : 2
Number of CDP neighbors     : 0
Number of sent optional TLV : 12
Number of received unknown TLV : 5

```

**Table 1-4 display lldp status command output description**

Field	Description
Global status of LLDP	Indicating whether or not LLDP is globally enabled
The current number of LLDP neighbors	Total number of the LLDP neighbor devices
The current number of CDP neighbors	The current number of CDP neighbors
LLDP neighbor information last changed time	The last changed time of LLDP neighbor information
Transmit interval	Interval to send LLDPDU
Hold multiplier	TTL multiplier
Reinit delay	Initialization delay
Transmit delay	Delay period to send LLDPDUs
Trap interval	Interval to send traps
Fast start times	Number of the LLDPDUs to be sent successively when a new neighboring device is detected
Port number [ <i>interface-type interface-number</i> ]	Port LLDP status
Port status of LLDP	Indicates whether or not LLDP is enabled on the port.
Admin status	LLDP mode of the port, which can be: <ul style="list-style-type: none"> <li>• TxRx. A port in this mode sends and receives LLDPDUs.</li> <li>• Rx_Only. A port in this mode receives LLDPDUs only.</li> <li>• Tx_Only. A port in this mode sends LLDPDUs only.</li> <li>• Disable. A port in this mode does not send or receive LLDPDUs.</li> </ul>
Trap Flag	Indicates whether or not trap is enabled.
Roll time	LLDP polling interval. A value of 0 indicates LLDP polling is disabled.
Number of neighbors	Number of the LLDP neighbors connecting to the port
Number of MED neighbors	Number of the MED neighbors connecting to the port
Number of CDP neighbors	Number of the CDP neighbors connecting to the port
Number of sent optional TLV	Number of the optional TLVs contained in an LLDPDU sent through the port
Number of received unknown TLV	Number of the unknown TLVs contained in a received LLDPDU

## display lldp tlv-config

### Syntax

```
display lldp tlv-config [ interface interface-type interface-number ]
```

### View

Any view

### Default level

1: Monitor level

### Parameters

**interface** *interface-type interface-number*. Specifies a port by its type and number.

### Description

Use the **display lldp tlv-config** command to display the TLVs that are currently sent through a port.

If no port is specified, this command displays all the TLVs that are currently sent through all the ports.

### Examples

# Display all the TLVs that are currently sent through the port GigabitEthernet1/0/2.

```
<Sysname> display lldp tlv-config interface GigabitEthernet 1/0/2
```

```
LLDP tlv-config of port 2 [GigabitEthernet1/0/2] :
```

NAME	STATUS	DEFAULT
------	--------	---------

Basic optional TLV :

Port Description TLV	YES	YES
----------------------	-----	-----

System Name TLV	YES	YES
-----------------	-----	-----

System Description TLV	YES	YES
------------------------	-----	-----

System Capabilities TLV	YES	YES
-------------------------	-----	-----

Management Address TLV	YES	YES
------------------------	-----	-----

IEEE 802.1 extend TLV :

Port VLAN ID TLV	YES	YES
------------------	-----	-----

Port And Protocol VLAN ID TLV	YES	YES
-------------------------------	-----	-----

VLAN Name TLV	YES	YES
---------------	-----	-----

IEEE 802.3 extend TLV :

MAC-Physic TLV	YES	YES
----------------	-----	-----

Power via MDI TLV	YES	YES
-------------------	-----	-----

Link Aggregation TLV	YES	YES
----------------------	-----	-----

Maximum Frame Size TLV	YES	YES
------------------------	-----	-----

LLDP-MED extend TLV :

Capabilities TLV	YES	YES
------------------	-----	-----

Network Policy TLV	YES	YES
--------------------	-----	-----

Location Identification TLV	NO	NO
-----------------------------	----	----

Extended Power via MDI TLV	YES	YES
----------------------------	-----	-----

Inventory TLV	YES	YES
---------------	-----	-----

**Table 1-5 display lldp tlv-config** command output description

Field	Description
LLDP tlv-config of port number [ <i>interface-type interface-number</i> ]	TLVs that are currently sent through a port
NAME	TLV type
STATUS	Indicates whether or not TLVs of a specific type are currently sent through a port
DEFAULT	Indicates whether or not TLVs of a specific type are sent through a port by default
Basic optional TLV	Basic TLVs, including: <ul style="list-style-type: none"> <li>• Port description TLV</li> <li>• System name TLV</li> <li>• System description TLV</li> <li>• System capabilities TLV</li> <li>• Management address TLV</li> </ul>
IEEE 802.1 extended TLV	IEEE 802.1 extended TLVs, including: <ul style="list-style-type: none"> <li>• Port VLAN ID TLV</li> <li>• Port and protocol VLAN ID TLV</li> <li>• VLAN name TLV</li> </ul>
IEEE 802.3 extended TLV	IEEE 802.3 extended TLVs, including: <ul style="list-style-type: none"> <li>• MAC-Physic TLV</li> <li>• Power via MDI TLV</li> <li>• Link aggregation TLV</li> <li>• Maximum frame size TLV</li> </ul>
LLDP-MED extend TLV	MED related LLDP TLVs, including: <ul style="list-style-type: none"> <li>• Capabilities TLV</li> <li>• Network Policy TLV</li> <li>• Location Identification TLV</li> <li>• Extended Power via MDI TLV</li> <li>• Inventory TLV, which can be hardware revision TLV, firmware revision TLV, software revision TLV, serial number TLV, manufacturer name TLV, model name TLV, and asset id TLV.</li> </ul>

## Ildp admin-status

### Syntax

```
lldp admin-status { disable | rx | tx | txrx }
```

```
undo lldp admin-status
```

### View

Ethernet interface view, port group view

### Default level

2: System level

## Parameters

**disable**: Specifies the **Disable** mode. A port in this mode does not send or receive LLDPDUs.

**rx**: Specifies the **Rx** mode. A port in this mode receives LLDPDUs only.

**tx**: Specifies the **Tx** mode. A port in this mode sends LLDPDUs only.

**txrx**: Specifies the **TxRx** mode. A port in this mode sends and receives LLDPDUs.

## Description

Use the **lldp admin-status** command to specify the LLDP operating mode for a port or all the ports in a port group.

Use the **undo lldp admin-status** command to restore the default LLDP operating mode.

The default LLDP operating mode is **TxRx**.

## Examples

# Configure the LLDP operating mode as **Rx** for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp admin-status rx
```

## lldp check-change-interval

### Syntax

**lldp check-change-interval** *value*

**undo lldp check-change-interval**

### View

Ethernet interface view, port group view

### Default level

2: System level

### Parameters

*value*: LLDP polling interval to be set, in the range 1 to 30 (in seconds).

### Description

Use the **lldp check-change-interval** command to enable LLDP polling and set the polling interval.

Use the **undo lldp check-change-interval** command to restore the default.

By default, LLDP polling is disabled.

With LLDP polling enabled, LLDP detects for local configuration changes periodically. A local configuration change triggers LLDPDU sending, through which neighboring devices can be informed of the configuration change timely.

### Examples

# Enable LLDP polling on GigabitEthernet 1/0/1, setting the polling interval to 30 seconds.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp check-change-interval 30
```

## Ildp compliance admin-status cdp

### Syntax

```
lldp compliance admin-status cdp { disable | txrx }
```

### View

Ethernet interface view, port group view

### Default Level

2: System level

### Parameters

**disable**: Specifies the disable mode, where CDP-compatible LLDP neither receives nor transmits CDP packets.

**txrx**: Specifies the TxRx mode, where CDP-compatible LLDP can send and receive CDP packets.

### Description

Use the **lldp compliance admin-status cdp** command to configure the operation mode of CDP-compatible LLDP on a port or port group.

By default, CDP-compatible LLDP operates in disable mode.

To have your device work with Cisco IP phones, you must enable CDP-compatible LLDP globally and then configure CDP-compatible LLDP to work in TxRx mode on the specified port(s).



#### Note

The command may be supported depending on your device.

---

### Examples

```
# Configure CDP-compatible LLDP to operate in TxRx mode on GigabitEthernet 1/0/1.
```

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp compliance admin-status cdp txrx
```

## Ildp compliance cdp

### Syntax

```
lldp compliance cdp
undo lldp compliance cdp
```

## View

System view

## Default Level

2: System level

## Parameters

None

## Description

Use the **lldp compliance cdp** command to enable global CDP compatibility.

Use the **undo lldp compliance cdp** command to restore the default.

By default, global CDP compatibility is disabled.

Note that, as the maximum TTL allowed by CDP is 255 seconds, your TTL configuration, that is, the product of the TTL multiplier and the LLDPDU sending interval, must be less than 255 seconds for CDP-compatible LLDP to work properly with Cisco IP phones.



### Note

The command may be supported depending on your device.

---

Related commands: **lldp hold-multiplier**, **lldp timer tx-interval**.

## Examples

# Enable LLDP to be compatible with CDP globally.

```
<Sysname> system-view  
[Sysname] lldp compliance cdp
```

## lldp enable

### Syntax

```
lldp enable  
undo lldp enable
```

### View

System view, Ethernet interface view, port group view

### Default level

2: System level

### Parameters

None

## Description

Use the **lldp enable** command to enable LLDP.

Use the **undo lldp enable** command to disable LLDP.

By default, LLDP is both enabled globally and on a port.

Note that LLDP takes effect on a port only when it is enabled both globally and on the port.

## Examples

```
# Disable LLDP on GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo lldp enable
```

## lldp encapsulation snap

### Syntax

```
lldp encapsulation snap
undo lldp encapsulation [ snap ]
```

### View

Ethernet interface view, port group view

### Default level

2: System level

### Parameters

None

## Description

Use the **lldp encapsulation snap** command to configure the encapsulation format for LLDPDUs as SNAP on a port or a group of ports.

Use the **undo lldp encapsulation** command to restore the default encapsulation format for LLDPDUs.

By default, Ethernet II encapsulation applies.



### Note

The command does not apply to LLDP-CDP packets, which use only SNAP encapsulation.

---

## Examples

```
# Configure the encapsulation format for LLDPDUs as SNAP on GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp encapsulation snap
```

## Ildp fast-count

### Syntax

```
ildp fast-count value  
undo ildp fast-count
```

### View

System view

### Default level

2: System level

### Parameters

*value*: Number of the LLDPDU's to be sent successively when a new neighboring device is detected. This argument ranges from 1 to 10.

### Description

Use the **ildp fast-count** command to set the number of the LLDPDU's to be sent successively when a new neighboring device is detected.

Use the **undo ildp fast-count** command to restore the default.

By default, the number is 3.

### Examples

# Configure to send four LLDP successively when a new neighboring device is detected.

```
<Sysname> system-view  
[Sysname] ildp fast-count 4
```

## Ildp hold-multiplier

### Syntax

```
ildp hold-multiplier value  
undo ildp hold-multiplier
```

### View

System view

### Default level

2: System level

### Parameters

*value*: TTL multiplier, in the range 2 to 10.

### Description

Use the **ildp hold-multiplier** command to set the TTL multiplier.

Use the **undo ildp hold-multiplier command** to restore the default.

The TTL multiplier defaults to 4.

You can set the TTL of the local device information by configuring the TTL multiplier.

The TTL of the information about a device is determined by the following expression:

$$\text{TTL multiplier} \times \text{LLDPDU sending interval}$$

You can set the TTL of the local device information by configuring the TTL multiplier. Note that the TTL can be up to 65535 seconds. TTLs longer than it will be rounded off to 65535 seconds.

To enable local device information to be updated on neighboring devices before being aged out, make sure the interval to send LLDPDUs is shorter than the TTL of the local device information.

## Examples

```
# Set the TTL multiplier to 6.
```

```
<Sysname> system-view
```

```
[Sysname] lldp hold-multiplier 6
```

## Ildp management-address-format string

### Syntax

```
lldp management-address-format string
```

```
undo lldp management-address-format
```

### View

Ethernet interface view, port group view

### Default Level

2: System level

### Parameters

None

### Description

Use the **lldp management-address-format string** command to configure the encapsulation format of the management address as strings in TLVs.

Use the **undo lldp management-address-format** command to restore the default.

By default, the management address is encapsulated in the form of numbers in TLVs.

## Examples

```
# Configure GigabitEthernet 1/0/1 to encapsulate the management address in the form of strings in management address TLVs.
```

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] lldp management-address-format string
```

## Ildp management-address-tlv

### Syntax

```
ildp management-address-tlv [ ip-address ]  
undo ildp management-address-tlv
```

### View

Ethernet interface view, port group view

### Default level

2: System level

### Parameters

*ip-address*: Management address to be set.

### Description

Use the **ildp management-address-tlv** command to enable the management address sending. This command also sets the management address.

Use the **undo ildp management-address-tlv** command to disable management address sending.

By default, the management address is sent through LLDPDUs, and the management address is the primary IP address of the VLAN with the least VLAN ID among the VLANs whose packets are permitted on the port. If the primary IP address is not configured, the management address is 127.0.0.1. For information about VLAN, refer to *VLAN Configuration* in the *Access Volume*.

Note that an LLDPDU carries only one management address. If you set the management address repeatedly, the latest one takes effect.

### Examples

```
# Set the management address to 192.6.0.1 for GigabitEthernet 1/0/1.
```

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] ildp management-address-tlv 192.6.0.1
```

## Ildp notification remote-change enable

### Syntax

```
ildp notification remote-change enable  
undo ildp notification remote-change enable
```

### View

Ethernet interface view, port group view

### Default level

2: System level

## Parameters

None

## Description

Use the **lldp notification remote-change enable** command to enable trap for a port or all the ports in a port group.

Use the **undo lldp notification remote-change enable** command to restore the default.

By default, trap is disabled on a port.

## Examples

```
# Enable trap for GigabitEthernet 1/0/1.
```

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] lldp notification remote-change enable
```

## Ildp timer notification-interval

### Syntax

```
lldp timer notification-interval value
```

```
undo lldp timer notification-interval
```

### View

System view

### Default level

2: System level

### Parameters

*value*: Interval to send trap messages, in the range 5 to 3600 (in seconds).

### Description

Use the **lldp timer notification-interval** command to set the interval to send trap messages.

Use the **undo lldp timer notification-interval** command to restore the default.

By default, the interval to send trap messages is 5 seconds.

### Examples

```
# Set the interval to send trap messages to 8 seconds.
```

```
<Sysname> system-view
```

```
[Sysname] lldp timer notification-interval 8
```

## Ildp timer reinit-delay

### Syntax

```
lldp timer reinit-delay value
```

```
undo lldp timer reinit-delay
```

## View

System view

## Default level

2: System level

## Parameters

*value*: Initialization delay period to be set, in the range 1 to 10 (in seconds).

## Description

Use the **lldp timer reinit-delay** command to set the initialization delay period.

Use the **undo lldp timer reinit-delay** command to restore the default.

By default, the initialization delay period is 2 seconds.

## Examples

```
# Set the initialization delay period to 4 seconds.
```

```
<Sysname> system-view  
[Sysname] lldp timer reinit-delay 4
```

## lldp timer tx-delay

### Syntax

```
lldp timer tx-delay value
```

```
undo lldp timer tx-delay
```

### View

System view

### Default level

2: System level

### Parameters

*value*: Delay period to send LLDPDUs, in the range 1 to 8192 (in seconds).

### Description

Use the **lldp timer tx-delay** command to set the delay period to send LLDPDUs.

Use the **undo lldp timer tx-delay** command to restore the default.

By default, the delay period to send LLDPDUs is 2 seconds.

### Examples

```
# Set the delay period to send LLDPDUs to 4 seconds.
```

```
<Sysname> system-view  
[Sysname] lldp timer tx-delay 4
```

## Ildp timer tx-interval

### Syntax

```
lldp timer tx-interval value  
undo lldp timer tx-interval
```

### View

System view

### Default level

2: System level

### Parameters

*value*: Interval to send LLDPDUs, in the range 5 to 32768 (in seconds).

### Description

Use the **lldp timer tx-interval** command to set the interval to send LLDPDUs.

Use the **undo lldp timer tx-interval** command to restore the default.

By default, the interval to send LLDPDUs is 30 seconds.

To enable local device information to be updated on neighboring devices before being aged out, make sure the interval to send LLDPDUs is shorter than the TTL of the local device information.

### Examples

```
# Set the interval to send LLDPDUs to 20 seconds.
```

```
<Sysname> system-view  
[Sysname] lldp timer tx-interval 20
```

## Ildp tlv-enable

### Syntax

```
lldp tlv-enable { basic-tlv { all | port-description | system-capability | system-description |  
system-name } | dot1-tlv { all | port-vlan-id | protocol-vlan-id [ vlan-id ] | vlan-name [ vlan-id ] } |  
dot3-tlv { all | link-aggregation | mac-physic | max-frame-size | power } | med-tlv { all | capability |  
inventory | location-id { civic-address device-type country-code { ca-type ca-value }&<1-10> |  
elin-address tel-number } | network-policy | power-over-ethernet } }  
undo lldp tlv-enable { basic-tlv { all | port-description | system-capability | system-description |  
system-name } | dot1-tlv { all | port-vlan-id | protocol-vlan-id | vlan-name } | dot3-tlv { all |  
link-aggregation | mac-physic | max-frame-size | power } | med-tlv { all | capability | inventory |  
location-id | network-policy | power-over-ethernet } }
```

### View

Ethernet interface view, port group view

### Default level

2: System level

## Parameters

**all:** Sends all the basic LLDP TLVs, all the IEEE 802.1 defined LLDP TLVs, or all the IEEE 802.3 defined LLDP TLVs; or sends all the MED related LLDP TLVs except location identification TLVs.

**basic-tlv:** Sends basic LLDP TLVs.

**port-description:** Sends port description TLVs.

**system-capability:** Sends system capabilities TLVs.

**system-description:** Sends system description TLVs.

**system-name:** Sends system name TLVs.

**dot1-tlv:** Sends IEEE 802.1 defined LLDP TLVs.

**port-vlan-id:** Sends port VLAN ID TLVs.

**protocol-vlan-id:** Sends port and protocol VLAN ID TLVs.

**vlan-name:** Sends VLAN name TLVs.

*vlan-id:* ID of the VLAN the TLVs (port and protocol VLAN ID TLVs or VLAN name TLVs) concerning which are to be sent, in the range 1 to 4094. This argument defaults to the least protocol VLAN ID.

**dot3-tlv:** Sends IEEE 802.3 defined LLDP TLVs.

**link-aggregation:** Sends link aggregation group TLVs.

**mac-physic:** Sends MAC/PHY configuration/status TLVs.

**max-frame-size:** Sends maximum frame size TLVS.

**power:** Sends power via MDI TLVs.

**med-tlv:** Sends MED related LLDP TLVs.

**capability:** Sends LLDP-MED capabilities TLVs.

**inventory:** Sends hardware revision TLVs, firmware revision TLVs, software revision TLVs, serial number TLVs, manufacturer name TLVs, model name TLVs, and asset ID TLVs.

**location-id:** Sends location identification TLVS.

**civic-address:** Inserts the address information about the intermediate device in location identification TLVs .

*device-type:* Device type value. A value of 0 specifies DHCP server; a value of 1 specifies switch, and a value of 2 specifies LLDP-MED endpoint.

*country-code:* Country code, conforming to ISO 3166.

{ *ca-type ca-value* }&<1-10>: Configures address information, where *ca-type* represents the address information type, in the range 0 to 255, *ca-value* represents address information, a string of 1 to 250 characters, and &<1-10> indicates that you can enter up to ten such parameters.

**elin-address:** Inserts telephone numbers for urgencies in location identification TLVs.

*tel-number:* Telephone number for urgencies, a string of 10 to 25 characters.

**network-policy:** Sends network policy TLVs.

**power-over-ethernet:** Sends extended power-via-MDI TLVs.

## Description

Use the **lldp tlv-enable** command to enable the sending of specific TLVs for a port or all the ports in a port group.

Use the **undo lldp tlv-enable** command to disable the sending of specific TLVs.

By default, all the TLVs except location identification TLVs are sent.

Note that:

- To enable MED related LLDP TLV sending, you need to enable LLDP-MED capabilities TLV sending first. Conversely, to disable LLDP-MED capabilities TLV sending, you need to disable the sending of other MED related LLDP TLV.
- To disable MAC/PHY configuration/status TLV sending, you need to disable LLDP-MED capabilities TLV sending first.
- Specifying the **all** keyword for basic LLDP TLVs and organization defined LLDP TLVs (including IEEE 802.1 defined LLDP TLVs and IEEE 802.3 defined LLDP TLVs) enables sending of all the corresponding LLDP TLVs. For MED related LLDP TLVs, the **all** keyword enables sending of all the MED related LLDP TLVs except location identification TLVs.
- Enabling the sending of LLDP-MED capabilities TLVs also enables the sending of MAC/PHY configuration/status TLVs.
- You can specify to send multiple types of TLVs by executing the **lldp tlv-enable** command repeatedly.

## Examples

# Enable the sending of link aggregation group TLVs on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp tlv-enable dot3-tlv link-aggregation
```

# Table of Contents

<b>1 Smart Link Configuration Commands</b> .....	<b>1-1</b>
Smart Link Configuration Commands.....	1-1
display smart-link flush.....	1-1
display smart-link group.....	1-2
flush enable.....	1-3
port.....	1-4
port smart-link group.....	1-4
preemption delay.....	1-5
preemption mode.....	1-6
protected-vlan.....	1-7
reset smart-link statistics.....	1-8
smart-link flush enable.....	1-8
smart-link group.....	1-9

# 1 Smart Link Configuration Commands

---

## Smart Link Configuration Commands

### display smart-link flush

#### Syntax

display smart-link flush

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

None

#### Description

Use the **display smart-link flush** command to display information about the received flush messages.

#### Examples

# Display information about the received flush messages.

```
<Sysname> display smart-link flush
Received flush packets                : 10
Receiving interface of the last flush packet : GigabitEthernet1/0/1
Receiving time of the last flush packet   : 19:19:03 2008/06/27
Device ID of the last flush packet       : 000f-e200-8500
Control VLAN of the last flush packet    : 1
```

**Table 1-1** display smart-link flush command output description

Field	Description
Received flush packets	Total number of received flush messages
Receiving interface of the last flush packet	The port that received the last flush message
Receiving time of the last flush packet	Time when the last flush message was received
Device ID of the last flush packet	Device ID carried in the last flush message
Control VLAN of the last flush packet	Control VLAN ID carried in the last flush message

## display smart-link group

### Syntax

```
display smart-link group { group-id | all }
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*group-id*: Smart link group ID, in the range 1 to 26.

**all**: Displays information about all smart link groups.

### Description

Use the **display smart-link group** command to display information about the specified or all smart link groups.

### Examples

```
# Display information about smart link group 1.
```

```
<Sysname> display smart-link group 1
Smart link group 1 information:
Device ID: 000f-e200-8500
Preemption mode: ROLE
Preemption delay: 1(s)
Control VLAN: 1
Protected VLAN: Reference Instance 0 to 2, 4
Member                Role    State   Flush-count  Last-flush-time
-----
GigabitEthernet1/0/1  MASTER ACTVIE   1           16:37:20 2008/04/21
GigabitEthernet1/0/2  SLAVE  STANDBY 2           17:45:20 2008/04/21
```

**Table 1-2** display smart-link group command output description

Field	Description
Smart link group 1 information	Information about smart link group 1
Device ID	Device ID
Preemption mode	Preemption mode, which can be <b>role</b> for preemption enabled or none for preemption disabled.
Preemption delay	The delay in seconds that the master port experiences before it can preempt the slave port in active state in role preemption mode.
Control-VLAN	Control VLAN ID

Field	Description
Protected VLAN	Protected VLANs of the smart link group. Referenced MSTIs are displayed here. To view the VLANs mapped to the referenced MSTIs, use the <b>display stp region-configuration</b> command.
Member	Member of the smart link group
Role	Port role: master or slave
State	Port state: active or standby
Flush-count	Number of transmitted flush messages
Last-flush-time	Time when the last flush message was transmitted (NA indicates that no flush message has been transmitted)

## flush enable

### Syntax

**flush enable** [ **control-vlan** *vlan-id* ]

**undo flush enable**

### View

Smart link group view

### Default Level

2: System level

### Parameters

**control-vlan** *vlan-id*: Specifies the control VLAN used for transmitting flush messages. The *vlan-id* argument ranges from 1 to 4094. If no VLAN is specified, VLAN 1 applies by default.

### Description

Use the **flush enable** command to enable flush update.

Use the **undo flush enable** command to disable flush update.

By default, flush update is enabled for smart link groups and VLAN 1 is used for flush message transmission.

Different smart link groups must be configured with different control VLANs.

Related commands: **smart-link flush enable**.

### Examples

# Enable flush update for smart link group 1.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] flush enable
```

## port

### Syntax

```
port interface-type interface-number { master | slave }  
undo port interface-type interface-number
```

### View

Smart link group view

### Default Level

2: System level

### Parameters

*interface-type interface-number*: Port type and port number.

**master**: Specifies a port as the master port.

**slave**: Specifies a port as the slave port.

### Description

Use the **port** command to assign the specified port as the master or slave port of the current smart link group.

Use the **undo port** command to remove the specified port from the smart link group.

Note that:

- Disable STP and RRPP on the ports you want to add to the smart link group, and make sure that the ports are not member ports of any aggregation group or service loopback group. On the other hand, you cannot enable STP or RRPP on a smart link group member port or assign a smart link group member port to an aggregation group or service loopback group.
- You can assign a port to a smart link group with the **port smart-link group** command in Ethernet interface view or Layer-2 aggregate interface view.

Related commands: **port smart-link group**.

### Examples

```
# Configure GigabitEthernet 1/0/1 as the slave port of smart link group 1.
```

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] undo stp enable  
[Sysname-GigabitEthernet1/0/1] quit  
[Sysname] smart-link group 1  
[Sysname-smlk-group1] protected-vlan reference-instance 0  
[Sysname-smlk-group1] port gigabitethernet 1/0/1 slave
```

## port smart-link group

### Syntax

```
port smart-link group group-id { master | slave }  
undo port smart-link group group-id
```

## View

Ethernet interface view, Layer-2 aggregate interface view

## Default Level

2: System level

## Parameters

*group-id*: Smart link group ID, in the range 1 to 26.

**master**: Specifies the port as the master port.

**slave**: Specifies the port as the slave port.

## Description

Use the **port smart-link group** command to configure the current port as a member of the specified smart link group.

Use the **port smart-link group** command to remove the port from the specified smart link group.

Note that:

- Disable STP and RRPP on the ports you want to add to the smart link group, and make sure that the ports are not member ports of any aggregation group or service loopback group. On the other hand, you cannot enable STP or RRPP on a smart link group member port or assign a smart link group member port to an aggregation group or service loopback group.
- You can assign a port to a smart link group with the **port** command in smart link group view.

Related commands: **port**.

## Examples

# Configure GigabitEthernet1/0/1 as the master port of smart link group 1.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 0
[Sysname-smlk-group1] quit
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] undo stp enable
[Sysname-GigabitEthernet1/0/1] port smart-link group 1 master
```

# Configure Layer-2 aggregate interface 1 as the master port of smart link group 1.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 0
[Sysname-smlk-group1] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] undo stp enable
[Sysname-Bridge-Aggregation1] port smart-link group 1 master
```

## preemption delay

### Syntax

**preemption delay** *delay-time*

## undo preemption delay

### View

Smart link group view

### Default Level

2: System level

### Parameters

*delay-time*: Preemption delay (in seconds), in the range of 0 to 300.

### Description

Use the **preemption delay** command to set the preemption delay. When role preemption is enabled, after the preemption delay is set, the master port waits for some time before taking over, so as to collaborate with the switchover of upstream devices.

Use the **undo preemption delay** command to restore the default.

The default preemption delay is 1 second.

The preemption delay configuration takes effect only when role preemption is enabled.

Related commands: **preemption mode**.

### Examples

# Enable role preemption and set the preemption delay to 10 seconds.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] preemption mode role
[Sysname-smlk-group1] preemption delay 10
```

## preemption mode

### Syntax

```
preemption mode role
undo preemption mode
```

### View

Smart link group view

### Default Level

2: System level

### Parameters

**role**: Configures the role preemption mode, which enables the master port to preempt the slave port in active state.

### Description

Use the **preemption mode** command to enable role preemption.

Use the **undo preemption mode** command to restore the default.

By default, role preemption is disabled.

## Examples

```
# Enable role preemption.
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] preemption mode role
```

## protected-vlan

### Syntax

```
protected-vlan reference-instance instance-id-list
undo protected-vlan [ reference-instance instance-id-list ]
```

### View

Smart link group view

### Default Level

2: System level

### Parameters

**reference-instance** *instance-id-list*: Specifies the MSTIs to be referenced in the form of *instance-id-list* = { *instance-id* [ **to** *instance-id* ] }&<1-10>, where the range of the *instance-id* argument is as specified in the command configuring MSTIs and &<1-10> indicates that you can provide up to ten MSTIs or MSTI lists.

### Description

Use the **protected-vlan** command to configure protected VLANs for a smart link group by referencing MSTIs. You can use the **display stp region-configuration** command to view the VLANs mapped to the referenced MSTIs.

Use the **undo protected-vlan** command to remove the specified protected VLANs from a smart link group by referencing the specified MSTIs. If no MSTI is specified, all the protected VLANs of the smart link group are removed.

By default, no protected VLAN is configured for a smart link group.

Note that:

- Before assigning ports to a smart link group, configure protected VLANs for the smart link group.
- You can remove all protected VLANs from a smart link group when the group is empty but not after a member port is assigned to it.
- Removing a smart link group also removes its protected VLANs.
- If the VLAN(s) mapped to a referenced MSTI changes, the protected VLAN(s) change accordingly.
- The VLANs that the member ports of a smart link group belong to must be configured as the protected VLANs of the smart link group.

Related commands: **smart-link group**, **display stp region-configuration** in *MSTP Commands* in the *Access Volume*.

## Examples

```
# Configure the VLANs mapped to MSTIs 1 through 10 and MSTI 12 as the protected VLANs of smart link group 1.
```

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 1 to 10 12
```

## reset smart-link statistics

### Syntax

```
reset smart-link statistics
```

### View

User view

### Default Level

2: System level

### Parameters

None

### Description

Use the **reset smart-link statistics** command to clear the statistics about flush messages.

## Examples

```
# Clear the statistics about flush messages.
```

```
<Sysname> reset smart-link statistics
```

## smart-link flush enable

### Syntax

```
smart-link flush enable [ control-vlan vlan-id-list ]
undo smart-link flush enable [ control-vlan vlan-id-list ]
```

### View

Ethernet interface view, Layer-2 aggregate interface view

### Default Level

2: System level

### Parameters

**control-vlan** *vlan-id-list*: Specifies the control VLANs used for receiving flush messages. The *vlan-id-list* is expressed in the form of *vlan-id-list* = { *vlan-id* [ **to** *vlan-id* ] }&<1-10>, where the *vlan-id* argument ranges from 1 to 4094 and &<1-10> indicates that you can provide up to ten VLAN IDs or VLAN ID lists.

## Description

Use the **smart-link flush enable** command to configure a VLAN for receiving flush messages, that is, a receive control VLAN, on a port in Ethernet interface view or on all ports in system view.

Use the **undo smart-link flush enable** command to disable flush message processing.

By default, flush messages are not processed.

Note that:

- If no VLAN is specified, VLAN 1 applies.
- This command cannot be used on member port of an aggregation group or service loopback group.

Related commands: **flush enable**.

## Examples

# Enable GigabitEthernet1/0/1 to process the flush messages received in VLAN 1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] smart-link flush enable
```

# Enable Layer-2 aggregate interface 1 to process the flush messages received in VLAN 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] smart-link flush enable
```

## smart-link group

### Syntax

```
smart-link group group-id
undo smart-link group group-id
```

### View

System view

### Default Level

2: System level

### Parameters

*group-id*: Smart link group ID, in the range 1 to 26.

## Description

Use the **smart-link group** command to create a smart link group and enter smart link group view.

Use the **undo link-aggregation group** command to remove a smart link group.

Note that a smart link group with member ports cannot be removed.

## Examples

# Create smart link group 1.

```
<Sysname> system-view
```

```
[Sysname] smart-link group 1
```

```
[Sysname-smlk-group1]
```

# Table of Contents

<b>1 Monitor Link Configuration Commands</b> .....	<b>1-1</b>
Monitor Link Configuration Commands.....	1-1
display monitor-link group.....	1-1
monitor-link group.....	1-2
port.....	1-2
port monitor-link group.....	1-3

# 1 Monitor Link Configuration Commands

---

## Monitor Link Configuration Commands

### display monitor-link group

#### Syntax

```
display monitor-link group { group-id | all }
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

*group-id*: Monitor link group ID, in the range 1 to 16.

**all**: Specifies all monitor link groups.

#### Description

Use the **display monitor-link group** command to display information about the specified or all smart link groups.

#### Examples

```
# Display information about monitor link group 1.
```

```
<Sysname> display monitor-link group 1
Monitor link group 1 information:
Group status: DOWN
Last-up-time: 16:37:20 2006/4/21
Last-down-time: 16:38:26 2006/4/21
Member                Role      Status
-----
GigabitEthernet1/0/1  UPLINK   DOWN
GigabitEthernet1/0/2  DOWNUPLINK DOWN
```

**Table 1-1 display monitor-link group** command output description

Field	Description
Group status	Monitor link group state, which can be up or down
Last-up-time	Last time when the monitor link group was up
Last-down-time	Last time when the monitor link group was down
Member	Member ports of the monitor link group

Field	Description
Role	Port role, which can be uplink or downlink
Status	Member link state, which can be up or down

## monitor-link group

### Syntax

```
monitor-link group group-id
undo monitor-link group group-id
```

### View

System view

### Default Level

2: System level

### Parameters

*group-id*: Monitor link group ID, in the range 1 to 16.

### Description

Use the **monitor-link group** command to create a monitor link group and enter monitor link group view. If the specified monitor link group already exists, you enter monitor link group view directly.

Use the **undo monitor-link group** command to remove a monitor link group.

Related commands: **port monitor-link group**, **port**.

### Examples

```
# Create monitor link group 1.
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1]
```

## port

### Syntax

```
port interface-type interface-number { uplink | downlink }
undo port interface-type interface-number
```

### View

Monitor link group view

### Default Level

2: System level

## Parameters

*interface-type interface-number*: Port type and port number.

**uplink**: Specifies an uplink port.

**downlink**: Specifies a downlink port.

## Description

Use the **port** command to assign a port to the monitor link group.

Use the **undo port** command to remove a port from the monitor link group.



### Note

- Both Ethernet ports and Layer-2 aggregate interfaces can be assigned to a monitor link group.
  - A port can be assigned to only one monitor link group.
  - Alternatively, you can assign a port to a monitor link group with the **port monitor-link group** command in Ethernet interface view or Layer-2 aggregate interface view.
- 

Related commands: **port monitor-link group**.

## Examples

# Configure member ports for monitor link group 1.

```
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1] port gigabitethernet 1/0/1 uplink
[Sysname-mtlk-group1] port gigabitethernet 1/0/2 downlink
```

## port monitor-link group

### Syntax

**port monitor-link group** *group-id* { **uplink** | **downlink** }

**undo port monitor-link group** *group-id*

### View

Ethernet interface view, Layer-2 aggregate interface view

### Default Level

2: System level

## Parameters

*group-id*: Monitor link group ID, in the range 1 to 16.

**uplink**: Specifies an uplink port.

**downlink**: Specifies a downlink port.

## Description

Use the **port monitor-link group** command to assign the port to the specified monitor link group.

Use the **undo port monitor-link group** command to remove the port from the specified monitor link group.

---



### Note

- Both Ethernet ports and Layer-2 aggregate interfaces can be assigned to a monitor link group.
  - A port can be assigned to only one monitor link group.
  - Alternatively, you can assign a port to a monitor link group with the **port** command in monitor link group view.
- 

Related commands: **port**.

## Examples

# Configure GigabitEthernet 1/0/1 as an uplink port of monitor link group 1.

```
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port monitor-link group 1 uplink
```

# Table of Contents

<b>1 VLAN Configuration Commands</b>	<b>1-1</b>
VLAN Configuration Commands	1-1
description	1-1
display interface vlan-interface	1-2
display vlan	1-3
interface vlan-interface	1-4
ip address	1-5
name	1-6
shutdown	1-7
vlan	1-7
Port-Based VLAN Configuration Commands	1-9
display port	1-9
port	1-10
port access vlan	1-10
port hybrid pvid vlan	1-11
port hybrid vlan	1-13
port link-type	1-14
port trunk permit vlan	1-15
port trunk pvid vlan	1-17
MAC Address-Based VLAN Configuration Commands	1-18
display mac-vlan	1-18
display mac-vlan interface	1-20
mac-vlan enable	1-20
mac-vlan mac-address	1-21
vlan precedence	1-22
Protocol-Based VLAN Configuration Commands	1-22
display protocol-vlan interface	1-22
display protocol-vlan vlan	1-23
port hybrid protocol-vlan	1-24
protocol-vlan	1-26
IP Subnet-Based VLAN Configuration Commands	1-28
display ip-subnet-vlan interface	1-28
display ip-subnet-vlan vlan	1-29
ip-subnet-vlan	1-30
port hybrid ip-subnet-vlan vlan	1-31
<b>2 Isolate-User-VLAN Configuration Commands</b>	<b>2-1</b>
Isolate-User-VLAN Configuration Commands	2-1
display isolate-user-vlan	2-1
isolate-user-vlan	2-2
isolate-user-vlan enable	2-4
<b>3 Voice VLAN Configuration Commands</b>	<b>3-1</b>
Voice VLAN Configuration Commands	3-1
display voice vlan oui	3-1

display voice vlan state.....	3-2
voice vlan aging.....	3-3
voice vlan enable.....	3-4
voice vlan mac-address.....	3-4
voice vlan mode auto.....	3-6
voice vlan security enable .....	3-6

# 1 VLAN Configuration Commands

---

## VLAN Configuration Commands

### description

#### Syntax

```
description text  
undo description
```

#### View

VLAN view, VLAN interface view

#### Default Level

2: System level

#### Parameters

*text*: Case-sensitive string that describes the current VLAN or VLAN interface. Spaces can be included in the description.

- For a VLAN, this is a string of 1 to 32 characters.
- For a VLAN interface, this is a string of 1 to 80 characters.

#### Description

Use the **description** command to configure the description of the current VLAN or VLAN interface.

Use the **undo description** command to restore the default.

For a VLAN, the default description is the VLAN ID, for example, **VLAN 0001**; for a VLAN interface, the default description is the name of the interface, for example, **Vlan-interface 1 Interface**.

You can configure a description to describe the function or connection of a VLAN or VLAN interface for management sake.

#### Examples

# Configure the description of VLAN 1 as **RESEARCH**.

```
<Sysname> system-view  
[Sysname] vlan 1  
[Sysname-vlan1] description RESEARCH
```

# Configure the description of VLAN-interface 2 as **VLAN-INTERFACE-2**.

```
<Sysname> system-view  
[Sysname] vlan 2  
[Sysname-vlan2] quit  
[Sysname] interface vlan-interface 2  
[Sysname-Vlan-interface2] description VLAN-INTERFACE-2
```

## display interface vlan-interface

### Syntax

```
display interface vlan-interface [ vlan-interface-id ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*vlan-interface-id*: VLAN interface number, in the range of the numbers of existing VLANs on the device.

### Description

Use the **display interface vlan-interface** command to display information about a specified or all VLAN interfaces if no interface is specified.

Related commands: **interface vlan-interface**.

### Examples

```
# Display the information of VLAN-interface 2.
```

```
<Sysname> display interface vlan-interface 2
Vlan-interface2 current state: DOWN
Line protocol current state: DOWN
Description: Vlan-interface2 Interface
The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 001e-c16f-ae69
IPv6 Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 001e-c16f-ae69
```

**Table 1-1** display interface vlan-interface command output description

Field	Description
Vlan-interface2 current state	The physical state of the VLAN interface, which can be one of the following: <ul style="list-style-type: none"><li>Administratively DOWN: The administrative state of the VLAN interface is down because it has been manually shut down with the <b>shutdown</b> command.</li><li>DOWN: The administrative state of this VLAN interface is up, but its physical state is down. It indicates that the VLAN corresponding to this interface does not contain any port in the UP state (possibly because the ports are not well connected or the lines have failed).</li><li>UP: both the administrative state and the physical state of this VLAN interface are up.</li></ul>
Line protocol current state	The link layer protocol state of a VLAN interface, which can be one of the following: <ul style="list-style-type: none"><li>DOWN: The protocol state of this VLAN interface is down, usually because no IP address is configured.</li><li>UP: The protocol state of this VLAN interface is up.</li></ul>

Field	Description
Description	The description string of a VLAN interface
The Maximum Transmit Unit	The MTU of a VLAN interface
Internet protocol processing :	IP packets processing ability. Disabled indicates that the interface is not configured with an IP address.
IP Packet Frame Type	IPv4 outgoing frame format
Hardware address	MAC address corresponding to a VLAN interface
IPv6 Packet Frame Type	IPv6 outgoing frame format

## display vlan

### Syntax

```
display vlan [ vlan-id1 [ to vlan-id2 ] | all | dynamic | reserved | static ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*vlan-id1*: Displays the information of a VLAN specified by VLAN ID in the range of 1 to 4094.

*vlan-id1* to *vlan-id2*: Displays the information of a range of VLANs specified by a VLAN ID range. Note that *vlan-id2* must be equal to or greater than *vlan-id1*.

**all**: Displays all current VLAN information except for the reserved VLANs.

**dynamic**: Displays the number of dynamic VLANs and the ID of each dynamic VLAN. Dynamic VLANs refer to VLANs that are generated through GVRP or those distributed by a RADIUS server.

**reserved**: Displays information of the reserved VLANs. Protocol modules determine which VLANs are reserved VLANs according to function implementation, and reserved VLANs serve protocol modules. You cannot do any configuration on reserved VLANs.

**static**: Displays the number of static VLANs and the ID of each static VLAN. Static VLANs refer to VLANs manually created.

### Description

Use the **display vlan** command to display VLAN information.

Related commands: **vlan**.

### Examples

```
# Display VLAN 2 information.
```

```
<Sysname> display vlan 2
```

```
VLAN ID: 2
```

```
VLAN Type: static
```

```
Route Interface: not configured
```

```

Description: VLAN 0002
Name: VLAN 0002
Tagged Ports:
    GigabitEthernet1/0/11    GigabitEthernet1/0/12
Untagged Ports: none

```

### # Display VLAN 3 information.

```

<Sysname> display vlan 3
VLAN ID: 3
VLAN Type: static
Route Interface: configured
IP Address: 1.1.1.1
Subnet Mask: 255.255.255.0
Description: VLAN 0003
Name: VLAN 0003
Tagged Ports: none
Untagged Ports: none

```

**Table 1-2 display vlan command output description**

Field	Description
VLAN ID	VLAN ID
VLAN Type	VLAN type (static or dynamic)
Route interface	Whether the VLAN interface is configured for the VLAN: not configured or configured
Description	VLAN description
Name	Name configured for the VLAN
IP Address	Primary IP address of the VLAN interface (available only on a VLAN interface configured with an IP address). You can use the <b>display interface vlan-interface</b> command in any view or the <b>display this</b> command in VLAN interface view to display its secondary IP address(es), if any.
Subnet Mask	Subnet mask of the primary IP address (available only on a VLAN interface configured with an IP address)
Tagged Ports	Ports through which packets of the VLAN are sent tagged
Untagged Ports	Ports through which packets of the VLAN are sent untagged

## interface vlan-interface

### Syntax

```

interface vlan-interface vlan-interface-id
undo interface vlan-interface vlan-interface-id

```

### View

System view

## Default Level

2: System level

## Parameters

*vlan-interface-id*: VLAN interface number, in the range of 1 to 4094.

## Description

Use the **interface vlan-interface** command to create a VLAN interface and enter its view or enter the view of an existing VLAN interface.

Before you can create the VLAN interface of a VLAN, create the VLAN first.

Use the **undo interface vlan-interface** command to remove the specified VLAN interface.

You can use the **ip address** command in VLAN interface view to configure an IP address for a VLAN interface to perform IP routing.

Related commands: **display interface Vlan-interface**.

## Examples

```
# Create VLAN-interface 2.
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2]
```

## ip address

### Syntax

```
ip address ip-address { mask | mask-length } [ sub ]
undo ip address [ ip-address { mask | mask-length } [ sub ] ]
```

### View

VLAN interface view

## Default Level

2: System level

## Parameters

*ip-address*: IP address to be assigned to the current VLAN interface, in dotted decimal format.

*mask*: Subnet mask in dotted decimal notation.

*mask-length*: Subnet mask length, the number of consecutive ones in the mask. The value range is 0 to 32.

**sub**: Indicates the address is a secondary IP address.

## Description

Use the **ip address** command to assign an IP address and subnet mask to a VLAN interface.

Use the **undo ip address** command to remove the IP address and subnet mask for a VLAN interface.

By default, no IP address is assigned to any VLAN interface.

In general conditions, you need to assign only one IP address for a VLAN interface. For a VLAN to connect to multiple subnets, you need to assign multiple IP addresses for the VLAN interface. Among these IP addresses, one is primary and the others are secondary. On an S4800G switch, you can assign up to ten IP addresses for a VLAN interface.

When configuring IP addresses for a VLAN interface, consider the following:

- You can assign only one primary IP address to an interface.
- Before removing the primary IP address, remove all secondary IP addresses.
- To remove all IP addresses, use the **undo ip address** command without any parameter.
- To remove the primary IP address, use the **undo ip address** *ip-address* { *mask* | *mask-length* } command.
- To remove a secondary IP address, use the **undo ip address** *ip-address* { *mask* | *mask-length* } **sub** command.

Related commands: **display ip interface** (*IP Address Commands* in the *IP Services Volume*).

## Examples

# Specify the IP address as 1.1.0.1, the subnet mask as 255.255.255.0 for VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip address 1.1.0.1 255.255.255.0
```

## name

### Syntax

**name** *text*

**undo name**

### View

VLAN interface view

### Default Level

2: System level

### Parameters

*text*: VLAN name, a string of 1 to 32 characters. Spaces and special characters can be included in the name.

### Description

Use the **name** command to configure a name for the current VLAN.

Use the **undo name** command to restore the default name of the VLAN.

The default name of a VLAN is its VLAN ID, **VLAN 0001** for example.

When 802.1X or MAC address authentication is configured on a switch, you can use a RADIUS server to issue VLAN configuration to ports that have passed the authentication. Some servers can send IDs or names of the issued VLANs to the switch. When there are a large number of VLANs, you can use VLAN names rather than VLAN IDs to better locate VLANs.

## Examples

```
# Configure the name of VLAN 2 as test vlan.
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] name test vlan
```

## shutdown

### Syntax

```
shutdown
undo shutdown
```

### View

VLAN interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **shutdown** command to shut down a VLAN interface.

Use the **undo shutdown** command to bring up a VLAN interface.

By default, a VLAN interface is up except when all ports in the VLAN are down.

You can use the **undo shutdown** command to bring up a VLAN interface after configuring related parameters and protocols for the VLAN interface. When a VLAN interface fails, you can shut down the interface with the **shutdown** command and then bring it up with the **undo shutdown** command. In this way, the interface may resume.

The state of any Ethernet port in a VLAN is independent of the VLAN interface state.

## Examples

```
# Shut down VLAN interface 2 and then bring it up.
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] shutdown
[Sysname-Vlan-interface2] undo shutdown
```

## vlan

### Syntax

```
vlan { vlan-id1 [ to vlan-id2 ] | all }
undo vlan { vlan-id1 [ to vlan-id2 ] | all }
```

## View

System view

## Default Level

2: System level

## Parameters

*vlan-id1*, *vlan-id2*: VLAN ID, in the range 1 to 4094.

*vlan-id1 to vlan-id2*: Specifies a VLAN range. A VLAN ID is in the range 1 to 4094. Note that *vlan-id2* must be equal to or greater than *vlan-id1*.

**all**: Creates or removes all VLANs except reserved VLANs. The keyword is not supported when the maximum number of VLANs that can be created on a device is less than 4094.

## Description

Use the **vlan** *vlan-id* command to create a VLAN and enter its view or enter the view of an existing VLAN.

Use the **vlan** *vlan-id1 to vlan-id2* command to create a range of VLANs specified by *vlan-id1 to vlan-id2*, except reserved VLANs.

Use the **undo vlan** command to remove the specified VLAN(s).



### Note

- As the default VLAN, VLAN 1 cannot be created or removed.
  - You cannot create/remove reserved VLANs reserved for specific functions.
  - You cannot use the **undo vlan** command to directly remove reserved VLANs, voice VLANs, management VLANs, dynamic VLANs, VLANs configured with QoS policies, control VLANs configured for smart link, or remote probe VLANs configured for port mirroring. To remove these VLANs, you need to first remove related configurations.
- 

Related commands: **display vlan**.

## Examples

# Enter VLAN 2 view.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2]
```

# Create VLAN 4 through VLAN 100.

```
<Sysname> system-view
[Sysname] vlan 4 to 100
Please wait..... Done.
```

# Port-Based VLAN Configuration Commands

## display port

### Syntax

```
display port { hybrid | trunk }
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**hybrid**: Displays hybrid ports.

**trunk**: Displays trunk ports.

### Description

Use the **display port** command to display information about the hybrid or trunk ports on the device, including the port names, default VLAN IDs, and allowed VLAN IDs.

### Examples

# Display information about the hybrid ports in the system.

```
<Sysname> display port hybrid
Interface          PVID  VLAN passing
GE1/0/6            1     Tagged:  1002
                   Untagged:1-2, 5-50, 100, 200
```

# Display information about the trunk ports in the system.

```
<Sysname> display port trunk
Interface          PVID  VLAN passing
GE1/0/1            100   2, 6-50, 100
GE1/0/11           1     1-2, 5-50, 100, 200, 1002
GE1/0/12           1     1-2, 5-50, 100, 200, 1002
```

**Table 1-3 display port** command output description

Field	Description
Interface	Port name
PVID	Default VLAN ID of the port
VLAN passing	VLANs whose packets are allowed to pass through the port.
Tagged	VLANs whose packets are required to pass through the port tagged.
Untagged	VLANs whose packets are required to pass through the port untagged.

## port

### Syntax

**port** *interface-list*

**undo port** *interface-list*

### View

VLAN view

### Default Level

2: System level

### Parameters

**interface** *interface-list*. Specifies an Ethernet port list or Layer-2 aggregate interface list, in the format of *interface-list* = { *interface-type interface-number* [ **to** *interface-type interface-number* ] }&<1-10>, where &<1-10> indicates that you can specify up to 10 ports or port ranges.

### Description

Use the **port** command to assign the specified access port(s) to the current VLAN.

Use the **undo port** command to remove the specified access port(s) from the current VLAN.

By default, all ports are in VLAN 1.

Note that:

- This command is only applicable on access ports.
- All ports are access ports by default. However, you can manually configure the port type. For more information, refer to **port link-type**.
- If you use this command to assign a Layer-2 aggregate interface to a VLAN, this command assigns the Layer-2 aggregate interface but not its member ports to the current VLAN. For detailed information about Layer-2 aggregate interfaces, refer to *Link Aggregation Configuration* in the *Access Volume*.

Related commands: **display vlan**.

### Examples

# Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to VLAN 2.

```
<Sysname> system-view
```

```
[Sysname] vlan 2
```

```
[Sysname-vlan2] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

# Assign Layer-2 aggregate interface **Bridge-aggregation 1** to VLAN 2.

```
<Sysname> system-view
```

```
[Sysname] vlan 2
```

```
[Sysname-vlan2] port bridge-aggregation 1
```

## port access vlan

### Syntax

**port access vlan** *vlan-id*

## undo port access vlan

### View

Ethernet interface view, port group view, Layer-2 aggregate interface view

### Default Level

2: System level

### Parameters

*vlan-id*: VLAN ID, in the range of 1 to 4094. Be sure that the VLAN specified by the VLAN ID already exists.

### Description

Use the **port access vlan** command to assign the current access port(s) to the specified VLAN.

Use the **undo port access vlan** command to restore the default.

By default, all access ports belong to VLAN 1.

You can assign an access port to only one VLAN. When doing that, note the following:

- In port group view, this command applies to all ports in the port group. For information about port groups, refer to *Ethernet Interface Configuration* in the *Access Volume*.
- In Layer-2 aggregate interface view, this command applies to the Layer-2 aggregate interface and all its member ports. After you perform the configuration, the system starts applying the configuration to the aggregate interface and its aggregation member ports. If the system fails to do that on the aggregate interface, it stops applying the configuration to the aggregation member ports. If it fails to do that on an aggregation member port, it simply skips the port and moves to the next port. For information about Layer-2 aggregate interfaces, refer to *Link Aggregation Configuration* in the *Access Volume*.

### Examples

# Assign GigabitEthernet 1/0/1 to VLAN 3.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port access vlan 3
```

# Assign Layer-2 aggregate interface **Bridge-aggregation 1** and its member ports to VLAN 3.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port access vlan 3
```

## port hybrid pvid vlan

### Syntax

**port hybrid pvid vlan** *vlan-id*

**undo port hybrid pvid**

## View

Ethernet interface view, port group view, Layer-2 aggregate interface view

## Default Level

2: System level

## Parameters

*vlan-id*: VLAN ID, in the range of 1 to 4094.

## Description

Use the **port hybrid pvid vlan** command to configure the default VLAN ID of the hybrid port.

Use the **undo port hybrid pvid** command to restore the default.

By default, the default VLAN of a hybrid port is VLAN 1.

You can use a nonexistent VLAN as the default VLAN for a hybrid port. Removing the default VLAN of a hybrid port with the **undo vlan** command does not affect the setting of the default VLAN on the port.

- In port group view, this command applies to all ports in the port group. For information about port groups, refer to *Ethernet Interface Configuration* in the *Access Volume*.
- In Layer-2 aggregate interface view, this command applies to the Layer-2 aggregate interface and all its member ports. After you perform the configuration, the system starts applying the configuration to the aggregate interface and its aggregation member ports. If the system fails to do that on the aggregate interface, it stops applying the configuration to the aggregation member ports. If it fails to do that on an aggregation member port, it simply skips the port and moves to the next port. For information about Layer-2 aggregate interfaces, refer to *Link Aggregation Configuration* in the *Access Volume*.
- The local and remote hybrid ports must use the same default VLAN ID for the traffic of the default VLAN to be transmitted properly.
- After configuring the default VLAN for a hybrid port, you must use the **port trunk permit vlan** command to configure the hybrid port to allow packets from the default VLAN to pass through, so that the port can forward packets from the default VLAN.

Related commands: **port link-type**, **port hybrid vlan**.

## Examples

```
# Configure VLAN 100 as the default VLAN of the hybrid port GigabitEthernet 1/0/1.
```

```
<Sysname> system-view
[Sysname] vlan 100
[Sysname-vlan100] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid tagged 100
[Sysname-GigabitEthernet1/0/1] port hybrid pvid vlan 100
```

```
# Configure VLAN 100 as the default VLAN of the hybrid Layer-2 aggregate interface
Bridge-aggregation 1.
```

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port hybrid pvid vlan 100
```

## port hybrid vlan

### Syntax

```
port hybrid vlan vlan-id-list { tagged | untagged }
```

```
undo port hybrid vlan vlan-id-list
```

### View

Ethernet interface view, port group view, Layer-2 aggregate interface view

### Default Level

2: System level

### Parameters

*vlan-id-list*: VLANs that the hybrid ports will be assigned to. This argument is expressed in the format of [ *vlan-id1* [ to *vlan-id2* ] ]&<1-10>, where *vlan-id* ranges from 1 to 4094 and &<1-10> indicates that you can specify up to 10 VLAN IDs or VLAN ID ranges. Be sure that the specified VLANs already exist.

**tagged**: Configures the port(s) to send the packets of the specified VLAN(s) with the tags kept.

**untagged**: Configures the port to send the packets of the specified VLAN(s) with the tags removed.

### Description

Use the **port hybrid vlan** command to assign the current hybrid port(s) to the specified VLAN(s).

Use the **undo port hybrid vlan** command to remove the current hybrid port(s) from the specified VLAN(s).

By default, a hybrid port only allows packets from VLAN 1 to pass through untagged.

A hybrid port can carry multiple VLANs. If you execute the **port hybrid vlan** command multiple times, the VLANs the hybrid port carries are the set of VLANs specified by *vlan-id-list* in each execution.

- In port group view, this command applies to all ports in the port group. For information about port groups, refer to *Ethernet Interface Configuration* in the *Access Volume*.
- In Layer-2 aggregate interface view, this command applies to the Layer-2 aggregate interface and all its member ports. After you perform the configuration, the system starts applying the configuration to the aggregate interface and its aggregation member ports. If the system fails to do that on the aggregate interface, it stops applying the configuration to the aggregation member ports. If it fails to do that on an aggregation member port, it simply skips the port and moves to the next port. For information about Layer-2 aggregate interfaces, refer to *Link Aggregation Configuration* in the *Access Volume*.

Related commands: **port link-type**.

### Examples

```
# Assign the hybrid port GigabitEthernet 1/0/1 to VLAN 2, VLAN 4, and VLAN 50 through VLAN 100, and configure GigabitEthernet 1/0/1 to send packets of these VLANs with tags kept.
```

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 2 4 50 to 100 tagged
```

# Assign hybrid ports in port group 2 to VLAN 2, and configure these hybrid ports to send packets of VLAN 2 with VLAN tags removed.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] port-group manual 2
[Sysname-port-group-manual-2] group-member gigabitethernet 1/0/1 to gigabitethernet 1/0/6
[Sysname-port-group-manual-2] port link-type hybrid
[Sysname-port-group-manual-2] port hybrid vlan 2 untagged
Configuring GigabitEthernet1/0/1... Done.
Configuring GigabitEthernet1/0/2... Done.
Configuring GigabitEthernet1/0/3... Done.
Configuring GigabitEthernet1/0/4... Done.
Configuring GigabitEthernet1/0/5... Done.
Configuring GigabitEthernet1/0/6... Done.
```

# Assign the hybrid Layer-2 aggregate interface **Bridge-aggregation 1** and its member ports to VLAN 2, and configure them to send packets of VLAN 2 with tags removed.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port link-type hybrid
[Sysname-Bridge-Aggregation1] port hybrid vlan 2 untagged
Please wait... Done.
Configuring GigabitEthernet1/0/2... Done.
Configuring GigabitEthernet1/0/3... Done.
```

Note that GigabitEthernet1/0/2 and GigabitEthernet1/0/3 are the member ports of the aggregation group corresponding to Bridge-aggregation 1.

## port link-type

### Syntax

```
port link-type { access | hybrid | trunk }
undo port link-type
```

### View

Ethernet interface view, port group view, Layer-2 aggregate interface view

### Default Level

2: System level

### Parameters

**access**: Configures the link type of a port as access.

**hybrid**: Configures the link type of a port as hybrid.

**trunk**: Configures the link type of a port as trunk.

### Description

Use the **port link-type** command to configure the link type of a port.

Use the **undo port link-type** command to restore the default link type of a port.

By default, any port is an access port.

- In port group view, this command applies to all ports in the port group. For information about port groups, refer to *Ethernet Interface Configuration* in the *Access Volume*.
- In Layer-2 aggregate interface view, this command applies to the Layer-2 aggregate interface and all its member ports. After you perform the configuration, the system starts applying the configuration to the aggregate interface and its aggregation member ports. If the system fails to do that on the aggregate interface, it stops applying the configuration to the aggregation member ports. If it fails to do that on an aggregation member port, it simply skips the port and moves to the next port. For information about Layer-2 aggregate interfaces, refer to *Link Aggregation Configuration* in the *Access Volume*.



#### Note

To change the link type of a port from trunk to hybrid or vice versa, you must set the link type to access first.

---

## Examples

# Configure GigabitEthernet 1/0/1 as a trunk port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
```

# Configure all the ports in the manual port group **group1** as hybrid ports.

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group manual group1] group-member gigabitethernet 1/0/2
[Sysname-port-group manual group1] group-member gigabitethernet 1/0/3
[Sysname-port-group manual group1] port link-type hybrid
```

# Configure Layer-2 aggregate interface **Bridge-aggregation 1** and its member ports as hybrid ports.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port link-type hybrid
```

## port trunk permit vlan

### Syntax

```
port trunk permit vlan { vlan-id-list | all }
undo port trunk permit vlan { vlan-id-list | all }
```

### View

Ethernet interface view, port group view, Layer-2 aggregate interface view

## Default Level

2: System level

## Parameters

*vlan-id-list*: VLANs that the trunk port(s) will be assigned to. This argument is expressed in the format of `[vlan-id1 [ to vlan-id2 ] ]&<1-10>`, where *vlan-id* ranges from 1 to 4094 and `&<1-10>` indicates that you can specify up to 10 VLAN IDs or VLAN ID ranges.

**all**: Permits all VLANs to pass through the trunk port(s). On GVRP-enabled trunk ports, you must configure the **port trunk permit vlan all** command to ensure that the traffic of all dynamically registered VLANs can pass through. However, When GVRP is disabled on a port, you are discouraged to configure the command on the port. This is to prevent users of unauthorized VLANs from accessing restricted resources through the port.

## Description

Use the **port trunk permit vlan** command to assign the current trunk port(s) to the specified VLAN(s).

Use the **undo port trunk permit vlan** command to remove the trunk port(s) from the specified VLANs.

By default, a trunk port allows only packets from VLAN 1 to pass through.

A trunk port can carry multiple VLANs. If you execute the **port trunk permit vlan** command multiple times, the VLANs the trunk port carries are the set of VLANs specified by *vlan-id-list* in each execution.

Note that on a trunk port, only traffic of the default VLAN can pass through untagged.

- In port group view, this command applies to all ports in the port group. For information about port groups, refer to *Ethernet Interface Configuration* in the *Access Volume*.
- In Layer-2 aggregate interface view, this command applies to the Layer-2 aggregate interface and all its member ports. After you perform the configuration, the system starts applying the configuration to the aggregate interface and its aggregation member ports. If the system fails to do that on the aggregate interface, it stops applying the configuration to the aggregation member ports. If it fails to do that on an aggregation member port, it simply skips the port and moves to the next port. For information about Layer-2 aggregate interfaces, refer to *Link Aggregation Configuration* in the *Access Volume*.

Related commands: **port link-type**.

## Examples

# Assign the trunk port GigabitEthernet 1/0/1 to VLAN 2, VLAN 4, and VLAN 50 through VLAN 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk permit vlan 2 4 50 to 100
Please wait..... Done.
```

# Assign the trunk Layer-2 aggregate interface **Bridge-aggregation 1** to VLAN 2, assuming that **Bridge-aggregation 1** does not have member ports.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port trunk permit vlan 2
Please wait... Done.
```

# Assign the trunk Layer-2 aggregate interface **Bridge-aggregation 1** to VLAN 13 and VLAN 15. Among the member ports of the aggregation group corresponding to **Bridge-aggregation 1**, GigabitEthernet 1/0/2 is an access port, and GigabitEthernet 1/0/3 is a trunk port.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port trunk permit vlan 13 15
Please wait... Done.
Error: Failed to configure on interface GigabitEthernet1/0/2! This port is not a Trunk port!
Configuring GigabitEthernet1/0/3... Done.
```

Among the output fields above, the message “Please wait... Done” indicates that the configuration on **Bridge-aggregation 1** succeeded; “Error: Failed to configure on interface GigabitEthernet1/0/2! This port is not a Trunk port!” indicates that the configuration failed on GigabitEthernet 1/0/2 because GigabitEthernet 1/0/2 was not a trunk port; “Configuring GigabitEthernet1/0/3... Done” indicates that the configuration on GigabitEthernet 1/0/3 succeeded.

## port trunk pvid vlan

### Syntax

```
port trunk pvid vlan vlan-id
undo port trunk pvid
```

### View

Ethernet interface view, port group view, Layer-2 aggregate interface view

### Default Level

2: System level

### Parameters

*vlan-id*: VLAN ID, in the range of 1 to 4094

### Description

Use the **port trunk pvid vlan** command to configure the default VLAN ID for the trunk port.

Use the **undo port trunk pvid** command to restore the default.

By default, the default VLAN of a trunk port is VLAN 1.

You can use a nonexistent VLAN as the default VLAN for a trunk port. Removing the default VLAN of a trunk port with the **undo vlan** command does not affect the setting of the default VLAN on the port.

- In port group view, this command applies to all ports in the port group. For information about port groups, refer to *Ethernet Interface Configuration* in the *Access Volume*.
- In Layer-2 aggregate interface view, this command applies to the Layer-2 aggregate interface and all its member ports. After you perform the configuration, the system starts applying the configuration to the aggregate interface and its aggregation member ports. If the system fails to do that on the aggregate interface, it stops applying the configuration to the aggregation member ports. If it fails to do that on an aggregation member port, it simply skips the port and moves to the next port. For information about Layer-2 aggregate interfaces, refer to *Link Aggregation Configuration* in the *Access Volume*.

- The local and remote trunk ports must use the same default VLAN ID for the traffic of the default VLAN to be transmitted properly.
- After configuring the default VLAN for a trunk port, you must use the **port trunk permit vlan** command to configure the trunk port to allow packets from the default VLAN to pass through, so that the port can forward packets from the default VLAN.

Related commands: **port link-type**, **port trunk permit vlan**.

## Examples

# Configure VLAN 100 as the default VLAN of the trunk port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

# Configure VLAN 100 as the default VLAN of the trunk Layer-2 aggregate interface **Bridge-aggregation 1**, assuming Bridge-aggregation 1 does not have member ports.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port trunk pvid vlan 100
```

# Configure VLAN 100 as the default VLAN of the trunk Layer-2 aggregate interface **Bridge-aggregation 1**. Among the member ports of the aggregation group corresponding to **Bridge-aggregation 1**, GigabitEthernet 1/0/2 is an access port and GigabitEthernet 1/0/3 is a trunk port.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port trunk pvid vlan 100
Error: Failed to configure on interface GigabitEthernet1/0/2! This port is not a Trunk port!
```

The output above shows that the configuration on Bridge-aggregation 1 and the member port GigabitEthernet 1/0/3 succeeded; the configuration on GigabitEthernet 1/0/2 failed because GigabitEthernet 1/0/2 was not a trunk port.

## MAC Address-Based VLAN Configuration Commands

### display mac-vlan

#### Syntax

```
display mac-vlan { all | dynamic | mac-address mac-address [ mask mac-mask ] | static | vlan vlan-id }
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

**all**: Displays all the MAC address-to-VLAN entries.

**dynamic:** Displays dynamically configured MAC address-to-VLAN entries.

**mac-address** *mac-address*: Displays the MAC address-to-VLAN entry containing the specified MAC address.

**mask** *mac-mask*: Displays the MAC address-to-VLAN entries with their MAC addresses in the specified range.

**static:** Displays the statically configured MAC address-to-VLAN entries.

**vlan** *vlan-id*: Displays the MAC address-to-VLAN entries associated with the specified VLAN.

## Description

Use the **display mac-vlan** command to display the specified MAC address-to-VLAN entries.

If **mac-address** *mac-addr* is specified while **mask** is not specified, only the MAC address-to-VLAN entry containing the specified MAC address is displayed.

## Examples

# Display all the MAC address-to-VLAN entries.

```
<Sysname> display mac-vlan all
The following MAC-VLAN address exist:
S: Static   D: Dynamic
MAC ADDR           MASK                               VLAN ID   PRIO   STATE
-----
0008-0000-0000     ffff-ff00-0000             5         3     S
0002-0001-0000     ffff-ffff-ffff             5         3     S&D

Total MAC VLAN address count:2
```

**Table 1-4 display mac-vlan** command output description

Field	Description
S: Static	The character <b>S</b> stands for the MAC address-to-VLAN entries that are configured statically.
D: Dynamic	The character <b>D</b> stands for the MAC address-to-VLAN entries that are configured dynamically.
MAC ADDR	MAC address of a MAC address-to-VLAN entry
MASK	Mask of the MAC address of a MAC address-to-VLAN entry
VLAN ID	VLAN ID of a MAC address-to-VLAN entry
PRIO	802.1p priority corresponding to the MAC address of a MAC address-to-VLAN entry
STATE	The state of a MAC address-to-VLAN entry, which can be: <ul style="list-style-type: none"><li>• <b>S</b>, indicating that the MAC address-to-VLAN entry is configured statically.</li><li>• <b>D</b>, indicating that the MAC address-to-VLAN entry is configured automatically through the authentication server</li><li>• <b>S&amp;D</b>, indicating that the MAC address-to-VLAN entry is configured both statically and dynamically</li></ul>

## display mac-vlan interface

### Syntax

**display mac-vlan interface**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display mac-vlan interface** command to display all the ports with MAC address-based VLAN enabled.

Related commands: **mac-vlan enable**.

### Examples

# Display all the interfaces with MAC address-based VLAN enabled.

```
<Sysname> display mac-vlan interface
MAC VLAN is enabled on following ports:
-----
GigabitEthernet1/0/1  GigabitEthernet1/0/2  GigabitEthernet1/0/3
```

## mac-vlan enable

### Syntax

**mac-vlan enable**

**undo mac-vlan enable**

### View

Ethernet port view

### Default Level

2: System level

### Parameters

None

### Description

Use the **mac-vlan enable** command to enable MAC address-based VLAN on a port.

Use the **undo mac-vlan enable** command to disable MAC address-based VLAN on a port.

By default, MAC address-based VLAN is disabled on a port.

## Examples

```
# Enable MAC address-based VLAN on GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-vlan enable
```

## mac-vlan mac-address

### Syntax

```
mac-vlan mac-address mac-address [ mask mac-mask ] vlan vlan-id [ priority pri ]
undo mac-vlan { all | mac-address mac-address [ mask mac-mask ] | vlan vlan-id }
```

### View

System view

### Default Level

2: System level

### Parameters

**mac-address** *mac-address*: Specifies a MAC address.

**mask** *mac-mask*: Specifies a mask for the MAC address in the format of H-H-H. The *mac-mask* argument is comprised of the high-order part (all the binary bits of which are 1s) and the low-order part (all the binary bits of which are 0s). By default, the hexadecimal digits of this argument are all Fs.

**vlan** *vlan-id*: Specifies a VLAN ID, in the range of 1 to 4094.

**priority** *pri*: Specifies the 802.1p priority value corresponding to the specified MAC address. This argument is in the range of 0 to 7.

**all**: Removes all the static MAC address-to-VLAN entries.

### Description

Use the **mac-vlan mac-address** command to associate the specified VLAN and priority value with the specified MAC addresses.

Use the **undo mac-vlan** command to remove the association.

Two MAC address-to-VLAN entry tables exist in a device. One table contains the MAC address-to-VLAN entries configured with the **mask** keyword specified. A MAC address-to-VLAN entry of this type describes the relationship between a group of MAC addresses and a VLAN, and a priority value. Another table contains the MAC address-to-VLAN entries configured without the **mask** keyword specified. A MAC address-to-VLAN entry of this type describes the relationship between a single MAC address and a VLAN, and a priority value. The system adds/removes MAC address-to-VLAN entries to/from the two tables according to your configuration.

## Examples

```
# Associate a single MAC address 0-1-1 with VLAN 100 and 802.1p priority 7.
<Sysname> system-view
[Sysname] mac-vlan mac-address 0-1-1 vlan 100 priority 7
```

# Associate the MAC addresses with the high-order six hexadecimal digits being 111122 with VLAN 100 and 802.1p priority 4.

```
<Sysname> system-view  
[Sysname] mac-vlan mac-address 1111-2222-3333 mask ffff-ff00-0000 vlan 100 priority 4
```

## vlan precedence

### Syntax

```
vlan precedence { mac-vlan | ip-subnet-vlan }  
undo vlan precedence
```

### View

Ethernet port view

### Default Level

2: System level

### Parameters

**mac-vlan**: Specifies to match VLANs based on MAC addresses preferentially.

**ip-subnet-vlan**: Specifies to match VLANs based on IP subnet settings preferentially.

### Description

Use the **vlan precedence** command to set the order of VLAN matching.

Use the **undo vlan precedence** command to restore the default.

By default, VLANs are matched based on MAC addresses preferentially.

Note that this command only applies to VLANs based on a single MAC address and IP subnet-based VLANs. If both the MAC address-based VLAN function and the IP subnet-based VLAN function are created on a port, MAC address-to-VLAN entries configured with the **mask** keyword specified are matched preferentially, and the left VLAN entries (VLAN entries based on a single MAC address and IP subnet-based VLANs) are matched as configured by the **vlan precedence** command.

### Examples

# Configure to match VLANs based on MAC addresses preferentially on GigabitEthernet 1/0/1.

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] vlan precedence mac-vlan
```

## Protocol-Based VLAN Configuration Commands

### display protocol-vlan interface

#### Syntax

```
display protocol-vlan interface { interface-type interface-number1 [ to interface-type  
interface-number2 ] | all }
```

## View

Any view

## Default Level

2: System level

## Parameters

*interface-type interface-number1*: Specifies an interface by its type and number.

*interface-type interface-number1 to interface-type interface-number2*: Specifies an interface range.

**all**: Displays information about protocol-based VLANs on all ports.

## Description

Use the **display protocol-vlan interface** command to display information about protocol-based VLANs for the specified port(s).

## Examples

# Display protocol-based VLAN information on GigabitEthernet 1/0/1.

```
[Sysname] display protocol-vlan interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
  VLAN ID   Protocol Index   Protocol Type
=====
      3       0             ipv4
```

The sample output shows that untagged packets received on GigabitEthernet 1/0/1 will be tagged with VLAN ID 2 if they carry AppleTalk packets or with VLAN ID 3 if they carry IPv4 packets.

**Table 1-5** display protocol-vlan interface command output description

Field	Description
Interface	Interface of which you want to view the information
VLAN ID	ID of the protocol-based VLAN bound with the port
Protocol Index	Protocol template index
Protocol Type	Protocol type specified by the protocol template

## display protocol-vlan vlan

### Syntax

```
display protocol-vlan vlan { vlan-id1 [ to vlan-id2 ] | all }
```

### View

Any view

### Default Level

2: System level

## Parameters

*vlan-id1*: ID of the protocol-based VLAN for which information is to be displayed, in the range of 1 to 4094.

*vlan-id1* **to** *vlan-id2*: Displays protocol-based VLAN information of a VLAN range from *vlan-id1* to *vlan-id2*. The *vlan-id2* argument specifies a protocol-based VLAN ID in the range of 1 to 4094, but you must ensure that its value is greater than or equal to that of *vlan-id1*.

**all**: Displays information about all protocol-based VLANs.

## Description

Use the **display protocol-vlan vlan** command to display the protocols and protocol indexes configured on the specified VLAN(s).

Related commands: **display vlan**.

## Examples

# Display the protocols and protocol indexes configured on all protocol-based-VLANs.

```
<Sysname> display protocol-vlan vlan all
VLAN ID:2
  Protocol Index      Protocol Type
  =====
          0           ipv4
VLAN ID:3
  Protocol Index      Protocol Type
  =====
          0           ipv4
          1           ipx snap
```

Refer to [Table 1-5](#) for description of the output.

## port hybrid protocol-vlan

### Syntax

**port hybrid protocol-vlan vlan** *vlan-id* { *protocol-index* [ **to** *protocol-end* ] | **all** }

**undo port hybrid protocol-vlan** { **vlan** *vlan-id* { *protocol-index* [ **to** *protocol-end* ] | **all** } | **all** }

### View

Ethernet interface view, port group view, Layer-2 aggregate interface view

### Default Level

2: System level

## Parameters

**vlan** *vlan-id*: Specifies a VLAN ID, in the range 1 to 4094.

*protocol-index*: Protocol index, ranging from 0 to 15, specified by the users or assigned by the system automatically when the protocol-based VLAN is created. You can use the **display protocol-vlan vlan all** command to display the protocol indexes.

**to protocol-end:** Specifies the end protocol index, ranging from 0 to 15. The *protocol-end* argument must be greater than or equal to the beginning protocol index.

**all:** Specifies all protocols bound with *vlan-id*.

## Description

Use the **port hybrid protocol-vlan vlan** command to associate the hybrid port(s) with a protocol-based VLAN.

Use the **undo port hybrid protocol-vlan** command to remove the association.

- In port group view, this command applies to all ports in the port group. For information about port groups, refer to *Ethernet Interface Configuration* in the *Access Volume*.
- In Layer-2 aggregate interface view, this command applies to the Layer-2 aggregate interface and all its member ports. After you perform the configuration, the system starts applying the configuration to the aggregate interface and its aggregation member ports. If the system fails to do that on the aggregate interface, it stops applying the configuration to the aggregation member ports. If it fails to do that on an aggregation member port, it simply skips the port and moves to the next port. For information about Layer-2 aggregate interfaces, refer to *Link Aggregation Configuration* in the *Access Volume*.

Before issuing this command, make sure that you have made the following configurations:

- Create a VLAN and associate it with specified protocols.
- Configure the link type as hybrid.
- Configure the port to allow the protocol-based VLAN to pass through.

Related commands: **display protocol-vlan interface**.

## Examples

# Associate the hybrid port GigabitEthernet 1/0/1 with protocol 0 (IPv4) in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] protocol-vlan ipv4
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 2 untagged
Please wait... Done
[Sysname-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 2 0
```

# Associate the hybrid Layer-2 aggregate interface **Bridge-aggregation 1** with protocol 0 in VLAN 2, assuming that **Bridge-aggregation 1** does not have member ports.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-Vlan2] protocol-vlan ipv4
[Sysname-Vlan2] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port link-type hybrid
[Sysname-Bridge-Aggregation1] port hybrid vlan 2 untagged
Please wait... Done
[Sysname-Bridge-Aggregation1] port hybrid protocol-vlan vlan 2 0
```

# Associate the hybrid Layer-2 aggregate interface **Bridge-aggregation 1** with protocol 0 in VLAN 2. Among the member ports of the aggregation group corresponding to **Bridge-aggregation 1**, GigabitEthernet 1/0/2 is an access port and GigabitEthernet 1/0/3 is a trunk port.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-Vlan2] protocol-vlan at
[Sysname-Vlan2] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation2] port link-type access
Please wait... Done.
Configuring GigabitEthernet1/0/2... Done.
Configuring GigabitEthernet1/0/3..... Done.
[Sysname-Bridge-Aggregation1] port link-type hybrid
[Sysname-Bridge-Aggregation1] port hybrid vlan 2 untagged
Please wait... Done.
Configuring GigabitEthernet1/0/2... Done.
Configuring GigabitEthernet1/0/3... Done.
[Sysname-Bridge-Aggregation1] port hybrid protocol-vlan vlan 2 0
```

## protocol-vlan

### Syntax

```
protocol-vlan [protocol-index] { at | ipv4 | ipv6 | ipx { ethernetii | llc | raw | snap } | mode { ethernetii | etype etype-id | llc { dsap dsap-id [ ssap ssap-id ] | ssap ssap-id } | snap etype etype-id } }
undo protocol-vlan { protocol-index [ to protocol-end ] | all }
```

### View

VLAN view

### Default Level

2: System level

### Parameters

**at**: Specifies the AppleTalk based VLAN.

**ipv4**: Specifies the IPv4 based VLAN.

**ipv6**: Specifies the IPv6 based VLAN.

**ipx**: Specifies the IPX based VLAN. The keywords **ethernetii**, **llc**, **raw**, and **snap** are encapsulation formats for IPX.

**mode**: Configures a user-defined protocol template for the VLAN, which could also have four encapsulation formats, namely, **ethernetii**, **llc**, **raw**, and **snap**.

**ethernetii etype etype-id**: Specifies to match Ethernet II encapsulation format and the corresponding protocol type values. The *etype-id* argument is the protocol type ID of inbound packets, in the range 0x0600 to 0xffff (excluding 0x0800, 0x809b, 0x8137, and 0x86dd).

**llc**: Specifies to match the **llc** encapsulation format.

**dsap dsap-id**: Specifies the destination service access point, in the range of 00 to 0xff.

**ssap** *ssap-id*: Specifies the source service access point, in the range of 00 to 0xff.

**snap etype** *etype-id*: Specifies to match SNAP encapsulation format and the corresponding protocol type values. The *etype-id* argument is the Ethernet type of inbound packets, in the range 0x0600 to 0xffff (excluding **ipx snap** under the **snap** encapsulation format).

*protocol-index*: Protocol index, ranging from 0 to 15, which specifies the protocol template to be bound with the current VLAN. System will automatically assign an index if this parameter is not specified.

**to** *protocol-end*: Specifies the end protocol index, ranging from 0 to 15. The *protocol-end* argument must be greater than or equal to the *protocol-index* argument.

**all**: Specifies to remove all the protocols bound with the current VLAN.



### Caution

- Do not configure both the *dsap-id* and *ssap-id* arguments in the **protocol-vlan** command as 0xe0 or 0xff when configuring the user-defined template for **llc** encapsulation. Otherwise, the encapsulation format of the matching packets will be the same as that of the **ipx llc** or **ipx raw** packets respectively. When either of the *dsap-id* and *ssap-id* arguments is configured, the system assigns **aa** to the other argument.
- When you use the **mode** keyword to configure a user-defined protocol template, do not set *etype-id* in **ethernetii etype** *etype-id* to 0x0800, 0x8137, 0x809b, or 0x86dd. Otherwise, the encapsulation format of the matching packets will be the same as that of the IPv4, IPX, AppleTalk, and IPv6 packets respectively.

---

## Description

Use the **protocol-vlan** command to configure the VLAN as a protocol based VLAN and configure the protocol template for the VLAN.

Use the **undo protocol-vlan** command to remove the configured protocol template.

By default, no VLAN is bound with any protocol template.

Related commands: **display protocol-vlan vlan**.



### Note

Do not configure a VLAN as both a protocol-based VLAN and a voice VLAN.

---

## Examples

# Configure VLAN 3 as an IPv4 based VLAN.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] protocol-vlan ipv4
```



### Caution

Because IP depends on ARP for address resolution in Ethernet, you are recommended to configure the IP and ARP templates in the same VLAN and associate them with the same port to prevent communication failure.

---

# Create an ARP protocol template for VLAN 3 (ARP code is 0x0806) to make VLAN 3 transmit ARP packets.

- To use Ethernet encapsulation, use the command:  
`[Sysname-vlan3] protocol-vlan mode ethernetii etype 0806`
- To use 802.3 encapsulation, use the command:  
`[Sysname-vlan3] protocol-vlan mode snap etype 0806`

## IP Subnet-Based VLAN Configuration Commands

### display ip-subnet-vlan interface

#### Syntax

**display ip-subnet-vlan interface** { *interface-list* | **all** }

#### View

Any view

#### Default Level

2: System level

#### Parameters

*interface-list*: Specifies an Ethernet port list in the format of *interface-list* = { *interface-type interface-number* [ **to** *interface-type interface-number* ] }&<1-10>, where *interface-type interface-number* represents the port type and port number and &<1-10> indicates that you can specify up to 10 ports or port ranges.

**all**: Displays IP subnet-based VLAN information about all the ports with IP subnet-based VLAN configured.

#### Description

Use the **display ip-subnet-vlan interface** command to display IP subnet-based VLANs and IP subnet indexes on the specified port(s).

#### Examples

# Display IP subnet-based VLANs and IP subnet indexes on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname]display ip-subnet-vlan interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
  VLAN ID   Subnet-Index   IP ADDRESS      NET MASK
=====
```

**Table 1-6** display ip-subnet-vlan interface command output description

Field	Description
Interface	Interface of which you want to view the information
VLAN ID	VLAN ID
Subnet-Index	Index of the IP subnet
IP ADDRESS	IP address of the subnet (either an IP address or a network address)
NET MASK	Mask of the IP subnet

## display ip-subnet-vlan vlan

### Syntax

```
display ip-subnet-vlan vlan { vlan-id [ to vlan-id ] | all }
```

### View

Any view

### Default Level

2: System level

### Parameters

*vlan-id*: VLAN ID, in the range 1 to 4094.

**to**: Specifies a VLAN ID range. The argument after this keyword must be greater than or equal to the one before this keyword.

**all**: Specifies all the VLANs.

### Description

Use the **display ip-subnet-vlan vlan** command to display the IP subnet information and IP subnet indexes on the specified VLAN(s).

Related commands: **display vlan**.

### Examples

# Display the IP subnet information of all VLANs.

```
<Sysname> display ip-subnet-vlan vlan all
```

```
VLAN ID: 3
```

```
Subnet Index      IP Address      Subnet Mask
```

```
=====
```

```
0                192.168.1.0    255.255.255.0
```

**Table 1-7 display ip-subnet-vlan vlan command output description**

Field	Description
VLAN ID	VLAN ID
Subnet Index	IP subnet index
IP Address	IP address of the subnet (can be an IP address or a network address)
Subnet Mask	Mask of the IP subnet

## ip-subnet-vlan

### Syntax

```
ip-subnet-vlan [ ip-subnet-index ] ip ip-address [ mask ]  
undo ip-subnet-vlan { ip-subnet-index [ to ip-subnet-end ] | all }
```

### View

VLAN view

### Default Level

2: System level

### Parameters

*ip-subnet-index*: Beginning IP subnet Index, in the range of 0 to 11. This value can be configured by users, or automatically numbered by system based on the order in which the IP subnets or IP addresses are associated with the VLAN.

**ip ip-address [mask]**: Specifies the source IP address or network address based on which the subnet-based VLANs are classified, in dotted decimal notation. The *mask* argument is the subnet mask of the source IP address or network address, in dotted decimal notation with a default value of 255.255.255.0.

**to**: Specifies an IP subnet index range.

*ip-subnet-end*: End IP subnet index, in the range of 0 to 11. This argument must be greater than or equal to the beginning IP subnet index.

**all**: Removes all the associations between VLANs and IP subnets or IP addresses.

### Description

Use the **ip-subnet-vlan** command to associate the current VLAN with a specified IP subnet or IP address.

Use the **undo ip-subnet-vlan** command to remove the association.

Note that the IP subnet or IP address cannot be a multicast network segment or a multicast address.

Related commands: **display ip-subnet-vlan vlan**.

### Examples

```
# Configure VLAN 3 as an IP subnet-based VLAN and associate it with the 192.168.1.0/24 network segment.
```

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0
```

## port hybrid ip-subnet-vlan vlan

### Syntax

```
port hybrid ip-subnet-vlan vlan vlan-id
undo port hybrid ip-subnet-vlan { vlan vlan-id | all }
```

### View

Ethernet interface view, port group view, Layer-2 aggregate interface view

### Default Level

2: System level

### Parameters

*vlan-id*: VLAN ID, in the range of 1 to 4094.

**all**: Specifies all VLANs.

### Description

Use the **port hybrid ip-subnet-vlan vlan** command to associate the current Ethernet port with the specified IP subnet-based VLAN.

Use the **undo port hybrid ip-subnet-vlan vlan** command to remove the association.

On an Ethernet port associated with an IP subnet-based VLAN, if the source IP address of a received untagged packet belongs to the corresponding IP subnet, the port tags the packet with the corresponding VLAN tag.

- In port group view, this command applies to all ports in the port group. For information about port groups, refer to *Ethernet Interface Configuration* in the *Access Volume*.
- In Layer-2 aggregate interface view, this command applies to the Layer-2 aggregate interface and all its member ports. After you perform the configuration, the system starts applying the configuration to the aggregate interface and its aggregation member ports. If the system fails to do that on the aggregate interface, it stops applying the configuration to the aggregation member ports. If it fails to do that on an aggregation member port, it simply skips the port and moves to the next port. For information about Layer-2 aggregate interfaces, refer to *Link Aggregation Configuration* in the *Access Volume*.

Currently, only hybrid ports support this feature. Before issuing this command, make sure that you have assigned the port to the IP subnet-based VLAN to be associated with.

Related commands: **display ip-subnet-vlan interface**.

### Examples

```
# Associate GigabitEthernet 1/0/1 with the IP subnet-based VLAN 3.
```

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0
[Sysname-vlan3] quit
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 3 untagged
Please wait... Done.
[Sysname-GigabitEthernet1/0/1] port hybrid ip-subnet-vlan vlan 3
```

# Associate the hybrid Layer-2 aggregate interface **Bridge-aggregation 1** with the IP subnet-based VLAN 3 (assuming that **Bridge-aggregation 1** does not have member ports).

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0
[Sysname-vlan3] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port link-type hybrid
[Sysname-Bridge-Aggregation1] port hybrid vlan 3 untagged
Please wait... Done
[Sysname-Bridge-Aggregation1] port hybrid ip-subnet-vlan vlan 3
```

# Associate the hybrid Layer-2 aggregate interface **Bridge-aggregation 1** with the IP subnet-based VLAN 3. Among the member ports of the aggregation group corresponding to **Bridge-aggregation 1**, GigabitEthernet 1/0/2 is an access port and GigabitEthernet 1/0/3 is a trunk port.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0
[Sysname-vlan3] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port link-type access
Please wait... Done.
Configuring GigabitEthernet1/0/2... Done.
Configuring GigabitEthernet1/0/3..... Done.
[Sysname-Bridge-Aggregation1] port link-type hybrid
[Sysname-Bridge-Aggregation1] port hybrid vlan 3 untagged
Please wait... Done.
Configuring GigabitEthernet1/0/2... Done.
Configuring GigabitEthernet1/0/3... Done.
[Sysname-Bridge-Aggregation1] port hybrid ip-subnet-vlan vlan 3
```

# 2 Isolate-User-VLAN Configuration Commands

---

## Isolate-User-VLAN Configuration Commands

### display isolate-user-vlan

#### Syntax

```
display isolate-user-vlan [ isolate-user-vlan-id ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

*isolate-user-vlan-id*: Isolate-user-VLAN ID, in the range of 1 to 4094.

#### Description

Use the **display isolate-user-vlan** command to display the mapping between an isolate-user-vlan and secondary VLAN(s), and the information of these VLANs.

Related commands: **isolate-user-vlan**, **isolate-user-vlan enable**.

#### Examples

# Display the mapping between an isolate-user-vlan and secondary VLANs.

```
<Sysname> display isolate-user-vlan
```

```
Isolate-user-VLAN VLAN ID : 2
```

```
Secondary VLAN ID : 3 4
```

```
VLAN ID: 2
```

```
VLAN Type: static
```

```
Isolate-user-VLAN type : isolate-user-VLAN
```

```
Route Interface: configured
```

```
IP Address: 1.1.1.1
```

```
Subnet Mask: 255.255.255.0
```

```
Description: VLAN 0002
```

```
Name: VLAN 0002
```

```
Tagged Ports: none
```

```
Untagged Ports:
```

```
    GigabitEthernet1/0/2
```

```
    GigabitEthernet1/0/3
```

```
    GigabitEthernet1/0/4
```

```
VLAN ID: 3
```

```
VLAN Type: static
```

```

Isolate-user-VLAN type : secondary
Route Interface: configured
IP Address: 2.2.2.2
Subnet Mask: 255.255.255.0
Description: VLAN 0003
Name: VLAN 0003
Tagged  Ports: none
Untagged Ports:
    GigabitEthernet1/0/2          GigabitEthernet1/0/3

```

```

VLAN ID: 4
VLAN Type: static
Isolate-user-VLAN type : secondary
Route Interface: not configured
Description: VLAN 0004
Name: VLAN 0004
Tagged  Ports: none
Untagged Ports:
    GigabitEthernet1/0/2          GigabitEthernet1/0/4

```

**Table 2-1 display isolate-user-vlan command output description**

Field	Description
Isolate-user-VLAN VLAN ID	Isolate-user-VLAN ID
Secondary VLAN ID	Secondary VLAN ID
VLAN ID	VLAN ID
VLAN Type	VLAN type, static or dynamic
Isolate-user-VLAN type	Current VLAN type, isolate-user-VLAN or secondary VLAN
Route Interface	Whether a VLAN interface is configured for the VLAN
IP Address	IP address of the VLAN interface, if configured. This field is not displayed if no IP address is configured for the VLAN interface.
Subnet Mask	Subnet mask of the VLAN interface, if configured. This field is not displayed if no mask is configured for the VLAN interface.
Description	VLAN description
Name	Name configured for the VLAN
Tagged Ports	Ports through which packets of this VLAN are sent tagged
Untagged Ports	Ports through which packets of this VLAN are sent untagged

## isolate-user-vlan

### Syntax

**isolate-user-vlan** *isolate-user-vlan-id* **secondary** *secondary-vlan-id* [ **to** *secondary-vlan-id* ]

**undo isolate-user-vlan** *isolate-user-vlan-id* [ **secondary** *secondary-vlan-id* [ **to** *secondary-vlan-id* ] ]

## View

System view

## Default Level

2: System level

## Parameters

*isolate-user-vlan-id*: Isolate-user-VLAN ID, in the range 1 to 4094.

**secondary** *secondary-vlan-id* [ **to** *secondary-vlan-id* ]: Specifies a secondary VLAN ID or a secondary VLAN ID range. The *secondary-vlan-id* argument is a secondary VLAN ID, in the range 1 to 4094.

## Description

Use the **isolate-user-vlan** command to associate an isolate-user-VLAN with the specified secondary VLAN(s).

Use the **undo isolate-user-vlan** command to remove the association.

By default, an isolate-user-VLAN is not associated with any secondary VLAN. .

Note that:

- To use the **isolate-user-vlan** command, each of the isolate-user-VLAN and the secondary VLAN(s) must have at least one port which allows its isolate-user-VLAN or secondary VLAN to pass through, and the default VLAN of the port must be its isolate-user-VLAN or secondary VLAN.
- The **undo isolate-user-vlan** command without the **secondary** *secondary-vlan-id* parameter specified removes the association between the specified isolate-user-VLAN and all its secondary VLANs, while the **undo isolate-user-vlan** command with the **secondary** *secondary-vlan-id* parameter specified only removes the association between the specified isolate-user-VLAN and the specified secondary VLANs.



### Note

After associating an isolate-user-VLAN with the specified secondary VLANs, you cannot add/remove a port to/from each involved VLAN or remove each involved VLAN. To do that, you must cancel the association first.

---

Related commands: **display isolate-user-vlan**.

## Examples

# Associate isolate-user-VLAN 2 with the secondary VLANs VLAN 3 and VLAN 4.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] isolate-user-vlan enable
[Sysname-vlan2] port gigabitethernet 1/0/2
[Sysname-vlan2] vlan 3
[Sysname-vlan3] port gigabitethernet 1/0/3
[Sysname-vlan3] vlan 4
```

```
[Sysname-vlan4] port gigabitethernet 1/0/4
[Sysname-vlan4] quit
[Sysname] isolate-user-vlan 2 secondary 3 to 4
```

## isolate-user-vlan enable

### Syntax

```
isolate-user-vlan enable
undo isolate-user-vlan enable
```

### View

VLAN view

### Default Level

2: System level

### Parameters

None

### Description

Use the **isolate-user-vlan enable** command to configure the current VLAN as an isolate-user-VLAN.

Use the **undo isolate-user-vlan enable** command to remove the isolate-user-VLAN configuration for the current VLAN.

By default, no VLAN is an isolate-user-VLAN.

An isolate-user-VLAN may include multiple ports, including the one connected to the upstream device.

Related commands: **display isolate-user-vlan**.

### Examples

# Configure VLAN 5 as an isolate-user-VLAN.

```
<Sysname> system-view
[Sysname] vlan 5
[Sysname-vlan5] isolate-user-vlan enable
```

# 3 Voice VLAN Configuration Commands

---

## Voice VLAN Configuration Commands

### display voice vlan oui

#### Syntax

```
display voice vlan oui
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

None

#### Description

Use the **display voice vlan oui** command to display the currently supported organizationally unique identifier (OUI) addresses, the OUI address masks, and the description strings.

Related commands: **voice vlan mac-address**.



#### Note

In general, as the first 24 bits of a MAC address (in binary format), an OUI address is a globally unique identifier assigned to a vendor by IEEE. OUI addresses mentioned in this document, however, are different from those in common sense. OUI addresses in this document are used to determine whether a received packet is a voice packet. They are the results of the AND operation of the two arguments *mac-address* and *oui-mask* in the **voice vlan mac-address** command.

---

#### Examples

```
# Display the currently supported OUI addresses.
```

```
<Sysname> display voice vlan oui
Oui Address      Mask              Description
0001-e300-0000   ffff-ff00-0000   Siemens phone
0003-6b00-0000   ffff-ff00-0000   Cisco phone
0004-0d00-0000   ffff-ff00-0000   Avaya phone
0060-b900-0000   ffff-ff00-0000   Philips/NEC phone
```

```

00d0-1e00-0000 ffff-ff00-0000 Pingtel phone
00e0-7500-0000 ffff-ff00-0000 Polycom phone
00e0-bb00-0000 ffff-ff00-0000 3com phone

```

**Table 3-1 display voice vlan oui command output description**

Field	Description
Oui Address	OUI addresses supported
Mask	Masks of the OUI addresses supported
Description	Description strings of the OUI addresses supported

## display voice vlan state

### Syntax

```
display voice vlan state
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display voice vlan state** command to display voice VLAN configuration.

Related commands: **voice vlan *vlan-id* enable**, **voice vlan enable**.

### Examples

```
# Display voice VLAN configurations.
```

```

<Sysname> display voice vlan state
Maximum of Voice VLANs: 8
Current Voice VLANs: 2
Voice VLAN security mode: Security
Voice VLAN aging time: 1440 minutes
Voice VLAN enabled port and its mode:
PORT                VLAN      MODE
-----
GigabitEthernet1/0/1    2        AUTO
GigabitEthernet1/0/2    3        AUTO

```

**Table 3-2 display voice vlan state** command output description

Field	Description
Maximum of Voice VLANs	Maximum number of voice VLANs supported by the system
Current Voice VLANs	Number of existing voice VLANs
Voice VLAN security mode	Security mode of the voice VLAN: Security for security mode; Normal for normal mode
Voice VLAN aging time	Aging time of the voice VLAN
Voice VLAN enabled port and its mode	Voice VLAN-enabled port and its voice VLAN assignment mode
PORT	Voice VLAN-enabled port name
VLAN	ID of the voice VLAN enabled on the port
MODE	Voice VLAN assignment mode of the port: manual or automatic.

## voice vlan aging

### Syntax

**voice vlan aging** *minutes*

**undo voice vlan aging**

### View

System view

### Default Level

2: System level

### Parameters

*minutes*: Voice VLAN aging time, in the range 5 to 43200 minutes.

### Description

Use the **voice vlan aging** command to configure the voice VLAN aging time.

Use the **undo voice vlan aging** command to restore the default.

By default, the voice VLAN aging time is 1440 minutes.

When a port in automatic voice VLAN assignment mode receives a voice packet, the system decides whether to assign the port to the voice VLAN based on the source MAC address of the voice packet. Upon assigning the port to the voice VLAN, the system starts the aging timer. If no voice packets are received on the port until the aging time expires, the system automatically removes the port from the voice VLAN. This aging time only applies to the ports in automatic voice VLAN assignment mode.

Related commands: **display voice vlan state**.

### Examples

# Configure the voice VLAN aging time as 100 minutes.

```
<Sysname> system-view  
[Sysname] voice vlan aging 100
```

## voice vlan enable

### Syntax

```
voice vlan vlan-id enable  
undo voice vlan enable
```

### View

Ethernet interface view

### Default Level

2: System level

### Parameters

*vlan-id*: VLAN to be configured as the voice VLAN for the current port.

### Description

Use the **voice vlan enable** command to enable the voice VLAN feature and configure a VLAN as the voice VLAN for the current Ethernet port.

Use the **undo voice vlan enable** command to disable the voice VLAN feature on an Ethernet port.

By default, the voice VLAN feature is disabled on ports.

You can enable the voice VLAN feature on a hybrid or trunk port operating in automatic voice VLAN assignment mode but not on an access port operating in automatic voice VLAN assignment mode.

You can configure different voice VLANs for different ports. An S4800G switch supports up to eight voice VLANs globally.

### Examples

```
# Enable the voice VLAN feature on GigabitEthernet 1/0/1.  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] voice vlan 2 enable
```

## voice vlan mac-address

### Syntax

```
voice vlan mac-address mac-address mask oui-mask [ description text ]  
undo voice vlan mac-address oui
```

### View

System view

### Default Level

2: System level

### Parameters

*mac-address*: Source MAC address of voice traffic, in the format of H-H-H, such as 1234-1234-1234.

**mask** *oui-mask*: Specifies the valid length of the OUI address by a mask in the format of H-H-H, formed by consecutive fs and 0s, for example, ffff-0000-0000. To filter the voice device of a specific vendor, set the mask to ffff-ff00-0000.

**description** *text*: Specifies a string that describes the OUI address. The string is of 1 to 30 case-sensitive characters.

*oui*: Specifies the OUI address to be removed, in the format of H-H-H, such as 1234-1200-0000. An OUI address is the logic AND result of *mac-address* and *oui-mask*. An OUI address cannot be a broadcast address, a multicast address, or an address of all 0s or all fs. You can use the **display voice vlan oui** command to display the OUI addresses supported currently.

## Description

Use the **voice vlan mac-address** command to add a recognizable OUI address.

Use the **undo voice vlan mac-address** command to remove a recognizable OUI address.

The system supports up to 16 OUI addresses.

By default, the system is configured with the default OUI addresses, as illustrated in [Table 3-3](#). You can remove the default OUI addresses and then add recognizable OUI addresses manually.

**Table 3-3** Default OUI addresses

Number	OUI	Description
1	0001-e300-0000	Siemens phone
2	0003-6b00-0000	Cisco phone
3	0004-0d00-0000	Avaya phone
4	00d0-1e00-0000	Pingtel phone
5	0060-b900-0000	Philips/NEC phone
6	00e0-7500-0000	Polycom phone
7	00e0-bb00-0000	3com phone

Related commands: **display voice vlan oui**.

## Examples

```
# Add a recognizable OUI address 1234-1200-0000 by specifying the MAC address as 1234-1234-1234 and the mask as fff-ff00-0000, and configure its description string as PhoneA.
```

```
<Sysname> system-view
[Sysname] voice vlan mac-address 1234-1234-1234 mask ffff-ff00-0000 description PhoneA
```

```
# Display the supported OUI addresses to verify the above configuration.
```

```
<Sysname> display voice vlan oui
Oui Address      Mask             Description
0001-e300-0000   ffff-ff00-0000 Siemens phone
0003-6b00-0000   ffff-ff00-0000 Cisco phone
0004-0d00-0000   ffff-ff00-0000 Avaya phone
00d0-1e00-0000   ffff-ff00-0000 Pingtel phone
0060-b900-0000   ffff-ff00-0000 Philips/NEC phone
00e0-7500-0000   ffff-ff00-0000 Polycom phone
```

```
00e0-bb00-0000 ffff-ff00-0000 3com phone
1234-1200-0000 ffff-ff00-0000 PhoneA

# Remove the OUI address 1234-1200-0000.

<Sysname> system-view
[Sysname] undo voice vlan mac-address 1234-1200-0000
```

## voice vlan mode auto

### Syntax

```
voice vlan mode auto
undo voice vlan mode auto
```

### View

Ethernet interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **voice vlan mode auto** command to configure the current port to operate in automatic voice VLAN assignment mode.

Use the **undo voice vlan mode auto** command to configure the current port to operate in manual voice VLAN assignment mode.

By default, a port operates in automatic voice VLAN assignment mode.

The voice VLAN modes of different ports are independent of one another.

To make voice VLAN take effect on a port which is enabled with voice VLAN and operates in manual voice VLAN assignment mode, you need to assign the port to the voice VLAN manually.

### Examples

```
# Configure GigabitEthernet 1/0/1 to operate in manual voice VLAN assignment mode.

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo voice vlan mode auto
```

## voice vlan security enable

### Syntax

```
voice vlan security enable
undo voice vlan security enable
```

### View

System view

## Default Level

2: System level

## Parameters

None

## Description

Use the **voice vlan security enable** command to enable voice VLAN security mode.

Use the **undo voice vlan security enable** command to disable voice VLAN security mode.

By default, voice VLAN security mode is not enabled.

## Examples

# Disable voice VLAN security mode.

```
<Sysname> system-view
```

```
[Sysname] undo voice vlan security enable
```

# Table of Contents

<b>1 GVRP Configuration Commands</b> .....	<b>1-1</b>
GVRP Configuration Commands .....	1-1
display garp statistics .....	1-1
display garp timer .....	1-2
display gvrp local-vlan interface .....	1-3
display gvrp state.....	1-3
display gvrp statistics.....	1-4
display gvrp status.....	1-5
display gvrp vlan-operation interface.....	1-5
garp timer hold.....	1-6
garp timer join.....	1-6
garp timer leave.....	1-7
garp timer leaveall .....	1-8
gvrp.....	1-9
gvrp registration.....	1-9
reset garp statistics.....	1-10

# 1 GVRP Configuration Commands

---

## GVRP Configuration Commands

### display garp statistics

#### Syntax

```
display garp statistics [ interface interface-list ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

**interface** *interface-list*. Defines one or multiple Ethernet ports for which the GARP statistics will be displayed. You can provide up to 10 Ethernet port lists, by each of which you can specify an individual port in the form of *interface-type interface-number*, or a port range in the form of *interface-type interface-number1 to interface-type interface-number2*, where the end-port number specified by *interface-number2* must be greater than the start-port number specified by *interface-number1*. If no ports are specified, this command displays the GARP statistics for all ports.

#### Description

Use the **display garp statistics** command to display the GARP statistics of the specified port(s) or all ports if no ports are specified.

This command displays the statistics about GVRP packets received, transmitted, and dropped on GVRP-enabled ports. When the system is restarted or after you perform the **reset garp statistics** command, the existing packet statistics are cleared and the system starts to collect new GARP statistics. With the statistics, you can judge whether a GVRP-enabled port is operating normally.

- If the number of received and transmitted GVRP packets on the port is the same as that on the remote port, it indicates that the two ends are transmitting and receiving GVRP packets normally and no registration information is lost.
- If there are dropped GVRP packets on the port, check its registration mode. GVRP packets are likely to be dropped if the registration mode is fixed or forbidden, because dynamic VLANs cannot be registered in either of the modes.

Related commands: **reset garp statistics**.

#### Examples

# Display GARP statistics on ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
<Sysname> display garp statistics interface gigabitethernet 1/0/1 to gigabitethernet 1/0/2
```

```
GARP statistics on port GigabitEthernet1/0/1
```

```
Number of GVRP Frames Received      : 0  
Number of GVRP Frames Transmitted   : 0  
Number of Frames Discarded          : 0
```

```
GARP statistics on port GigabitEthernet1/0/2
```

```
Number of GVRP Frames Received      : 0  
Number of GVRP Frames Transmitted   : 0  
Number of Frames Discarded          : 0
```

## display garp timer

### Syntax

```
display garp timer [ interface interface-list ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**interface** *interface-list*: Defines one or multiple Ethernet ports. You can provide up to 10 Ethernet port lists, by each of which you can specify an individual port in the form of *interface-type interface-number*, or a port range in the form of *interface-type interface-number1 to interface-type interface-number2*, where the end-port number specified by *interface-number2* must be greater than the start-port number specified by *interface-number1*. If no ports are specified, this command displays the GARP timer settings on all ports.

### Description

Use the **display garp timer** command to display GARP timer settings of specific ports.

Related commands: **garp timer hold**, **garp timer join**, **garp timer leave**, **garp timer leaveall**.

### Examples

```
# Display GARP timers on port GigabitEthernet 1/0/1.
```

```
<Sysname> display garp timer interface gigabitethernet 1/0/1  
GARP timers on port GigabitEthernet1/0/1
```

```
Garp Join Time      : 20 centiseconds  
Garp Leave Time     : 60 centiseconds  
Garp LeaveAll Time  : 1000 centiseconds  
Garp Hold Time      : 10 centiseconds
```

## display gvrp local-vlan interface

### Syntax

**display gvrp local-vlan interface** *interface-type interface-number*

### View

Any view

### Default Level

0: Visit level

### Parameters

**interface** *interface-type interface-number*. Specifies an interface by its type and number.

### Description

Use the **display gvrp local-vlan interface** command to display the local VLAN information maintained by GVRP on the specified port.

### Examples

# Display the local VLAN information maintained by GVRP on GigabitEthernet 1/0/1.

```
<Sysname> display gvrp local-vlan interface gigabitethernet 1/0/1
Following VLANs exist in GVRP local database:
 1(default),2-500
```

## display gvrp state

### Syntax

**display gvrp state interface** *interface-type interface-number* **vlan** *vlan-id*

### View

Any view

### Default Level

0: Visit level

### Parameters

**interface** *interface-type interface-number*. Specifies an interface by its type and number.

**vlan** *vlan-id*: Specifies a VLAN ID, in the range of 1 to 4094.

### Description

Use the **display gvrp state** command to display the current GVRP state.

### Examples

# Display the GVRP state of VLAN 2, which GigabitEthernet 1/0/1 belongs to.

```
<Sysname> display gvrp state interface gigabitethernet 1/0/1 vlan 2
```

GVRP state of VLAN 2 on port GigabitEthernet1/0/1

```
Applicant state machine      : VP
Registrar state machine      : MTR
```

## display gvrp statistics

### Syntax

```
display gvrp statistics [ interface interface-list ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**interface** *interface-list*: Defines one or multiple Ethernet ports. You can provide up to 10 Ethernet port lists, by each of which you can specify an individual port in the form of *interface-type interface-number*, or a port range in the form of *interface-type interface-number1 to interface-type interface-number2*, where the end-port number specified by *interface-number2* must be greater than the start-port number specified by *interface-number1*. If no ports are specified, this command displays the GVRP statistics for all trunk ports.

### Description

Use the **display gvrp statistics** command to display the GVRP statistics of specified or all trunk ports.

### Examples

```
# Display statistics about GVRP for trunk port GigabitEthernet 1/0/1.
```

```
<Sysname> display gvrp statistics interface gigabitethernet 1/0/1
GVRP statistics on port GigabitEthernet1/0/1
```

```
GVRP Status                : Enabled
GVRP Running                : YES
GVRP Failed Registrations   : 0
GVRP Last Pdu Origin        : 000F-E207-F2E0
GVRP Registration Type      : Normal
```

**Table 1-1** display gvrp statistics command output description

Field	Description
GVRP Status	Indicates whether GVRP is enabled or disabled.
GVRP Running	Indicates whether GVRP is running.
GVRP Failed Registrations	Indicates the number of GVRP registration failures.
GVRP Last Pdu Origin	Indicates the source MAC address in the last GVRP PDU.
GVRP Registration Type	Indicates the GVRP registration type on the port.

## display gvrp status

### Syntax

```
display gvrp status
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display gvrp status** command to display the global enable/disable state of GVRP.

### Examples

```
# Display the global GVRP enable/disable state.
```

```
<Sysname> display gvrp status
          GVRP is enabled
```

## display gvrp vlan-operation interface

### Syntax

```
display gvrp vlan-operation interface interface-type interface-number
```

### View

Any view

### Default Level

0: Visit level

### Parameters

**interface** *interface-type interface-number*: Specifies an interface by its type and number.

### Description

Use the **display gvrp vlan-operation interface** command to display the information about dynamic VLAN operations performed on a port.

### Examples

```
# Display the information about dynamic VLAN operations performed on GigabitEthernet 1/0/1.
```

```
<Sysname> display gvrp vlan-operation interface gigabitethernet 1/0/1
          Dynamic VLAN operations on port GigabitEthernet1/0/1
```

```
          Operations of creating VLAN           : 2-100
          Operations of deleting VLAN          : none
```

Operations of adding VLAN to TRUNK : 2-100  
Operations of deleting VLAN from TRUNK : none

## garp timer hold

### Syntax

```
garp timer hold timer-value  
undo garp timer hold
```

### View

Ethernet interface view, Layer-2 aggregate interface view, port group view

### Default Level

2: System level

### Parameters

*timer-value*: Hold timer setting (in centiseconds), which must be a multiple of 5 in the range of 10 (inclusive) and half of the Join timer setting (inclusive). When the Join timer is set to the default, the value range for the Hold timer is 10 (inclusive) to 10 (inclusive).



#### Note

One second equals 100 centiseconds.

---

### Description

Use the **garp timer hold** command to set the GARP Hold timer for an Ethernet port, Layer-2 aggregate interface, or all ports in a port group.

Use the **undo garp timer hold** command to restore the default of the GARP Hold timer. This may fail if the default is beyond the valid value range for the Hold timer.

By default, the hold timer is set to 10 centiseconds.

Related commands: **display garp timer**, **garp timer join**.

### Examples

```
# Set the GARP Hold timer to 15 centiseconds, assuming that the Join timer is 30 centiseconds.
```

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] garp timer hold 15
```

## garp timer join

### Syntax

```
garp timer join timer-value  
undo garp timer join
```

## View

Ethernet interface view, Layer-2 aggregate interface view, port group view

## Default Level

2: System level

## Parameters

*timer-value*: Join timer setting (in centiseconds), which must be a multiple of 5 in the range of two times the Hold timer (inclusive) and half of the Leave timer (inclusive). When the Hold timer and the Leave timer are set to their default, the value range for the Join timer is 20 (inclusive) to 25 (inclusive).

## Description

Use the **garp timer join** command to set the GARP Join timer for an Ethernet port, Layer-2 aggregate interface, or all ports in a port group.

Use the **undo garp timer join** command to restore the default of the GARP Join timer. This may fail if the default is beyond the valid value range for the Join timer.

By default, the Join timer is set to 20 centiseconds.

Related commands: **display garp timer**, **garp timer hold**, **garp timer leave**.

## Examples

# Set the GARP Join timer to 25 centiseconds, assuming that both the Hold timer and the Leave timer are using the default.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] garp timer join 25
```

## garp timer leave

### Syntax

**garp timer leave** *timer-value*

**undo garp timer leave**

### View

Ethernet interface view, Layer-2 aggregate interface view, port group view

### Default Level

2: System level

### Parameters

*timer-value*: Leave timer setting (in centiseconds), which must be a multiple of 5 between two times the Join timer (exclusive) and the LeaveAll timer setting (exclusive). When the Join timer and the LeaveAll timer are set to their default, the value range for the Leave timer is 45 (inclusive) to 995 (inclusive).

### Description

Use the **garp timer leave** command to set the GARP Leave timer for an Ethernet port, Layer-2

aggregate interface, or all ports in a port group.

Use the **undo garp timer leave** command to restore the default of the GARP Leave timer. This may fail if the default is beyond the valid value range for the Leave timer.

By default, the Leave timer is set to 60 centiseconds.

Related commands: **display garp timer**, **garp timer join**, **garp timer leaveall**.

## Examples

# Set the GARP Leave timer to 100 centiseconds, assuming that both the Join timer and the LeaveAll timer are using the default.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] garp timer leave 100
```

## garp timer leaveall

### Syntax

**garp timer leaveall** *timer-value*

**undo garp timer leaveall**

### View

System view

### Default Level

2: System level

### Parameters

*timer-value*: Leaveall timer setting (in centiseconds), which must be a multiple of 5 in the range of the maximum Leave timer on the device (exclusive) and 32765 (inclusive). When the Leave timers on all ports are set to the default, the value range for the LeaveAll timer is 65 (inclusive) to 32765 (inclusive).

### Description

Use the **garp timer leaveall** command to set the GARP LeaveAll timer.

Use the **undo garp timer leaveall** command to restore the default. This may fail if the default is beyond the valid value range for the LeaveAll timer. .

By default, the setting of the LeaveAll timer is 1000 centiseconds.

Related commands: **display garp timer**, **garp timer leave**.

## Examples

# Set the leaveall timer to 100 centiseconds, assuming that the Leave timer on every port is set to 60 centiseconds.

```
<Sysname> system-view
[Sysname] garp timer leaveall 100
```

## **gvrp**

### **Syntax**

```
gvrp  
undo gvrp
```

### **View**

System view, Ethernet interface view, Layer-2 aggregate interface view, port group view

### **Default Level**

2: System level

### **Parameters**

None

### **Description**

Use the **gvrp** command to enable GVRP globally (in system view), on a port (in Ethernet or Layer-2 aggregate interface view), or on all ports in a port group (in port group view).

Use the **undo gvrp** command to disable GVRP globally, on a port, or on all ports in a port group depending on the view where the command is executed.

By default, GVRP is disabled.

Note that:

- To enable GVRP on a port, you need to enable it globally first and then on the port.
- You can use this command on trunk ports only.
- You cannot change the link type of a GVRP-enabled trunk port.

Related commands: **display gvrp status**.

### **Examples**

```
# Enable GVRP globally.  
  
<Sysname> system-view  
[Sysname] gvrp  
GVRP is enabled globally.
```

## **gvrp registration**

### **Syntax**

```
gvrp registration { fixed | forbidden | normal }  
undo gvrp registration
```

### **View**

Ethernet interface view, Layer-2 aggregate interface view, port group view

### **Default Level**

2: System level

## Parameters

**fixed:** Sets the registration type to fixed.

**forbidden:** Sets the registration type to forbidden.

**normal:** Sets the registration type to normal.

## Description

Use the **gvrp registration** command to configure the GVRP registration type on a port (in Ethernet or Layer-2 aggregate interface view) or all ports in a port group (in port group view).

Use the **undo gvrp registration** command to restore the default on a port, or on all ports in a port group depending on the view the command is executed.

The default GVRP registration type is normal.

Note that, this command is only available on trunk ports.

Related commands: **display garp statistics**.

## Examples

# Set the GVRP registration type to **fixed** on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] gvrp registration fixed
```

## reset garp statistics

### Syntax

```
reset garp statistics [ interface interface-list ]
```

### View

User view

### Default Level

2: System level

## Parameters

**interface** *interface-list*. Defines one or multiple Ethernet ports for which the GARP statistics are to be cleared. You can provide up to 10 Ethernet port lists, by each of which you can specify an individual port in the form of *interface-type interface-number*, or a port range in the form of *interface-type interface-number1 to interface-type interface-number2*, where the end-port number specified by *interface-number2* must be greater than the start-port number specified by *interface-number1*. If no ports are specified, this command clears the GARP statistics on all ports.

## Description

Use the **reset garp statistics** command to clear the GARP statistics on specified ports or all ports if no ports are specified.

The cleared statistics include the statistics about GVRP packets sent, received and dropped. You can use this command in conjunction with the **display garp statistics** command to display GARP statistics.

Related commands: **display gvrp statistics**.

### Examples

# Clear the GARP statistics on all ports.

```
<Sysname> reset garp statistics
```

# Table of Contents

<b>1 QinQ Configuration Commands</b> .....	<b>1-1</b>
QinQ Configuration Commands.....	1-1
raw-vlan-id inbound .....	1-1
qinq enable .....	1-2
qinq ethernet-type.....	1-3
qinq vid .....	1-4

# 1 QinQ Configuration Commands

---



Throughout this document, customer network VLANs (CVLANs), also called inner VLANs, refer to the VLANs that a customer uses on the private network; and service provider network VLANs (SVLANs), also called outer VLANs, refer to the VLANs that a service provider uses to carry VLAN tagged traffic for customers.

---

## QinQ Configuration Commands

### raw-vlan-id inbound

#### Syntax

```
raw-vlan-id inbound { all | vlan-list }  
undo raw-vlan-id inbound { all | vlan-list }
```

#### View

QinQ view

#### Default Level

2: System level

#### Parameters

*vlan-list*: Specifies one or multiple CVLANs in the format of *vlan-list* = { *vlan-id* [ **to** *vlan-id* ] }<1-10>. You can provide up to 10 VLAN ID lists, by each of which you can specify an individual VLAN ID in the form of *vlan-id*, or a VLAN ID range in the form of *vlan-id* **to** *vlan-id*, where the VLAN ID after **to** must be greater than the VLAN ID before **to**. The *vlan-id* argument ranges from 1 to 4094.

**all**: Specifies all VLAN IDs.

#### Description

Use the **raw-vlan-id inbound** command to tag frames of the specified CVLANs with the current SVLAN.

Use the **undo raw-vlan-id inbound** command to remove the configuration.



### Caution

- You can run this command in the same view many times. A new configuration does not overwrite the previous ones and the configured values are arranged in an ascending order automatically.
  - An inner VLAN tag corresponds to only one outer VLAN tag.
  - If you want to change the outer VLAN tag, you need to delete the old outer tag configuration and then configure a new outer VLAN tag.
- 

Related commands: **qinq vid**.

### Examples

# Configure GigabitEthernet 1/0/1 to tag frames of VLAN 3, VLAN 5, and VLAN 20 through VLAN 100 with SVLAN 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qinq vid 100
[Sysname-GigabitEthernet1/0/1-vid-100] raw-vlan-id inbound 3 5 20 to 100
```

### qinq enable

#### Syntax

**qinq enable**

**undo qinq enable**

#### View

Ethernet interface view, Layer-2 aggregate interface view, port group view

#### Default Level

2: System level

#### Parameters

None

#### Description

Use the **qinq enable** command to enable basic QinQ on the current Ethernet port(s).

Use the **undo qinq enable** command to disable basic QinQ on the current Ethernet port(s).

By default, basic QinQ is disabled on Ethernet ports.

A basic QinQ-enabled port tags received frames with the port's default VLAN tag.

Note that:

- Configuration made in Ethernet interface view takes effect on the current port only. Configuration made in Layer-2 aggregate interface view takes effect on the Layer-2 aggregate interface and the member ports in its aggregation group. Configuration made in port group view takes effect on all ports in the port group.

- You can configure this command on a Layer-2 aggregate interface and its member ports separately. Configuration made on an aggregation member port takes effect immediately. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.

## Examples

# Enable basic QinQ on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qinq enable
```

# Enable basic QinQ on port group 1.

```
<Sysname> system-view
[Sysname] port-group manual 1
[Sysname-port-group-manual-1] group-member gigabitethernet 1/0/1 to gigabitethernet 1/0/6
[Sysname-port-group-manual-1] qinq enable
```

## qinq ethernet-type

### Syntax

**qinq ethernet-type** { **customer-tag** | **service-tag** } *hex-value*

**undo qinq ethernet-type** { **customer-tag** | **service-tag** }

### View

System view

### Default Level

2: System level

### Parameters

**customer-tag**: Indicates the TPID value in the CVLAN tag.

**service-tag**: Indicates the TPID value in the SVLAN tag.

*hex-value*: Hexadecimal protocol type value, in the range of 0x0001 to 0xFFFF. However, do not set it to any of the protocol type values listed in [Table 1-1](#).

**Table 1-1** Common protocol type values

Protocol type	Value
ARP	0x0806
PUP	0x0200
RARP	0x8035
IP	0x0800
IPv6	0x86DD
PPPoE	0x8863/0x8864
MPLS	0x8847/0x8848
IPX/SPX	0x8137

Protocol type	Value
IS-IS	0x8000
LACP	0x8809
802.1x	0x888E
Cluster	0x88A7
Reserved	0xFFFFD/0xFFFFE/0xFFFF

## Description

Use the **qinq ethernet-type** command to configure the TPID value in VLAN tags.

Use the **undo qinq ethernet-type** command in system view to restore the TPID value in VLAN tags to the system default; use the **undo qinq ethernet-type** command in Ethernet interface view, Layer-2 aggregate interface view, or port group view to restore the TPID value in VLAN tags to the global setting.

By default, the TPID value in both SVLAN tags and CVLAN tags is 0x8100.

Note that :

Configuration made in system view takes effect on all ports.

## Examples

# Set the TPID value in the SVLAN tags to 0x8200 globally.

```
<Sysname> system-view
[Sysname] qinq ethernet-type service-tag 8200
```

## qinq vid

### Syntax

**qinq vid** *vlan-id*

**undo qinq vid** *vlan-id*

### View

Ethernet interface view, Layer-2 aggregate interface view, port group view

### Default Level

2: System level

### Parameters

*vlan-id*: Outer VLAN ID, in the range of 1 to 4094.

## Description

Use the **qinq vid** command to enter QinQ view and configure the outer VLAN tag for the port to add.

Use the **undo qinq vid** command to remove all configurations corresponding to the outer VLAN ID performed in QinQ view.

By default, the outer VLAN tag is the port's default VLAN tag.

Note that:

- Configuration made in Ethernet interface view takes effect on the current port only. Configuration made in Layer-2 aggregate interface view takes effect on the Layer-2 aggregate interface and the member ports in its aggregation group. Configuration made in port group view takes effect on all ports in the port group.
- You can configure this command on a Layer-2 aggregate interface and its member ports separately. Configuration made on an aggregation member port takes effect immediately. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.

Related commands: **raw-vlan-id inbound**.

## Examples

# Configure GigabitEthernet 1/0/1 to tag frames with outer VLAN 10.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qinq vid 10
```

# Configure all the ports in port group 1 to tag frames with outer VLAN 10.

```
<Sysname> system-view
[Sysname] port-group manual 1
[Sysname-port-group-manual-1] group-member gigabitethernet 1/0/1 to gigabitethernet 1/0/6
[Sysname-port-group-manual-1] qinq vid 10
```

# Table of Contents

<b>1 BPDU Tunneling Configuration Commands</b> .....	<b>1-1</b>
BPDU Tunneling Configuration Commands .....	1-1
bpd-tunnel dot1q stp.....	1-1
bpd-tunnel tunnel-dmac.....	1-2

# 1 BPDU Tunneling Configuration Commands

---

## BPDU Tunneling Configuration Commands

### bpdu-tunnel dot1q stp

#### Syntax

```
bpdu-tunnel dot1q stp
undo bpdu-tunnel dot1q stp
```

#### View

Ethernet interface view, Layer-2 aggregate interface view, port group view

#### Default Level

2: System level

#### Parameters

None

#### Description

Use the **bpdu-tunnel dot1q stp** command to enable BPDU tunneling for STP on the current port or ports.

Use the **undo bpdu-tunnel dot1q stp** command to disable BPDU tunneling for STP on the port or ports.

By default, BPDU tunneling for STP is disabled.

Note that:

- Configuration made in Ethernet interface view takes effect on the current port only. Configuration made in Layer-2 aggregate interface view takes effect only on the Layer-2 aggregate interface. Configuration made in port group view takes effect on all ports in the port group.
- Configuration made on an aggregation group member port takes effect after the port exits the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.
- Before you can enable BPDU tunneling for STP on a port, disable STP on the port first.

#### Examples

```
# Enable BPDU tunneling for STP on GigabitEthernet 1/0/1.
```

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo stp enable
[Sysname-GigabitEthernet1/0/1] bpdu-tunnel dot1q stp
```

```
# Enable BPDU tunneling for STP on all the ports in port group 1.
```

```
<Sysname> system-view
[Sysname] port-group manual 1
[Sysname-port-group-manual-1] group-member gigabitethernet 1/0/1 to gigabitethernet 1/0/6
[Sysname-port-group-manual-1] undo stp enable
[Sysname-port-group-manual-1] bpdu-tunnel dot1q stp
```

## bpdu-tunnel tunnel-dmac

### Syntax

**bpdu-tunnel tunnel-dmac** *mac-address*

**undo bpdu-tunnel tunnel-dmac**

### View

System view

### Default Level

2: System level

### Parameters

*mac-address*: Destination multicast MAC address for BPDU tunnel frames, in the format of H-H-H. The allowed values are 0100-0CCD-CDD0, 0100-0CCD-CDD1, 0100-0CCD-CDD2, and 010F-E200-0003.

### Description

Use the **bpdu-tunnel tunnel-dmac** command to configure the destination multicast MAC address for BPDU tunnel frames.

Use the **undo bpdu-tunnel tunnel-dmac** command to restore the default value.

By default, the destination multicast MAC address for BPDU tunnel frames is 0x010F-E200-0003.

### Examples

# Set the destination multicast MAC address for BPDU tunnel frames to 0100-0CCD-CDD0.

```
<Sysname> system-view
[Sysname] bpdu-tunnel tunnel-dmac 0100-0ccd-cdd0
```

# Table of Contents

<b>1 VLAN Mapping Configuration Commands</b> .....	<b>1-1</b>
VLAN Mapping Configuration Commands.....	1-1
qinq enable downlink .....	1-1
qinq enable uplink.....	1-2

# 1 VLAN Mapping Configuration Commands

---



VLAN mapping is achieved mainly through QoS policies. This chapter introduces part of the commands for ports involved in many-to-one VLAN mapping. For QoS policy configuration commands, refer to *QoS Commands* in the *QoS Volume*.

---

## VLAN Mapping Configuration Commands

### qinq enable downlink

#### Syntax

```
qinq enable downlink
undo qinq enable
```

#### View

Ethernet interface view, port group view

#### Default Level

2: System level

#### Parameters

None

#### Description

Use the **qinq enable downlink** command to enable customer-side QinQ on the current Ethernet port(s).

Use the **undo enable downlink** command to disable customer-side QinQ on the current Ethernet port(s).

By default, customer-side QinQ is disabled on Ethernet ports.

Configuration made in Ethernet interface view takes effect on the current port only, while configuration made in port group view takes effect on all ports in the port group.

#### Examples

```
# Enable customer-side QinQ on GigabitEthernet 1/0/1.
```

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] qinq enable downlink
```

# Enable customer-side QinQ on port group 1.

```
<Sysname> system-view
```

```
[Sysname] port-group manual 1
```

```
[Sysname-port-group-manual-1] group-member gigabitethernet 1/0/1 to gigabitethernet 1/0/6
```

```
[Sysname-port-group-manual-1] qinq enable downlink
```

## qinq enable uplink

### Syntax

**qinq enable uplink**

**undo qinq enable**

### View

Ethernet interface view, port group view

### Default Level

2: System level

### Parameters

None

### Description

Use the **qinq enable uplink** command to enable service provider-side QinQ on the current Ethernet port(s).

Use the **undo enable downlink** command to disable service provider-side QinQ on the current Ethernet port(s).

By default, service provider-side QinQ is disabled on Ethernet ports.

Configuration made in Ethernet interface view takes effect on the current port only, while configuration made in port group view takes effect on all ports in the port group.

### Examples

# Enable service provider-side QinQ on GigabitEthernet 1/0/1.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] qinq enable uplink
```

# Enable service provider-side QinQ on port group 1.

```
<Sysname> system-view
```

```
[Sysname] port-group manual 1
```

```
[Sysname-port-group-manual-1] group-member gigabitethernet 1/0/1 to gigabitethernet 1/0/6
```

```
[Sysname-port-group-manual-1] qinq enable uplink
```

# Table of Contents

<b>1 Ethernet OAM Configuration Commands</b> .....	<b>1-1</b>
OAM Configuration Commands .....	1-1
display oam .....	1-1
display oam configuration.....	1-4
display oam critical-event .....	1-6
display oam link-event .....	1-7
oam enable.....	1-8
oam errored-frame period.....	1-9
oam errored-frame threshold.....	1-10
oam errored-frame-period period .....	1-10
oam errored-frame-period threshold .....	1-11
oam errored-frame-seconds period.....	1-12
oam errored-frame-seconds threshold.....	1-12
oam errored-symbol period .....	1-13
oam errored-symbol threshold .....	1-13
oam loopback .....	1-14
oam mode.....	1-15
reset oam.....	1-15

# 1 Ethernet OAM Configuration Commands

---

## OAM Configuration Commands

### display oam

#### Syntax

```
display oam { local | remote } [ interface interface-type interface-number ]
```

#### View

Any view

#### Default Level

2: System level

#### Parameters

**local**: Displays the Ethernet OAM connection information of the local end.

**remote**: Displays the Ethernet OAM connection information of the remote end.

**interface** *interface-type interface-number*: Specify a port by its type and number.

#### Description

Use the **display oam** command to display the information about an Ethernet OAM connection, including connection status, information contained in Ethernet OAM packet header, and Ethernet OAM packet statistics.

If you do not specify the **interface** keyword, this command displays the information about all the Ethernet OAM connections.

Related commands: **reset oam**.

#### Examples

# Display the information about the Ethernet OAM connection established on the local port GigabitEthernet 1/0/1.

```
<Sysname> display oam local interface gigabitethernet 1/0/1
Port          : GigabitEthernet1/0/1
Link Status   : Up
EnableStatus  : Enable
Local_oam_mode : Active      Local_pdu          : ANY
Local_mux_action : FWD        Local_par_action    : FWD
```

OAMLocalFlagsField :

```
-----
Link Fault          : 0          Dying Gasp          : 0
Critical Event      : 0          Local Evaluating    : COMPLETE
```

Remote Evaluating : COMPLETE

Packets statistic :

Packets	Send	Receive
OAMPDU	645	648
OAMInformation	645	648
OAMEventNotification	0	--
OAMUniqueEventNotification	--	0
OAMDuplicateEventNotification	--	0

**Table 1-1 display oam local command output description**

Field	Description
Port	Port index
Link Status	Link status
EnableStatus	Ethernet OAM state (enabled or disabled)
Local_oam_mode	Local Ethernet OAM mode, which can be: <ul style="list-style-type: none"> <li>Active, indicating the port operates in the active Ethernet OAM mode</li> <li>Passive, indicating the port operates in the passive Ethernet OAM mode</li> </ul>
Local_pdu	The way in which the local end processes Ethernet OAMPDUs: <ul style="list-style-type: none"> <li>RX_INFO, indicating the port only receives Information OAMPDUs and does not send any Ethernet OAMPDUs.</li> <li>LF_INFO, indicating the port only sends the Information OAMPDUs without Information TLV triplets and with their link error flag bits being set.</li> <li>INFO, indicating the port sends and receives only Information OAMPDUs.</li> <li>ANY, indicating the port sends and receives Ethernet OAMPDUs of any type.</li> </ul>
Local_mux_action	Working mode of the local transmitter, which can be: <ul style="list-style-type: none"> <li>FWD, indicating the port can send any packets.</li> <li>DISCARD, indicating the port only sends Ethernet OAMPDUs.</li> </ul>
Local_par_action	Working mode of the local receiver, which can be: <ul style="list-style-type: none"> <li>FWD, indicating the port can receive any packets.</li> <li>DISCARD, indicating the port only receives Ethernet OAMPDUs.</li> <li>LB, indicating Ethernet OAM loopback testing is enabled on the port. In this case, all the packets other than Ethernet OAMPDUs received are returned to their sources along the ways they come.</li> </ul>
OAMLocalFlagsField	Local flags inserted in the local flag fields of the Ethernet OAMPDUs sent.
Link Fault	Indicates whether an Ethernet OAM link error is present: 0 for no and 1 for yes.
Dying Gasp	Indicates whether a fatal error is present: 0 for no and 1 for yes.
Critical Event	Indicates whether a critical error is present: 0 for no and 1 for yes.

Field	Description
Local Evaluating	Indicates whether the local-to-remote configuration negotiation is complete: <ul style="list-style-type: none"> <li>• COMPLETE for completed</li> <li>• REVERSED for uncompleted</li> </ul>
Remote Evaluating	Indicates whether the remote-to-local configuration negotiation is complete: <ul style="list-style-type: none"> <li>• COMPLETE for completed</li> <li>• REVERSED for uncompleted</li> </ul>
Packets statistic	Statistics about Ethernet OAMPDUs sent and received
OAMPDU	Total number of the Ethernet OAMPDUs sent and received
OAMInformation	Number of the Information OAMPDUs sent and received
OAMEventNotification	Number of the Event notification OAMPDUs sent and received
OAMUniqueEventNotification	Number of the unduplicated Event notification OAMPDUs sent or received uniquely.
OAMDuplicateEventNotification	Number of the duplicate Event notification OAMPDUs sent or received.

# Display the Ethernet OAM information of the peer port GigabitEthernet 1/0/1.

```
<Sysname> display oam remote interface gigabitethernet 1/0/1
Port          : GigabitEthernet1/0/1
Link Status   : Up
Information of the latest received OAM packet:
OAMRemoteMACAddress      : 00e0-fd73-6502
OAMRemotePDUConfiguration : 1500

OAMRemoteState :
-----
Remote_mux_action      : FWD          Remote_par_action      : FWD

OAMRemoteConfiguration :
-----
OAM Mode                : Active      Unidirectional Support : YES
Loopback Support        : YES          Link Events              : YES
Variable Retrieval      : NO

OAMRemoteFlagsField :
-----
Link Fault              : 0          Dying Gasp               : 0
Critical Event          : 0          Local Evaluating         : COMPLETE
Remote Evaluating      : COMPLETE
```

**Table 1-2** display oam remote port command output description

Field	Description
Port	Port index
Link Status	Link status
Information of the latest received OAM packet	Information about the latest received Ethernet OAMPDU
OAMRemoteMACAddress	MAC address of the Ethernet OAM peer
OAMRemotePDUConfiguration	Maximum Ethernet OAMPDU size allowed
OAMRemoteState	State of the Ethernet OAM peer
Remote_mux_action	Peer sending mode. Refer to <a href="#">Table 1-1</a> for more.
Remote_par_action	Peer receiving mode. Refer to <a href="#">Table 1-1</a> for more.
OAMRemoteConfiguration	Configuration of the peer Ethernet OAM entity
OAM Mode	Ethernet OAM mode
Unidirectional Support	Indicates whether unidirectional transmission is supported (YES or NO)
Loopback Support	Indicates whether Ethernet OAM loopback testing is supported (YES or NO)
Link Events	Indicates whether Ethernet OAM link error events are supported (YES or NO)
Variable Retrieval	Indicates whether MIB variable retrieval is supported (YES or NO)
OAMRemoteFlagsField	Values of the peer Ethernet OAM flag fields in OAM packets
Link Fault	Indicates whether a link fault is present: 0 for no and 1 for yes.
Dying Gasp	Indicate whether a fatal fault is present: 0 for no and 1 for yes.
Critical Event	Indicate whether a critical fault is present: 0 for no and 1 for yes.
Local Evaluating	Indicates whether the local-to-remote configuration negotiation is complete: <ul style="list-style-type: none"> <li>• COMPLETE for completed</li> <li>• REVERSED for uncompleted</li> </ul>
Remote Evaluating	Indicates whether the remote-to-local configuration negotiation is complete: <ul style="list-style-type: none"> <li>• COMPLETE for completed</li> <li>• REVERSED for uncompleted</li> </ul>

## display oam configuration

### Syntax

**display oam configuration**

### View

Any view

## Default Level

2: System level

## Parameters

None

## Description

Use the **display oam configuration** command to display global Ethernet OAM configuration, including the periods and thresholds for Ethernet OAM link error event detection.

Related commands: **oam errored-symbol period**, **oam errored-symbol threshold**, **oam errored-frame period**, **oam errored-frame threshold**, **oam errored-frame-period period**, **oam errored-frame-period threshold**, **oam errored-frame-seconds period**, **oam errored-frame-seconds threshold**.

## Examples

# Display global Ethernet OAM configuration.

```
<Sysname> display oam configuration
```

```
Configuration of the link event window/threshold :
```

```
-----  
Errored-symbol Event period(in seconds)      :      1  
Errored-symbol Event threshold                :      1  
Errored-frame Event period(in seconds)       :      1  
Errored-frame Event threshold                :      1  
Errored-frame-period Event period(in ms)     :    1000  
Errored-frame-period Event threshold         :      1  
Errored-frame-seconds Event period(in seconds) :     60  
Errored-frame-seconds Event threshold        :      1
```

**Table 1-3 display oam configuration** command output description

Field	Description
Configuration of the link event window/threshold	Detection intervals and triggering thresholds configured for link events
Errored-symbol Event period (in seconds)	Errored symbol detection interval, which defaults to one second.
Errored-symbol Event threshold	Errored symbol event triggering threshold, which defaults to 1.
Errored-frame Event period (in seconds)	Errored frame detection interval, which defaults to one second.
Errored-frame Event threshold	Errored frame event triggering threshold, which defaults to 1.
Errored-frame-period Event period (in ms)	Errored frame period detection interval, which defaults to 1000 milliseconds.
Errored-frame-period Event threshold	Errored frame period event triggering threshold, which defaults to 1.
Errored-frame-seconds Event period (in seconds)	Errored frame seconds detection interval, which defaults to 60 seconds.

Field	Description
Errored-frame-seconds Event threshold	Errored frame seconds event triggering threshold, which defaults to 1.

## display oam critical-event

### Syntax

**display oam critical-event** [ **interface** *interface-type interface-number*]

### View

Any view

### Default Level

2: System level

### Parameters

**interface** *interface-type interface-number*. Specify a port by its type and number.

### Description

Use the **display oam critical-event** command to display the statistics on critical Ethernet OAM link events occurred on a port.

If you do not specify the **interface** keyword, this command displays the statistics on the critical Ethernet OAM link events occurred on all the ports of the switch.

### Examples

# Display the statistics on critical Ethernet OAM link events occurred on all the ports.

```
<Sysname> display oam critical-event
```

```
Port          : GigabitEthernet1/0/1
```

```
Link Status   : Up
```

```
Event statistic :
```

```
-----
Link Fault    :0   Dying Gasp      : 0   Critical Event    : 0
```

**Table 1-4** display oam critical-event command output description

Field	Description
Port	Port index
Link Status	Link status
Event statistic	Statistics on critical Ethernet OAM link events
Link Fault	Indicates whether a link fault is present: 0 for no and 1 for yes.
Dying Gasp	Indicate whether a fatal fault is present: 0 for no and 1 for yes.
Critical Event	Indicate whether a critical fault is present: 0 for no and 1 for yes.

## display oam link-event

### Syntax

```
display oam link-event { local | remote } [ interface interface-type interface-number ]
```

### View

Any view

### Default Level

2: System level

### Parameters

**local**: Displays the statistics on the local Ethernet OAM link error events.

**remote**: Displays the statistics on the peer Ethernet OAM link error events.

**interface** *interface-type interface-number*: Specify a port by its type and number.

### Description

Use the **display oam link-event** command to display the statistics on Ethernet OAM link error events occurred on a local port or a peer port. Ethernet OAM link error events include errored symbol events, errored frame events, errored frame period events, and errored frame seconds events.

If you do not specify the **interface** keyword, this command displays the statistics on the Ethernet OAM link error events occurred on all the local/peer ports.

Related commands: **display oam configuration**, **reset oam**.

### Examples

# Display the statistics on Ethernet OAM link error events occurred on all the local ports.

```
<Sysname> display oam link-event local
Port          : GigabitEthernet1/0/1
Link Status   : Up

OAMLocalErrFrameEvent : (ms = milliseconds)
-----
Event Time Stamp      : 3539          Errored Frame Window : 10(100ms)
Errored Frame Threshold : 5          Errored Frame         : 1488111
Error Running Total   : 260908758    Event Running Total   : 307

OAMLocalErrFramePeriodEvent :
-----
Event Time Stamp      : 3539          Errored Frame Window : 976500
Errored Frame Threshold : 1          Errored Frame         : 1042054
Error Running Total   : 260909151    Event Running Total   : 471

OAMLocalErrFrameSecsSummaryEvent : (ms = milliseconds)
-----
Event Time Stamp      : 3389
Errored Frame Second Summary Window : 600(100ms)
```

```

Errored Frame Second Summary Threshold : 1
Errored Frame Second Summary          : 60
Error Running Total                    : 292      Event Running Total    : 5

```

**Table 1-5** display oam link-event local command output description

Field	Description
Port	Port index
Link Status	Link status
OAMLocalErrFrameEvent : (ms = milliseconds)	<p>Information about local errored frame events.</p> <ul style="list-style-type: none"> <li>• Event Time Stamp: time when an errored frame event occurred (in 100 milliseconds).</li> <li>• Errored Frame Window: Error frame detection interval (in 100 milliseconds).</li> <li>• Errored Frame Threshold: error threshold that triggers an errored frame event.</li> <li>• Errored Frame: the number of detected error frames over the specific detection interval.</li> <li>• Error Running Total: the total number of error frames.</li> <li>• Event Running Total: the total number of errored frame events that have occurred.</li> </ul>
OAMLocalErrFramePeriodEvent	<p>Information about local errored frame period events:</p> <ul style="list-style-type: none"> <li>• Event Time Stamp: time when an errored frame event occurred (in 100 milliseconds).</li> <li>• Errored Frame Window: maximum number of 64-byte frames that can be transmitted through an Ethernet port over the configured error frame period detection interval. See <b>oam errored-frame-period period</b> command for more information.</li> <li>• Errored Frame Threshold: error threshold that triggers an error frame period event.</li> <li>• Errored Frame: the number of detected error frames over a detection interval.</li> <li>• Error Running Total: the total number of error frames that have detected.</li> <li>• Event Running Total: the total number of error frame period events.</li> </ul>
OAMLocalErrFrameSecsSummaryEvent : (ms = milliseconds)	<p>Information about local errored frame seconds events:</p> <ul style="list-style-type: none"> <li>• Event Time Stamp: time when an error frame seconds event occurred (in terms of 100 milliseconds).</li> <li>• Errored Frame Second Summary Window: error frame second detection interval (in 100 milliseconds).</li> <li>• Errored Frame Second Summary Threshold: error threshold that triggers an error frame seconds event.</li> <li>• Errored Frame Second Summary: the number of detected error frame seconds over a detection interval.</li> <li>• Error Running Total: the total number of error frame seconds.</li> <li>• Event Running Total: the total number of error frame seconds events that have occurred.</li> </ul>

## oam enable

### Syntax

**oam enable**

**undo oam enable**

### View

Ethernet port view

### Default Level

2: System level

### Parameters

None

### Description

Use the **oam enable** command to enable Ethernet OAM on the Ethernet port.

Use the **undo oam enable** command to disable Ethernet OAM on the Ethernet port.

By default, Ethernet OAM is disabled on all Ethernet ports.

### Examples

```
# Enable OAM on port GigabitEthernet 1/0/1.  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] oam enable
```

## oam errored-frame period

### Syntax

**oam errored-frame period** *period-value*

**undo oam errored-frame period**

### View

System view

### Default Level

2: System level

### Parameters

*period-value*: Errored frame detection interval, ranging from 1 to 60 (in seconds).

### Description

Use the **oam errored-frame period** command to set the errored frame detection interval.

Use the **undo oam errored-frame period** command to restore the default.

By default, the errored frame detection interval is one second.

Related commands: **oam errored-frame threshold**, **display oam link-event**, **display oam configuration**.

### Examples

```
# Set the errored frame detection interval to 10 seconds.
```

```
<Sysname> system-view
[Sysname] oam errored-frame period 10
```

## oam errored-frame threshold

### Syntax

```
oam errored-frame threshold threshold-value
undo oam errored-frame threshold
```

### View

System view

### Default Level

2: System level

### Parameters

*threshold-value*: Errored frame event triggering threshold, ranging from 0 to 4294967295.

### Description

Use the **oam errored-frame threshold** command to set the errored frame event triggering threshold.

Use the **undo oam errored-frame threshold** command to restore the default.

By default, the errored frame event triggering threshold is 1.

Related commands: **oam errored-frame period**, **display oam link-event**, **display oam configuration**.

### Examples

```
# Set the errored frame event triggering threshold to 100.
```

```
<Sysname> system-view
[Sysname] oam errored-frame threshold 100
```

## oam errored-frame-period period

### Syntax

```
oam errored-frame-period period period-value
undo oam errored-frame-period period
```

### View

System view

### Default Level

2: System level

### Parameters

*period-value*: Errored frame period detection interval, ranging from 100 to 60000 (in milliseconds).

## Description

Use the **oam errored-frame-period period** command to set the errored frame period detection interval.

Use the **undo oam errored-frame-period period** command to restore the default.

By default, the errored frame period detection interval is 1000 milliseconds.

As for errored frame period event detection, the system first uses the following expression to convert the errored frame period detection interval to the maximum number of 64-byte frames that can be transmitted through an Ethernet port in the period:

$$\text{bandwidth} * \text{period} / (64 * 8 * 1000),$$

where **bandwidth** is the port bandwidth (in bps) and “period” is the configured period (in milliseconds).

Related commands: **oam errored-frame-period threshold**, **display oam link-event**, **display oam configuration**.

## Examples

```
# Set the errored frame period detection interval to 10 seconds, that is, 10000 milliseconds.
```

```
<Sysname> system-view
[Sysname] oam errored-frame-period period 10000
```

## oam errored-frame-period threshold

### Syntax

**oam errored-frame-period threshold** *threshold-value*

**undo oam errored-frame-period threshold**

### View

System view

### Default Level

2: System level

### Parameters

*threshold-value*: Errored frame period event triggering threshold, ranging from 0 to 4294967295.

## Description

Use the **oam errored-frame-period threshold** command to set the errored frame period event triggering threshold.

Use the **undo oam errored-frame-period threshold** command to restore the default.

By default, the errored frame period event triggering threshold is 1.

Related commands: **oam errored-frame-period period**, **display oam link-event**, **display oam configuration**.

## Examples

```
# Set the errored frame period event triggering threshold to 100.
```

```
<Sysname> system-view
```

```
[Sysname] oam errored-frame-period threshold 100
```

## oam errored-frame-seconds period

### Syntax

```
oam errored-frame-seconds period period-value  
undo oam errored-frame-seconds period
```

### View

System view

### Default Level

2: System level

### Parameters

*period-value*: Errored frame seconds detection interval, ranging from 10 to 900 (in seconds).

### Description

Use the **oam errored-frame-seconds period** command to set the errored frame seconds detection interval.

Use the **undo oam errored-frame-seconds period** command to restore the default.

By default, the errored frame seconds detection interval is 60 seconds.

Related commands: **oam errored-frame-seconds threshold**, **display oam link-event**, **display oam configuration**.

### Examples

```
# Set the errored frame seconds detection interval to 100 seconds.
```

```
<Sysname> system-view  
[Sysname] oam errored-frame-seconds period 100
```

## oam errored-frame-seconds threshold

### Syntax

```
oam errored-frame-seconds threshold threshold-value  
undo oam errored-frame-seconds threshold
```

### View

System view

### Default Level

2: System level

### Parameters

*threshold-value*: Errored frame seconds event triggering threshold, ranging from 0 to 900.

## Description

Use the **oam errored-frame-seconds threshold** command to set the errored frame seconds event triggering threshold.

Use the **undo oam errored-frame-seconds threshold** command to restore the default.

By default, the errored frame seconds event triggering threshold is 1.

Related commands: **oam errored-frame-seconds period**, **display oam link-event**, **display oam configuration**.

## Examples

```
# Set the errored frame seconds event triggering threshold to 100.
```

```
<Sysname> system-view  
[Sysname] oam errored-frame-seconds threshold 100
```

## oam errored-symbol period

### Syntax

```
oam errored-symbol period period-value  
undo oam errored-symbol period
```

### View

System view

### Default Level

2: System level

### Parameters

*period-value*: Errored symbol detection interval, ranging from 1 to 60 (in seconds).

## Description

Use the **oam errored-symbol period** command to set the errored symbol detection interval.

Use the **undo oam errored-symbol period** command to restore the default.

By default, the errored symbol detection interval is one second.

Related commands: **oam errored-symbol threshold**, **display oam link-event**, **display oam configuration**.

## Examples

```
# Set the errored symbol detection interval to 10 seconds.
```

```
<Sysname> system-view  
[Sysname] oam errored-symbol period 10
```

## oam errored-symbol threshold

### Syntax

```
oam errored-symbol threshold threshold-value  
undo oam errored-symbol threshold
```

## View

System view

## Default Level

2: System level

## Parameters

*threshold-value*: Errored symbol event triggering threshold, ranging from 0 to 4294967295.

## Description

Use the **oam errored-symbol threshold** command to set the errored symbol event triggering threshold.

Use the **undo oam errored-symbol threshold** command to restore the default.

By default, the errored symbol event triggering threshold is 1.

Related commands: **oam errored-symbol period**, **display oam link-event**, **display oam configuration**.

## Examples

```
# Set the errored symbol event triggering threshold to 100.
```

```
<Sysname> system-view  
[Sysname] oam errored-symbol threshold 100
```

## oam loopback

### Syntax

```
oam loopback  
undo oam loopback
```

### View

Ethernet port view

### Default Level

2: System level

### Parameters

None

### Description

Use the **oam loopback** command to enable Ethernet OAM loopback testing on an Ethernet port.

Use the **undo loopback** command to disable Ethernet OAM loopback testing.

By default, Ethernet OAM loopback testing is disabled.

Related commands: **oam enable**, **oam mode**.

### Examples

```
# Enable Ethernet OAM loopback testing on GigabitEthernet1/0/1.
```

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] oam mode active
[Sysname-GigabitEthernet1/0/1] oam enable
[Sysname-GigabitEthernet1/0/1] oam loopback
```

## oam mode

### Syntax

```
oam mode { active | passive }
```

### View

Ethernet port view

### Default Level

2: System level

### Parameters

**active:** Specifies the active Ethernet OAM mode.

**passive:** Specifies the passive Ethernet OAM mode.

### Description

Use the **oam mode** command to set the Ethernet OAM operating mode for an Ethernet port.

By default, an Ethernet OAM-enabled Ethernet port operates in the active Ethernet OAM mode.

Note that, for an Ethernet OAM-enabled Ethernet port, the Ethernet OAM operating mode cannot be changed. To do this, you need to disable Ethernet OAM on the port first.

Related commands: **oam enable**.

### Examples

# Configure GigabitEthernet 1/0/1 to operate in the active Ethernet OAM mode.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] oam mode active
```

## reset oam

### Syntax

```
reset oam [ interface interface-type interface-number ]
```

### View

User view

### Default Level

2: System level

## Parameters

**interface** *interface-type interface-number*. Specify a port by its type and number.

## Description

Use the **reset oam** command to clear the statistics on Ethernet OAM packets and Ethernet OAM link error events of an Ethernet port.

If you do not specify the **interface** keyword, this command clears the statistics on Ethernet OAM packets and Ethernet OAM link error events of all the ports.

Related commands: **display oam**, **display oam link-event**.

## Examples

# Clear the statistics on Ethernet OAM packets and Ethernet OAM link error events of all the ports.

```
<Sysname> reset oam
```

# Table of Contents

<b>1 Connectivity Fault Detection Configuration Commands</b> .....	<b>1-1</b>
Connectivity Fault Detection Configuration Commands .....	1-1
cfd cc enable .....	1-1
cfd cc interval.....	1-1
cfd enable .....	1-2
cfd linktrace .....	1-3
cfd linktrace auto-detection .....	1-4
cfd loopback .....	1-5
cfd ma.....	1-6
cfd md.....	1-7
cfd mep.....	1-7
cfd mep enable .....	1-8
cfd mip-rule.....	1-9
cfd remote-mep .....	1-10
cfd service-instance.....	1-11
display cfd linktrace-reply .....	1-12
display cfd linktrace-reply auto-detection .....	1-13
display cfd ma.....	1-14
display cfd md.....	1-15
display cfd mep.....	1-16
display cfd mp.....	1-18
display cfd remote-mep .....	1-20
display cfd service-instance .....	1-21
display cfd status .....	1-22

# 1 Connectivity Fault Detection Configuration

## Commands

---

### Connectivity Fault Detection Configuration Commands

#### **cfd cc enable**

##### Syntax

```
cfd cc service-instance instance-id mep mep-id enable  
undo cfd cc service-instance instance-id mep mep-id enable
```

##### View

Ethernet port view

##### Default level

2: System level

##### Parameters

**service-instance** *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

**mep** *mep-id*: Specifies the ID of an MEP, ranging from 1 to 8191.

##### Description

Use the **cfd cc enable** command to enable CCM sending on a specified MEP.

Use the **undo cfd cc enable** command to cancel the configuration.

By default, the CCM sending function is disabled.

Related commands: **cfd cc interval**.

##### Examples

# On port GigabitEthernet 1/0/1, Enable CCM sending on service point 3.

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] cfd cc service-instance 5 mep 3 enable
```

#### **cfd cc interval**

##### Syntax

```
cfd cc interval interval-field-value service-instance instance-id  
undo cfd cc interval service-instance instance-id
```

## View

System view

## Default level

2: System level

## Parameters

*interval-field-value*: Value of the interval field in CCM messages, ranging from 4 to 7.

**service-instance** *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

## Description

Use the **cfid cc interval** command to set the value of the interval field in the CCM messages.

Use the **undo cfid cc interval** command to restore the value to the default value.

By default, the value of this field is 4 for all CCMs sent.

The relationship between the interval field value in the CCM messages, the time interval to send CCM messages and the timeout time of the remote MEP is illustrated in [Table 1-1](#).

**Table 1-1** Relationship of interval field value, time interval for sending CCMs and timeout time of remote MEP

Interval field value	Time interval for CCM	Timeout time of remote MEP
4	1 second	3.5 seconds
5	10 second	35 seconds
6	60 seconds	210 seconds
7	600 seconds	2100 seconds

Related commands: **cfid cc enable**.

## Examples

# Set the value of the interval field in CCMs to 7.

```
<Sysname> system-view  
[Sysname] cfid cc interval 7 service-instance 2
```

## cfid enable

### Syntax

**cfid enable**

**undo cfid enable**

### View

System view

### Default level

2: System level

## Parameters

None

## Description

Use the **cfid enable** command to enable CFD.

Use the **undo cfid enable** command to disable CFD.

By default, CFD is disabled.

## Examples

```
# Enable CFD.
```

```
<Sysname> system-view
```

```
[Sysname] cfid enable
```

```
Note: CFD has been enabled.
```

## cfid linktrace

### Syntax

```
cfid linktrace service-instance instance-id mep mep-id { target-mep target-mep-id | target-mac mac-address } [ ttl tvl-value ] [ hw-only ]
```

### View

System view

### Default level

2: System level

## Parameters

**service-instance** *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

**mep** *mep-id*: Specifies the ID of the MEP that sends LTMs, ranging from 1 to 8191.

**target-map** *target-mep-id*: Specifies the ID of the MEP that receives LTM, ranging from 1 to 8191.

**target-mac** *mac-address*: Specifies the destination MAC address, in the format of H-H-H.

**tvl** *tvl-value*: Specifies the time to live value, ranging from 1 to 255 and defaulting to 64.

**hw-only**: Indicates the hw-only position of the LTMs sent. When this keyword is present and the MIP that receives LTMs cannot find the destination MAC address in its forwarding table, the MIP will not forward these broadcast messages. Otherwise, the LTMs will be forwarded.

## Description

Use the **cfid linktrace** command to find the path between the specified MEP and the destination MEP, which is achieved through the transmission of LTMs between the two and detection of the responding LTRs.

Related commands: **cfid linktrace auto-detection**.

## Examples

```
# Send LTM messages.
```

```
<Sysname> system-view
```

```
[Sysname] cfd linktrace service-instance 1 mep 1101 target-mep 2001
Linktrace to MEP 2001 with the sequence number 1101-43361 :
MAC Address          TTL      Forwarded      Relay Action
0010-FC00-6512      63      No             None
```

**Table 1-2 cfd linktrace command output description**

Field	Description
Linktrace to MEP <i>mep-id</i> with the sequence number <i>sequence-number</i>	Linktrace to MEP <i>mep-id</i> with the sequence number <i>sequence-number</i>
MAC Address	Source MAC address in the LTR messages
TTL	Hop count when the LTM passes the device
Forwarded	<ul style="list-style-type: none"> <li>• Yes means that the current device forwards LTMs.</li> <li>• No means that the current device does not forward LTMs.</li> </ul>
Relay Action	<ul style="list-style-type: none"> <li>• Found: Indicates that the forwarding device found the destination MAC address in its MAC address table.</li> <li>• Unknown: Indicates that the forwarding device failed to find the destination MAC address in its MAC address table.</li> <li>• None: Indicates that it is a MEP that responded to the LTM message. A MEP does not need to find the destination MAC address.</li> </ul>

## cfd linktrace auto-detection

### Syntax

```
cfd linktrace auto-detection [ size size-value ]
undo cfd linktrace auto-detection
```

### View

System view

### Default level

2: System level

### Parameters

**size** *size-value*: Specifies the size of the buffer used to store the auto-detection result, ranging from 1 to 100 (in terms of sending times).

This value defaults to 5, which means the buffer stores the results of the recent five auto-detections.

### Description

Use the **cfd linktrace auto-detection** command to enable the auto sending of linktrace messages.

Use the **undo cfd linktrace auto-detection** command to disable this function.

By default, this function is disabled.

Note that:

- After LT messages automatic sending is enabled, if a MEP fails to receive the CCMs from the remote MEP, the link between the two is regarded as faulty and LTMs will be sent out. (The destination of the LTMs is the remote MEP, and the maximum value of TTL is 255.) Based on the LTRs that echo back, the fault source can be located.
- Once you disable LT messages automatic sending, the content stored in the buffer will be removed.

Related commands: **cfp linktrace**.

## Examples

```
# Enable automatic LT messages sending.
<Sysname> system-view
[Sysname] cfp linktrace auto-detection size 100
```

## cfp loopback

### Syntax

```
cfp loopback service-instance instance-id mep mep-id { target-mep target-mep-id | target-mac mac-address } [ number loopback-number ]
```

### View

System view

### Default level

2: System level

### Parameters

**service-instance** *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

**mep** *mep-id*: Specifies the ID of a MEP, ranging from 1 to 8191.

**target-mep** *target-mep-id*: Specifies the ID of the destination MEP for LBM packets, ranging from 1 to 8191.

**target-mac** *mac-address*: Specifies the destination MAC address, in the format of H-H-H.

**number** *loopback-number*: Specifies the number of the LBMs packets sent, ranging from 1 to 10 and defaulting to 5.

### Description

Use the **cfp loopback** command to enable LB function so that LBMs can be sent from the specified MEP to other MEPs in the same service instance, and LBR messages can be received.

By default, LB is not enabled.

## Examples

```
# Enable LB to check link state.
<Sysname> system-view
[Sysname] cfp loopback service-instance 1 mep 1101 target-mep 2001
Loopback to 0010-FC00-6512 with the sequence number start from 1101-43404:
Reply from 0010-FC00-6512: sequence number=1101-43404
Reply from 0010-FC00-6512: sequence number=1101-43405
```

```

Reply from 0010-FC00-6512: sequence number=1101-43406
Reply from 0010-FC00-6512: sequence number=1101-43407
Reply from 0010-FC00-6512: sequence number=1101-43408
Send:5          Received:5          Lost:0

```

**Table 1-3 cfd loopback** command output description

Field	Description
Loopback to <i>mac-address</i> with the sequence number start from <i>sequence-number</i>	Sends LBMs to <i>mac-address</i> with the sequence number starting with <i>sequence-number</i>
Reply from <i>mac-address</i>	Reply from <i>mac-address</i>
sequence number	Sequence number in the LBR messages
Send	Number of LBMs sent
Received	Number of LBR messages received
Lost	Number of lost LBMs

## cfd ma

### Syntax

```

cfd ma ma-name md md-name vlan vlan-id
undo cfd ma ma-name md md-name

```

### View

System view

### Default level

2: System level

### Parameters

**ma-name**: Name of the MA, a string of 1 to 48 characters, composed of letters, numbers or underlines, but cannot start with an underline character.

**md** *md-name*: Specifies the name of an MD, a string of 1 to 48 characters, composed of letters, numbers or underlines, but cannot start with an underline character.

**vlan** *vlan-id*: Specifies the ID of the VLAN where MA is in service, ranging from 1 to 4094.

### Description

Use the **cfd ma** command to create MA(s) in an MD.

Use the **undo cfd ma** command to delete specified MA in an MD.

By default, no MA is created.

Note that:

- Before creating an MA, you must create an MD first.
- When deleting an MA, you will also delete the configurations related to that MA.

Related commands: **cfd md**.

## Examples

```
# Create an MA.  
<Sysname> system-view  
[Sysname] cfd md test_md level 3  
[Sysname] cfd ma test_ma md test_md vlan 100
```

## cfp md

### Syntax

```
cfp md md-name level level-value  
undo cfp md md-name
```

### View

System view

### Default level

2: System level

### Parameters

*md-name*: Name of an MD, a string of 1 to 48 characters, composed of letters, numbers or underlines, but cannot start with an underline character.

**level** *level-value*: Specifies an MD level, ranging from 0 to 7.

### Description

Use the **cfp md** command to create an MD.

Use the **undo cfp md** command to delete an MD.

By default, no MD is created.

Note that:

- You can create only one MD with a specific level. MD cannot be created if you enter an invalid MD name or an existing MD name.
- When deleting an MD, you will also delete the configurations related to that MD.

## Examples

```
# Create an MD.  
<Sysname> system-view  
[Sysname] cfp md test_md level 3
```

## cfp mep

### Syntax

```
cfp mep mep-id service-instance instance-id { inbound | outbound }  
undo cfp mep mep-id service-instance instance-id
```

### View

Ethernet port view

## Default level

2: System level

## Parameters

*mep-id*: ID of MEP, ranging from 1 to 8191.

**service-instance** *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

**inbound**: Creates an inward-facing MEP.

**outbound**: Creates an outward-facing MEP.

## Description

Use the **cfm mep** command to create a MEP on a port.

Use the **undo cfm mep** command to delete the specified MEP.

By default, no MEP is configured on a device port.

In creating a MEP, the service instance you specified defines the MD and MA that the MEP belongs to.

## Examples

# Create a MEP.

```
<Sysname> system-view
[Sysname] cfm md test_md level 3
[Sysname] cfm ma test_ma md test_md vlan 100
[Sysname] cfm service-instance 5 md test_md ma test_ma
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] cfm mep 3 service-instance 5 inbound
```

## cfm mep enable

### Syntax

**cfm mep service-instance** *instance-id* **mep** *mep-id* **enable**

**undo cfm mep service-instance** *instance-id* **mep** *mep-id* **enable**

### View

Ethernet port view

## Default level

2: System level

## Parameters

**service-instance** *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

**mep** *mep-id*: Specifies the ID of a MEP, ranging from 1 to 8191.

## Description

Use the **cfm mep enable** command to enable the MEP configured on a port.

Use the **undo cfm mep enable** command to disable the MEP.

By default, MEP is disabled on a port and cannot respond to LTM and LBM messages unless you enable it.

Related commands: **cfm mep**.

## Examples

```
# Enable MEP.
```

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] cfm mep service-instance 5 mep 3 enable
```

## cfm mip-rule

### Syntax

```
cfm mip-rule { explicit | default } service-instance instance-id
```

```
undo cfm mip-rule service-instance instance-id
```

### View

System view

### Default level

2: System level

### Parameters

**service-instance** *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

**explicit**: This rule means that if the lower level MA is not configured with MIPs, whether the current MA will create MIPs depends on whether the lower level MA is configured with MEPs.

**default**: This rule means that if the lower level MA is not configured with MIPs, the current MA will create MIPs.

### Description

Use the **cfm mip-rule** command to configure the rule for generating MIPs.

Use the **undo cfm mip-rule** command to delete the rule for generating MIPs.

By default, no rules for generating MIPs are configured, nor are the MIPs themselves.

MIPs are generated on each port automatically according to the rules configured. If a port has no MIP, the system will check the MAs in each MD (from low to high level), and follow the rules in [Table 1-4](#) to create or not create MIPs (within a single VLAN):

**Table 1-4** Rules for generating MIPs

MIP exists on low level MA	The cfd mip-rule command is configured as	MEP exists on low level MA	Create MIP or not
Yes	—	—	No
No	<b>Explicit</b>	No	No
		Yes	Yes
	<b>Default</b>	—	Yes

Each of the following actions or cases can cause MIPs to be created or deleted after you have configured this command:

- Enabling CFD (use the **cfd enable** command)
- Creating or deleting the MEPs on a port
- Changes occur to the VLAN attribute of a port
- The rule specified in the **cfd mip-rule** command changes

### Examples

# Configure the rules for generating MIPs.

```
<Sysname> system-view
[Sysname] cfd mip-rule default service-instance 5
```

### cfd remote-mep

#### Syntax

```
cfd remote-mep remote-mep-id service-instance instance-id mep mep-id
undo cfd remote-mep remote-mep-id service-instance instance-id mep mep-id
```

#### View

Ethernet port view

#### Default level

2: System level

#### Parameters

*remote-mep-id*: ID of the remote MEP, ranging from 1 to 8191.

**service-instance** *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

**mep** *mep-id*: Specifies the ID of a MEP, ranging from 1 to 8191.

#### Description

Use the **cfd remote-mep** command to configure the remote MEP for the specified local MEP (the two must be in the same service instance) on the local port. After this, the local MEP can receive CCMs from the remote MEP.

Use the **undo cfd remote-mep** command to delete the remote MEP configured on the local port.

Note that the remote MEP ID and local MEP ID cannot be the same.

## Examples

```
# Configure a remote MEP.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] cfd remote-mep 9 service-instance 5 mep 3
```

## cfd service-instance

### Syntax

```
cfd service-instance instance-id md md-name ma ma-name
undo cfd service-instance instance-id
```

### View

System view

### Default level

2: System level

### Parameters

*instance-id*: Service instance ID, ranging from 1 to 32767.

**md** *md-name*: Specifies the name of an MD, a string of 1 to 48 characters, composed of letters, numbers or underlines, but cannot start with an underline character.

**ma** *ma-name*: Specifies the name of an MA, a string of 1 to 48 characters, composed of letters, numbers or underlines, but cannot start with an underline character.

### Description

Use the **cfd service-instance** command to create a service instance.

Use the **undo cfd service-instance** command to delete a service instance.

By default, no service instance is created.

Note that:

- You must create MD and MA prior to creating service instance.
- The service instance ID uniquely identifies an MA in an MD.
- When deleting a service instance, you are deleting the configurations related to that service instance as well.
- Deleting a service instance simply breaks up the connection between the service instance and the corresponding MA, the MA itself is not deleted.

Related commands: **cfd md**, **cfd ma**.

## Examples

```
# Create a service instance.
<Sysname> system-view
[Sysname] cfd md test_md level 3
[Sysname] cfd ma test_ma md test_md vlan 100
[Sysname] cfd service-instance 5 md test_md ma test_ma
```

## display cfd linktrace-reply

### Syntax

```
display cfd linktrace-reply [ service-instance instance-id [ mep mep-id ] ]
```

### View

Any view

### Default level

2: System level

### Parameters

**service-instance** *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

**mep** *mep-id*: Specifies the ID of a MEP, ranging from 1 to 8191.

### Description

Use the **display cfd linktrace-reply** command to display the LTR information received by a MEP.

Note that:

- If this command is used without specifying MEP, the information of LTRs of all MEPs in the current service instance is displayed.
- If this command is used without specifying service instance, the information of LTRs of all MEPs is displayed.

### Examples

# Display the information of LTR message.

```
<Sysname> display cfd linktrace-reply
Service instance: 1      MEP ID: 1003
MAC Address             TTL      Forwarded      Relay Action
00E0-FC27-6502         63      Yes            Found
00E0-FC00-6510         62      Yes            Found
00E0-FC52-BAA0         61      No             None

Service instance: 2      MEP ID: 1023
MAC Address             TTL      Forwarded      Relay Action
00E0-FC27-6502         63      No             None
```

**Table 1-5** display cfd linktrace-reply command output description

Field	Description
Service instance	Service instance to which the MEPs that send LTMs belong
MEP ID	ID of the MEP that sends LTMs
MAC Address	Source MAC address in the LTR message
TTL	Hop count when LTM passes the device
Forwarded	<ul style="list-style-type: none"><li>• Yes means that the device has forwarded the LTMs.</li><li>• No means that the device did not forward the LTMs.</li></ul>

Field	Description
Relay Action	<ul style="list-style-type: none"> <li>• Found: Indicates that the forwarding device found the destination MAC address in its MAC address table.</li> <li>• Unknown: Indicates that the forwarding device failed to find the destination MAC address in its MAC address table.</li> <li>• None: Indicates that it is a MEP that responded to the LTM message. A MEP does not need to find the destination MAC address.</li> </ul>

## display cfd linktrace-reply auto-detection

### Syntax

**display cfd linktrace-reply auto-detection** [ *size size-value* ]

### View

Any view

### Default level

2: System level

### Parameters

**size** *size-value*: Specifies the times of recent auto-detections, ranging from 1 to 100.

### Description

Use the **display cfd linktrace-reply auto-detection** command to display the content of the LTR messages received as responses to the automatically sent LTMs.

These LTR messages are stored in the buffer after you executed the **cfd linktrace auto-detection** command. With the **size** parameter not specified, this command will display the information of all LTRs stored in the buffer.

### Examples

# Display the content of the LTRs received as responses to the LTMs sent.

```
<Sysname> display cfd linktrace-reply auto-detection
Service instance: 1      MEP ID: 1003      Time: 2006/05/22 10:43:57
Target MEP ID: 2005    TTL: 64
MAC Address             TTL      Forwarded      Relay Action
00E0-FC27-6502         63      Yes            Found
00E0-FC00-6510         62      Yes            Found
00E0-FC52-BAA0         61      No             None

Service instance: 2      MEP ID: 1023      Time: 2006/05/22 10:44:06
Target MEP ID: 2025    TTL: 64
MAC Address             TTL      Forwarded      Relay Action
00E0-FC27-6502         63      No             None
```

**Table 1-6** display cfd linktrace-reply auto-detection command output description

Field	Description
Service instance	Service instance to which the MEPs that sent LTM messages belong
MEP ID	ID of the MEP that sends LTMs
Time	Time of the LTMs automatically sent
Target MEP ID	ID of the target MEP
TTL	Initial hop count of the automatically sent LTMs
MAC Address	Source MAC address in the LTR messages
TTL	Hop count when LTM passes the device
Forwarded	<ul style="list-style-type: none"><li>• Yes means that the device has forwarded the LTMs.</li><li>• No means that the device did not forward the LTMs.</li></ul>
Relay Action	<ul style="list-style-type: none"><li>• Found: Indicates that the forwarding device found the destination MAC address in its MAC address table.</li><li>• Unknown: Indicates that the forwarding device failed to find the destination MAC address in its MAC address table.</li><li>• None: Indicates that it is a MEP that responded to the LTM message. A MEP does not need to find the destination MAC address.</li></ul>

## display cfd ma

### Syntax

```
display cfd ma [ [ ma-name ] md md-name ]
```

### View

Any view

### Default level

2: System level

### Parameters

*ma-name*: Name of MA, ranging from 1 to 48 characters, composed of letters, numbers or underlines, but cannot start with an underline character.

**md** *md-name*: Specifies the name of an MD, ranging from 1 to 48 characters, composed of letters, numbers or underlines, but cannot start with an underline character.

### Description

Use the **display cfd ma** command to display the configuration of a specified MA.

Note that:

- If MD is not specified, this command will display the MA configurations of all MDs on the device.
- If both MD and MA are specified, this command will display the specified MA configuration.
- If only MD is specified, this command will display the configurations of all MAs in that MD.

### Examples

```
# Display the MA configuration information.
```

```

<Sysname> display cfd ma
3 maintenance domain(s) configured.
Maintenance domain: mdtest_5
1 maintenance association(s) belong(s) to maintenance domain mdtest_5:
Maintenance association: matest_5
Service instance: 5          VLAN: 5          Level: 5

Maintenance domain: mdtest_6
2 maintenance association(s) belong(s) to maintenance domain mdtest_6:
Maintenance association: matest_6
Service instance: 6          VLAN: 6          Level: 6

Maintenance association: matest_16
Service instance: 0          VLAN: 100       Level: 6

Maintenance domain: mdtest_7
1 maintenance association(s) belong(s) to maintenance domain mdtest_7:
Maintenance association: matest_7
Service instance: 7          VLAN: 7          Level: 7

```

**Table 1-7 display cfd ma command output description**

Field	Description
3 maintenance domain(s) configured.	Number of MDs configured
Maintenance domain	Name of the MD
1 maintenance association(s) belong(s) to maintenance domain mdtest_5	Number of MAs configured in the MD
Maintenance association	Name of the MA
Service instance	Service instance of the MA
VLAN	VLAN to which the service instance belongs
Level	Level of the MD to which the MA belongs

## display cfd md

### Syntax

```
display cfd md
```

### View

Any view

### Default level

2: System level

### Parameters

None

## Description

Use the **display cfd md** command to display the MD configuration information.

## Examples

```
# Display the MD configuration information.
```

```
<Sysname> display cfd md
CFD is enabled.
8 maintenance domain(s) configured:
Level: 0      Maintenance domain: mdtest_0
Level: 1      Maintenance domain: mdtest_1
Level: 2      Maintenance domain: mdtest_2
Level: 3      Maintenance domain: mdtest_3
Level: 4      Maintenance domain: mdtest_4
Level: 5      Maintenance domain: mdtest_5
Level: 6      Maintenance domain: mdtest_6
Level: 7      Maintenance domain: mdtest_7
```

**Table 1-8 display cfd md command output description**

Field	Description
8 maintenance domain(s) configured	Number of MDs configured
Level	Level of MD, each level allows only one MD.
Maintenance domain	Name of MD

## display cfd mep

### Syntax

```
display cfd mep mep-id service-instance instance-id
```

### View

Any view

### Default level

2: System level

### Parameters

*mep-id*: MEP ID, ranging from 1 to 8191.

**service-instance** *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

## Description

Use the **display cfd mep** command to display the attribute and operating information of MEP(s).

## Examples

```
# Display the attribute and operating information of a MEP.
```

```
<Sysname> display cfd mep 50 service-instance 1
```

```

Interface: GigabitEthernet1/0/2
Maintenance domain: mdtest_1
Maintenance association: matest_1
Level: 1          VLAN: 1          Direction: Outbound
Administrative state: Active          CCM send: Enable
FNG state: FNG_DEFECT_REPORTED

CCM:
Current state: CCI_WAITING
Interval: 1s          SendCCM: 12018

Loopback:
NextSeqNumber: 8877
SendLBR: 0          ReceiveInOrderLBR: 0          ReceiveOutOrderLBR: 0

Linktrace:
NextSeqNumber: 8877
SendLTR: 0          ReceiveLTM: 0

No CCM from some remote MEPs is received.

One or more streams of error CCMS is received. The last-received CCM:
Maintenance domain:mdtest1
Maintenance association:matest1
MEP:5          Sequence Number:0x50A
MAC Address: 000F-E25D-F31B
Received Time: 2008/04/26 12:51:31

One or more streams of cross-connect CCMS is received. The last-received CCM:
Maintenance domain:mdtest1
Maintenance association:matest1
MEP:6          Sequence Number:0x63A
MAC Address: 000F-E25D-578C
Received Time: 2008/04/26 12:51:33

Some other MEPs are transmitting the RDI bit.

```

**Table 1-9 display cfd mep command output description**

Field	Description
Interface	Interface that an MD belongs to
Maintenance domain	MD that a MEP belongs to
Maintenance association	MA that a MEP belongs to
Level	Level of the MD
VLAN	VLAN that the MA belongs to
Direction	Direction of the MEPs
Administrative state	State of MEP, either Active or Inactive

Field	Description
CCM send	Whether the MEP sends CCM
FNG state	State of FNG (Fault Notification Generator), including: FNG_RESET, FNG_DEFECT, FNG_REPORT_DEFECT, FNG_DEFECT_REPORTED, FNG_DEFECT_CLEARING
CCM	Information related to CCM
Current state	State of CCMs sent, including: CCI_IDLE, CCI_WAITING
Interval	Interval to send CCM
SendCCM	Number of CCMs that have been sent by the MEPs
Loopback	Information related to Loopback
NextSeqNumber	Sequence number of the next LBM to be sent
SendLBR	Number of LBRs that have been sent
ReceiveInOrderLBR	Number of LBR messages received in correct sequence
ReceiveOutOrderLBR	Number of LBR messages received out of order
Linktrace	Information related to linktrace
NextSeqNumber	Sequence number of the next LTM to be sent
SendLTR	Number of LTRs sent
ReceiveLTM	Number of LTMs received
No CCM from some remote MEPs is received.	Failure to receive CCMs from some remote MEPs (This information is displayed only when some CCMs are lost.)
One or more streams of error CCMs is received. The last-received CCM:	Display the content of the last CCM when one or more error CCMs are received. (This information is displayed only when error CCM(s) is/are received.)
Maintenance domain	MD of the last error CCM message
Maintenance association	MA of the last error CCM message
MEP	ID of the MEP that sent the last error CCM message
Sequence Number	Sequence number of the last error CCM
MAC Address	MAC address of the peer that sent the error CCM message
Received Time	Time when the last error CCM is received
One or more streams of cross-connect CCMs is received. The last-received CCM:	Cross-connect CCMs are received, and the content of the last cross-connect CCM is displayed. (This information is displayed only when cross-connect CCM(s) is/are received.)
Some other MEPs are transmitting the RDI bit.	CCMs with RDI bits misplaced are received from other MEPs. (This information is displayed only when this type of CCM(s) is/are received.)

## display cfd mp

### Syntax

**display cfd mp** [ **interface** *interface-type interface-number* ]

## View

Any view

## Default level

1: Monitor level

## Parameters

**interface** *interface-type interface-number*: Specifies a port by its type and number.

## Description

Use the **display cfd mp** command to display the MP information.

If no port is specified, this command will display the MP information of all ports.

The information displayed is ordered by port name primarily, and within a single port, ordered by VLAN ID (from small to big), and within a single VLAN, in the order of outward-facing MEPs (from low to high level), MIPs, and inward-facing MEPs (from high to low level).

## Examples

# Display the MP information.

```
<Sysname> display cfd mp
Interface GigabitEthernet1/0/1   VLAN 100
MEP ID: 100      Level: 0      Service instance: 100      Direction: Outbound
Maintenance domain: mdtest0
Maintenance association: mainmd0

MEP ID: 105      Level: 5      Service instance: 105      Direction: Outbound
Maintenance domain: mdtest5
Maintenance association: mainmd5

MIP              Level: 6      Service instance: 106
Maintenance domain: mdtest6
Maintenance association: mainmd6

MEP ID: 104      Level: 4      Service instance: 104      Direction: Inbound
Maintenance domain: mdtest4
Maintenance association: mainmd4

MEP ID: 102      Level: 2      Service instance: 102      Direction: Inbound
Maintenance domain: mdtest2
Maintenance association: mainmd2

Interface GigabitEthernet1/0/4   VLAN 1
MEP ID: 9         Level: 6      Service instance: 6        Direction: Outbound
Maintenance domain: mdtest6
Maintenance association: matest6
```

**Table 1-10 display cfd mp command output description**

Field	Description
Interface GigabitEthernet1/0/1 VLAN 100	MP configuration of the specified VLAN on the specified port
MEP ID	ID of the MEP
MIP	A MIP in the MP
Level	MD level that an MP belongs to
Service instance	Service instance to which the MP belongs
Direction	Direction of the MP
Maintenance domain	MD to which an MP belongs
Maintenance association	MA to which an MP belongs

## display cfd remote-mep

### Syntax

**display cfd remote-mep service-instance** *instance-id* **mep** *mep-id*

### View

Any view

### Default level

2: System level

### Parameters

**service-instance** *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

**mep** *mep-id*: Specifies the ID of a MEP, ranging from 1 to 8191.

### Description

Use the **display cfd remote-mep** command to display the information of the remote MEP.

### Examples

# Display the information of the remote MEP.

```
<Sysname> display cfd remote-mep service-instance 4 mep 10
MEP ID   MAC Address      State      Time                MAC Status
20       00E0-FC00-6565  OK        2006/03/06 02:36:38  UP
30       00E0-FC27-6502  OK        2006/03/06 02:36:38  DOWN
40       00E0-FC00-6510  FAILED    2006/03/06 02:36:39  DOWN
50       00E0-FC52-BAA0  OK        2006/03/06 02:36:44  DOWN
60       0010-FC00-6502  OK        2006/03/06 02:36:42  DOWN
```

**Table 1-11 display cfd remote-mep command output description**

Field	Description
MEP ID	ID of the remote MED
MAC Address	MAC address of the remote MEP device
State	Running state of MEP, either OK or FAILED
Time	Recent time of the remote MEP when it is FAILED or OK.
MAC Status	State of the port indicated by the last CCM received from the remote MEP, either UP or DOWN

## display cfd service-instance

### Syntax

**display cfd service-instance** [ *instance-id* ]

### View

Any view

### Default level

2: System level

### Parameters

*instance-id*: Service instance, ranging from 1 to 32767.

### Description

Use the **display cfd service-instance** command to display the configuration information of service instance.

Without specifying the service instance ID, the command will display the configuration information of all service instances. With service instance ID specified, this command will display the configuration information of the specified service instance.

### Examples

# Display the service instance configuration information.

```
<Sysname> display cfd service-instance
2 service instance(s) configured:
Service instance 5:
Maintenance domain: mdtest_5
Maintenance association: matest_5
Level: 5          VLAN: 5          MIP rule: None          CCM interval: 1s

Service instance 6:
Maintenance domain: mdtest_6
Maintenance association: matest_6
Level: 6          VLAN: 6          MIP rule: None          CCM interval: 1s
```

```

<Sysname> display cfd service-instance 7
Service instance 7:
Maintenance domain: mdtest_7
Maintenance association: matest_7
Level: 7          VLAN: 7          MIP rule: None          CCM interval: 1s
MEP ID: 731      Interface: GigabitEthernet1/0/1          Direction: Inbound

```

**Table 1-12** display cfd service-instance command output description

Field	Description
2 service instance(s) are configured.	Number of service instance configured.
Service instance 5	Service instance ID
Maintenance domain	MD of the service instance
Maintenance association:	MA of the service instances
Level	MD level
VLAN	VLAN that the MA belongs to
MIP rule	MIP generation rules configured on service instance
CCM interval	Interval to send CCMs
MEP ID	ID of MEPs configured on the service instance
Interface	Interface of the MEP configured on the service instance
Direction	Direction of the MEPs configured on the service instance

## display cfd status

### Syntax

```
display cfd status
```

### View

Any view

### Default level

2: System level

### Parameters

None

### Description

Use the **display cfd status** command to display the status of CFD (enabled or disabled).

### Examples

```
# Display the status of CFD.
```

```

<Sysname> display cfd status
CFD is enabled.

```

# Table of Contents

<b>1 MSTP Configuration Commands</b> .....	<b>1-1</b>
MSTP Configuration Commands .....	1-1
active region-configuration .....	1-1
check region-configuration .....	1-1
display stp .....	1-2
display stp abnormal-port .....	1-6
display stp down-port .....	1-7
display stp history .....	1-8
display stp region-configuration .....	1-9
display stp root .....	1-10
display stp tc .....	1-11
instance .....	1-12
region-name .....	1-12
reset stp .....	1-13
revision-level .....	1-14
stp bpdu-protection .....	1-14
stp bridge-diameter .....	1-15
stp compliance .....	1-16
stp config-digest-snooping .....	1-17
stp cost .....	1-18
stp edged-port .....	1-19
stp enable .....	1-20
stp loop-protection .....	1-21
stp max-hops .....	1-21
stp mcheck .....	1-22
stp mode .....	1-23
stp no-agreement-check .....	1-24
stp pathcost-standard .....	1-24
stp point-to-point .....	1-26
stp port priority .....	1-27
stp port-log .....	1-28
stp priority .....	1-28
stp region-configuration .....	1-29
stp root primary .....	1-30
stp root secondary .....	1-31
stp root-protection .....	1-31
stp tc-protection .....	1-32
stp tc-protection threshold .....	1-33
stp timer forward-delay .....	1-33
stp timer hello .....	1-34
stp timer max-age .....	1-35
stp timer-factor .....	1-36
stp transmit-limit .....	1-37



# 1 MSTP Configuration Commands

---

## MSTP Configuration Commands

### active region-configuration

#### Syntax

```
active region-configuration
```

#### View

MST region view

#### Default Level

2: System level

#### Parameters

None

#### Description

Use the **active region-configuration** command to activate your MST region configuration.

When you carry out this command, MSTP will replace the currently running MST region-related parameters with the parameters you have just configured, and will perform spanning tree calculation again.

Related commands: **instance**, **region-name**, **revision-level**, **vlan-mapping modulo**, **check region-configuration**.

#### Examples

```
# Activate MST region configuration manually.  
<Sysname> system-view  
[Sysname] stp region-configuration  
[Sysname-mst-region] active region-configuration
```

### check region-configuration

#### Syntax

```
check region-configuration
```

#### View

MST region view

#### Default Level

2: System level

## Parameters

None

## Description

Use the **check region-configuration** command to view all the configuration information of the MST region, including the region name, VLAN-to-MSTI mapping and revision level settings.

Be sure that your MST region configurations are correct, especially the VLAN-to-MSTI mapping table. As defined in the MSTP protocol, MSTP-enabled devices are in the same MST region only when they have the same format selector (protocol format selector defined in 802.1s, which is 0 by default and unconfigurable), region name, VLAN-to-MSTI mapping table, and MSTP revision level settings. A device will be in a different region if it is different in any of these four settings.

You can view all the MST region-related configuration information by using this command and determine the MST region the device is currently in, or check whether the MST region configuration is correct.

Related commands: **instance**, **region-name**, **revision-level**, **vlan-mapping modulo**, **active region-configuration**.

## Examples

# View all the configuration information of the MST region.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] check region-configuration
Admin Configuration
  Format selector :0
  Region name    :00b010000001
  Revision level :0

  Instance  Vlans Mapped
    0       1 to 9, 11 to 4094
    15      10
```

**Table 1-1** check region-configuration command output description

Field	Description
Format selector	Configuration format selector of the MST region
Region name	MST region name
Revision level	Revision level of the MST region
Instance Vlans Mapped	VLAN-to-MSTI mappings in the MST region

## display stp

### Syntax

```
display stp [ instance instance-id ] [ interface interface-list | slot slot-number ] [ brief ]
```

## View

Any view

## Default Level

1: Monitor level

## Parameters

**instance** *instance-id*: Displays the spanning tree information of a particular MSTI. The effective range of *instance-id* is 0 to 32, with 0 representing the common internal spanning tree (CIST).

**interface** *interface-list*: Specifies a port list, in the format of *interface-list* = { *interface-type interface-number* [ **to** *interface-type interface-number* ] }&<1-10>, where &<1-10> indicates that you can specify up to 10 ports or port ranges.

**slot** *slot-number*: Displays the spanning tree information of the specified device in the IRF stack. If no stack exists, this command only displays the spanning tree information of the current device. Replace the *slot-number* argument with the member ID of the device in the IRF stack.

**brief**: Displays brief information.

## Description

Use the **display stp** command to view the MSTP status information and statistics information.

Based on the MSTP status information and statistics information, you can analyze and maintain the network topology or check whether MSTP is working normally.

Note that:

- If you do not specify any MSTI ID or port list, this command will display the MSTP information of all MSTIs on all ports. The displayed information is sequenced by MSTI ID and by port name in each MSTI.
- If you specify an MSTI ID, this command will display the MSTP information on all ports in that MSTI. The displayed information is sequenced by port name.
- If you specify a port list, this command will display the MSTP information of all MSTIs on the specified ports. The displayed information is sequenced by MSTI ID, and by port name in each MSTI.
- If you specify both an MSTI ID and a port list, this command will display the MSTP information on the specified ports in the specified MSTI.

The MSTP status information includes:

- CIST global parameters: Protocol work mode, device priority in the CIST (Priority), MAC address, hello time, max age, forward delay, maximum hops, common root of the CIST, external path cost from the device to the CIST common root, regional root, the internal path cost from the device to the regional root, CIST root port of the device, and status of the BPDU guard function (enabled or disabled).
- CIST port parameters: Port status, role, priority, path cost, designated bridge, designated port, edge port/non-edge port, whether connecting to a point-to-point link, maximum transmission rate (transmit limit), status of the root guard function (enabled or disabled), BPDU format, boundary port/non-boundary port, hello time, max age, forward delay, message age, remaining hops, and whether rapid state transition enabled for designated ports.
- MSTI global parameters: MSTI ID, bridge priority of the MSTI, regional root, internal path cost, MSTI root port, and master bridge.

- MSTI port parameters: Port status, role, priority, path cost, designated bridge, designated port, remaining hops, and whether rapid state transition enabled (for designated ports).

The statistics information includes:

- The number of TCN BPDUs, configuration BPDUs, RST BPDUs and MST BPDUs sent from each port
- The number of TCN BPDUs, configuration BPDUs, RST BPDUs, MST BPDUs and wrong BPDUs received on each port
- The number of BPDUs discarded on each port

Related commands: **reset stp**.

## Examples

# View the brief MSTP status information and statistics information.

```
<Sysname> display stp instance 0 interface gigabitethernet 1/0/1 to gigabitethernet 1/0/4
brief
MSTID      Port                               Role  STP State  Protection
-----
0          GigabitEthernet1/0/1             DESI  FORWARDING NONE
0          GigabitEthernet1/0/2             DESI  FORWARDING NONE
0          GigabitEthernet1/0/3             DESI  FORWARDING NONE
0          GigabitEthernet1/0/4             DESI  FORWARDING NONE
```

**Table 1-2 display stp command output description**

Field	Description
MSTID	MSTI ID in the MST region
Port	Port name, corresponding to each MSTI
Role	Port role
STP State	MSTP status on the port, including forwarding, discarding, and learning
Protection	Protection type on the port, including root guard, loop guard, and BPDU guard

# View the detailed MSTP status information and statistics information.

```
<Sysname> display stp instance 0 interface gigabitethernet 1/0/2
-----[CIST Global Info][Mode MSTP]-----
CIST Bridge           :32768.000f-e200-2200
Bridge Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC        :0.00e0-fc0e-6554 / 200200
CIST RegRoot/IRPC     :32768.000f-e200-2200 / 0
CIST RootPortId       :128.48
BPDU-Protection       :disabled
Bridge Config-
Digest-Snooping       :disabled
TC or TCN received    :2
Time since last TC    :0 days 0h:5m:42s

----[Port2(GigabitEthernet1/0/2)][FORWARDING]----
Port Protocol         :enabled
Port Role              :CIST Designated Port
```

```

Port Priority           :128
Port Cost(Legacy)     :Config=auto / Active=200
Desg. Bridge/Port    :32768.000f-e200-2200 / 128.2
Port Edged            :Config=disabled / Active=disabled
Point-to-point        :Config=auto / Active=true
Transmit Limit        :10 packets/hello-time
Protection Type       :None
MST BPDU Format        :Config=auto / Active=legacy
Port Config-
Digest-Snooping       :disabled
Rapid transition      :false
Num of Vlans Mapped  :1
PortTimes              :Hello 2s MaxAge 20s FwDly 15s MsgAge 2s RemHop 20
BPDU Sent              :186
                       TCN: 0, Config: 0, RST: 0, MST: 186
BPDU Received         :0
                       TCN: 0, Config: 0, RST: 0, MST: 0

```

**Table 1-3 display stp command output description**

Field	Description
CIST Bridge	CIST bridge ID
Bridge Times	Major parameters for the bridge: <ul style="list-style-type: none"> <li>• Hello: Hello timer</li> <li>• MaxAge: Max Age timer</li> <li>• FWDly: Forward delay timer</li> <li>• Max Hop: Max hops within the MST region</li> </ul>
CIST Root/ERPC	CIST root and external path cost
CIST RegRoot/IRPC	CIST regional root and internal path cost
CIST RootPortId	CIST root port ID
BPDU-Protection	Indicates whether BPDU protection is enabled globally.
Bridge Config-Digest-Snooping	Indicates whether Digest Snooping is enabled globally on the bridge.
TC or TCN received	Number of received TC/TCN packets
Time since last TC	Time since the latest topology change
Port Protocol	Indicates whether STP is enabled on the port
Port Role	Port role, which can be Alternate, Backup, Root, Designated, Master, or Disabled
Port Priority	Port priority
Port Cost(Legacy)	Path cost of the port. The field in the bracket indicates the standard used for port path cost calculation, which can be <b>legacy</b> , <b>dot1d-1998</b> , or <b>dot1t</b> . <b>Config</b> indicates the configured value, and <b>Active</b> indicates the actual value.
Desg. Bridge/Port	Designated bridge ID and port ID of the port The port ID displayed is insignificant for a port which does not support port priority.

Field	Description
Port Edged	Indicates whether the port is an edge port. <b>Config</b> indicates the configured value, and <b>Active</b> indicates the actual value.
Point-to-point	Indicates whether the port is connected to a point-to-point link. <b>Config</b> indicates the configured value, and <b>Active</b> indicates the actual value.
Transmit Limit	The maximum number of packets sent within each Hello time
Protection Type	Protection type on the port, including root guard and loop guard
MST BPDU Format	Format of the MST BPDUs that the port can send, which can be legacy or 802.1s. <b>Config</b> indicates the configured value, and <b>Active</b> indicates the actual value.
Port Config-Digest-Snooping	Indicates whether digest snooping is enabled on the port.
Rapid transition	Indicates whether the current port rapidly transitions to the forwarding state.
Num of Vlans Mapped	Number of VLANs mapped to the current MSTI
PortTimes	Major parameters for the port: <ul style="list-style-type: none"> <li>• Hello: Hello timer</li> <li>• MaxAge: Max Age timer</li> <li>• FWDly: Forward delay timer</li> <li>• MsgAge: Message Age timer</li> <li>• Remain Hop: Remaining hops</li> </ul>
BPDU Sent	Statistics on sent BPDUs
BPDU Received	Statistics on received BPDUs

## display stp abnormal-port

### Syntax

```
display stp abnormal-port
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display stp abnormal-port** command to view the information about abnormally blocked ports.

Any of the following reasons may cause a port to be abnormally blocked:

- Root guard function
- Loop guard function
- MSTP BPDU format incompatibility protection function

## Examples

# View information about abnormally blocked ports.

```
<Sysname> display stp abnormal-port
```

MSTID	Blocked Port	Reason
1	GigabitEthernet1/0/1	ROOT-Protected
2	GigabitEthernet1/0/2	LOOP-Protected
2	GigabitEthernet1/0/3	Formatcompatibility-Protected

**Table 1-4 display stp abnormal-port command output description**

Field	Description
MSTID	MSTI ID
Blocked Port	Name of a blocked port, which corresponds to the related MSTI
Reason	Reason that caused abnormal blocking of the port. <ul style="list-style-type: none"><li>• ROOT-Protected: root guard function</li><li>• LOOP-Protected: loop guard function</li><li>• Formatcompatibility-Protected: MSTP BPDU format incompatibility protection function</li></ul>

## display stp down-port

### Syntax

```
display stp down-port
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display stp down-port** command to display the information about ports blocked by STP protection functions.

These functions include:

- BPDU attack guard function
- MSTP BPDU format frequent change protection function

## Examples

# View the information about ports blocked by STP protection functions.

```
<Sysname> display stp down-port
```

Down Port	Reason
GigabitEthernet1/0/1	BPDU-Protected
GigabitEthernet1/0/2	Formatfrequency-Protected

**Table 1-5 display stp abnormal-port command output description**

Field	Description
Down Port	Name of a blocked port
Reason	Reason that caused the port to be blocked. <ul style="list-style-type: none"> <li>• BPDU-Protected: BPDU attack guard function</li> <li>• Formatfrequency-Protected: MSTP BPDU format frequent change protection function</li> </ul>

## display stp history

### Syntax

```
display stp [ instance instance-id ] history [ slot slot-number ]
```

### View

Any view

### Default Level

0: Visit level

### Parameters

**instance** *instance-id*: Displays the historic port role calculation information of a particular MSTI. The effective range of *instance-id* is 0 to 32, with 0 representing the common internal spanning tree (CIST).

**slot** *slot-number*: Displays the historic port role calculation information of the specified device in the IRF stack. If no stack exists, this command only displays the historic port role calculation information of the current device. Replace the *slot-number* argument with the member ID of the device in the IRF stack.

### Description

Use the **display stp history** command to view the historic port role calculation information of the specified MSTI or all MSTIs.

Note that:

- If you do not specify an MSTI ID, this command will display the historic port role calculation information of all MSTIs. The displayed information is sequenced by MSTI ID, and by port role calculation time in each MSTI.
- If you specify an MSTI ID, this command will display the historic port role calculation information of only this specified MSTI by the sequence of port role calculation time.

### Examples

# View the historic port role calculation information of the card on slot 1 in MSTI 2.

```
<Sysname> display stp instance 2 history slot 1
----- STP slot 1 history trace -----
----- Instance 2 -----
Port GigabitEthernet1/0/1
  Role change   : ROOT->DESI (Aged)
  Time          : 2006/08/08 00:22:56
```

```

Port priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1

Port GigabitEthernet1/0/2
Role change   : ALTER->ROOT
Time          : 2006/08/08 00:22:56
Port priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2

```

**Table 1-6 display stp history command output description**

Field	Description
Port	Port name
Role change	A role change of the port ("Age" means that the change was caused by expiry of the received configuration BPDU)
Time	Time of port role calculation
Port priority	Port priority

## display stp region-configuration

### Syntax

```
display stp region-configuration
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display stp region-configuration** command to view the currently effective configuration information of the MST region, including the region name, revision level, and user-configured VLAN-to-MSTI mappings.

Related commands: **stp region-configuration**.

### Examples

# View the currently effective MST region configuration information.

```

<Sysname> display stp region-configuration
Oper Configuration
Format selector :0
Region name     :hello
Revision level  :0

Instance  Vlans Mapped
0         21 to 4094

```

1	1 to 10
2	11 to 20

**Table 1-7** display stp region-configuration command output description

Field	Description
Format selector	MSTP-defined format selector
Region name	MST region name
Revision level	Revision level of the MST region
Instance Vlans Mapped	VLAN-to-MSTI mappings in the MST region

## display stp root

### Syntax

**display stp root**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display stp root** command to view the root bridge information of all MSTIs.

### Examples

# View the root bridge information of all MSTIs.

```
<Sysname> display stp root
```

```
MSTID      Root Bridge ID      ExtPathCost  IntPathCost  Root Port
0          0.0013.1923.da80   0            0
```

**Table 1-8** display stp root command output description

Field	Description
MSTID	MSTI ID
Root Bridge ID	Root bridge ID
ExtPathCost	External path cost
IntPathCost	Internal path cost
Root Port	Root port name (displayed only if a port of the current device is the root port of MSTIs)

## display stp tc

### Syntax

```
display stp [ instance instance-id ] tc [ slot slot-number ]
```

### View

Any view

### Default Level

0: Visit level

### Parameters

**instance** *instance-id*: Displays the statistics of TC/TCN BPDUs received and sent by all ports in a particular spanning tree instance. The effective range of *instance-id* is 0 to 32, with 0 representing the common internal spanning tree (CIST).

**slot** *slot-number*: Displays the statistics of TC/TCN BPDUs received and sent by all ports on the specified device in the IRF stack. If no stack exists, this command only displays the information of the current device. Replace the *slot-number* argument with the member ID of the device in the IRF stack.

### Description

Use the **display stp tc** command to view the statistics of TC/TCN BPDUs received and sent.

Note that:

- If you do not specify an MSTI ID, this command will display the statistics of TC/TCN BPDUs received and sent by all ports in all spanning tree instances. The displayed information is sequenced by instance ID and by port name in each spanning tree instance.
- If you specify an MSTI ID, this command will display the statistics of TC/TCN BPDUs received and sent by all ports in the specified MSTI, in port name order.

### Examples

# View the statistics of TC/TCN BPDUs received and sent by all ports on the card on slot 1 in MSTI 0.

```
<Sysname> display stp instance 0 tc slot 1
----- STP slot 1 TC or TCN count -----
MSTID      Port                               Receive      Send
  0         GigabitEthernet1/0/1                6             4
  0         GigabitEthernet1/0/2                0             2
```

**Table 1-9 display stp tc** command output description

Field	Description
MSTID	MSTI ID in the MST region
Port	Port name
Receive	Number of TC/TCN BPDUs received on each port
Send	Number of TC/TCN BPDUs sent by each port

## instance

### Syntax

```
instance instance-id vlan vlan-list  
undo instance instance-id [vlan vlan-list]
```

### View

MST region view

### Default Level

2: System level

### Parameters

*instance-id*: MSTI ID. The effective range of *instance-id* is 0 to 32, with 0 representing the common internal spanning tree (CIST).

**vlan** *vlan-list*: Specifies a VLAN list in the format of *vlan-list* = { *vlan-id* [ **to** *vlan-id2* ] &<1-10>}, in which *vlan-id* represents the VLAN ID and ranges from 1 to 4094. &<1-10> indicates you can specify up to 10 VLAN IDs or VLAN ID ranges.

### Description

Use the **instance** command to map the specified VLAN(s) to the specified MSTI.

Use the **undo instance** command to remap the specified VLAN(s) or all VLANs to the CIST (MSTI 0).

By default, all VLANs are mapped to the CIST.

Notice that:

- If you specify no VLAN in the **undo instance** command, all VLANs mapped to the specified MSTI will be remapped to the CIST.
- You cannot map the same VLAN to different MSTIs. If you map a VLAN that has been mapped to an MSTI to a new MSTI, the old mapping will be automatically removed.

Related commands: **region-name**, **revision-level**, **check region-configuration**, **vlan-mapping modulo**, **active region-configuration**.

### Examples

```
# Map VLAN 2 to MSTI 1.  
<Sysname> system-view  
[Sysname] stp region-configuration  
[Sysname-mst-region] instance 1 vlan 2
```

## region-name

### Syntax

```
region-name name  
undo region-name
```

### View

MST region view

## Default Level

2: System level

## Parameters

*name*: MST region name, a string of 1 to 32 characters.

## Description

Use the **region-name** command to configure the MST region name of your device.

Use the **undo region-name** command to restore the default MST region name.

By default, the MST region name of a device is its MAC address.

The MST region name, the VLAN-to-MSTI mapping table and the MSTP revision level of a device jointly determine the MST region the device belongs to.

Related commands: **instance**, **revision-level**, **check region-configuration**, **vlan-mapping modulo**, **active region-configuration**.

## Examples

```
# Set the MST region name of the device to "hello".
```

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] region-name hello
```

## reset stp

### Syntax

```
reset stp [ interface interface-list ]
```

### View

User view

## Default Level

1: Monitor level

## Parameters

**interface** *interface-list*: Specifies a port list, in the format of *interface-list* = { *interface-type interface-number* [ **to** *interface-type interface-number* ] }&<1-10>, where &<1-10> indicates that you can specify up to 10 ports or port ranges.

## Description

Use the **reset stp** command to clear the MSTP statistics information.

The MSTP statistics information includes the numbers of TCN BPDUs, configuration BPDUs, RST BPDUs and MST BPDUs sent/received through the specified port(s) (STP BPDUs and TCN BPDUs are counted only for the CIST).

Note that this command clears the spanning tree-related statistics information on the specified port(s) if you specify the *interface-list* argument; otherwise, this command clears the spanning tree-related statistics on all ports.

Related commands: **display stp**.

## Examples

```
# Clear the spanning tree-related statistics information on ports GigabitEthernet1/0/1 through GigabitEthernet1/0/3.
```

```
<Sysname> reset stp interface gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

## revision-level

### Syntax

```
revision-level level
```

```
undo revision-level
```

### View

MST region view

### Default Level

2: System level

### Parameters

*level*: MSTP revision level, in the range of 0 to 65535.

### Description

Use the **region-level** command to configure the MSTP revision level of your device.

Use the **undo region-level** command to restore the default MSTP revision level.

By default, the MSTP revision level is 0.

The MSTP revision level, the MST region name and the VLAN-to-MSTI mapping table of a device jointly determine the MST region the device belongs to.

Related commands: **instance**, **region-name**, **check region-configuration**, **vlan-mapping modulo**, **active region-configuration**.

## Examples

```
# Set the MSTP revision level of the MST region to 5.
```

```
<Sysname> system-view
```

```
[Sysname] stp region-configuration
```

```
[Sysname-mst-region] revision-level 5
```

## stp bpdu-protection

### Syntax

```
stp bpdu-protection
```

```
undo stp bpdu-protection
```

### View

System view

## Default Level

2: System level

## Parameters

None

## Description

Use the **stp bpdu-protection** command to enable the BPDU guard function for the device.

Use the **undo stp bpdu-protection** command to disable the BPDU guard function for the device.

By default, the BPDU guard function is disabled.

## Examples

```
# Enable the BPDU guard function for the device.
```

```
<Sysname> system-view
```

```
[Sysname] stp bpdu-protection
```

## stp bridge-diameter

### Syntax

```
stp bridge-diameter bridge-number
```

```
undo stp bridge-diameter
```

### View

System view

## Default Level

2: System level

## Parameters

*bridge-number*: Specifies the switched network diameter, in the range of 2 to 7.

## Description

Use the **stp bridge-diameter** command to specify the network diameter, namely the maximum possible number of stations between any two terminal devices on the switched network.

Use the **undo stp bridge-diameter** command to restore the default.

By default, the network diameter of the switched network is 7.

An appropriate setting of hello time, forward delay and max age can speed up network convergence. The values of these timers are related to the network size. You can set these three timers indirectly by setting the network diameter. Based on the network diameter you configured, MSTP automatically sets an optimal hello time, forward delay, and max age for the device. With the network diameter set to 7 (the default), the three timer are also set to their defaults.

Note that this configuration is effective for the CIST and root bridge only, and not for MSTIs.

Related commands: **stp timer forward-delay**, **stp timer hello**, **stp timer max-age**.

## Examples

```
# Set the network diameter of the switched network to 5.
<Sysname> system-view
[Sysname] stp bridge-diameter 5
```

## stp compliance

### Syntax

```
stp compliance { auto | dot1s | legacy }
undo stp compliance
```

### View

Ethernet interface view, port group view, Layer-2 aggregate interface view

### Default Level

2: System level

### Parameters

**auto**: Configures the port(s) to recognize the MSTP BPDU format automatically and accordingly determine the format of MSTP BPDUs to send.

**dot1s**: Configures the port(s) to receive and send only standard-format (802.1s-compliant) MSTP BPDUs.

**legacy**: Configures the port(s) to receive and send only compatible-format MSTP BPDUs.

### Description

Use the **stp compliance** command to configure the mode the port(s) will use to recognize and send MSTP BPDUs.

Use the **undo stp compliance** command to restore the system default.

The default mode is **auto**, namely all ports recognize the BPDU format automatically.

Note that:

- Configured in interface view, the setting takes effect on the current port only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer-2 aggregate interface view, the setting takes effect only on the aggregate interface. Configured on the member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.
- If the mode is set to **auto** on a port, the port automatically recognizes and resolves the received compatible-format BPDUs or 802.1s-compliant BPDUs, and sends, when needed, compatible-format or 802.1s-compliant BPDUs.
- If the mode is set to **legacy** or **dot1s** on a port, the port can only receive and send BPDUs of the specified format. If the port is configured not to detect the packet format automatically while it works in the MSTP mode, and if it receives a packet in the format other than the configured format, it will become a designated port and remain in the discarding state to prevent the occurrence of a loop.

## Examples

```
# Configure GigabitEthernet 1/0/1 to receive and send only standard-format (802.1s) MSTP packets.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp compliance dot1s
```

## stp config-digest-snooping

### Syntax

```
stp config-digest-snooping
undo stp config-digest-snooping
```

### View

System view, Ethernet interface view, port group view, Layer-2 aggregate interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **stp config-digest-snooping** command to enable Digest Snooping.

Use the **undo stp config-digest-snooping** command to disable Digest Snooping.

The feature is disabled by default.

Note that:

- Configured in system view, the setting takes effect globally; configured in interface view, the setting takes effect on the current port only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer-2 aggregate interface view, the setting takes effect only on the aggregate interface. Configured on the member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.
- You need to enable this feature both globally and on ports connected to other vendors' devices to make it take effect. It is recommended to enable the feature on all associated ports first and then globally, making all configured ports take effect at the same time to minimize the impact, and disable the feature globally to disable it on all associated ports.
- It is not recommended to enable Digest Snooping on the MST region edge ports to avoid loops.

## Examples

```
# Enable Digest Snooping globally.
<Sysname> system-view
[Sysname] stp config-digest-snooping

# Enable Digest Snooping on GigabitEthernet 1/0/1.
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp config-digest-snooping
```

## stp cost

### Syntax

```
stp [ instance instance-id ] cost cost
undo stp [ instance instance-id ] cost
```

### View

Ethernet interface view, port group view, Layer-2 aggregate interface view

### Default Level

2: System level

### Parameters

**instance** *instance-id*: Sets the path cost of the port(s) in a particular MSTI. The effective range of *instance-id* is 0 to 32, with 0 representing the common internal spanning tree (CIST).

**cost**: Path cost of the port, the effective range of which depends on the path cost calculation standard adopted.

- With the IEEE 802.1d-1998 standard selected for path cost calculation, the *cost* argument ranges from 1 to 65535.
- With the IEEE 802.1t standard selected for path cost calculation, the *cost* argument ranges from 1 to 200000000.
- With the private standard selected for path cost calculation, the *cost* argument ranges from 1 to 200000.

### Description

Use the **stp cost** command to set the path cost of the port(s) in the specified MSTI or all MSTIs.

Use the **undo stp cost** command to restore the system default.

By default, the device automatically calculates the path costs of ports in each MSTI based on the corresponding standard.

- Configured in interface view, the setting takes effect on the current port only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer-2 aggregate interface view, the setting takes effect only on the aggregate interface. Configured on the member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.
- If you set *instance-id* to 0, you are setting the path cost of the port in the CIST. The path cost setting of a port can affect the role selection of the port. Setting different path costs for the same port in different MSTIs allows different VLAN traffic flows to be forwarded along different physical links, thus to achieve VLAN-based load balancing. When the path cost of a port is changed, MSTP will re-compute the role of the port and initiate a state transition.
- If you do not provide **instance** *instance-id*, your configuration will take effect in the CIST instance only.

## Examples

```
# Set the path cost of port GigabitEthernet 1/0/3 in MSTI 2 to 200.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] stp instance 2 cost 200
```

## stp edged-port

### Syntax

```
stp edged-port { enable | disable }
undo stp edged-port
```

### View

Ethernet interface view, port group view, Layer-2 aggregate interface view

### Default Level

2: System level

### Parameters

**enable**: Configures the current port(s) to be an edge port or edge ports.

**disable**: Configures the current port(s) to be a non-edge port or non-edge ports.

### Description

Use the **stp edged-port enable** command to configure the port(s) to be an edge port or edge ports.

Use the **stp edged-port disable** or **undo stp edged-port enable** command to configure the port(s) to be a non-edge port or non-edge ports.

All ports are non-edge ports by default.

Note that:

- Configured in interface view, the setting takes effect on the current port only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer-2 aggregate interface view, the setting takes effect only on the aggregate interface. Configured on the member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.
- If a port directly connects to a user terminal rather than another device or a shared LAN segment, this port is regarded as an edge port. When the network topology changes, an edge port will not cause a temporary loop. Therefore, configuring a port as an edge port can enable the port to transition to the forwarding state rapidly. We recommend that you configure a port directly connecting to a user terminal as an edge port to enable it to transition to the forwarding state rapidly.
- Normally, configuration BPDUs from other devices cannot reach an edge port because it does not connect to any other device. Before the BPDU guard function is enabled, if a port receives a configuration BPDU, the port is working actually as a non-edge port even if you have configured it as an edge port.

## Examples

```
# Configure GigabitEthernet 1/0/1 as a non-edge port.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp edged-port disable
```

## stp enable

### Syntax

```
stp enable
undo stp enable
```

### View

System view, Ethernet port view, port group view, Layer-2 aggregate interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **stp enable** command to enable MSTP globally in system view, on a port in interface view, or on multiple ports in port group view.

Use the **undo stp enable** command to disable MSTP globally or on the port(s).

By default, MSTP is enabled on all ports and globally.

MSTP takes effect when it is enabled both globally and on the port. To control MSTP flexibly, you can use the **undo stp enable** command to disable MSTP on ports that are not intended to take part in spanning tree calculation and thus to save CPU resources.

Note that:

- Configured in Layer-2 aggregate interface view, the setting takes effect only on the aggregate interface. Configured on a member port in an aggregation group, the setting takes effect only after the port leaves the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.
- After you enable MSTP, the switch works in STP-compatible mode, RSTP mode or MSTP mode depending on the MSTP mode setting, which is configurable with the **stp mode** command. After MSTP is disabled, the switch becomes a transparent bridge.
- After being enabled, MSTP dynamically maintains the spanning tree status of VLANs based on received configuration BPDUs. After being disabled, it stops maintaining the spanning tree status.

Related commands: **stp mode**.

## Examples

```
# Enable MSTP globally.
<Sysname> system-view
[Sysname] stp enable
```

```
# Disable MSTP on port GigabitEthernet1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo stp enable
```

## stp loop-protection

### Syntax

```
stp loop-protection
undo stp loop-protection
```

### View

Ethernet interface view, port group view, Layer-2 aggregate interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **stp loop-protection** command to enable the loop guard function on the port(s).

Use the **undo stp loop-protection** command to restore the system default.

By default, the loop guard function is disabled.

Note that:

- Configured in interface view, the setting takes effect on the current port only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer-2 aggregate interface view, the setting takes effect only on the aggregate interface. Configured on the member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.

### Examples

```
# Enable the loop guard function on GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp loop-protection
```

## stp max-hops

### Syntax

```
stp max-hops hops
undo stp max-hops
```

### View

System view

## Default Level

2: System level

## Parameters

*hops*: Maximum hops, in the range of 1 to 40

## Description

Use the **stp max-hops** command to set the maximum hops of the MST region on the device.

Use the **undo stp max-hops** command to restore the maximum hops to the default setting.

By default, the maximum number of hops of an MST region is 20.

The maximum hops configured in an MST region limit the size of the MST region. In an MST region, the maximum hops configured on the regional root bridge are the maximum hops of this MST region. After a configuration BPDU leaves the root bridge, its hop count is decremented by 1 each time it passes a device. When its hop count reaches 0, it will be discarded by the device that received it. As a result, devices beyond the maximum hop count are unable to take part in spanning tree calculation, and thereby the size of the MST region is limited.

Devices other than the root bridge in an MST region use the maximum hops setting on the root bridge.

## Examples

```
# Set the maximum hops of the MST region to 35.
```

```
<Sysname> system-view  
[Sysname] stp max-hops 35
```

## stp mcheck

### Syntax

```
stp mcheck
```

### View

System view, Ethernet interface view, Layer-2 aggregate interface view

## Default Level

2: System level

## Parameters

None

## Description

Use the **stp mcheck** command to carry out the mCheck operation globally or on the current port.

In a switched network, if a port on the device running MSTP (or RSTP) connects to a device running STP, this port will automatically migrate to the STP-compatible mode. However, if the device running STP is removed, the port will not be able to migrate automatically to the MSTP (or RSTP) mode, but will remain working in the STP-compatible mode. In this case, you can perform an mCheck operation to force the port to migrate to the MSTP (or RSTP) mode.

Note that:

- The **stp mcheck** command is meaningful only when the device works in the MSTP (or RSTP-compatible) mode, not in the STP-compatible mode.
- Configured in system view, the setting takes effect globally; configured in interface view, the setting takes effect on the current port only.
- Configured in Layer-2 aggregate interface view, the setting takes effect only on the aggregate interface. Configured on the member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration in the Access Volume*.

Related commands: **stp mode**.

## Examples

```
# Carry out mCheck on GigabitEthernet 1/0/1.
```

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp mcheck
```

## stp mode

### Syntax

```
stp mode { stp | rstp | mstp }
undo stp mode
```

### View

System view

### Default Level

2: System level

### Parameters

**stp**: Configures the MSTP-enabled device to work in STP-compatible mode.

**rstp**: Configures an MSTP-enabled device to work in RSTP mode.

**mstp**: Configures an MSTP-enabled device to work in MSTP mode.

### Description

Use the **stp mode** command to configure the MSTP work mode of the device.

Use the **undo stp mode** command to restore the MSTP work mode to the default setting.

By default, an MSTP-enabled device works in MSTP mode.

Related commands: **stp mcheck**, **stp enable**.

## Examples

```
# Configure the MSTP-enabled device to work in STP-compatible mode.
```

```
<Sysname> system-view
[Sysname] stp mode stp
```

## stp no-agreement-check

### Syntax

```
stp no-agreement-check
undo stp no-agreement-check
```

### View

Ethernet interface view, port group view, Layer-2 aggregate interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **stp no-agreement-check** command to enable No Agreement Check on the port(s).

Use the **undo stp no-agreement-check** command to disable No Agreement Check on the port(s).

By default, No Agreement Check is disabled.

Note that:

- Configured in interface view, the setting takes effect on the current port only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer-2 aggregate interface view, the setting takes effect only on the aggregate interface. Configured on the member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.



#### Note

To use the No Agreement Check feature, enable it on the root port.

---

### Examples

```
# Enable No Agreement Check on GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp no-agreement-check
```

## stp pathcost-standard

### Syntax

```
stp pathcost-standard { dot1d-1998 | dot1t | legacy }
undo stp pathcost-standard
```

## View

System view

## Default Level

2: System level

## Parameters

**dot1d-1998:** The device calculates the default path cost for ports based on IEEE 802.1d-1998.

**dot1t:** The device calculates the default path cost for ports based on IEEE 802.1t.

**legacy:** The device calculates the default path cost for ports based on a private standard.

## Description

Use the **stp pathcost-standard** command to specify a standard for the device to use when calculating the default path costs for ports of the device.

Use the **undo stp pathcost-standard** command to restore the system default.

The default standard used by the device is **legacy**.

Note that if you change the standard that the device uses in calculating the default path cost, the port path cost value set through the **stp cost** command will be invalid.

**Table 1-10** Link speed vs. path cost

Link speed	Duplex state	Path cost in 802.1d-1998 standard	Path cost in IEEE 802.1t standard	Path cost in private standard
0	—	65535	200,000,000	200,000
10 Mbps	Single Port	100	2,000,000	2,000
	Aggregate Link 2 Ports	100	1,000,000	1,800
	Aggregate Link 3 Ports	100	666,666	1,600
	Aggregate Link 4 Ports	100	500,000	1,400
100 Mbps	Single Port	19	200,000	200
	Aggregate Link 2 Ports	19	100,000	180
	Aggregate Link 3 Ports	19	66,666	160
	Aggregate Link 4 Ports	19	50,000	140
1000 Mbps	Single Port	4	20,000	20
	Aggregate Link 2 Ports	4	10,000	18
	Aggregate Link 3 Ports	4	6,666	16
	Aggregate Link 4 Ports	4	5,000	14
10 Gbps	Single Port	2	2,000	2
	Aggregate Link 2 Ports	2	1,000	1
	Aggregate Link 3 Ports	2	666	1
	Aggregate Link 4 Ports	2	500	1

When calculating path cost for an aggregate interface, 802.1d-1998 does not take into account the number of member ports in its aggregation group as 802.1t does. The calculation formula of 802.1t is: Path Cost = 200,000,000/link speed (in 100 kbps), where link speed is the sum of the link speed values of the non-blocked ports in the aggregation group.

## Examples

```
# Configure the device to calculate the default path cost for ports based on IEEE 802.1d-1998.
```

```
<Sysname> system-view  
[Sysname] stp pathcost-standard dot1d-1998
```

```
# Configure the device to calculate the default path cost for ports based on IEEE 802.1t.
```

```
<Sysname> system-view  
[Sysname] stp pathcost-standard dot1t
```

## stp point-to-point

### Syntax

```
stp point-to-point { auto | force-false | force-true }  
undo stp point-to-point
```

### View

Ethernet interface view, port group view, Layer-2 aggregate interface view

### Default Level

2: System level

### Parameters

**auto**: Specifies automatic detection of the link type.

**force-false**: Specifies the non-point-to-point link type.

**force-true**: Specifies the point-to-point link type.

### Description

Use the **stp point-to-point** command to specify whether the current port(s) is/are connected to a point-to-point link or point-to-point links.

Use the **undo stp point-to-point** command to restore the system default.

The default setting is **auto**; namely the MSTP-enabled device automatically detects whether a port connects to a point-to-point link.

Note that:

- Configured in interface view, the setting takes effect on the current port only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer-2 aggregate interface view, the setting takes effect only on the aggregate interface. Configured on the member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.
- When connecting to a non-point-to-point link, a port is incapable of rapid state transition.
- If the current port is a Layer-2 aggregate interface or if it works in full duplex mode, the link to which the current port connects is a point-to-point link. We recommend that you use the default setting, namely let MSTP detect the link status automatically.
- This setting takes effect on the CIST and all MSTIs. If a port is configured as connecting to a point-to-point link or a non-point-to-point link, the setting takes effect for the port in all MSTIs. If the

physical link to which the port connects is not a point-to-point link and you force it to be a point-to-point link by configuration, your configuration may incur a temporary loop.

## Examples

```
# Configure port GigabitEthernet 1/0/3 as connecting to a point-to-point link.
```

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] stp point-to-point force-true
```

## stp port priority

### Syntax

```
stp [ instance instance-id ] port priority priority
```

```
undo stp [ instance instance-id ] port priority
```

### View

Ethernet interface view, port group view, Layer-2 aggregate interface view

### Default Level

2: System level

### Parameters

**instance** *instance-id*: Sets the priority of the current port(s) in a particular spanning tree instance. The effective range of *instance-id* is 0 to 32, with 0 representing the common internal spanning tree (CIST).

*priority*: Port priority, in the range of 0 to 240 in steps of 16 (0, 16, 32..., for example).

### Description

Use the **stp port priority** command to set the priority of the port(s).

Use the **undo stp port priority** command to restore the system default.

By default, the port priority is 128.

Note that:

- Configured in interface view, the setting takes effect on the current port only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer-2 aggregate interface view, the setting takes effect only on the aggregate interface. Configured on the member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.
- If you set *instance-id* to 0, you are setting the priority of the port in the CIST. The priority of a port can affect the role selection of the port in the specified MSTI.
- Setting different priorities for the same port in different MSTIs allows different VLAN traffic flows to be forwarded along different physical links, thus to achieve VLAN-based load balancing.
- When the priority of a port is changed in an MSTI, MSTP will re-compute the role of the port and initiate a state transition in the MSTI.
- If you do not provide **instance** *instance-id*, your configuration will take effect in the CIST only.

## Examples

```
# Set the priority of port GigabitEthernet 1/0/3 in MSTI 2 to 16.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] stp instance 2 port priority 16
```

## stp port-log

### Syntax

```
stp port-log { all | instance instance-id }
undo stp port-log { all | instance instance-id }
```

### View

System view

### Default Level

2: System level

### Parameters

**all**: Enables output of port state transition information for all MSTIs.

**instance** *instance-id*: Enables output of port state transition information for the specified MSTI. The effective range of *instance-id* is 0 to 32, with 0 representing the common internal spanning tree (CIST).

### Description

Use the **stp port-log** command to enable output of port state transition information for the specified MSTI or all MSTIs.

Use the **undo stp port-log** command to disable output of port state transition information for the specified MSTI or all MSTIs.

By default, the output of port state transition information is enabled.

## Examples

```
# Enable output of port state transition information for MSTI 2.
<Sysname> system-view
[Sysname] stp port-log instance 2
%Aug 16 00:49:41:856 2006 Sysname MSTP/3/PDISC: Instance 2's GigabitEthernet1/0/1 has been
set to discarding state!
%Aug 16 00:49:41:856 2006 Sysname MSTP/3/PFWD: Instance 2's GigabitEthernet1/0/2 has been
set to forwarding state!
// The information above shows that in MSTI 2 the state of GigabitEthernet 1/0/1 has changed to
discarding and that of GigabitEthernet 1/0/2 has changed to forwarding.
```

## stp priority

### Syntax

```
stp [ instance instance-id ] priority priority
```

**undo stp [ instance *instance-id* ] priority**

## View

System view

## Default Level

2: System level

## Parameters

**instance** *instance-id*: Sets the priority of the device in a particular spanning tree instance. The effective range of *instance-id* is 0 to 32, with 0 representing the common internal spanning tree (CIST).

*priority*: Port priority, in the range of 0 to 61440 in steps of 4096, namely you can set up to 16 priority values, such as 0, 4096, 8192..., on the device.

## Description

Use the **stp priority** command to set the priority of the device.

Use the **undo stp priority** command to restore the default device priority.

By default, the device priority is 32768.

The device priority is involved in spanning tree calculation. The device priority is set on a per-MSTI basis. An MSTP-enabled device can have different priorities in different MSTIs.

If you do not provide **instance** *instance-id*, your configuration will take effect in the CIST instance only.

## Examples

```
# Set the device priority in MSTI 1 to 4096.
```

```
<Sysname> system-view
```

```
[Sysname] stp instance 1 priority 4096
```

## stp region-configuration

### Syntax

**stp region-configuration**

**undo stp region-configuration**

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **stp region-configuration** command to enter MST region view.

Use the **undo stp region-configuration** command to restore the default MST region configurations.

By default, the default settings are used for all the three MST region parameters. Namely, the device's MST region name is the device's MAC address, all VLANs are mapped to the CIST, and the MSTP revision level is 0.

After you enter MST region view, you can configure the parameters related to the MST region, including the region name, VLAN-to-MSTI mappings and revision level.

## Examples

```
# Enter MST region view.  
<Sysname> system-view  
[Sysname] stp region-configuration  
[Sysname-mst-region]
```

## stp root primary

### Syntax

```
stp [ instance instance-id ] root primary  
undo stp [ instance instance-id ] root
```

### View

System view

### Default Level

2: System level

### Parameters

**instance** *instance-id*: Configures the device as the root bridge in a particular MSTI. The effective range of *instance-id* is 0 to 32, with 0 representing the common internal spanning tree (CIST).

### Description

Use the **stp root primary** command to configure the current device as the root bridge.

Use the **undo stp root** command to restore the system default.

By default, a device is not a root bridge.

Note that:

- If you do not provide **instance** *instance-id*, your configuration will take effect in the CIST instance only.
- There is only one root bridge in effect in an MSTI. If two or more devices have been designated to be root bridges of the same MSTI, MSTP will select the device with the lowest MAC address as the root bridge.
- You can specify a root bridge for each MSTI without caring about the device priority. After specifying the current device as the root bridge or a secondary root bridge, you cannot change the priority of the device.

## Examples

```
# Specify the current device as the root bridge of MSTI 0.  
<Sysname> system-view  
[Sysname] stp instance 0 root primary
```

## stp root secondary

### Syntax

```
stp [ instance instance-id ] root secondary
undo stp [ instance instance-id ] root
```

### View

System view

### Default Level

2: System level

### Parameters

**instance** *instance-id*: Configures the device as a secondary root bridge in a particular MSTI. The effective range of *instance-id* is 0 to 32, with 0 representing the common internal spanning tree (CIST).

### Description

Use the **stp root secondary** command to configure the device as a secondary root bridge.

Use the **undo stp root** command to restore the system default.

By default, a device is not a secondary root bridge.

Note that:

- If you do not provide **instance** *instance-id*, your configuration will take effect in the CIST instance only.
- You can configure one or more secondary root bridges for each MSTI. When the root bridge of an MSTI fails or is shut down, the secondary root bridge can take over the role of the root bridge of the specified MSTI. If you specify more than one secondary root bridge, the secondary root bridge with the lowest MAC address will become the root bridge.
- After specifying the current device as the root bridge or a secondary root bridge, you cannot change the priority of the device.

### Examples

```
# Specify the current device as the secondary root bridge of MSTI 0.
```

```
<Sysname> system-view
[Sysname] stp instance 0 root secondary
```

## stp root-protection

### Syntax

```
stp root-protection
undo stp root-protection
```

### View

Ethernet interface view, port group view, Layer-2 aggregate interface view

### Default Level

2: System level

## Parameters

None

## Description

Use the **stp root-protection** command to enable the root guard function on the port(s).

Use the **undo stp root-protection** command to disable the root guard function on the port(s).

By default, the root guard function is disabled.

Note that:

- Configured in interface view, the setting takes effect on the current port only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer-2 aggregate interface view, the setting takes effect only on the aggregate interface. Configured on the member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.

## Examples

```
# Enable the root guard function for GigabitEthernet 1/0/1.  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] stp root-protection
```

## stp tc-protection

### Syntax

```
stp tc-protection enable  
stp tc-protection disable
```

### View

System view

### Default Level

2: System level

## Parameters

None

## Description

Use the **stp tc-protection enable** command to enable the TC-BPDU attack guard function for the device.

Use the **stp tc-protection disable** command to disable the TC-BPDU attack guard function for the device.

By default, the TC-BPDU attack guard function is enabled.

## Examples

```
# Enable the TC-BPDU attack guard function for the device.
```

```
<Sysname> system-view
[Sysname] stp tc-protection enable
```

## stp tc-protection threshold

### Syntax

```
stp tc-protection threshold number
undo stp tc-protection threshold
```

### View

System view

### Default Level

2: System level

### Parameters

*number*: Maximum number of times the device refreshes forwarding address entries within a certain period of time immediately after it receives the first TC-BPDU, in the range of 1 to 255.

### Description

Use the **stp tc-protection threshold** command to configure the maximum number of times the device refreshes forwarding address entries within 10 seconds immediately after it receives the first TC-BPDU.

Use the **undo stp tc-protection threshold** command to restore the system default.

By default, the device refreshes forwarding address entries a maximum of six times within a certain period of time immediately after it receives the first TC-BPDU.

### Examples

# Set the maximum number of times the device refreshes forwarding address entries within a certain period of time immediately after it receives the first TC-BPDU to 10.

```
<Sysname> system-view
[Sysname] stp tc-protection threshold 10
```

## stp timer forward-delay

### Syntax

```
stp timer forward-delay centi-seconds
undo stp timer forward-delay
```

### View

System view

### Default Level

2: System level

### Parameters

*centi-seconds*: Forward delay in centiseconds, ranging from 400 to 3000 in steps of 100.

## Description

Use the **stp timer forward-delay** command to set the forward delay timer of the device.

Use the **undo stp timer forward-delay** command to restore the system default.

By default, the forward delay timer is set to 1,500 centiseconds.

In order to prevent temporary loops, a port must go through an intermediate state, the learning state, before it transitions from the discarding state to the forwarding state, and must wait a certain period of time before it transitions from one state to another to keep synchronized with the remote device during state transition. The forward delay timer set on the root bridge determines the time interval of state transition.

If the current device is the root bridge, the state transition interval of the device depends on the set forward delay value; for a non- root bridge, its state transition interval is determined by the forward delay timer set on the root bridge.

The settings of the hello time, forward delay and max age timers must meet the following formulae:

- $2 \times (\text{forward delay} - 1 \text{ second}) \geq \text{max age}$
- $\text{Max age} \geq 2 \times (\text{hello Time} + 1 \text{ second})$

MSTP can work effectively on the entire network only when the above-mentioned conditions are met; otherwise, topology changes will frequently occur. We recommend that you specify the network diameter of the switched network in the **stp root primary** command and let MSTP automatically calculate optimal settings of these three timers.

Related commands: **stp timer hello**, **stp timer max-age**, **stp bridge-diameter**.

## Examples

```
# Set the forward delay timer of the device to 2,000 centiseconds.
```

```
<Sysname> system-view  
[Sysname] stp timer forward-delay 2000
```

## stp timer hello

### Syntax

```
stp timer hello centi-seconds
```

```
undo stp timer hello
```

### View

```
System view
```

### Default Level

```
2: System level
```

### Parameters

*centi-seconds*: Hello time in centiseconds, ranging from 100 to 1000 in steps of 100.

## Description

Use the **stp timer hello** command to set the hello time of the device.

Use the **undo stp timer hello** command to restore the system default.

By default, the hello time is set to 200 centiseconds.

Hello time is the time interval at which MSTP-enabled devices send configuration BPDUs to maintain spanning tree. If a device fails to receive configuration BPDUs within the set period of time, a new spanning tree calculation process will be triggered due to timeout. The root bridge sends configuration BPDUs at the interval of the hello time set on the device, while non-root bridges use the hello time set on the root bridge.

The settings of the hello time, forward delay and max age timers must meet the following formulae:

- $2 \times (\text{forward delay} - 1 \text{ second}) \geq \text{max age}$
- $\text{Max age} \geq 2 \times (\text{hello time} + 1 \text{ second})$

MSTP can work effectively on the entire network only when the above-mentioned conditions are met; otherwise, topology changes will frequently occur. We recommend that you specify the network diameter of the switched network in the **stp root primary** command and let MSTP automatically calculate optimal settings of these three timers.

Related commands: **stp timer forward-delay**, **stp timer max-age**, **stp bridge-diameter**.

## Examples

```
# Set the hello time of the device to 400 centiseconds.
```

```
<Sysname> system-view  
[Sysname] stp timer hello 400
```

## stp timer max-age

### Syntax

```
stp timer max-age centi-seconds  
undo stp timer max-age
```

### View

System view

### Default Level

2: System level

### Parameters

*centi-seconds*: Max age in centiseconds, ranging from 600 to 4000 in steps of 100.

### Description

Use the **stp timer max-age** command to set the max age timer of the device.

Use the **undo stp timer max-age** command to restore the system default.

By default, the max age is set to 2,000 centiseconds.

MSTP can detect link failures and automatically restore the forwarding state of the redundant link. In the CIST, the device determines whether a configuration BPDU received on a port has expired based on the max age timer. If a port receives a configuration BPDU that has expired, that MSTI needs to be re-computed.

The max age timer is not meaningful for MSTIs. If the current device is the root bridge of the CIST, it determines whether a configuration BPDU has expired based on the configured max age timer; if the current device is not the root bridge of the CIST, it uses the max age timer set on the CIST root bridge.

The settings of the hello time, forward delay and max age timers must meet the following formulae:

- $2 \times (\text{forward delay} - 1 \text{ second}) \geq \text{max age}$
- $\text{Max age} \geq 2 \times (\text{hello time} + 1 \text{ second})$

MSTP can work effectively on the entire network only when the above-mentioned conditions are met; otherwise, topology changes will frequently occur. We recommend that you specify the network diameter in the **stp root primary** command and let MSTP automatically calculate an optimal setting of these three timers.

Related commands: **stp timer forward-delay**, **stp timer hello**, **stp bridge-diameter**.

## Examples

```
# Set the max age timer of the device to 1,000 centiseconds.
```

```
<Sysname> system-view  
[Sysname] stp timer max-age 1000
```

## stp timer-factor

### Syntax

```
stp timer-factor number  
undo stp timer-factor
```

### View

System view

### Default Level

2: System level

### Parameters

*number*: Timeout factor, in the range of 1 to 20.

### Description

Use the **stp timer-factor** command to configure the timeout time of the device by setting the timeout factor. Timeout time = timeout factor  $\times$  3  $\times$  hello time.

Use the **undo stp timer-factor** command to restore the default timeout factor.

By default, the timeout factor of the device is set to 3.

After the network topology is stabilized, each non-root-bridge device forwards configuration BPDUs to the surrounding devices at the interval of hello time to check whether any link is faulty. Typically, if a device does not receive a BPDU from the upstream device within nine times the hello time, it will assume that the upstream device has failed and start a new spanning tree calculation process.

In a very stable network, this kind of spanning tree calculation may occur because the upstream device is busy. In this case, you can avoid such unwanted spanning tree calculations by lengthening the timeout time (by setting the timeout factor to 4 or more). We recommend that you set the timeout factor to 5, or 6, or 7 for a stable network.

## Examples

```
# Set the timeout factor of the device to 7.
<Sysname> system-view
[Sysname] stp timer-factor 7
```

## stp transmit-limit

### Syntax

```
stp transmit-limit packet-number
undo stp transmit-limit
```

### View

Ethernet interface view, port group view, Layer-2 aggregate interface view

### Default Level

2: System level

### Parameters

*packet-number*: Maximum number of MSTP packets that the port(s) can send within each hello time, namely the maximum transmission rate of the port, in the range of 1 to 255.

### Description

Use the **stp transmit-limit** command to set the maximum transmission rate of the port(s).

Use the **undo stp transmit-limit** command to restore the system default.

By default, the maximum transmission rate of all ports of the device is 10.

Note that:

- Configured in interface view, the setting takes effect on the current port only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer-2 aggregate interface view, the setting takes effect only on the aggregate interface. Configured on the member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.
- A larger maximum transmission rate value represents more MSTP packets that the port will send within each hello time, but this means that more device resources will be used. An appropriate maximum transmission rate setting can prevent MSTP from using excessive bandwidth resources during network topology changes.

## Examples

```
# Set the maximum transmission rate of port GigabitEthernet 1/0/1 to 5.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp transmit-limit 5
```

## vlan-mapping modulo

### Syntax

**vlan-mapping modulo** *modulo*

### View

MST region view

### Default Level

2: System level

### Parameters

*modulo*: Modulo value, in the range of 1 to 32.

### Description

Use the **vlan-mapping modulo** command to map VLANs in the current MST region to MSTIs according to the specified modulo value.

By default, all VLANs are mapped to the CIST (MSTI 0).

You cannot map the same VLAN to different MSTIs. If you map a VLAN that has been mapped to an MSTI to a new MSTI, the old mapping will be automatically removed.



#### Note

By using the **vlan-mapping modulo** command, you can quickly specify a VLAN for each MSTI. This command maps each VLAN to the MSTI whose ID is  $(\text{VLAN ID}-1) \% \text{modulo} + 1$ , where  $(\text{VLAN ID}-1) \% \text{modulo}$  is the modulo operation for  $(\text{VLAN ID}-1)$ . If the modulo value is 15, for example, then VLAN 1 will be mapped to MSTI 1, VLAN 2 to MSTI 2, VLAN 15 to MSTI 15, VLAN 16 to MSTI 1, and so on.

---

Related commands: **region-name**, **revision-level**, **check region-configuration**, **active region-configuration**.

### Examples

# Map VLANs to MSTIs as per modulo 8.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] vlan-mapping modulo 8
```

# Table of Contents

<b>1 RRPP Configuration Commands</b> .....	<b>1-1</b>
RRPP Configuration Commands .....	1-1
control-vlan .....	1-1
display rrpp brief .....	1-2
display rrpp ring-group .....	1-3
display rrpp statistics .....	1-4
display rrpp verbose .....	1-7
domain ring .....	1-9
protected-vlan .....	1-10
reset rrpp statistics .....	1-11
ring .....	1-12
ring enable .....	1-14
rrpp domain .....	1-15
rrpp enable .....	1-16
rrpp ring-group .....	1-16
timer .....	1-17

# 1 RRPP Configuration Commands

---

## RRPP Configuration Commands

### control-vlan

#### Syntax

**control-vlan** *vlan-id*

**undo control-vlan**

#### View

RRPP domain view

#### Default Level

2: System level

#### Parameters

*vlan-id*: Control VLAN ID, in the range 2 to 4093.

#### Description

Use the **control-vlan** command to specify a control VLAN for an RRPP domain.

Use the **undo control-vlan** command to remove the control VLAN configured for an RRPP domain.

Note that:

- The control VLAN must be a new one.
- You need only configure a control VLAN for the primary ring. However, the control VLAN of a subring is assigned automatically by the system and its VLAN ID is the control VLAN ID of the primary ring plus 1. So, you should select two consecutive new VLANs. Otherwise, the configuration fails.
- Before configuring rings for an RRPP domain, make sure the RRPP domain is configured with a control VLAN.
- Before configuring RRPP rings for an RRPP domain, you can delete or modify the control VLAN configured for the RRPP domain. However, after configuring RRPP rings for an RRPP domain, you cannot delete or modify the control VLAN of the domain.
- Deleting an RRPP domain deletes its control VLAN at the same time.
- You cannot use the **undo vlan all** command to delete a control VLAN.
- Do not enable QinQ or VLAN mapping on the control VLAN. Otherwise, RRPPDUs cannot be forwarded properly.

Related commands: **rrpp domain**, **protected-vlan**.

#### Examples

```
# Configure the control VLAN of RRPP domain 1 as VLAN 100.
```

```
<Sysname> system-view
```

```
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
```

## display rrpp brief

### Syntax

**display rrpp brief**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display rrpp brief** command to display the brief information of RRPP configuration.

### Examples

# Display the brief information of RRPP configuration.

```
<Sysname> display rrpp brief
Flags for Node Mode :
M -- Master , T -- Transit , E -- Edge , A -- Assistant-Edge

RRPP Protocol Status: Enable
Number of RRPP Domains: 2

Domain ID      : 1
Control VLAN   : Major 5      Sub 6
Protected VLAN: Reference Instance 0 to 2, 4
Hello Timer    : 1 sec Fail Timer : 3 sec
Ring Ring Node Primary/Common Secondary/Edge Enable
ID Level Mode Port Port Status
-----
1 1 M GigabitEthernet1/0/1 GigabitEthernet1/0/2 Yes

Domain ID      : 2
Control VLAN   : Major 10     Sub 11
Protected VLAN: Reference Instance 0 to 2, 4
Hello Timer    : 1 sec Fail Timer : 3 sec
Ring Ring Node Primary/Common Secondary/Edge Enable
ID Level Mode Port Port Status
-----
1 0 T GigabitEthernet1/0/3 GigabitEthernet1/0/4 Yes
2 1 E GigabitEthernet1/0/3 GigabitEthernet1/0/5 Yes
GigabitEthernet1/0/4
```

**Table 1-1 display rrpp brief** command output description

Field	Description
Flags for Node Mode	RRPP node mode: M represents master node, T represents transit node, E represents edge node and A represents assistant edge node
RRPP Protocol Status	RRPP protocol status: Enable (globally enabled)/Disable (globally disabled)
Number of RRPP Domains	Number of RRPP domains configured
Domain ID	RRPP domain ID
Control VLAN	Control VLANs of an RRPP domain: Major and Sub
Protected VLAN	List of VLANs protected by the RRPP domain. MSTIs are displayed here. To get the VLANs corresponding to these MSTIs, use the <b>display stp region-configuration</b> command.
Hello Timer	Hello Timer value configured in seconds
Fail Timer	Fail Timer value configured in seconds
Ring ID	RRPP ring ID
Ring Level	RRPP ring level, with 0 representing primary ring and 1 representing subring
Node Mode	Node mode
Primary/Common Port	Primary port when the node mode is master node or transit node; common port when the node mode is edge node or assistant edge node; "-" appears when the port is not configured on the ring.
Secondary/Edge Port	Secondary port when the node mode is master node or transit node; edge port when the node mode is edge node or assistant edge node; "-" appears when the port is not configured on the ring.
Enable Status	RRPP ring status: Yes indicates enabled and No indicates disabled.

## display rrpp ring-group

### Syntax

```
display rrpp ring-group [ ring-group-id ]
```

### View

Any view

### Default Level

1: Monitor Level

### Parameters

*ring-group-id*: Ring group ID, in the range 1 to 8.

## Description

Use the **display rrpp ring-group** command to display the ring group configuration. If no ring group ID is specified, the configuration of all ring groups is displayed. For an edge node ring group, the subring sending Edge-Hello packets is also displayed.

Related commands: **domain ring**.

## Examples

```
# Display the ring group configuration.
```

```
<Sysname> display rrpp ring-group
```

```
Ring Group 1:
```

```
domain 1 ring 1 to 3, 5
```

```
domain 2 ring 1 to 3, 5
```

```
domain 1 ring 1 is the sending ring
```

```
Ring Group 2:
```

```
domain 1 ring 4, 6 to 7
```

```
domain 2 ring 4, 6 to 7
```

**Table 1-2 display rrpp ring-group** command output description

Field	Description
Ring Group xx	RRPP ring group ID
domain xx ring xx	Subrings in the ring group
domain xx ring xx is the sending ring	The sending ring of the ring group is ring xx in RRPP domain xx

## display rrpp statistics

### Syntax

```
display rrpp statistics domain domain-id [ring ring-id]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*domain-id*: RRPP domain ID, in the range 1 to 8.

*ring-id*: RRPP ring ID, in the range 1 to 64.

### Description

Use the **display rrpp statistics** command to display RRPP message statistics.

Note that:

- If you have specified an RRPP ring ID in the command, RRPP message statistics of the specified RRPP ring in the specified RRPP domain on the current device appears. Otherwise, RRPP message statistics of all RRPP rings in the specified RRPP domain appears.
- If some port belongs to more than one ring, its packets are taken statistics based on the rings. You will view the statistics of the port under the current ring.
- When a ring transits from inactive status into active status, its packets will be counted again..

Related commands: **reset rrpp statistics**.

## Examples

# Display RRPP message statistics of ring 1 in RRPP domain 1.

```
<Sysname> display rrpp statistics domain 1 ring 1
Ring ID      : 1
Ring Level   : 1
Node Mode    : Master
Active Status : Yes
Primary port : GigabitEthernet1/0/1
Packet      Link      Common      Complete   Edge   Major Packet
Direct Hello Down      Flush FDB   Flush FDB  Hello Fault Total
-----
Send 16424    0         0           1          0     0     16425
Rcv   0        0         0           0          0     0     0
Secondary port: GigabitEthernet1/0/2
Packet      Link      Common      Complete   Edge   Major Packet
Direct Hello Down      Flush FDB   Flush FDB  Hello Fault Total
-----
Send  0       0         0           0          0     0     0
Rcv 16378    0         0           1          0     0    16379
```

# Display RRPP message statistics of RRPP domain 2.

```
<Sysname> display rrpp statistics domain 2
Ring ID      : 1
Ring Level   : 0
Node Mode    : Master
Active Status : Yes
Primary port : GigabitEthernet1/0/3
Packet      Link      Common      Complete   Edge   Major Packet
Direct Hello Down      Flush FDB   Flush FDB  Hello Fault Total
-----
Send 16924    0         0           1          0     0    16925
Rcv   0        0         0           0          0     0     0
Secondary port: GigabitEthernet1/0/4
Packet      Link      Common      Complete   Edge   Major Packet
Direct Hello Down      Flush FDB   Flush FDB  Hello Fault Total
-----
Send  0       0         0           0          0     0     0
Rcv 16878    0         0           1          0     0    16879

Ring ID      : 2
```

```

Ring Level      : 1
Node Mode      : Edge
Active Status   : No
Common port    : GigabitEthernet1/0/3
Packet         Link          Common      Complete   Edge   Major Packet
Direct Hello   Down           Flush FDB  Flush FDB  Hello Fault Total
-----
Send  0         0           0          0          0     0     0
Rcv   0         0           0          0          0     0     0
Common port    : GigabitEthernet1/0/4
Packet         Link          Common      Complete   Edge   Major Packet
Direct Hello   Down           Flush FDB  Flush FDB  Hello Fault Total
-----
Send  0         0           0          0          0     0     0
Rcv   0         0           0          0          0     0     0
Edge port      : GigabitEthernet1/0/5
Packet         Link          Common      Complete   Edge   Major Packet
Direct Hello   Down           Flush FDB  Flush FDB  Hello Fault Total
-----
Send  0         0           0          0          0     0     0
Rcv   0         0           0          0          0     0     0

```

**Table 1-3 display rrrp statistics** command output description

Field	Description
Ring ID	RRPP ring ID
Ring Level	RRPP ring level: 0 for primary ring and 1 for subring
Node Mode	Node mode: master node, transit node, edge node and assistant edge node
Active Status	RRPP ring activation status: Yes indicates active and No indicates inactive (An RRPP is active only if the RRPP ring is enabled and the RRPP protocol is globally enabled)
Primary Port	The primary port field means the node mode is master node or transit node. "-" appears when the port is not configured on the ring, and in this case, no corresponding statistics appears.
Secondary Port	The secondary port field means the node mode is master node or transit node. "-" appears when the port is not configured on the ring, and in this case, no corresponding statistics appears.
Common Port	The common port field means the node mode is edge node or assistant edge node. "-" appears when the port is not configured on the ring, and in this case, no corresponding statistics appears.
Edge Port	The edge port field means the node mode is edge node or assistant edge node. "-" appears when the port is not configured on the ring, and in this case, no corresponding statistics appears.
Packet Direct	Packet transmission direction on the port: Send or Rcv
Hello	Hello packet statistics received/sent on the port
Link-Down	Link-Down packet statistics received/sent on the port
Common Flush FDB	Common-Flush-FDB packet statistics received/sent on the port

Field	Description
Complete Flush FDB	Complete-Flush-FDB packet statistics received/sent on the port
Edge Hello	Edge-Hello packet statistics received/sent on the port
Major Fault	Major-Fault packet statistics received/sent on the port
Packet Total	Total number of packets received/sent on the port. Here only Hello, Link-Down, Common-Flush-FDB, Complete-Flush-FDB, Edge-Hello, and Major-Fault packets of RRPP are counted.

## display rrpp verbose

### Syntax

```
display rrpp verbose domain domain-id [ ring ring-id ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*domain-id*: RRPP domain ID, in the range 1 to 8.

*ring-id*: RRPP ring ID, in the range 1 to 64.

### Description

Use the **display rrpp verbose** command to display detailed information about RRPP configuration.

If you have specified an RRPP ring ID in the command, the detailed information of the specified ring in the specified RRPP domain appears. Otherwise, the detailed information of all the rings in the specified RRPP domain appears.

### Examples

# Display the detailed information of ring 1 in RRPP domain 1.

```
<Sysname> display rrpp verbose domain 1 ring 1
Domain ID      : 1
Control VLAN   : Major 5    Sub 6
Protected VLAN: Reference Instance 0 to 2, 4
Hello Timer    : 1 sec  Fail Timer : 3 sec
Ring ID        : 1
Ring Level     : 1
Node Mode      : Master
Ring State     : Complete
Enable Status  : Yes    Active Status: Yes
Primary port   : GigabitEthernet1/0/1    Port status: UP
Secondary port : GigabitEthernet1/0/2    Port status: BLOCKED
```

# Display the detailed information of all the rings in RRPP domain 2.

```
<Sysname> display rrpp verbose domain 2
```

```

Domain ID      : 2
Control VLAN   : Major 10    Sub 11
Protected VLAN: Reference Instance 3, 5 to 7
Hello Timer    : 1 sec  Fail Timer : 3 sec

Ring ID       : 1
Ring Level    : 0
Node Mode     : Master
Ring State    : Complete
Enable Status : Yes    Active Status: Yes
Primary port  : GigabitEthernet1/0/4    Port status: UP
Secondary port: GigabitEthernet1/0/5    Port status: BLOCKED

Ring ID       : 2
Ring Level    : 1
Node Mode     : Edge
Ring State    : -
Enable Status : No    Active Status: No
Common port   : GigabitEthernet1/0/4    Port status: -
               GigabitEthernet1/0/5    Port status: -
Edge port     : GigabitEthernet1/0/3    Port status: -

```

**Table 1-4 display rrpp verbose command output description**

Field	Description
Domain ID	RRPP domain ID
Control VLAN	Control VLANs of the RRPP domain, including major control VLAN and sub control VLAN
Protected VLAN	List of VLANs protected by the RRPP domain. MSTIs are displayed here. To get the VLANs corresponding to these MSTIs, use the <b>display stp region-configuration</b> command.
Hello Timer	Hello Timer value configured in seconds
Fail Timer	Fail Timer value configured in seconds
Ring ID	RRPP ring ID
Ring Level	RRPP ring level, with 0 representing primary ring and 1 representing subring
Node Mode	Node mode: master node, transit node, edge node and assistant edge node
Ring State	RRPP ring state. This field makes sense only when the node mode field is master node. "Complete" appears when the ring is in health state; "Failed" appears when the ring is in disconnect state; and "-" appears in all the other cases.
Enable Status	RRPP ring enable status: Yes indicates enabled and No indicates disabled
Active Status	RRPP ring activation status: Yes indicates active and No indicates inactive The current ring is active only when the RRPP protocol and the RRPP ring are enabled simultaneously. Through this field, you can get to know the enable status of the RRPP protocol.

Field	Description
Primary Port	The primary port field means the node mode is master node or transit node. "-" appears when the port is not configured on the ring.
Secondary Port	The secondary port field means the node mode is master node or transit node. - appears when the port is not configured on the ring.
Common Port	The common port field means the node mode is edge node or assistant edge node. "-" appears when the port is not configured on the ring.
Edge Port	The edge port field means the node mode is edge node or assistant edge node. "-" appears when the port is not configured on the ring.
Port status	Port status includes down, up and blocked; "-" appears in one of the following cases: <ul style="list-style-type: none"> <li>the ring is inactive</li> <li>the port is not configured on the ring</li> </ul>

## domain ring

### Syntax

```
domain domain-id ring ring-id-list
undo domain domain-id [ring ring-id-list]
```

### View

Ring group view

### Default Level

2: System level

### Parameters

*domain-id*: RRPP domain ID, in the range of 1 to 8.

*ring-id-list*: RRPP subring ID list expressed in the format of *ring-id-list*={ *ring-id* [ **to** *ring-id* ] }&<1-10>, where the *ring-id* argument is an RRPP subring ID in the range of 1 to 64 and &<1-10> indicates that you can input up to ten RRPP ring ID ranges.

### Description

Use the **domain ring** command to configure subrings for a ring group.

Use the **undo domain ring** command to remove the specified subring(s) from a ring group. If no subring ID list is specified, all subrings in the ring group are removed in the specified domain.

Note that:

- To be compatible with old-version RRPP, which does not support protected VLAN configuration, an RRPP domain protects all VLANs on a device started with an old-version configuration file.
- You can configure ring groups only on edge nodes or assistant-edge nodes.
- A subring can be assigned to only one ring group.
- A device must be of the same type, an edge node or an assistant-edge node, in the subrings in a ring group.
- The subrings in a ring group must have the same link in the primary ring. Otherwise, the ring group cannot function properly.

- An edge node ring group and its corresponding assistant-edge node ring group must be the same in configurations and activation status.

Moreover, you must perform the following operations in an orderly fashion. Otherwise, the assistant-edge node may not be able to receive Edge-Hello packets, and thus erroneously consider the primary ring to be faulty.

- To assign an activated ring to a ring group, first assign the ring to the assistant-edge node ring group and then to the edge node ring group.
- To remove an activated ring from a ring group, first remove the ring from the edge node ring group and then from the assistant-edge node ring group.
- To remove the whole ring group, do that on the edge node first and then on the assistant-edge node.
- When activating rings in a ring group, do that on the assistant-edge node first and then on the edge node.
- When deactivating rings in a ring group, do that on the edge node first and then on the assistant-edge node.

Related commands: **rrpp ring-group**, **display rrpp ring-group**.

## Examples

```
# Configure subrings for ring group 1.
<Sysname> system-view
[Sysname] rrpp ring-group 1
[Sysname-rrpp-ring-group1] domain 1 ring 1 to 3 5
[Sysname-rrpp-ring-group1] domain 2 ring 1 to 3 5
```

## protected-vlan

### Syntax

```
protected-vlan reference-instance instance-id-list
undo protected-vlan [ reference-instance instance-id-list ]
```

### View

```
RRPP domain view
```

### Default Level

```
2: System level
```

### Parameters

**reference-instance** *instance-id-list*: Specifies the MSTIs to be referenced. The range of the *instance-id-list* argument is as specified in the command configuring MSTIs.

### Description

Use the **protected-vlan** command to configure the protected VLANs for the RRPP domain. The protected VLANs are specified by the MSTIs. You can use the **display stp region-configuration** command to check the VLANs corresponding to the specified MSTIs.

Use the **undo protected-vlan** command to remove the protected VLANs of the RRPP domain. If no MSTI is specified, all protected VLANs of the RRPP domain are removed.

By default, no protected VLAN is specified for an RRPP domain.

Note that:

- Before configuring rings for an RRPP domain, you must configure protected VLANs for the domain first.
- Before configuring rings for an RRPP domain, you can delete or modify the protected VLANs configured for the RRPP domain; after configuring rings for an RRPP domain, you can delete or modify the protected VLANs configured for the RRPP domain, however, you cannot delete all the protected VLANs configured for the domain.
- Deleting an RRPP domain deletes its protected VLANs at the same time.
- When the VLAN-to-MSTI mappings change, the protected VLANs of an RRPP domain also changes according to the MSTIs configured for the domain.
- All the VLANs permitted to pass through RRPP ports must be configured as protected VLANs of the RRPP domain.

Related commands: **rrpp domain**, **control-vlan**, **display stp region-configuration** in *MSTP Configuration Commands* in the *Access Volume*.

## Examples

# Configure VLANs mapped to MSTI 2 and MSTI 3 as the protected VLANs of RRPP domain 1.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protected-vlan reference-instance 2 to 3
```

## reset rrpp statistics

### Syntax

```
reset rrpp statistics domain domain-id [ ring ring-id ]
```

### View

User view

### Default Level

1: Monitor level

### Parameters

*domain-id*: RRPP domain ID, in the range 1 to 8.

*ring-id*: RRPP ring ID, in the range 1 to 64.

### Description

Use the **reset rrpp statistics** command to clear RRPP message statistics.

If you have specified an RRPP ring ID in the command, RRPP message statistics of the specified RRPP ring in the specified RRPP domain on the current device is cleared. Otherwise, RRPP message statistics of all RRPP rings in the specified RRPP domain is cleared.

Related commands: **display rrpp statistics**.

## Examples

```
# Clear the RRPP message statistics of ring 10 in RRPP domain 10.
```

```
<Sysname> reset rrpp statistics domain 1 ring 10
```

## ring

### Syntax

```
ring ring-id node-mode { { master | transit } [ primary-port interface-type interface-number ]  
[ secondary-port interface-type interface-number ] level level-value | { edge | assistant-edge }  
[ edge-port interface-type interface-number ] }  
undo ring ring-id
```

### View

RRPP domain view

### Default Level

2: System level

### Parameters

*ring-id*: RRPP ring ID, in the range 1 to 64.

**master**: Specifies the device as the master node of the RRPP ring.

**transit**: Specifies the device as the transit node of the RRPP ring.

**primary-port**: Specifies the port as a primary port.

**secondary-port**: Specifies the port as a secondary port.

*interface-type interface-number*: Port type and port number.

*level-value*: RRPP ring level, with 0 representing primary ring and 1 representing subring.

**edge**: Specifies the device as the edge node of the RRPP ring.

**assistant-edge**: Specifies the device as the assistant edge node of the RRPP ring.

**edge-port**: Specifies the port as an edge port.

### Description

Use the **ring** command to configure the node mode of the device and the role of the port accessing the RRPP ring.

Use the **undo ring** command to remove the configuration.

Ports connected to an RRPP ring must meet the following conditions:

- The link type of these ports must be trunk.
- They must be Layer 2 GE ports.
- They must not be member ports of any aggregation group, service loopback group, or smart link group.
- STP is disabled on them.
- The 802.1p priority of trusted packets on the ports is configured, so that RRPP packets take higher precedence than data packets when passing through the ports.
- Do not enable OAM remote loopback function on an RRPP port. Otherwise, this may cause temporary broadcast storm.

- You are recommended not to configure physical-link-state change suppression time on a port accessing an RRPP ring to accelerate topology convergence. For details, refer to *Ethernet Interface Configuration* in the *Access Volume*.

Note that:

- RRPP ports cannot be configured if the RRPP ring is enabled.
- Make sure the control VLAN exists before configuring the RRPP ring.
- Before configuring rings for an RRPP domain, configure the protected VLANs for the RRPP domain first.
- You must first configure the primary ring and then the subring when configuring an RRPP domain. A ring ID cannot be applied to more than one RRPP ring in the same RRPP domain.
- If a device resides on multiple RRPP rings in an RRPP domain, only one primary ring exists within these rings. The device plays a role of either edge node or assistant edge node on other subrings.
- Modifying the node mode, port mode and ring level of an RRPP ring is prohibited after configuration. If needed, you must first delete the existing configuration.
- You must configure the primary ring and then subrings when you configure the edge node and the assistant edge node.
- Moreover, you must remove all subring configurations before deleting the primary ring configuration of the edge node and the assistant edge node. However, the enabled RRPP ring cannot be deleted.



#### Note

For a device, the total number of rings configurable in all RRPP domains cannot be greater than 16.

---

Related command: **control-vlan**, **protected-vlan**, and **ring enable**.

### Examples

# Specify the device as the master node of primary ring 10 in RRPP domain 1, GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protect-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 10 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

# Specify the device as the transit node of primary ring 10 in RRPP domain 1, GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protect-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 10 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

# Specify the device as the master node of subring 20 in RRPP domain 1, GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protect-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 20 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
```

# Specify the device as the transit node of primary ring 20 in RRPP domain 1, GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protect-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 20 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
```

# Specify the device as the edge node of primary ring 20 in RRPP domain 1, and GigabitEthernet 1/0/1 as the edge port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protect-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 20 node-mode edge edge-port gigabitethernet 1/0/1
```

# Specify the device as the assistant edge node of primary ring 20 in RRPP domain 1, and GigabitEthernet 1/0/1 as the edge port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protect-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 20 node-mode assistant-edge edge-port gigabitethernet 1/0/1
```

## ring enable

### Syntax

**ring** *ring-id* enable

**undo ring** *ring-id* enable

### View

RRPP domain view

### Default Level

2: System level

### Parameters

*ring-id*: RRPP ring ID, in the range 1 to 64.

## Description

Use the **ring enable** command to enable the RRPP ring.

Use the **undo ring enable** command to disable the RRPP ring.

By default, the RRPP ring is disabled.

Note that:

- To enable subrings, you must first enable the primary ring before enabling subrings.
- You must first disable all the subrings in the RRPP domain and then disable the primary ring.
- To activate the RRPP domain, RRPP protocol and the RRPP ring must be enabled simultaneously.

Related commands: **rrpp enable**.

## Examples

# Enable RRPP ring 10 in RRPP domain 1.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protect-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 10 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[Sysname-rrpp-domain1] ring 10 enable
```

## rrpp domain

### Syntax

**rrpp domain** *domain-id*

**undo rrpp domain** *domain-id*

### View

System view

### Default Level

2: System level

### Parameters

*domain-id*: RRPP domain ID, in the range 1 to 8.

## Description

Use the **rrpp domain** command to create an RRPP domain and enter its view.

Use the **undo rrpp domain** command to remove an RRPP domain.

Note that:

- When you delete an RRPP domain, the control VLAN of it will be deleted at the same time.
- When you delete an RRPP domain, you must ensure it has no RRPP ring.

Related commands: **control-vlan**, **ring**, **ring enable**, **rrpp enable**, **timer**.

## Examples

```
# Create RRPP domain 1.
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1]
```

## rrpp enable

### Syntax

```
rrpp enable
undo rrpp enable
```

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **rrpp enable** command to enable RRPP protocol.

Use the **undo rrpp enable** command to disable RRPP protocol.

By default, RRPP protocol is disabled.

To activate the RRPP domain, RRPP protocol and the RRPP ring must be enabled simultaneously.

Related commands: **ring enable**.

## Examples

```
# Enable RRPP protocol.
<Sysname> system-view
[Sysname] rrpp enable
```

## rrpp ring-group

### Syntax

```
rrpp ring-group ring-group-id
undo rrpp ring-group ring-group-id
```

### View

System view

### Default Level

2: System level

## Parameters

*ring-group-id*: Ring group ID, in the range 1 to 8.

## Description

Use the **rrpp ring-group** command to create an RRPP ring group and enter ring group view.

Use the **undo rrpp ring-group** command to delete an RRPP ring group. After removing a ring group, all subrings in the ring group do not belong to any ring group.

Note that:

- RRPP configured with ring groups cannot interoperate with RRPP that does not support ring group configuration.
- The subrings assigned to the same ring group must have the same edge node. Similarly, they must have the same assistant-edge node. Additionally, these subrings must have the same link in the primary ring.
- As an edge node ring group and an assistant-edge node group are configured on different devices. If the two groups are configured with different subrings, the ring group function fails.
- To remove a ring group, remove the edge node ring group, and then the corresponding assistant-edge node ring group.

Related commands: **domain ring**, **display rrpp ring-group**.

## Examples

```
# Create ring group 1 and enter its view.
```

```
<Sysname> system-view
[Sysname] rrpp ring-group 1
[Sysname-rrpp-ring-group1]
```

## timer

### Syntax

```
timer hello-timer hello-value fail-timer fail-value
undo timer
```

### View

RRPP domain view

### Default Level

2: System level

## Parameters

*hello-value*: Hello timer value, in the range 1 to 10 seconds.

*fail-value*: Fail timer value, in the range 3 to 30 seconds.

## Description

Use the **timer** command to specify the value of the timers of the RRPP domain.

Use the **undo timer** command to restore it to the default value.

By default, the Hello timer value is 1 second and the Fail timer value is 3 seconds.

Note that the Fail timer value must be greater than or equal to three times of the Hello timer value.

### Examples

# Set the Hello timer value to 2 seconds and the Fail timer value to 7 seconds.

```
<Sysname> system-view
```

```
[Sysname] rrpp domain 1
```

```
[Sysname-rrpp-domain1] timer hello-timer 2 fail-timer 7
```

# Table of Contents

<b>1 Port Mirroring Configuration Commands .....</b>	<b>1-1</b>
Port Mirroring Configuration Commands .....	1-1
display mirroring-group.....	1-1
mirroring-group .....	1-2
mirroring-group mirroring-port .....	1-3
mirroring-group monitor-egress.....	1-4
mirroring-group monitor-port .....	1-5
mirroring-group remote-probe vlan.....	1-6
mirroring-port .....	1-7
monitor-port .....	1-8

# 1 Port Mirroring Configuration Commands

---

## Port Mirroring Configuration Commands

### display mirroring-group

#### Syntax

```
display mirroring-group { groupid | all | local | remote-destination | remote-source }
```

#### View

Any view

#### Default Level

2: System level

#### Parameters

*groupid*: Number of the port mirroring group to be displayed, in the range of 1 to 4.

**all**: Displays all port mirroring groups.

**local**: Displays local mirroring groups.

**remote-destination**: Displays remote destination mirroring groups.

**remote-source**: Displays remote source port mirroring groups.

#### Description

Use the **display mirroring-group** command to display information about the specified port mirroring group or groups.

The output varies by port mirroring group type and is sorted by mirroring group number.

#### Examples

# Display information about all the port mirroring groups.

```
<Sysname> display mirroring-group all
mirroring-group 1:
  type: local
  status: active
  mirroring port:
    GigabitEthernet1/0/1  both
  monitor port: GigabitEthernet1/0/10
mirroring-group 2:
  type: remote-source
  status: active
  mirroring port:
    GigabitEthernet1/0/3  both
```

```
monitor egress port: GigabitEthernet1/0/11
remote-probe vlan: 200
```

**Table 1-1** Description on the fields of the **display mirroring-group** command

Field	Description
mirroring-group	Number of the port mirroring group
type	Type of the port mirroring group, which can be one of the following: local, remote-source, or remote-destination.
status	Status of the port mirroring group, which can be active or inactive.
mirroring port	Source mirroring port
monitor port	Destination mirroring port
monitor egress port	Outbound mirroring port
remote-probe vlan	Remote mirroring VLAN

## mirroring-group

### Syntax

```
mirroring-group groupid { local | remote-destination | remote-source }
undo mirroring-group { groupid | all | local | remote-destination | remote-source }
```

### View

System view

### Default Level

2: System level

### Parameters

*groupid*: Specifies the number of the port mirroring group to be created or removed, in the range of 1 to 4.

**all**: Removes all port mirroring groups.

**local**: Creates a local mirroring group or removes all local mirroring groups with the **undo** command.

**remote-destination**: Creates a remote destination mirroring group or removes all remote destination mirroring groups with the **undo** command.

**remote-source**: Creates a remote source mirroring group or removes all remote source mirroring groups with the **undo** command.

### Description

Use the **mirroring-group** command to create a port mirroring group.

Use the **undo mirroring-group** command to remove the specified port mirroring group or groups.

To mirror packets from a port to another port on the same device, create a local mirroring group.

To mirror packets from a port (a mirroring port) on the current device to another port (the monitor port) either on the same device or on a different device, create remote mirroring groups. When doing that,

create the remote source mirroring group on the device where the mirroring port is located and create the remote destination mirroring group on the device where the monitor port is located.

## Examples

# Create a local port mirroring group numbered 1.

```
<Sysname> system-view  
[Sysname] mirroring-group 1 local
```

# Create remote destination mirroring group numbered 2.

```
<Sysname> system-view  
[Sysname] mirroring-group 2 remote-destination
```

## mirroring-group mirroring-port

### Syntax

**mirroring-group** *groupid* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }

**undo mirroring-group** *groupid* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }

### View

System view

### Default Level

2: System level

### Parameters

*groupid*: Number of a local or remote source mirroring group, in the range of 1 to 4.

*mirroring-port-list*: A list of ports/port ranges to be assigned to or removed from the port mirroring group specified by *groupid*. The total number of single ports plus port ranges cannot exceed eight. In the list, a single port takes the form of *interface-type interface-number*. A port range takes the form *interface-type start-interface-number to interface-type end-interface-number*, where the end port number must be greater than the start port number.

**both**: Mirrors both inbound and outbound packets on the specified port(s).

**inbound**: Mirrors only inbound packets on the specified port(s).

**outbound**: Mirrors only outbound packets on the specified port(s).

### Description

Use the **mirroring-group mirroring-port** command to assign ports to a local or remote source mirroring group as mirroring ports.

Use the **undo mirroring-group mirroring-port** command to remove mirroring ports from the mirroring group.

By configuring a port as a mirroring port, you can track the packets received from or/and sent out the port.

Before you can assign a port to a mirroring group, create the mirroring group first.

Note that:

- A mirroring port cannot be a member port of an existing port mirroring group.

- You cannot add a mirroring port for a remote destination mirroring group.
- When removing a mirroring port from a mirroring group, make sure the traffic direction you specified in the **undo mirroring-group mirroring-port** command matches the actual monitored direction of the port.

## Examples

# Configure mirroring ports in port mirroring group 1, assuming that the mirroring group already exists.

```
<Sysname> system-view
[Sysname] mirroring-group 1 mirroring-port GigabitEthernet 1/0/1 to GigabitEthernet 1/0/5
both
```

# Remove source mirroring ports from port mirroring group 1.

```
[Sysname] undo mirroring-group 1 mirroring-port GigabitEthernet 1/0/1 to GigabitEthernet
1/0/3 both
```

## mirroring-group monitor-egress

### Syntax

In system view:

**mirroring-group** *groupid* **monitor-egress** *monitor-egress-port-id*

**undo mirroring-group** *groupid* **monitor-egress** *monitor-egress-port-id*

In Ethernet port view:

**mirroring-group** *groupid* **monitor-egress**

**undo mirroring-group** *groupid* **monitor-egress**

### View

System view, Ethernet port view

### Default Level

2: System level

### Parameters

*groupid*: Number of a remote source mirroring group, in the range of 1 to 4.

*monitor-egress-port-id*: Port to be configured as the egress port. It takes the form of *interface-type interface-number*, where *interface-type* specifies the port type and *interface-number* specifies the port number.

### Description

Use the **mirroring-group monitor-egress** command to configure a port as the egress port in a remote source mirroring group.

Use the **undo mirroring-group monitor-egress** command to remove the egress port from the mirroring group.

Note that:

- Only remote source port mirroring groups can have outbound mirroring ports. A port mirroring group can have only one outbound mirroring port.

- The outbound port cannot be a member port of the current mirroring group.
- It is not recommended to configure STP, RSTP, MSTP, 802.1x, IGMP Snooping, static ARP and MAC address learning on the outbound mirroring port; otherwise, the mirroring function may be affected.

## Examples

# Configure port GigabitEthernet 1/0/1 as the egress port of remote source mirroring group 1 in system view.

```
<Sysname> system-view
[Sysname] mirroring-group 1 remote-source
[Sysname] mirroring-group 1 monitor-egress GigabitEthernet 1/0/1
```

# Configure port GigabitEthernet 1/0/2 as the egress port of remote source mirroring group 2 in Ethernet port view.

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-source
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] mirroring-group 2 monitor-egress
```

## mirroring-group monitor-port

### Syntax

```
mirroring-group groupid monitor-port monitor-port-id
undo mirroring-group groupid monitor-port monitor-port-id
```

### View

System view

### Default Level

2: System level

### Parameters

*groupid*: Number of a local or remote destination mirroring group, in the range of 1 to 4.

*monitor-port-id*: Port to be assigned to the specified mirroring group as the monitor port. The argument takes the form of *interface-type interface-number*, where *interface-type* specifies the port type and *interface-number* specifies the port number.

### Description

Use the **mirroring-group monitor-port** command to assign a port to a local or remote destination mirroring group as the monitor port.

Use the **undo mirroring-group monitor-port** command to remove the monitor port from the local or remote destination mirroring group.

Note that:

- Before assigning a port to a mirroring group, make sure that the group already exists.
- A port mirroring group can contain only one destination port.
- The destination port cannot be a member port of the current mirroring group.

- The destination mirroring port can be an access, trunk, or hybrid port. It must be assigned to the remote mirroring VLAN.
- A remote source port mirroring group cannot contain destination ports.
- Before configuring the destination port for a port mirroring group, make sure the port mirroring group exists.
- Do not enable STP, RSTP, or MSTP on the destination port. Otherwise, the mirroring function may be affected.
- Do not use the destination mirroring port for any purpose other than port mirroring.

## Examples

# Configure GigabitEthernet 1/0/1 as the monitor port in remote destination mirroring group 1.

```
<Sysname> system-view
[Sysname] mirroring-group 1 remote-destination
[Sysname] mirroring-group 1 monitor-port GigabitEthernet 1/0/1
```

## mirroring-group remote-probe vlan

### Syntax

```
mirroring-group groupid remote-probe vlan rprobe-vlan-id
undo mirroring-group groupid remote-probe vlan rprobe-vlan-id
```

### View

System view

### Default Level

2: System level

### Parameters

*groupid*: Number of a remote source or destination mirroring group, in the range of 1 to 4.

*rprobe-vlan-id*: ID of the VLAN to be configured as the remote probe VLAN. This VLAN must be a static VLAN that already exists.

### Description

Use the **mirroring-group remote-probe vlan** command to specify a VLAN as the remote probe VLAN for a remote source or destination mirroring group.

Use the **undo mirroring-group remote-probe vlan** command to remove the remote probe VLAN from the remote source or destination mirroring group.

Note that:

- Only remote source port mirroring groups or remote destination port mirroring groups can have remote mirroring VLANs. A port mirroring group can have only one remote mirroring VLAN.
- To remove a VLAN operating as a remote port mirroring VLAN, you need to restore it to a normal VLAN first. A remote port mirroring group gets invalid if the corresponding remote port mirroring VLAN is removed.
- You are recommended to use a remote mirroring VLAN for remote mirroring only.

## Examples

# Specify VLAN 2 as the remote probe VLAN of port mirroring group 1, assuming that VLAN 2 already exists.

```
<Sysname> system-view
[Sysname] mirroring-group 1 remote-source
[Sysname] mirroring-group 1 remote-probe vlan 2
```

## mirroring-port

### Syntax

```
[ mirroring-group groupid ] mirroring-port { inbound | outbound | both }
undo [ mirroring-group groupid ] mirroring-port { inbound | outbound | both }
```

### View

Ethernet port view

### Default Level

2: System level

### Parameters

*groupid*: Number of a local or remote source mirroring group, in the range of 1 to 4.

**both**: Mirrors both inbound and outbound packets on the current port.

**inbound**: Mirrors only inbound packets on the current port.

**outbound**: Mirrors only outbound packets on the current port.

### Description

Use the **mirroring-port** command to assign the current port to a local or remote source mirroring group as a mirroring port.

Use the **undo mirroring-port** command to remove the current port from the port mirroring group.

When assigning a port to a mirroring group as a mirroring port, note that:

- If no mirroring group is specified, the port is assigned to port mirroring group 1.
- Whether you assign the port to port mirroring group 1 or any other mirroring group, ensure that the mirroring group already exists.
- A mirroring port cannot be a member port of an existing port mirroring group.
- You cannot add a mirroring port for a remote destination mirroring group.
- When removing a mirroring port from a mirroring group, make sure the traffic direction you specified in the **undo [ mirroring-group *groupid* ] mirroring-port** command matches the actual monitored direction of the port.

## Examples

# Configure GigabitEthernet 1/0/1 as a source mirroring port of remote source port mirroring group 2.

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-source
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mirroring-group 2 mirroring-port both
```

## monitor-port

### Syntax

```
[ mirroring-group groupid ] monitor-port  
undo [ mirroring-group groupid ] monitor-port
```

### View

Ethernet port view

### Default Level

2: System level

### Parameters

*groupid*: Number of a local or remote destination mirroring group, in the range of 1 to 4.

### Description

Use the **monitor-port** command to assign the current port to a local or remote destination mirroring group as the monitor port.

Use the **undo monitor-port** command to remove the current port from the mirroring group.

When assigning a port to a mirroring group as the monitor port, note that:

- If no mirroring group is specified, the port is assigned to port mirroring group 1.
- The port cannot belong to any other mirroring group.
- Whether you assign the port to port mirroring group 1 or any other mirroring group, ensure that the mirroring group already exists.
- The remote destination mirroring port can be an access, trunk, or hybrid port. It must be assigned to the remote mirroring VLAN.
- Do not enable STP, RSTP, or MSTP on the destination port. Otherwise, the mirroring function may be affected.
- Do not use the destination mirroring port for any purpose other than port mirroring.

### Examples

# Configure GigabitEthernet 1/0/1 as the monitor port in local mirroring group numbered 1.

```
<Sysname> system-view  
[Sysname] mirroring-group 1 local  
[Sysname] interface GigabitEthernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] monitor-port
```

# IP Services Volume Organization

---

## Manual Version

6W100-20090120

## Product Version

Release 2202

## Organization

The IP Services Volume is organized as follows:

Features	Description
IP Address	An IP address is a 32-bit address allocated to a network interface on a device that is attached to the Internet. This document introduces the commands for IP address configuration
ARP	Address Resolution Protocol (ARP) is used to resolve an IP address into a data link layer address. This document introduces the commands for: <ul style="list-style-type: none"><li>• Configuring ARP</li><li>• Configuring Gratuitous ARP</li><li>• Proxy ARP and Local Proxy ARP configuration</li><li>• ARP Attack Defense configuration</li></ul>
DHCP	DHCP is built on a client-server model, in which the client sends a configuration request and then the server returns a reply to send configuration parameters such as an IP address to the client. This document introduces the commands for: <ul style="list-style-type: none"><li>• DHCP server configuration</li><li>• DHCP relay agent configuration</li><li>• DHCP Client configuration</li><li>• DHCP Snooping configuration</li><li>• BOOTP Client configuration</li></ul>
DNS	Used in the TCP/IP application, Domain Name System (DNS) is a distributed database which provides the translation between domain name and the IP address. This document introduces the commands for: <ul style="list-style-type: none"><li>• Configuring the DNS Client</li><li>• Configuring the DNS Proxy</li></ul>
IP Performance	In some network environments, you need to adjust the IP parameters to achieve best network performance. This document introduces the commands for: <ul style="list-style-type: none"><li>• Enabling Reception and Forwarding of Directed Broadcasts to a Directly Connected Network</li><li>• Configuring TCP Attributes</li><li>• Configuring ICMP to Send Error Packets</li></ul>

Features	Description
UDP Helper	UDP Helper functions as a relay agent that converts UDP broadcast packets into unicast packets and forwards them to a specified server. This document introduces the commands for UDP Helper configuration
URPF	Unicast Reverse Path Forwarding (URPF) protects a network against source address spoofing attacks. This document introduces the commands for URPF configuration
IPv6 Basics	<p>Internet protocol version 6 (IPv6), also called IP next generation (IPng), was designed by the Internet Engineering Task Force (IETF) as the successor to Internet protocol version 4 (IPv4). This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• IPv6 overview</li> <li>• Basic IPv6 functions configuration</li> <li>• IPv6 NDP configuration</li> <li>• PMTU discovery configuration</li> <li>• IPv6 TCP properties configuration</li> <li>• ICMPv6 packet sending configuration</li> <li>• IPv6 DNS Client configuration</li> </ul>
Tunneling	<p>Tunneling is an encapsulation technique, which utilizes one network transport protocol to encapsulate packets of another network transport protocol and transfer them over the network. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• IPv6 manually tunnel configuration</li> <li>• 6to4 tunnel configuration</li> <li>• ISATAP tunnel configuration</li> </ul>
sFlow	Based on packet sampling, Sampled Flow (sFlow) is a traffic monitoring technology mainly used to collect and analyze traffic statistics. This document introduces the commands for sFlow Configuration

# Table of Contents

<b>1 IP Addressing Configuration Commands .....</b>	<b>1-1</b>
IP Addressing Configuration Commands.....	1-1
display ip interface.....	1-1
display ip interface brief.....	1-3
ip address .....	1-4

# 1 IP Addressing Configuration Commands

---

## IP Addressing Configuration Commands

### display ip interface

#### Syntax

```
display ip interface [ interface-type interface-number ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

*interface-type interface-number*: Specifies an interface by its type and number.

#### Description

Use the **display ip interface** command to display information about a specified or all Layer 3 interfaces.

#### Examples

# Display information about interface VLAN-interface 1.

```
<Sysname> display ip interface vlan-interface 1
Vlan-interfacel current state : DOWN
Line protocol current state : DOWN
Internet Address is 1.1.1.1/8 Primary
Broadcast address : 1.255.255.255
The Maximum Transmit Unit : 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 0
ARP packet input number:           0
  Request packet:                   0
  Reply packet:                     0
  Unknown packet:                   0
TTL invalid packet number:         0
ICMP packet input number:          0
  Echo reply:                       0
  Unreachable:                      0
  Source quench:                    0
  Routing redirect:                 0
  Echo request:                     0
```

```

Router advert:          0
Router solicit:        0
Time exceed:           0
IP header bad:         0
Timestamp request:     0
Timestamp reply:       0
Information request:   0
Information reply:     0
Netmask request:       0
Netmask reply:         0
Unknown type:          0

```

**Table 1-1 display ip interface command output description**

Field	Description
current state	<p>Current physical state of the interface, which can be</p> <ul style="list-style-type: none"> <li>• Administrative DOWN: Indicates that the interface is administratively down; that is, the interface is shut down with the <b>shutdown</b> command.</li> <li>• DOWN: Indicates that the interface is administratively up but its physical state is down, which may be caused by a connection or link failure.</li> <li>• UP: Indicates that both the administrative and physical states of the interface are up.</li> </ul>
Line protocol current state	<p>Current state of the link layer protocol, which can be</p> <ul style="list-style-type: none"> <li>• DOWN: Indicates that the protocol state of the interface is down, which is usually because that no IP address is assigned to the interface.</li> <li>• UP: Indicates that the protocol state of the interface is up.</li> </ul>
Internet Address	<p>IP address of an interface followed by:</p> <ul style="list-style-type: none"> <li>• Primary: Identifies a primary IP address, or</li> <li>• Sub: Identifies a secondary IP address.</li> </ul>
Broadcast address	Broadcast address of the subnet attached to an interface
The Maximum Transmit Unit	Maximum transmission units on the interface, in bytes
input packets, bytes, multicasts output packets, bytes, multicasts	Unicast packets, bytes, and multicast packets received on an interface (the statistics start at the device startup)
ARP packet input number: Request packet: Reply packet: Unknown packet:	<p>Total number of ARP packets received on the interface (the statistics start at the device startup), including</p> <ul style="list-style-type: none"> <li>• ARP request packets</li> <li>• ARP reply packets</li> <li>• Unknown packets</li> </ul>
TTL invalid packet number	Number of TTL-invalid packets received on the interface (the statistics start at the device startup)

Field	Description
ICMP packet input number:	Total number of ICMP packets received on the interface (the statistics start at the device startup), including the following packets: <ul style="list-style-type: none"> <li>• Echo reply packet</li> <li>• Unreachable packets</li> <li>• Source quench packets</li> <li>• Routing redirect packets</li> <li>• Echo request packets</li> <li>• Router advertisement packets</li> <li>• Router solicitation packets</li> <li>• Time exceeded packets</li> <li>• IP header bad packets</li> <li>• Timestamp request packets</li> <li>• Timestamp reply packets</li> <li>• Information request packets</li> <li>• Information reply packets</li> <li>• Netmask request packets</li> <li>• Netmask reply packets</li> <li>• Unknown type packets</li> </ul>
Echo reply:	
Unreachable:	
Source quench:	
Routing redirect:	
Echo request:	
Router advert:	
Router solicit:	
Time exceed:	
IP header bad:	
Timestamp request:	
Timestamp reply:	
Information request:	
Information reply:	
Netmask request:	
Netmask reply:	
Unknown type:	

## display ip interface brief

### Syntax

```
display ip interface brief [ interface-type [ interface-number ] ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*interface-type*: Interface type.

*interface-number*: Interface number.

### Description

Use the **display ip interface brief** command to display brief information about a specified or all layer 3 interfaces.

Without the interface type and interface number specified, the information about all layer 3 interfaces is displayed; with only the interface type specified, the information about all layer 3 interfaces of the specified type is displayed; with both the interface type and interface number specified, only the information about the specified interface is displayed.

Related commands: **display ip interface**.

### Examples

```
# Display brief information about VLAN interfaces.
```

```

<Sysname> display ip interface brief vlan-interface
*down: administratively down
(s): spoofing
Interface                Physical Protocol IP Address      Description
Vlan-interface1         up        up        6.6.6.6        Vlan-inte...
Vlan-interface2         up        up        7.7.7.7        VLAN2

```

**Table 1-2 display ip interface brief command output description**

Field	Description
*down: administratively down	The interface is administratively shut down with the <b>shutdown</b> command.
(s) : spoofing	Spoofing attribute of the interface. It indicates that an interface whose network layer protocol is displayed up may have no link present or the link is set up only on demand.
Interface	Interface name
Physical	Physical state of the interface, which can be <ul style="list-style-type: none"> <li>• *down: Indicates that the interface is administratively down; that is, the interface is shut down with the <b>shutdown</b> command.</li> <li>• down: Indicates that the interface is administratively up but its physical state is down, which may be caused by a connection or link failure.</li> <li>• up: Indicates that both the administrative and physical states of the interface are up.</li> </ul>
Protocol	Link layer protocol state of the interface, which can be <ul style="list-style-type: none"> <li>• down: Indicates that the protocol state of the interface is down, which is usually because that no IP address is assigned to the interface.</li> <li>• up: Indicates that the protocol state of the interface is up.</li> </ul>
IP Address	IP address of the interface (If no IP address is configured, "unassigned" is displayed.)
Description	Interface description information, for which at most 12 characters can be displayed. If there are more than 12 characters, only the first nine characters are displayed.

## ip address

### Syntax

```

ip address ip-address { mask | mask-length } [ sub ]
undo ip address [ ip-address { mask | mask-length } [ sub ] ]

```

### View

Interface view

### Default Level

2: System level

## Parameters

*ip-address*: IP address of interface, in dotted decimal notation.

*mask*: Subnet mask in dotted decimal notation.

*mask-length*: Subnet mask length, the number of consecutive ones in the mask.

**sub**: Secondary IP address for the interface. Currently, up to nine secondary IP addresses are supported on an interface.

## Description

Use the **ip address** command to assign an IP address and mask to the interface.

Use the **undo ip address** command to remove all IP addresses from the interface.

Use the **undo ip address** *ip-address* { *mask* | *mask-length* } command to remove the primary IP address.

Use the **undo ip address** *ip-address* { *mask* | *mask-length* } **sub** command to remove a secondary IP address.

By default, no IP address is assigned to any interface.

When assigning IP addresses to an interface, consider the following:

- You can assign only one primary IP address to an interface.
- The primary and secondary IP addresses can be located in the same network segment.
- Before removing the primary IP address, remove all secondary IP addresses.
- You cannot assign a secondary IP address to the interface that is configured to borrow an IP address through IP unnumbered or obtain one through BOOTP, or DHCP.

Related commands: **display ip interface**.

## Examples

# Assign VLAN-interface 1 a primary IP address 129.12.0.1 and a secondary IP address 202.38.160.1, with subnet masks being 255.255.255.0.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip address 129.12.0.1 255.255.255.0
[Sysname-Vlan-interface1] ip address 202.38.160.1 255.255.255.0 sub
```

# Table of Contents

<b>1 ARP Configuration Commands</b>	<b>1-1</b>
ARP Configuration Commands	1-1
arp check enable	1-1
arp max-learning-num	1-1
arp static	1-2
arp timer aging	1-3
display arp	1-4
display arp <i>ip-address</i>	1-5
display arp timer aging	1-6
display arp vpn-instance	1-6
reset arp	1-7
Gratuitous ARP Configuration Commands	1-8
gratuitous-arp-sending enable	1-8
gratuitous-arp-learning enable	1-9
<b>2 Proxy ARP Configuration Commands</b>	<b>2-1</b>
Proxy ARP Configuration Commands	2-1
display local-proxy-arp	2-1
display proxy-arp	2-1
local-proxy-arp enable	2-2
proxy-arp enable	2-2
<b>3 ARP Attack Defense Configuration Commands</b>	<b>3-1</b>
ARP Source Suppression Configuration Commands	3-1
arp source-suppression enable	3-1
arp source-suppression limit	3-1
display arp source-suppression	3-2
ARP Defense Against IP Packet Attack Configuration Commands	3-3
arp resolving-route enable	3-3
ARP Active Acknowledgement Configuration Commands	3-3
arp anti-attack active-ack enable	3-3
Source MAC Address Based ARP Attack Detection Configuration Commands	3-4
arp anti-attack source-mac	3-4
arp anti-attack source-mac aging-time	3-5
arp anti-attack source-mac exclude-mac	3-6
arp anti-attack source-mac threshold	3-6
display arp anti-attack source-mac	3-7
ARP Packet Source MAC Address Consistency Check Configuration Commands	3-8
arp anti-attack valid-ack enable	3-8
ARP Packet Rate Limit Configuration Commands	3-8
arp rate-limit	3-8
ARP Detection Configuration Commands	3-9
arp detection enable	3-9
arp detection mode	3-10
arp detection static-bind	3-11

arp detection trust.....	3-11
arp detection validate .....	3-12
display arp detection.....	3-13
display arp detection statistics.....	3-13
reset arp detection statistics.....	3-14

# 1 ARP Configuration Commands

---

## ARP Configuration Commands

### arp check enable

#### Syntax

```
arp check enable
undo arp check enable
```

#### View

System view

#### Default Level

2: System level

#### Parameters

None

#### Description

Use the **arp check enable** command to enable ARP entry check. With this function enabled, the device cannot learn any ARP entry with a multicast MAC address. Configuring such a static ARP entry is not allowed either; otherwise, the system displays error messages.

Use the **undo arp check enable** command to disable the function. After the ARP entry check is disabled, the device can learn the ARP entry with a multicast MAC address, and you can also configure such a static ARP entry on the device.

By default, ARP entry check is enabled.

#### Examples

```
# Enable ARP entry check.
<Sysname> system-view
[Sysname] arp check enable
```

### arp max-learning-num

#### Syntax

```
arp max-learning-num number
undo arp max-learning-num
```

#### View

Ethernet interface view, VLAN interface view, Layer-2 aggregate interface view

## Default Level

2: System level

## Parameters

*number*: Maximum number of dynamic ARP entries that a interface can learn. The value is in the range 0 to 8192.

## Description

Use the **arp max-learning-num** command to configure the maximum number of dynamic ARP entries that a interface can learn.

Use the **undo arp max-learning-num** command to restore the default.

By default, the maximum number of dynamic ARP entries that a interface can learn is 8192.

## Examples

# Specify VLAN-interface 40 to learn up to 500 dynamic ARP entries.

```
<Sysname> system-view
[Sysname] interface vlan-interface 40
[Sysname-Vlan-interface40] arp max-learning-num 500
```

## arp static

### Syntax

**arp static** *ip-address mac-address* [ *vlan-id interface-type interface-number* ] [ **vpn-instance** *vpn-instance-name* ]

**undo arp** *ip-address* [ *vpn-instance-name* ]

### View

System view

## Default Level

2: System level

## Parameters

*ip-address*: IP address in an ARP entry.

*mac-address*: MAC address in an ARP entry, in the format H-H-H.

*vlan-id*: ID of a VLAN to which a static ARP entry belongs to, in the range 1 to 4094.

*interface-type interface-number*: Interface type and interface number.

**vpn-instance** *vpn-instance-name*: Name of a VPN instance, a case-sensitive string of 1 to 31 characters.

## Description

Use the **arp static** command to configure a static ARP entry in the ARP mapping table.

Use the **undo arp** command to remove an ARP entry.

Note that:

- A static ARP entry is effective when the device works normally. However, when the VLAN or VLAN interface to which an ARP entry corresponds is deleted, the entry, if permanent, will be deleted, and if non-permanent and resolved, will become unresolved.
- The `vlan-id` argument is used to specify the corresponding VLAN of an ARP entry and must be the ID of an existing VLAN. In addition, the Ethernet interface following the argument must belong to that VLAN. The VLAN interface of the VLAN must have been created.
- If no VPN instance is specified in the `undo arp` command, corresponding ARP entries of all VPN instances are removed.

Related commands: **reset arp**, **display arp**.

## Examples

```
# Configure a static ARP entry, with the IP address being 202.38.10.2, the MAC address being
000f-e201-0000, and the outbound interface being GigabitEthernet 1/0/1 of VLAN 10.
```

```
<Sysname> system-view
[Sysname] arp static 202.38.10.2 000f-e201-0000 10 gigabitethernet 1/0/1
```

## arp timer aging

### Syntax

```
arp timer aging aging-time
undo arp timer aging
```

### View

System view

### Default Level

2: System level

### Parameters

*aging-time*: Aging time for dynamic ARP entries in minutes, in the range 1 to 1,440.

### Description

Use the **arp timer aging** command to set aging time for dynamic ARP entries.

Use the **undo arp timer aging** command to restore the default.

By default, the aging time for dynamic ARP entries is 20 minutes.

Related commands: **display arp timer aging**.

## Examples

```
# Set aging time for dynamic ARP entries to 10 minutes.
```

```
<Sysname> system-view
[Sysname] arp timer aging 10
```

## display arp

### Syntax

```
display arp [ [ all | dynamic | static ] [ slot slot-number ] | vlan vlan-id | interface interface-type interface-number ] [ [ verbose ] [ { begin | exclude | include } regular-expression ] | count ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**all**: Displays all ARP entries.

**dynamic**: Displays dynamic ARP entries.

**static**: Displays static ARP entries.

**slot slot-number**: Displays the ARP entries of the specified device. If the device is in an IRF stack, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF stack, the *slot-number* argument represents the device ID.

**vlan vlan-id**: Displays the ARP entries of the specified VLAN. The VLAN ID ranges from 1 to 4,094.

**interface interface-type interface-number**: Displays the ARP entries of the interface specified by the argument *interface-type interface-number*.

**verbose**: Displays detailed information about ARP entries.

**|**: Uses a regular expression to specify the ARP entries to be displayed. For detailed information about regular expressions, refer to *Basic System Configuration* in the *System Volume*.

**begin**: Displays ARP entries from the first one containing the specified string.

**exclude**: Displays the ARP entries that do not contain the specified string.

**include**: Displays the ARP entries containing the specified string.

*regular-expression*: A case-sensitive string for matching, consisting of 1 to 256 characters.

**count**: Displays the number of ARP entries.

### Description

Use the **display arp** command to display ARP entries in the ARP mapping table.

If no parameter is specified, all ARP entries are displayed.

Related commands: **arp static**, **reset arp**.

### Examples

# Display the detailed information of all ARP entries.

```
<Sysname> display arp all verbose
```

```

                                     Type: S-Static   D-Dynamic
IP Address      MAC Address      VLAN ID  Interface      Aging Type
Vpn-instance Name
20.1.1.1        00e0-fc00-0001  N/A     N/A             N/A   S
test
```

```

193.1.1.70      00e0-fe50-6503  100      GE1/0/1      14      D
[No Vrf]
192.168.0.115  000d-88f7-9f7d  1        GE1/0/2      18      D
[No Vrf]
192.168.0.39   0012-a990-2241  1        GE1/0/3      20      D
[No Vrf]

```

**Table 1-1 display arp command output description**

Field	Description
IP Address	IP address in an ARP entry
MAC Address	MAC address in an ARP entry
VLAN ID	VLAN ID contained a static ARP entry
Interface	Outbound interface in an ARP entry
Aging	Aging time for a dynamic ARP entry in minutes ("N/A" means unknown aging time or no aging time)
Type	ARP entry type: D for dynamic, S for static
Vpn-instance Name	Name of VPN instance. [No Vrf] means no VPN instance is configured for the corresponding ARP.

# Display the number of all ARP entries.

```

<Sysname> display arp all count
Total Entry(ies): 4

```

## display arp ip-address

### Syntax

```

display arp ip-address [ slot slot-number ] [ verbose ] [ | { begin | exclude | include }
regular-expression ]

```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ip-address*: Displays the ARP entry for the specified IP address.

**slot slot-number**: Displays the ARP entry for the specified device. If the device is in an IRF stack, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF stack, the *slot-number* argument represents the device ID.

**verbose**: Displays the detailed information about ARP entries.

|: Uses a regular expression to specify the ARP entries to be displayed. For detailed information about regular expressions, refer to *Basic System Configuration* in the *System Volume*.

**begin**: Displays the ARP entries from the first one containing the specified string.

**exclude:** Displays the ARP entries that do not contain the specified string.

**include:** Displays the ARP entries that contain the specified string.

*regular-expression:* A case-sensitive string for matching, consisting of 1 to 256 characters.

## Description

Use the **display arp ip-address** command to display the ARP entry for a specified IP address.

Related commands: **arp static**, **reset arp**.

## Examples

# Display the corresponding ARP entry for the IP address 20.1.1.1.

```
<Sysname> display arp 20.1.1.1
                Type: S-Static    D-Dynamic
IP Address      MAC Address      VLAN ID  Interface      Aging Type
20.1.1.1        00e0-fc00-0001  N/A     N/A            N/A    S
```

## display arp timer aging

### Syntax

```
display arp timer aging
```

### View

Any view

### Default Level

2: System level

### Parameters

None

### Description

Use the **display arp timer aging** command to display the aging time for dynamic ARP entries.

Related commands: **arp timer aging**.

### Examples

# Display the aging time for dynamic ARP entries.

```
<Sysname> display arp timer aging
Current ARP aging time is 10 minute(s)
```

## display arp vpn-instance

### Syntax

```
display arp vpn-instance vpn-instance-name [ | { begin | exclude | include } regular-expression |
count ]
```

### View

Any view

## Default Level

1: Monitor level

## Parameters

*vpn-instance-name*: Name of VPN instance, a case-sensitive string of 1 to 31 characters excluding spaces. With this argument specified, the ARP entries for a specific VPN instance are displayed.

*|*: Uses a regular expression to specify the ARP entries to be displayed. For detailed information about regular expressions, refer to *Basic System Configuration* in the *System Volume*.

**begin**: Displays the ARP entries from the first one that contains the specified string.

**exclude**: Displays the ARP entries that do not contain the specified string.

**include**: Displays the ARP entries that contain the specified string.

*regular-expression*: A case-sensitive character string for matching, consisting of 1 to 256 characters.

**count**: Displays the number of ARP entries.

## Description

Use the **display arp vpn-instance** command to display the ARP entries for a specified VPN instance.

Related commands: **arp static**, **reset arp**.

## Examples

# Display ARP entries for the VPN instance named test.

```
<Sysname> display arp vpn-instance test
```

IP Address	Type: S-Static    D-Dynamic		Interface	Aging Type	
	MAC Address	VLAN ID			
20.1.1.1	00e0-fc00-0001	N/A	N/A	N/A	S

## reset arp

### Syntax

```
reset arp { all | dynamic | slot slot-number | static | interface interface-type interface-number }
```

### View

User view

## Default Level

2: System level

## Parameters

**all**: Clears all ARP entries except authorized ARP entries.

**dynamic**: Clears all dynamic ARP entries.

**static**: Clears all static ARP entries.

**slot slot-number**: Clears the ARP entries for the specified device. If the device is in an IRF stack, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF stack, the *slot-number* argument represents the device ID.

**interface** *interface-type interface-number*. Clears the ARP entries for the interface specified by the argument *interface-type interface-number*.

### Description

Use the **reset arp** command to clear ARP entries except authorized ARP entries from the ARP mapping table.

With **interface** *interface-type interface-number* or **slot** *slot-number* specified, the command clears only dynamic ARP entries of the interface or the specified device in the stack.

Related commands: **arp static**, **display arp**.

### Examples

```
# Clear all static ARP entries.
```

```
<Sysname> reset arp static
```

## Gratuitous ARP Configuration Commands

### gratuitous-arp-sending enable

#### Syntax

```
gratuitous-arp-sending enable
```

```
undo gratuitous-arp-sending enable
```

#### View

```
System view
```

#### Default Level

```
2: System level
```

#### Parameters

```
None
```

#### Description

Use the **gratuitous-arp-sending enable** command to enable a device to send gratuitous ARP packets when receiving ARP requests from another network segment.

Use the **undo gratuitous-arp-sending enable** command to restore the default.

By default, a device cannot send gratuitous ARP packets when receiving ARP requests from another network segment.

### Examples

```
# Disable a device from sending gratuitous ARP packets.
```

```
<Sysname> system-view
```

```
[Sysname] undo gratuitous-arp-sending enable
```

## gratuitous-arp-learning enable

### Syntax

```
gratuitous-arp-learning enable
undo gratuitous-arp-learning enable
```

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **gratuitous-arp-learning enable** command to enable the gratuitous ARP packet learning function.

Use the **undo gratuitous-arp-learning enable** command to disable the function.

By default, the function is enabled.

With this function enabled, a device receiving a gratuitous ARP packet can add the source IP and MAC addresses carried in the packet to its own dynamic ARP table if it finds no ARP entry in the cache corresponding to the source IP address of the ARP packet exists; if the corresponding ARP entry exists in the cache, the device updates the ARP entry regardless of whether this function is enabled.

### Examples

# Enable the gratuitous ARP packet learning function.

```
<Sysname> system-view
[Sysname] gratuitous-arp-learning enable
```

# 2 Proxy ARP Configuration Commands

---

## Proxy ARP Configuration Commands

### display local-proxy-arp

#### Syntax

```
display local-proxy-arp [ interface vlan-interface vlan-id ]
```

#### View

Any view

#### Default Level

2: System level

#### Parameters

**interface vlan-interface** *vlan-id*: Displays the local proxy ARP status of the specified VLAN interface.

#### Description

Use the **display local-proxy-arp** command to display the status of the local proxy ARP.

Related commands: **local-proxy-arp enable**.

#### Examples

# Display the status of the local proxy ARP on VLAN-interface 2.

```
<Sysname> display local-proxy-arp interface vlan-interface 2
Interface Vlan-interface2
Local Proxy ARP status: enabled
```

### display proxy-arp

#### Syntax

```
display proxy-arp [ interface vlan-interface vlan-id ]
```

#### View

Any view

#### Default Level

2: System level

#### Parameters

**interface vlan-interface** *vlan-id*: Displays the proxy ARP status of the VLAN interface specified by the argument *vlan-id*.

## Description

Use the **display proxy-arp** command to display the proxy ARP status.

If an interface is specified, proxy ARP status of the specified interface is displayed; if no interface is specified, proxy ARP status of all interfaces is displayed.

Related commands: **proxy-arp enable**.

## Examples

# Display the proxy ARP status on VLAN-interface 1.

```
<Sysname> display proxy-arp interface vlan-interface 1
Proxy ARP status: disabled
```

## local-proxy-arp enable

### Syntax

```
local-proxy-arp enable
undo local-proxy-arp enable
```

### View

VLAN interface view

### Default Level

2: System level

### Parameters

None

## Description

Use the **local-proxy-arp enable** command to enable local proxy ARP.

Use the **undo local-proxy-arp enable** command to disable local proxy ARP.

By default, local proxy ARP is disabled.

Related commands: **display local-proxy-arp**.

## Examples

# Enable local proxy ARP on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] local-proxy-arp enable
```

## proxy-arp enable

### Syntax

```
proxy-arp enable
undo proxy-arp enable
```

## View

VLAN interface view

## Default Level

2: System level

## Parameters

None

## Description

Use the **proxy-arp enable** command to enable proxy ARP.

Use the **undo proxy-arp enable** command to disable proxy ARP.

By default, proxy ARP is disabled.

Related commands: **display proxy-arp**.

## Examples

# Enable proxy ARP on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] proxy-arp enable
```

# 3 ARP Attack Defense Configuration Commands

---

## ARP Source Suppression Configuration Commands

### arp source-suppression enable

#### Syntax

```
arp source-suppression enable
undo arp source-suppression enable
```

#### View

System view

#### Default Level

2: System level

#### Parameters

None

#### Description

Use the **arp source-suppression enable** command to enable the ARP source suppression function.

Use the **undo arp source-suppression enable** command to disable the function.

By default, the ARP source suppression function is disabled.

Related commands: **display arp source-suppression**.

#### Examples

# Enable the ARP source suppression function.

```
<Sysname> system-view
[Sysname] arp source-suppression enable
```

### arp source-suppression limit

#### Syntax

```
arp source-suppression limit limit-value
undo arp source-suppression limit
```

#### View

System view

#### Default Level

2: System level

## Parameters

*limit-value*: Specifies the maximum number of packets with the same source IP address but unresolvable destination IP addresses that the device can receive in five seconds. It ranges from 2 to 1024.

## Description

Use the **arp source-suppression limit** command to set the maximum number of packets with the same source IP address but unresolvable destination IP addresses that the device can receive in five seconds.

Use the **undo arp source-suppression limit** command to restore the default value, which is 10.

With this feature configured, whenever the number of packets with unresolvable destination IP addresses from a host within five seconds exceeds the specified threshold, the device suppress the sending host from triggering any ARP requests within the following five seconds.

Related commands: **display arp source-suppression**.

## Examples

# Set the maximum number of packets with the same source address but unresolvable destination IP addresses that the device can receive in five seconds to 100.

```
<Sysname> system-view
[Sysname] arp source-suppression limit 100
```

## display arp source-suppression

### Syntax

```
display arp source-suppression
```

### View

Any view

### Default Level

2: System level

### Parameters

None

### Description

Use the **display arp source-suppression** command to display information about the current ARP source suppression configuration.

### Examples

# Display information about the current ARP source suppression configuration.

```
<Sysname> display arp source-suppression
ARP source suppression is enabled
Current suppression limit: 100
Current cache length: 16
```

**Table 3-1** display arp source-suppression command output description

Field	Description
ARP source suppression is enabled	The ARP source suppression function is enabled
Current suppression limit	Maximum number of packets with the same source IP address but unresolvable IP addresses that the device can receive in five seconds
Current cache length	Size of cache used to record source suppression information

## ARP Defense Against IP Packet Attack Configuration Commands

### arp resolving-route enable

#### Syntax

```
arp resolving-route enable
undo arp resolving-route enable
```

#### View

System view

#### Default Level

2: System level

#### Parameters

None

#### Description

Use the **arp resolving-route enable** command to enable ARP defense against IP packet attacks.

Use the **undo arp resolving-route enable** command to disable the function.

By default, the function of ARP defense against IP packet attacks is enabled.

#### Examples

```
# Disable ARP defense against IP packet attacks.
<Sysname> system-view
[Sysname] undo arp resolving-route enable
```

## ARP Active Acknowledgement Configuration Commands

### arp anti-attack active-ack enable

#### Syntax

```
arp anti-attack active-ack enable
undo arp anti-attack active-ack enable
```

## View

System view

## Default Level

2: System level

## Parameters

None

## Description

Use the **arp anti-attack active-ack enable** command to enable the ARP active acknowledgement function.

Use the **undo arp anti-attack active-ack enable** command to restore the default.

By default, the ARP active acknowledgement function is disabled.

Typically, this feature is configured on gateway devices to identify invalid ARP packets.

With this feature enabled, the gateway, upon receiving an ARP packet with a different source MAC address from that in the corresponding ARP entry, checks whether the ARP entry has been updated within the last minute:

- If yes, the ARP entry is not updated;
- If not, the gateway sends a unicast request to the source MAC address of the ARP entry.

Then,

- If a response is received within five seconds, the ARP packet is ignored;
- If no response is received, the gateway sends a unicast request to the source MAC address of the ARP packet.

Then,

- If a response is received within five seconds, the gateway updates the ARP entry;
- If not, the ARP entry is not updated.

## Examples

```
# Enable the ARP active acknowledgement function.
```

```
<Sysname> system-view
```

```
[Sysname] arp anti-attack active-ack enable
```

# Source MAC Address Based ARP Attack Detection Configuration Commands

## arp anti-attack source-mac

### Syntax

```
arp anti-attack source-mac { filter | monitor }
```

```
undo arp anti-attack source-mac [ filter | monitor ]
```

## View

System view

## Default Level

2: System level

## Parameters

**filter**: Specifies the **filter** mode.

**monitor**: Specifies the **monitor** mode.

## Description

Use the **arp anti-attack source-mac** command to enable source MAC address based ARP attack detection and specify the detection mode.

Use the **undo arp anti-attack source-mac** command to restore the default.

By default, source MAC address based ARP attack detection is disabled.

After you enable this feature, the device checks the source MAC address of ARP packets received from the VLAN. If the number of ARP packets received from a source MAC address within five seconds exceeds the specified threshold:

- In filter detection mode, the device displays an alarm and filters out the ARP packets from the MAC address.
- In monitor detection mode, the device only displays an alarm.

Note that: If no detection mode is specified in the **undo arp anti-attack source-mac** command, both detection modes are disabled.

## Examples

```
# Enable filter-mode source MAC address based ARP attack detection
```

```
<Sysname> system-view  
[Sysname] arp anti-attack source-mac filter
```

## arp anti-attack source-mac aging-time

### Syntax

```
arp anti-attack source-mac aging-time time
```

```
undo arp anti-attack source-mac aging-time
```

### View

System view

## Default Level

2: System level

## Parameters

*time*: Aging timer for protected MAC addresses, in the range of 60 to 6000 seconds.

## Description

Use the **arp anti-attack source-mac aging-time** command to configure the aging timer for protected MAC addresses.

Use the **undo arp anti-attack source-mac aging-time** command to restore the default.

By default, the aging timer for protected MAC addresses is 300 seconds (five minutes).

## Examples

```
# Configure the aging timer for protected MAC addresses as 60 seconds.
<Sysname> system-view
[Sysname] arp anti-attack source-mac aging-time 60
```

## arp anti-attack source-mac exclude-mac

### Syntax

```
arp anti-attack source-mac exclude-mac mac-address&<1-n>
undo arp anti-attack source-mac exclude-mac [ mac-address&<1-n> ]
```

### View

System view

### Default Level

2: System level

### Parameters

*mac-address*&<1-n>: MAC address list. The *mac-address* argument indicates a protected MAC address in the format H-H-H. &<1-n> indicates the number of protected MAC addresses that you can configure. The maximum of the n argument is 10.

### Description

Use the **arp anti-attack source-mac exclude-mac** command to configure protected MAC addresses which will be excluded from ARP packet detection.

Use the **undo arp anti-attack source-mac exclude-mac** command to remove the configured protected MAC addresses.

By default, no protected MAC address is configured.

Note that: If no MAC address is specified in the **undo arp anti-attack source-mac exclude-mac** command, all the configured protected MAC addresses are removed.

## Examples

```
# Configure a protected MAC address.
<Sysname> system-view
[Sysname] arp anti-attack source-mac exclude-mac 2-2-2
```

## arp anti-attack source-mac threshold

### Syntax

```
arp anti-attack source-mac threshold threshold-value
undo arp anti-attack source-mac threshold
```

### View

System view

## Default Level

2: System level

## Parameters

*threshold-value*: Threshold for source MAC address based ARP attack detection, in the range 10 to 100.

## Description

Use the **arp anti-attack source-mac threshold** command to configure the threshold for source MAC address based ARP attack detection. If the number of ARP packets sent from a MAC address within five seconds exceeds this threshold, the device considers this an attack.

Use the **undo arp anti-attack source-mac threshold** command to restore the default.

By default, the threshold for source MAC address based ARP attack detection is 50.

## Examples

```
# Configure the threshold for source MAC address based ARP attack detection as 30.
```

```
<Sysname> system-view  
[Sysname] arp anti-attack source-mac threshold 30
```

## display arp anti-attack source-mac

### Syntax

```
display arp anti-attack source-mac { slot slot-number | interface interface-type interface-number }
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**interface** *interface-type interface-number*: Displays attacking MAC addresses detected on the interface.

**slot** *slot-number*: Displays attacking MAC addresses detected on the specified device. If the device is in an IRF stack, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF stack, the *slot-number* argument represents the device ID.

### Description

Use the **display arp anti-attack source-mac** command to display attacking MAC addresses detected by source MAC address based ARP attack detection.

On a device, if no interface is specified, the **display arp anti-attack source-mac** command displays attacking MAC addresses detected on all the interfaces.

### Examples

```
# Display the attacking MAC addresses detected by source MAC address based ARP attack detection.
```

```
<Sysname> display arp anti-attack source-mac slot 1
```

Source-MAC	VLAN-ID	Interface	Aging-time
23f3-1122-3344	4094	GE1/0/1	10
23f3-1122-3355	4094	GE1/0/2	30
23f3-1122-33ff	4094	GE1/0/3	25
23f3-1122-33ad	4094	GE1/0/4	30
23f3-1122-33ce	4094	GE1/0/5	2

## ARP Packet Source MAC Address Consistency Check Configuration Commands

### arp anti-attack valid-ack enable

#### Syntax

```
arp anti-attack valid-check enable
undo arp anti-attack valid-check enable
```

#### View

System view

#### Default Level

2: System level

#### Parameters

None

#### Description

Use the **arp anti-attack valid-check enable** command to enable ARP packet source MAC address consistency check on the gateway. After you execute this command, the gateway device can filter out ARP packets with the source MAC address in the Ethernet header different from the sender MAC address in the ARP message.

Use the **undo arp anti-attack valid-check enable** command to disable ARP packet source MAC address consistency check.

By default, ARP packet source MAC address consistency check is disabled.

#### Examples

```
# Enable ARP packet source MAC address consistency check.
```

```
<Sysname> system-view
[Sysname] arp anti-attack valid-check enable
```

## ARP Packet Rate Limit Configuration Commands

### arp rate-limit

#### Syntax

```
arp rate-limit { disable | rate pps drop }
undo arp rate-limit
```

## View

Layer 2 Ethernet port view

## Default Level

2: System level

## Parameters

**disable**: Disables ARP packet rate limit.

**rate pps**: ARP packet rate in pps, in the range 50 to 500.

**drop**: Discards the exceeded packets.

## Description

Use the **arp rate-limit** command to configure or disable ARP packet rate limit. If a rate is specified, exceeded packets are discarded.

Use the **undo arp rate-limit** command to restore the default.

By default, ARP packet rate limit is enabled, and the ARP packet rate limit is 100 pps.

## Examples

# Specify the ARP packet rate on GigabitEthernet 1/0/1 as 60 pps, and exceeded packets are discarded.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp rate-limit rate 60 drop
```

# ARP Detection Configuration Commands

## arp detection enable

### Syntax

**arp detection enable**

**undo arp detection enable**

### View

VLAN view

### Default Level

2: System level

### Parameters

None

### Description

Use the **arp detection enable** command to enable ARP detection for the VLAN.

Use the **undo arp detection enable** command to disable ARP detection for the VLAN.

By default, ARP detection is disabled for a VLAN.

## Examples

```
# Enable ARP detection for VLAN 1.
<Sysname> system-view
[Sysname] vlan 1
[Sysname-Vlan1] arp detection enable
```

## arp detection mode

### Syntax

```
arp detection mode { dhcp-snooping | dot1x | static-bind } *
undo arp detection mode [ dhcp-snooping | dot1x | static-bind ] *
```

### View

System view

### Default Level

2: System level

### Parameters

**dhcp-snooping**: Implements ARP attack detection based on DHCP snooping entries. This mode is mainly used to prevent source address spoofing attacks.

**dot1x**: Implements ARP attack detection based on 802.1X security entries. This mode is mainly used to prevent source address spoofing attacks.

**static-bind**: Implements ARP attack detection based on static IP-to-MAC binding entries. This mode is mainly used to prevent gateway spoofing attacks.

### Description

Use the **arp detection mode** command to specify an ARP attack detection mode.

Use the **undo arp detection mode** command to cancel the specified ARP detection mode or all ARP detection modes. If all detection modes are cancelled, ARP detection is not performed.

By default, no ARP detection mode is specified, that is, ARP detection based on DHCP snooping entries/802.1X security entries/static IP-to-MAC bindings is not enabled.

Note that:

- You can specify the three modes at the same time.
- In dot1x mode: if an entry with matching source IP and MAC addresses, port index, and VLAN ID is found, the ARP packet is considered valid and can pass the detection; If an entry with no matching IP address but with a matching OUI MAC address is found, the ARP packet is considered valid and can pass the detection; if otherwise, the ARP packet is discarded.
- In static-bind mode: If an entry with a matching IP address but with a different MAC address is found, the ARP packet is considered invalid and discarded; if an entry with both matching IP and MAC addresses is found, the ARP packet is considered valid and can pass the detection; if no match is found, the ARP packet is considered valid and can pass the detection.
- If no ARP detection mode is specified in the undo arp detection mode command, all configured ARP detection modes are disabled.

## Examples

```
# Enable ARP detection based on DHCP snooping entries.
<Sysname> system-view
[Sysname] arp detection mode dhcp-snooping
```

## arp detection static-bind

### Syntax

```
arp detection static-bind ip-address mac-address
undo arp detection static-bind [ ip-address ]
```

### View

System view

### Default Level

2: System level

### Parameters

*ip-address*: IP address of the static binding.

*mac-address*: MAC address of the static binding, in the format of H-H-H.

### Description

Use the **arp detection static-bind** command to configure a static IP-to-MAC binding.

Use the **undo arp detection static-bind** command to remove the configure static binding.

By default, no static IP-to-MAC binding is configured.

With ARP detection based on static IP-to-MAC bindings configured, the device, upon receiving an ARP packet from an ARP trusted/untrusted port, compares the source IP and MAC addresses of the ARP packet against the static IP-to-MAC bindings.

- If an entry with a matching IP address but different MAC address is found, the ARP packet is considered invalid and discarded.
- If an entry with both matching IP and MAC addresses is found, the ARP packet is considered valid and can pass the detection.
- If no match is found, the ARP packet is considered valid and can pass the detection.

Note that: If no IP address is specified in the **undo arp detection static-bind** command, all configured static IP-to-MAC bindings are removed.

## Examples

```
# Configure a static IP-to-MAC binding.
<Sysname> system-view
[Sysname] arp detection static-bind 192.168.1.2 2-1-201
```

## arp detection trust

### Syntax

```
arp detection trust
```

## undo arp detection trust

### View

Layer 2 Ethernet port view

### Default Level

2: System level

### Parameters

None

### Description

Use the **arp detection trust** command to configure the port as an ARP trusted port.

Use the **undo arp detection trust** command to configure the port as an ARP untrusted port.

By default, the port is an ARP untrusted port.

### Examples

```
# Configure GigabitEthernet 1/0/1 as an ARP trusted port.  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] arp detection trust
```

## arp detection validate

### Syntax

```
arp detection validate { dst-mac | ip | src-mac } *  
undo arp detection validate [ dst-mac | ip | src-mac ] *
```

### View

System view

### Default Level

2: System level

### Parameters

**dst-mac**: Checks the target MAC address of ARP responses. If the target MAC address is all-zero, all-one, or inconsistent with the destination MAC address in the Ethernet header, the packet is considered invalid and discarded.

**ip**: Checks the source and destination IP addresses of ARP packets. The all-zero, all-one or multicast IP addresses are considered invalid and the corresponding packets are discarded. With this keyword specified, the source and destination IP addresses of ARP replies, and the source IP address of ARP requests will be checked.

**src-mac**: Checks whether the source MAC address of an ARP packet is identical to that in its Ethernet header. If they are identical, the packet is considered valid; otherwise, the packet is discarded.

## Description

Use the **arp detection validate** command to configure ARP detection based on specified objects. You can specify one or more objects in one command line.

Use the **undo arp detection validate** command to remove detected objects. If no keyword is specified, all the detected objects are removed.

By default, ARP detection based on specified objects is disabled.

## Examples

```
# Enable the checking of the MAC addresses and IP addresses of ARP packets.
```

```
<Sysname> system-view  
[Sysname] arp detection validate dst-mac src-mac ip
```

## display arp detection

### Syntax

```
display arp detection
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display arp detection** command to display the VLAN(s) enabled with ARP detection.

Related commands: **arp detection enable**.

## Examples

```
# Display the VLANs enabled with ARP detection.
```

```
<Sysname> display arp detection  
ARP detection is enabled in the following VLANs:  
1, 2, 4-5
```

**Table 3-2 display arp detection** command output description

Field	Description
ARP detection is enabled in the following VLANs	VLANs that are enabled with ARP detection

## display arp detection statistics

### Syntax

```
display arp detection statistics [ interface interface-type interface-number ]
```

## View

Any view

## Default Level

1: Monitor level

## Parameters

**interface** *interface-type interface-number*. Displays the ARP detection statistics of a specified interface.

## Description

Use the **display arp detection statistics** command to display statistics about ARP detection. This command only displays numbers of discarded packets. If no interface is specified, the statistics of all the interfaces will be displayed.

## Examples

# Display the ARP detection statistics of all the interfaces.

```
<Sysname> display arp detection statistics
State: U-Untrusted T-Trusted
ARP packets dropped by ARP inspect checking:
Interface(State)      IP      Src-MAC  Dst-MAC  Inspect
GE1/0/1(U)           40      0        0        78
GE1/0/2(U)           0       0        0        0
GE1/0/3(T)           0       0        0        0
GE1/0/4(U)           0       0        30       0
```

**Table 3-3** display arp detection statistics command output description

Field	Description
Interface(State)	State T or U identifies a trusted or untrusted port.
IP	Number of ARP packets discarded due to invalid source and destination IP addresses
Src-MAC	Number of ARP packets discarded due to invalid source MAC address
Dst-MAC	Number of ARP packets discarded due to invalid destination MAC address
Inspect	Number of ARP packets that failed to pass ARP detection (based on DHCP snooping entries/802.1X security entries/static IP-to-MAC bindings)

## reset arp detection statistics

### Syntax

**reset arp detection statistics** [ **interface** *interface-type interface-number* ]

### View

User view

## Default Level

2: System level

## Parameters

**interface** *interface-type interface-number*: Clears the ARP detection statistics of a specified interface.

## Description

Use the **reset arp detection statistics** command to clear ARP detection statistics of a specified interface. If no interface is specified, the statistics of all the interfaces will be cleared.

## Examples

# Clear the ARP detection statistics of all the interfaces.

```
<Sysname> reset arp detection statistics
```

# Table of Contents

<b>1 DHCP Server Configuration Commands</b> .....	<b>1-1</b>
DHCP Server Configuration Commands .....	1-1
bims-server .....	1-1
bootfile-name .....	1-2
dhcp enable .....	1-2
dhcp server apply ip-pool .....	1-3
dhcp select server global-pool .....	1-4
dhcp server detect .....	1-5
dhcp server forbidden-ip .....	1-5
dhcp server ip-pool .....	1-6
dhcp server ping packets .....	1-7
dhcp server ping timeout .....	1-7
dhcp server relay information enable .....	1-8
display dhcp server conflict .....	1-9
display dhcp server expired .....	1-9
display dhcp server free-ip .....	1-10
display dhcp server forbidden-ip .....	1-11
display dhcp server ip-in-use .....	1-12
display dhcp server statistics .....	1-13
display dhcp server tree .....	1-14
dns-list .....	1-16
domain-name .....	1-16
expired .....	1-17
forbidden-ip .....	1-18
gateway-list .....	1-19
nbns-list .....	1-19
netbios-type .....	1-20
network .....	1-21
network ip range .....	1-21
network mask .....	1-22
option .....	1-23
reset dhcp server conflict .....	1-24
reset dhcp server ip-in-use .....	1-24
reset dhcp server statistics .....	1-25
static-bind client-identifier .....	1-25
static-bind ip-address .....	1-26
static-bind mac-address .....	1-27
tftp-server domain-name .....	1-28
tftp-server ip-address .....	1-29
voice-config .....	1-29
<b>2 DHCP Relay Agent Configuration Commands</b> .....	<b>2-1</b>
DHCP Relay Agent Configuration Commands .....	2-1
dhcp relay address-check .....	2-1

dhcp relay information circuit-id format-type .....	2-2
dhcp relay information circuit-id string.....	2-2
dhcp relay information enable .....	2-3
dhcp relay information format.....	2-4
dhcp relay information remote-id format-type .....	2-5
dhcp relay information remote-id string.....	2-6
dhcp relay information strategy .....	2-7
dhcp relay release ip .....	2-7
dhcp relay security static .....	2-8
dhcp relay security tracker .....	2-9
dhcp relay server-detect.....	2-9
dhcp relay server-group.....	2-10
dhcp relay server-select .....	2-11
dhcp select relay.....	2-12
display dhcp relay.....	2-12
display dhcp relay information.....	2-13
display dhcp relay security .....	2-14
display dhcp relay security statistics .....	2-15
display dhcp relay security tracker .....	2-16
display dhcp relay server-group .....	2-16
display dhcp relay statistics.....	2-17
reset dhcp relay statistics .....	2-19
<b>3 DHCP Client Configuration Commands .....</b>	<b>3-1</b>
DHCP Client Configuration Commands.....	3-1
display dhcp client .....	3-1
ip address dhcp-alloc.....	3-3
<b>4 DHCP Snooping Configuration Commands .....</b>	<b>4-1</b>
DHCP Snooping Configuration Commands.....	4-1
dhcp-snooping .....	4-1
dhcp-snooping information circuit-id format-type .....	4-2
dhcp-snooping information circuit-id string.....	4-2
dhcp-snooping information enable .....	4-3
dhcp-snooping information format.....	4-4
dhcp-snooping information remote-id format-type .....	4-5
dhcp-snooping information remote-id string.....	4-6
dhcp-snooping information strategy .....	4-7
dhcp-snooping trust .....	4-7
display dhcp-snooping.....	4-8
display dhcp-snooping information.....	4-9
display dhcp-snooping packet statistics .....	4-10
display dhcp-snooping trust.....	4-11
reset dhcp-snooping .....	4-12
reset dhcp-snooping packet statistics .....	4-12
<b>5 BOOTP Client Configuration Commands .....</b>	<b>5-1</b>
BOOTP Client Configuration Commands .....	5-1
display bootp client.....	5-1
ip address bootp-alloc .....	5-2



# 1 DHCP Server Configuration Commands

---



## Note

- The DHCP server configuration is supported only on VLAN interfaces and loopback interfaces. The subaddress pool configuration is not supported on loopback interfaces.
  - DHCP snooping must be disabled on the DHCP server.
- 

## DHCP Server Configuration Commands

### bims-server

#### Syntax

```
bims-server ip ip-address [ port port-number ] sharekey key  
undo bims-server
```

#### View

DHCP address pool view

#### Default Level

2: System level

#### Parameters

**ip** *ip-address*: Specifies an IP address for the BIMS server.

**port** *port-number*: Specifies a port number for the BIMS server in the range 1 to 65534.

**sharekey** *key*: Specifies a shared key for the BIMS server, which is a string of 1 to 16 characters.

#### Description

Use the **bims-server** command to specify the IP address, port number, and shared key of the BIMS server in the DHCP address pool for the client.

Use the **undo bims-server** command to remove the specified BIMS server information.

By default, no BIMS server information is specified.

If you execute the **bims-server** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**.

## Examples

# Specify the IP address 1.1.1.1, port number 80, shared key aabbcc of the BIMS server in DHCP address pool 0 for the client.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bims-server ip 1.1.1.1 port 80 sharekey aabbcc
```

## bootfile-name

### Syntax

**bootfile-name** *bootfile-name*

**undo bootfile-name**

### View

DHCP address pool view

### Default Level

2: System level

### Parameters

*bootfile-name*: Boot file name, a string of 1 to 63 characters.

### Description

Use the **bootfile-name** command to specify a bootfile name in the DHCP address pool for the client.

Use the **undo bootfile-name** command to remove the specified bootfile name.

By default, no bootfile name is specified.

If you execute the **bootfile-name** command repeatedly, the latest configuration will overwrite the previous one.

## Examples

# Specify the bootfile name **aaa.cfg** in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bootfile-name aaa.cfg
```

## dhcp enable

### Syntax

**dhcp enable**

**undo dhcp enable**

### View

System view

## Default Level

2: System level

## Parameters

None

## Description

Use the **dhcp enable** command to enable DHCP.

Use the **undo dhcp enable** command to disable DHCP.

By default, DHCP is disabled.



### Note

You need to enable DHCP before performing DHCP server and relay agent configurations.

---

## Examples

```
# Enable DHCP.
```

```
<Sysname> system-view  
[Sysname] dhcp enable
```

## dhcp server apply ip-pool

### Syntax

```
dhcp server apply ip-pool pool-name  
undo dhcp server apply ip-pool [ pool-name ]
```

### View

Interface view

## Default Level

2: System level

## Parameters

*pool-name*: DHCP address pool name, a case-insensitive string in the range of 1 to 35 characters.

## Description

Use the **dhcp server apply ip-pool** command to apply an extended address pool on an interface.

Use the **undo dhcp server apply ip-pool** command to remove the configuration.

By default, no extended address pool is applied on an interface, and the server assigns an IP address from a common address pool to a client when the client's request arrives at the interface.

Note that:

- If you execute the **dhcp server apply ip-pool** command on an interface, when a client's request arrives at the interface, the server assigns an IP address from this extended address pool only.
- Only an extended address pool can be applied on an interface. The address pool to be referenced must already exist.

Related commands: **dhcp server ip-pool**.

## Examples

# Apply extended DHCP address pool 0 on VLAN-interface 1.

```
<system> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp server apply ip-pool 0
```

## dhcp select server global-pool

### Syntax

```
dhcp select server global-pool [ subaddress ]
undo dhcp select server global-pool subaddress
```

### View

Interface view

### Default Level

2: System level

### Parameters

**subaddress**: Supports subaddress allocation. That is, the DHCP server and clients are on the same network segment, and the server allocates IP addresses from the address pool containing the network segment of the first subaddress if several subaddresses exist.

### Description

Use the **dhcp select server global-pool** command to enable the DHCP server on specified interface(s). After the interface receives a DHCP request, the DHCP server will allocate an IP address from the address pool.

Use the **undo dhcp select server global-pool subaddress** command to cancel the support for subaddress allocation.

By default, the DHCP server is enabled on an interface.

## Examples

# Enable the DHCP server on VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp select server global-pool
```

## dhcp server detect

### Syntax

```
dhcp server detect
undo dhcp server detect
```

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **dhcp server detect** command to enable unauthorized DHCP server detection.

Use the **undo dhcp server detect** command to disable the function.

By default, the function is disabled.

With this function enabled, upon receiving a DHCP request, the DHCP server will record the IP addresses of DHCP servers which ever offered IP addresses to the DHCP client and the receiving interface. Each server detected is recorded only once. The administrator can get this information from logs to check out unauthorized DHCP servers.

### Examples

```
# Enable unauthorized DHCP server detection.
```

```
<Sysname> system-view
[Sysname] dhcp server detect
```

## dhcp server forbidden-ip

### Syntax

```
dhcp server forbidden-ip low-ip-address [ high-ip-address ]
undo dhcp server forbidden-ip low-ip-address [ high-ip-address ]
```

### View

System view

### Default Level

2: System level

### Parameters

*low-ip-address*: Start IP address of the IP address range to be excluded from dynamic allocation.

*high-ip-address*: End IP address of the IP address range to be excluded from dynamic allocation. The end IP address must have a higher sequence than the start one.

## Description

Use the **dhcp server forbidden-ip** command to exclude IP addresses from dynamic allocation.

Use the **undo dhcp server forbidden-ip** command to remove the configuration.

By default, all IP addresses in a DHCP address pool are assignable except IP addresses of the DHCP server interfaces.

Note that:

- When you use the **dhcp server forbidden-ip** command to exclude an IP address that is bound to a user from dynamic assignment, the address can be still assigned to the user.
- When you use the **undo dhcp server forbidden-ip** command to remove the configuration, the specified address/address range must be consistent with the one specified with the **dhcp server forbidden-ip** command. If you have configured to exclude an address range from dynamic assignment, you need to specify the same address range in the **undo dhcp server forbidden-ip** command instead of specifying one IP address.
- Using the **dhcp server forbidden-ip** command repeatedly can exclude multiple IP address ranges from allocation.

Related commands: **dhcp server ip-pool**, **network**, **static-bind ip-address**.

## Examples

```
# Exclude the IP address range 10.110.1.1 to 10.110.1.63 from dynamic allocation.
```

```
<Sysname> system-view
```

```
[Sysname] dhcp server forbidden-ip 10.110.1.1 10.110.1.63
```

## dhcp server ip-pool

### Syntax

```
dhcp server ip-pool pool-name [ extended ]
```

```
undo dhcp server ip-pool pool-name [ extended ]
```

### View

System view

### Default Level

2: System level

### Parameters

*pool-name*: Global address pool name, which is a unique pool identifier, a string of 1 to 35 characters.

**extended**: Specifies the address pool as an extended address pool. If this keyword is not specified, the address pool is a common address pool.

## Description

Use the **dhcp server ip-pool** command to create a DHCP address pool and enter its view. If the pool was created, you will directly enter its view.

Use the **undo dhcp server ip-pool** command to remove the specified DHCP address pool.

By default, no DHCP address pool is created.

Related commands: **dhcp enable**.

## Examples

```
# Create the common address pool identified by 0.
```

```
<Sysname> system-view  
[Sysname] dhcp server ip-pool 0  
[Sysname-dhcp-pool-0]
```

## dhcp server ping packets

### Syntax

```
dhcp server ping packets number
```

```
undo dhcp server ping packets
```

### View

System view

### Default Level

2: System level

### Parameters

*number*: Number of ping packets, in the range of 0 to 10. 0 means no ping operation.

### Description

Use the **dhcp server ping packets** command to specify the maximum number of ping packets on the DHCP server.

Use the **undo dhcp server ping packets** command to restore the default.

The number defaults to 1.

## Examples

```
# Specify the maximum number of ping packets as 10.
```

```
<Sysname> system-view  
[Sysname] dhcp server ping packets 10
```

## dhcp server ping timeout

### Syntax

```
dhcp server ping timeout milliseconds
```

```
undo dhcp server ping timeout
```

### View

System view

### Default Level

2: System level

## Parameters

*milliseconds*: Response timeout value for ping packets in milliseconds, in the range of 0 to 10,000. 0 means no ping operation.

## Description

Use the **dhcp server ping timeout** command to configure response timeout time of the ping packet on the DHCP server.

Use the **undo dhcp server ping timeout** command to restore the default.

The time defaults to 500 ms.

## Examples

```
# Specify the response timeout time as 1000 ms.
```

```
<Sysname> system-view  
[Sysname] dhcp server ping timeout 1000
```

## dhcp server relay information enable

### Syntax

```
dhcp server relay information enable
```

```
undo dhcp server relay information enable
```

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **dhcp server relay information enable** command to enable the DHCP server to handle Option 82.

Use the **undo dhcp server relay information enable** command to configure the DHCP server to ignore Option 82.

By default, the DHCP server handles Option 82.

### Examples

```
# Configure the DHCP server to ignore Option 82.
```

```
<Sysname> system-view  
[Sysname] undo dhcp server relay information enable
```

## display dhcp server conflict

### Syntax

```
display dhcp server conflict { all | ip ip-address }
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**all**: Displays information about all IP address conflicts.

*ip-address*: Displays conflict information for the IP address.

### Description

Use the **display dhcp server conflict** command to display information about IP address conflicts.

Related commands: **reset dhcp server conflict**.

### Examples

# Display information about all IP address conflicts.

```
<Sysname> display dhcp server conflict all
  Address           Discover time
  4.4.4.1           Apr 25 2007 16:57:20
  4.4.4.2           Apr 25 2007 17:00:10
  --- total 2 entry ---
```

**Table 1-1** display dhcp server conflict command output description

Field	Description
Address	Conflicted IP address
Discover Time	Time when the conflict was discovered

## display dhcp server expired

### Syntax

```
display dhcp server expired { all | ip ip-address | pool [ pool-name ] }
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**all**: Displays the lease expiration information of all DHCP address pools.

**ip ip-address:** Displays the lease expiration information of a specified IP address.

**pool [ pool-name ]:** Displays the lease expiration information of a specified address pool. The *pool name* is a string of 1 to 35 characters. If the *pool name* is not specified, the lease expiration information of all address pools is displayed.

## Description

Use the **display dhcp server expired** command to display the lease expiration information of specified DHCP address pool(s) or an IP address.

DHCP will assign these expired IP addresses to DHCP clients after all addresses have been assigned.

## Examples

# Display information about lease expirations in all DHCP address pools.

```
<Sysname> display dhcp server expired all
Global pool:
  IP address      Client-identifier/   Lease expiration     Type
                  Hardware address
4.4.4.6          3030-3066-2e65-3230- Apr 25 2007 17:10:47 Release
                  302e-3130-3234-2d45-
                  7468-6572-6e65-7430-
                  2f31
--- total 1 entry ---
```

**Table 1-2 display dhcp server expired** command output description

Field	Description
Global pool	Information about lease expiration of a DHCP address pool
IP address	Expired IP addresses
Client-identifier/Hardware address	IDs or MACs of clients whose IP addresses were expired
Lease expiration	The lease expiration time
Type	Types of lease expirations. Currently, this field is set to Release.

## display dhcp server free-ip

### Syntax

```
display dhcp server free-ip
```

### View

Any view

### Default Level

1: Monitor level

## Parameters

None

## Description

Use the **display dhcp server free-ip** command to display information about assignable IP addresses which have never been assigned.

## Examples

```
# Display information about assignable IP addresses.
<Sysname> display dhcp server free-ip
IP Range from 10.0.0.0          to 10.0.0.255
```

## display dhcp server forbidden-ip

### Syntax

```
display dhcp server forbidden-ip
```

### View

Any view

### Default Level

1: Monitor level

## Parameters

None

## Description

Use the **display dhcp server forbidden-ip** command to display IP addresses excluded from dynamic allocation in DHCP address pool.

## Examples

```
# Display IP addresses excluded from dynamic allocation in the DHCP address pool.
```

```
<Sysname> display dhcp server forbidden-ip
Global:
IP Range from 1.1.0.2          to 1.1.0.3
IP Range from 1.1.1.2          to 1.1.1.3
Pool name: 2
1.1.1.5          1.1.1.6
```

**Table 1-3** display dhcp server forbidden-ip command output description

Field	Description
Global	Globally excluded IP addresses specified with the <b>dhcp server forbidden-ip</b> command in system view. No address pool can assign these IP addresses.
Pool name	Excluded IP addresses specified with the <b>forbidden-ip</b> command in DHCP address pool view. They cannot be assigned from the current extended address pool only.

## display dhcp server ip-in-use

### Syntax

```
display dhcp server ip-in-use { all | ip ip-address | pool [ pool-name ] }
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**all**: Displays the binding information of all DHCP address pools.

**ip ip-address**: Displays the binding information of a specified IP address.

**pool [ pool-name ]**: Displays the binding information of a specified address pool. The *pool name* is a string of 1 to 35 characters. If no *pool name* is specified, the binding information of all address pools is displayed.

### Description

Use the **display dhcp server ip-in-use** command to display the binding information of DHCP address pool(s) or an IP address.

Related commands: **reset dhcp server ip-in-use**.

### Examples

```
# Display the binding information of all DHCP address pools.
```

```
<Sysname> display dhcp server ip-in-use all
```

```
Global pool:
```

IP address	Client-identifier/ Hardware address	Lease expiration	Type
10.1.1.1	4444-4444-4444	NOT Used	Manual

```
--- total 1 entry ---
```

**Table 1-4** display dhcp server ip-in-use command output description

Field	Description
Global pool	Binding information of a DHCP address pool
IP address	Bound IP address
Client-identifier/Hardware address	Client's ID or MAC of the binding
Lease expiration	Lease expiration time

Field	Description
Type	Binding types, including Manual, Auto:OFFERED and Auto:COMMITTED. <ul style="list-style-type: none"> <li>• Manual: Static binding</li> <li>• Auto:OFFERED: The binding sent in the DHCP-OFFER message from the server to the client.</li> <li>• Auto:COMMITTED: The binding sent in the DHCP-ACK message from the server to the client.</li> </ul>

## display dhcp server statistics

### Syntax

**display dhcp server statistics**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display dhcp server statistics** command to display the statistics of the DHCP server.

Related commands: **reset dhcp server statistics**.

### Examples

# Display the statistics on the DHCP server.

```
<Sysname> display dhcp server statistics
Global Pool:
  Pool Number:                1
  Binding:
    Auto:                      1
    Manual:                    0
    Expire:                    0
BOOTP Request:                10
  DHCPDISCOVER:               5
  DHCPREQUEST:                3
  DHCPDECLINE:                0
  DHCPRELEASE:                2
  DHCPINFORM:                 0
  BOOTPREQUEST:               0
BOOTP Reply:                  6
  DHCPOFFER:                  3
  DHCPACK:                    3
  DHCPNAK:                    0
```

```

BOOTPREPLY:                0
Bad Messages:              0

```

**Table 1-5** display dhcp server statistics command output description

Field	Description
Global Pool	Statistics of a DHCP address pool
Pool Number	The number of address pools
Auto	The number of dynamic bindings
Manual	The number of static bindings
Expire	The number of expired bindings
BOOTP Request	The number of DHCP requests sent from DHCP clients to the DHCP server, including: <ul style="list-style-type: none"> <li>• DHCPDISCOVER</li> <li>• DHCPREQUEST</li> <li>• DHCPDECLINE</li> <li>• DHCPRELEASE</li> <li>• DHCPINFORM</li> <li>• BOOTPREQUEST</li> </ul>
BOOTP Reply	The number of DHCP replies sent from the DHCP server to DHCP clients, including: <ul style="list-style-type: none"> <li>• DHCPOFFER</li> <li>• DHCPACK</li> <li>• DHCPNAK</li> <li>• BOOTPREPLY</li> </ul>
Bad Messages	The number of erroneous messages

## display dhcp server tree

### Syntax

```
display dhcp server tree { all | pool [ pool-name ] }
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**all**: Displays information of all DHCP address pools.

**pool [ pool-name ]**: Displays information of a specified address pool. The *pool name* argument is a string of 1 to 35 characters. If no *pool name* is specified, information of all address pools will be displayed.

### Description

Use the **display dhcp server tree** command to display information of DHCP address pool(s).

## Examples

# Display information of all DHCP address pools.

```
<Sysname> display dhcp server tree all
```

Global pool:

Pool name: 0

```
network 20.1.1.0 mask 255.255.255.0
```

```
Sibling node:1
```

```
option 2 ip-address 1.1.1.1
```

```
expired 1 0 0
```

Pool name: 1

```
static-bind ip-address 10.10.1.2 mask 255.0.0.0
```

```
static-bind mac-address 00e0-00fc-0001
```

```
PrevSibling node:0
```

```
expired unlimited
```

Extended pool:

Pool name: 2

```
network ip range 1.1.1.0 1.1.1.255
```

```
network mask 255.255.255.0
```

```
expired 0 0 2
```

**Table 1-6 display dhcp server tree command output description**

Field	Description
Global pool	Information of a common address pool
Pool name	Address pool name
network	Network segment for address allocation
static-bind ip-address 10.10.1.2 mask 255.0.0.0 static-bind mac-address 00e0-00fc-0001	The IP address and MAC address of the static binding
Sibling node	The sibling node of the current node, nodes of this kind in the output information include: <ul style="list-style-type: none"> <li>Child node: The child node (subnet segment) address pool of the current node</li> <li>Parent node: The parent node (nature network segment) address pool of the current node</li> <li>Sibling node: The latter sibling node of the current node (another subnet of the same nature network). The earlier the sibling node is configured, the higher order the sibling node has.</li> <li>PrevSibling node: The previous sibling node of the current node</li> </ul>
option	Self-defined DHCP options
expired	The lease duration, in the format of day, hour, and minute
Extended pool	Information of an extended address pool

Field	Description
network ip range	Range of assignable IP addresses in the extended address pool
network mask	Mask of IP addresses assigned from the extended address pool

## dns-list

### Syntax

```
dns-list ip-address&<1-8>
undo dns-list { ip-address | all }
```

### View

DHCP address pool view

### Default Level

2: System level

### Parameters

*ip-address&<1-8>*: DNS server IP address. &<1-8> means you can specify up to eight DNS server addresses separated by spaces.

**all**: Specifies all DNS server addresses to be removed.

### Description

Use the **dns-list** command to specify DNS server addresses in a DHCP address pool.

Use the **undo dns-list** command to remove DNS server addresses from a DHCP address pool.

By default, no DNS server address is specified.

If you repeatedly use the **dns-list** command, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**.

### Examples

```
# Specify the DNS server address 10.1.1.254 for the DHCP client in DHCP address pool 0.
```

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] dns-list 10.1.1.254
```

## domain-name

### Syntax

```
domain-name domain-name
undo domain-name
```

### View

DHCP address pool view

## Default Level

2: System level

## Parameters

*domain-name*: Domain name suffix for DHCP clients, a string of 1 to 50 characters.

## Description

Use the **domain-name** command to specify a domain name suffix for the DHCP clients in the DHCP address pool.

Use the **undo domain-name** command to remove the specified domain name suffix.

No domain name suffix is specified by default.

Related commands: **dhcp server ip-pool**.

## Examples

```
# Specify a domain name suffix of mydomain.com for the DHCP clients in DHCP address pool 0.
```

```
<Sysname> system-view  
[Sysname] dhcp server ip-pool 0  
[Sysname-dhcp-pool-0] domain-name mydomain.com
```

## expired

### Syntax

```
expired { day day [ hour hour [ minute minute ] ] | unlimited }
```

```
undo expired
```

### View

DHCP address pool view

## Default Level

2: System level

## Parameters

**day** *day*: Specifies the number of days, in the range of 0 to 365.

**hour** *hour*: Specifies the number of hours, in the range of 0 to 23.

**minute** *minute*: Specifies the number of minutes, in the range of 0 to 59.

**unlimited**: Specifies the infinite duration, which is actually 136 years.

## Description

Use the **expired** command to specify the lease duration in a DHCP address pool.

Use the **undo expired** command to restore the default lease duration in a DHCP address pool.

The lease duration defaults to one day.

Note that if the lease duration you specified is beyond the year 2106, the system regards the lease as expired.

Related commands: **dhcp server ip-pool**.

## Examples

```
# Specify the lease duration as one day, two hours and three minutes in DHCP address pool 0.
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] expired day 1 hour 2 minute 3
```

## forbidden-ip

### Syntax

```
forbidden-ip ip-address&<1-8>
undo forbidden-ip { ip-address&<1-8> | all }
```

### View

DHCP address pool view

### Default Level

2: System level

### Parameters

*ip-address*&<1-8>: IP addresses to be excluded from dynamic allocation. &<1-8> indicates that you can specify up to eight IP addresses, separated with spaces.

**all**: Specifies all the IP addresses excluded from dynamic allocation.

### Description

Use the **forbidden-ip** command to exclude IP addresses from dynamic allocation in an extended address pool.

Use the **undo forbidden-ip** command to cancel specified or all excluded IP addresses.

By default, all IP addresses in an extended address pool are assignable except the IP addresses of the DHCP server interfaces.

Note that:

- Only the extended address pools support this command.
- IP addresses specified with the **forbidden-ip** command in DHCP address pool view are excluded from dynamic address allocation in the current extended address pool only. They are assignable in other address pools.
- Repeatedly using the **forbidden-ip** command can exclude multiple IP address ranges from dynamic allocation.

Related commands: **dhcp server ip-pool**.

## Examples

```
# Exclude IP addresses 192.168.1.3 and 192.168.1.10 from dynamic allocation for extended address pool 0.
<Sysname> system-view
[Sysname] dhcp server ip-pool 0 extended
[Sysname-dhcp-pool-0] forbidden-ip 192.168.1.3 192.168.1.10
```

## gateway-list

### Syntax

```
gateway-list ip-address&<1-8>  
undo gateway-list { ip-address | all }
```

### View

DHCP address pool view

### Default Level

2: System level

### Parameters

*ip-address&<1-8>*: Gateway IP address. &<1-8> means you can specify up to eight gateway addresses separated by spaces.

**all**: Specifies all gateway IP addresses to be removed.

### Description

Use the **gateway-list** command to specify gateway address(es) in a DHCP address pool.

Use the **undo gateway-list** command to remove specified gateway address(es) specified for the DHCP client from a DHCP address pool.

By default, no gateway address is specified.

If you use the **gateway-list** command repeatedly, the latest configuration will overwrite the previous one.

### Examples

```
# Specify the gateway address 10.110.1.99 in DHCP address pool 0.  
<Sysname> system-view  
[Sysname] dhcp server ip-pool 0  
[Sysname-dhcp-pool-0] gateway-list 10.110.1.99
```

## nbns-list

### Syntax

```
nbns-list ip-address&<1-8>  
undo nbns-list { ip-address | all }
```

### View

DHCP address pool view

### Default Level

2: System level

### Parameters

*ip-address&<1-8>*: WINS server IP address. &<1-8> means you can specify up to eight WINS server addresses separated by spaces.

**all**: Specifies all WINS server addresses to be removed.

## Description

Use the **nbns-list** command to specify WINS server address(es) in a DHCP address pool.

Use the **undo nbns-list** command to remove the specified WINS server address(es).

By default, no WINS server address is specified.

If you use the **nbns-list** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**, **netbios-type**.

## Examples

```
# Specify WINS server address 10.12.1.99 in DHCP address pool 0.
```

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] nbns-list 10.12.1.99
```

## netbios-type

### Syntax

```
netbios-type { b-node | h-node | m-node | p-node }
```

```
undo netbios-type
```

### View

DHCP address pool view

### Default Level

2: System level

### Parameters

**b-node**: Broadcast node. A b-node client sends the destination name in a broadcast message. The destination returns the name-to-IP mapping to the client after receiving the message.

**p-node**: Peer-to-peer node. A p-node client sends the destination name in a unicast message to the WINS server, and the WINS server returns the mapping to the client.

**m-node**: Mixed node, a combination of a b-node first and p-node second. An m-node client broadcasts the destination name, if there is no response, and then unicasts the destination name to the WINS server to get the mapping.

**h-node**: Hybrid node, a combination of a p-node first and b-node second. An h-node is a b-node with the peer-to-peer communication mechanism. An h-node client unicasts the destination name to the WINS server, if there is no response, and then broadcasts it to get the mapping from the destination.

## Description

Use the **netbios-type** command to specify the client NetBIOS node type in a DHCP address pool.

Use the **undo netbios-type** command to remove the specified client NetBIOS node type.

By default, no NetBIOS node type is specified.

Related commands: **dhcp server ip-pool**, **nbns-list**.

## Examples

```
# Specify the NetBIOS node type as b-node in DHCP address pool 0.
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] netbios-type b-node
```

## network

### Syntax

```
network network-address [ mask-length | mask mask ]
undo network
```

### View

DHCP address pool view

### Default Level

2: System level

### Parameters

*network-address*: IP address range for dynamic allocation. If no mask length and mask is specified, the natural mask will be used.

*mask-length*: Mask length, in the range of 1 to 30.

**mask** *mask*: Specifies the IP address network mask, in dotted decimal format.

### Description

Use the **network** command to specify the IP address range for dynamic allocation in a DHCP address pool.

Use the **undo network** command to remove the specified address range.

No IP address range is specified by default.

Note that you can specify only one network segment for each common address pool. If you use the **network** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**, **dhcp server forbidden-ip**.

## Examples

```
# Specify 192.168.8.0/24 as the address range for dynamic allocation in DHCP address pool 0.
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] network 192.168.8.0 mask 255.255.255.0
```

## network ip range

### Syntax

```
network ip range min-address max-address
undo network ip range [ min-address max-address ]
```

## View

DHCP address pool view

## Default Level

2: System level

## Parameters

*min-address*: Lowest IP address for dynamic allocation.

*max-address*: Highest IP address for dynamic allocation.

## Description

Use the **network ip range** command to specify the IP address range for dynamic allocation in an extended address pool.

Use the **undo network ip range** command to remove the specified address range.

No IP address range is specified by default.

Note that:

- Only the extended address pools support this command.
- You can specify only one IP address range for each extended address pool. If you use the **network ip range** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**.

## Examples

# Specify 192.168.8.1 through 192.168.8.150 as the address range for dynamic allocation in extended address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0 extended
[Sysname-dhcp-pool-0] network ip range 192.168.8.1 192.168.8.150
```

## network mask

### Syntax

**network mask** *mask*

**undo network mask** [ *mask* ]

### View

DHCP address pool view

### Default Level

2: System level

### Parameters

*mask*: Network mask, in dotted decimal notation.

## Description

Use the **network mask** command to specify the IP address mask for dynamic allocation in an extended address pool.

Use the **undo network mask** command to remove the specified IP address mask.

No IP address mask is specified by default.

Note that:

- Only the extended address pools support this command.
- If you specify an IP address range for an extended address pool without an IP address mask, the extended address pool is not valid, and therefore the system cannot assign IP addresses from the extended address pool.

Related commands: **dhcp server ip-pool**, **network ip range**.

## Examples

# Specify 255.255.255.0 as the IP address mask for dynamic allocation in extended address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0 extended
[Sysname-dhcp-pool-0] network mask 255.255.255.0
```

## option

### Syntax

```
option code { ascii ascii-string | hex hex-string&<1-16> | ip-address ip-address&<1-8> }
undo option code
```

### View

DHCP address pool view

### Default Level

2: System level

### Parameters

**code**: Self-defined option number, in the range of 2 to 254, excluding 12, 50 to 55, 57 to 61, and 82.

**ascii** *ascii-string*: Specifies an ASCII string with 1 to 63 characters.

**hex** *hex-string*&<1-16>: Specifies hex digit strings. &<1-16> indicates that you can specify up to 16 hex digit strings, separated by spaces. Each string contains 2, 4, 6 or 8 hex digits.

**ip-address** *ip-address*&<1-8>: Specifies IP addresses. &<1-8> indicates that you can specify up to eight IP addresses, separated by spaces.

## Description

Use the **option** command to configure a self-defined DHCP option in a DHCP address pool.

Use the **undo option** command to remove a self-defined DHCP option from a DHCP address pool.

The **option** command is not configured by default.

If you use the **option** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**.

## Examples

```
# Configure the hex digits 0x11 and 0x22 for the self-defined DHCP Option 100 in DHCP address pool 0.
```

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] option 100 hex 11 22
```

## reset dhcp server conflict

### Syntax

```
reset dhcp server conflict { all | ip ip-address }
```

### View

User view

### Default Level

2: System level

### Parameters

**all**: Clears the statistics of all IP address conflicts.

**ip *ip-address***: Clears the conflict statistics of a specified IP address.

### Description

Use the **reset dhcp server conflict** command to clear statistics of IP address conflict(s).

Related commands: **display dhcp server conflict**.

### Examples

```
# Clears the statistics of all IP address conflicts.
<Sysname> reset dhcp server conflict all
```

## reset dhcp server ip-in-use

### Syntax

```
reset dhcp server ip-in-use { all | ip ip-address | pool [ pool-name ] }
```

### View

User view

### Default Level

2: System level

### Parameters

**all**: Clears the IP address dynamic binding information of all DHCP address pools.

**ip *ip-address***: Clears the dynamic binding information of a specified IP address.

**pool** [ *pool-name* ]: Clears the dynamic binding information of a specified address pool. The *pool name* is a string of 1 to 35 characters. If no *pool name* is specified, the dynamic binding information of all address pools is cleared.

### Description

Use the **reset dhcp server ip-in-use** command to clear dynamic IP address binding information.

Related commands: **display dhcp server ip-in-use**

### Examples

```
# Clear the binding information of IP address 10.110.1.1.  
<Sysname> reset dhcp server ip-in-use ip 10.110.1.1
```

## reset dhcp server statistics

### Syntax

```
reset dhcp server statistics
```

### View

User view

### Default Level

2: System level

### Parameters

None

### Description

Use the **reset dhcp server statistics** command to clear the statistics of the DHCP server.

Related commands: **display dhcp server statistics**.

### Examples

```
# Clear the statistics of the DHCP server.  
<Sysname> reset dhcp server statistics
```

## static-bind client-identifier

### Syntax

```
static-bind client-identifier client-identifier  
undo static-bind client-identifier
```

### View

DHCP address pool view

### Default Level

2: System level

## Parameters

*client-identifier*: The client ID of a static binding, a string with 4 to 160 characters in the format of H-H-H..., each H indicates 4 hex digits except the last H indicates 2 or 4 hex digits. For example, aabb-cccc-dd is a valid ID, while aabb-c-dddd and aabb-cc-dddd are both invalid.

## Description

Use the **static-bind client-identifier** command to specify the client ID of a static binding in a DHCP address pool.

Use the **undo static-bind client-identifier** command to remove the client ID of a static binding from a DHCP address pool.

By default, no client ID is specified.

Note that:

- Use the **static-bind client-identifier** command together with the **static-bind ip-address** command to accomplish a static binding configuration.
- The ID of the static binding of a client must be identical to the ID displayed by using the **display dhcp client verbose** command on the client. Otherwise, the client cannot obtain an IP address.
- If you use the **static-bind client-identifier** or **static-bind mac-address** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**, **static-bind ip-address**, **static-bind mac-address**, **display dhcp client verbose**.

## Examples

# Bind the client ID aaaa-bbbb to the IP address 10.1.1.1 with the mask 255.255.255.0 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[Sysname-dhcp-pool-0] static-bind client-identifier aaaa-bbbb
```

## static-bind ip-address

### Syntax

**static-bind ip-address** *ip-address* [ *mask-length* | **mask** *mask* ]

**undo static-bind ip-address**

### View

DHCP address pool view

### Default Level

2: System level

### Parameters

*ip-address*: IP address of a static binding. If no mask and mask length is specified, the natural mask is used.

*mask-length*: Mask length of the IP address, that is, the number of ones in the mask, in the range of 0 to 32.

**mask** *mask*: Specifies the IP address mask, in dotted decimal format.

## Description

Use the **static-bind ip-address** command to specify an IP address in a DHCP address pool for a static binding.

Use the **undo static-bind ip-address** command to remove the statically bound IP address.

By default, no IP address is statically bound in a DHCP address pool.

Note that:

- Use the **static-bind ip-address** command together with the **static-bind mac-address** or **static-bind client-identifier** command to accomplish a static binding configuration.
- The IP address of the static binding cannot be an interface address of the DHCP server. Otherwise, an IP address conflict may occur, and the bound client cannot obtain an IP address correctly.
- If you use the **static-bind ip-address** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**, **static-bind client-identifier**, **static-bind mac-address**.

## Examples

# Bind the client MAC address 0000-e03f-0305 to the IP address 10.1.1.1 with the mask 255.255.255.0 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[Sysname-dhcp-pool-0] static-bind mac-address 0000-e03f-0305
```

## static-bind mac-address

### Syntax

**static-bind mac-address** *mac-address*

**undo static-bind mac-address**

### View

DHCP address pool view

### Default Level

2: System level

### Parameters

*mac-address*: The MAC address of a static binding, in the format of H-H-H.

## Description

Use the **static-bind mac-address** command to statically bind a MAC address to an IP address in a DHCP address pool.

Use the **undo static-bind mac-address** command to remove the statically bound MAC address.

By default, no MAC address is statically bound.

Note that:

- Use the **static-bind mac-address** command together with the **static-bind ip-address** command to complete a static binding configuration.
- If you use the **static-bind mac-address** or **static-bind client-identifier** command repeatedly, the latest configuration will overwrite the previous one.

Relate command: **dhcp server ip-pool**, **static-bind client-identifier** and **static-bind ip-address**.

## Examples

# Bind the client MAC address 0000-e03f-0305 to the IP address 10.1.1.1 with the mask 255.255.255.0 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[Sysname-dhcp-pool-0] static-bind mac-address 0000-e03f-0305
```

## tftp-server domain-name

### Syntax

```
tftp-server domain-name domain-name
undo tftp-server domain-name
```

### View

DHCP address pool view

### Default Level

2: System level

### Parameters

*domain-name*: TFTP server name, a string of 1 to 63 characters.

### Description

Use the **tftp-server domain-name** command to specify a TFTP server name in a DHCP address pool.

Use the **undo tftp-server domain-name** command to remove the TFTP server name from a DHCP address pool.

By default, no TFTP server name is specified.

Using the **tftp-server domain-name** command repeatedly will overwrite the previous configuration.

## Examples

# Specify the TFTP server name as aaa in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] tftp-server domain-name aaa
```

## tftp-server ip-address

### Syntax

```
tftp-server ip-address ip-address  
undo tftp-server ip-address
```

### View

DHCP address pool view

### Default Level

2: System level

### Parameters

*ip-address*: TFTP server IP address.

### Description

Use the **tftp-server ip-address** command to specify the TFTP server IP address in a DHCP address pool.

Use the **undo tftp-server ip-address** command to remove the TFTP server IP address from a DHCP address pool.

By default, no TFTP server address is specified.

Using the **tftp-server ip-address** command repeatedly will overwrite the previous configuration.

### Examples

```
# Specify the TFTP server address 10.1.1.1 in DHCP address pool 0.  
<Sysname> system-view  
[Sysname] dhcp server ip-pool 0  
[Sysname-dhcp-pool-0] tftp-server ip-address 10.1.1.1
```

## voice-config

### Syntax

```
voice-config { as-ip ip-address | fail-over ip-address dialer-string | ncp-ip ip-address | voice-vlan  
vlan-id { disable | enable } }  
undo voice-config [ as-ip | fail-over | ncp-ip | voice-vlan ]
```

### View

DHCP address pool view

### Default Level

2: System level

### Parameters

**as-ip ip-address**: Specifies IP address for the backup network calling processor.

**fail-over ip-address dialer-string**: Specifies the failover IP address and dialer string. The *dialer-string* is a string of 1 to 39 characters, which can be 0 to 9, and “\*”.

**ncp-ip** *ip-address*: Specifies IP address for the primary network calling processor.

**voice-vlan** *vlan-id*: Specifies the voice VLAN ID, in the range of 2 to 4094.

- **disable**: Disables the specified voice VLAN ID, meaning DHCP clients will not take this ID as their voice VLAN.
- **enable**: Enables the specified voice VLAN ID, meaning DHCP clients will take this ID as their voice VLAN.

## Description

Use the **voice-config** command to configure specified Option 184 contents in a DHCP address pool.

Use the **undo voice-config** command to remove specified Option 184 contents from a DHCP address pool.

By default, no Option 184 content is configured.

Note that specifying the IP address of a network calling processor first is necessary to make other configured parameters take effect.

## Examples

# Configure Option 184 in DHCP address pool 0: the primary network calling processor 10.1.1.1, backup network calling processor 10.2.2.2, voice VLAN ID 3 that is enabled, the failover IP address 10.3.3.3 and dialer string 99\*.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] voice-config ncp-ip 10.1.1.1
[Sysname-dhcp-pool-0] voice-config as-ip 10.2.2.2
[Sysname-dhcp-pool-0] voice-config voice-vlan 3 enable
[Sysname-dhcp-pool-0] voice-config fail-over 10.3.3.3 99*
```

# 2 DHCP Relay Agent Configuration Commands

---



## Note

- The DHCP relay agent configuration is supported only on VLAN interfaces.
  - DHCP snooping cannot be configured on the DHCP relay agent.
- 

## DHCP Relay Agent Configuration Commands

### dhcp relay address-check

#### Syntax

```
dhcp relay address-check { disable | enable }
```

#### View

Interface view

#### Default Level

2: System level

#### Parameters

**disable**: Disables IP address match check on the relay agent.

**enable**: Enables IP address match check on the relay agent.

#### Description

Use the **dhcp relay address-check enable** command to enable IP address match check on the relay agent.

Use the **dhcp relay address-check disable** command to disable IP address match check on the relay agent.

By default, the function is disabled.

If a requesting client's IP and MAC addresses do not match any binding (both dynamic and static bindings) on the DHCP relay agent, the client cannot access external networks via the DHCP relay agent.

Note that: The **dhcp relay address-check enable** command only checks IP and MAC addresses of clients.

#### Examples

```
# Enable IP address match check on the DHCP relay agent.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay address-check enable
```

## dhcp relay information circuit-id format-type

### Syntax

```
dhcp relay information circuit-id format-type { ascii | hex }
undo dhcp relay information circuit-id format-type
```

### View

Interface view

### Default Level

2: System level

### Parameters

**ascii**: Specifies the code type for the circuit ID sub-option as **ascii**.

**hex**: Specifies the code type for the circuit ID sub-option as **hex**.

### Description

Use the **dhcp relay information circuit-id format-type** command to configure the code type for the non-user-defined circuit ID sub-option.

Use the **undo dhcp relay information circuit-id format-type** command to restore the default.

By default, the code type for the circuit ID sub-option depends on the specified padding format of Option 82. Each field has its own code type.

Note that:

This command applies to configuring the non-user-defined circuit ID sub-option only. After you configure the padding content for the circuit ID sub-option using the **dhcp relay information circuit-id string** command, ASCII is adopted as the code type.

### Examples

# Configure the code type for the non-user-defined circuit ID sub-option as **ascii**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information circuit-id format-type ascii
```

## dhcp relay information circuit-id string

### Syntax

```
dhcp relay information circuit-id string circuit-id
undo dhcp relay information circuit-id string
```

### View

Interface view

## Default Level

2: System level

## Parameters

*circuit-id*: Padding content for the user-defined circuit ID sub-option, a case-sensitive string of 3 to 63 characters.

## Description

Use the **dhcp relay information circuit-id string** command to configure the padding content for the user-defined circuit ID sub-option.

Use the **undo dhcp relay information circuit-id string** command to restore the default.

By default, the padding content for the circuit ID sub-option depends on the padding format of Option 82.

Note that:

After you configure the padding content for the circuit ID sub-option using this command, ASCII is adopted as the code type.

Related commands: **dhcp relay information format**.

## Examples

```
# Configure the padding content for the circuit ID sub-option as company001.
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information circuit-id string company001
```

## dhcp relay information enable

### Syntax

```
dhcp relay information enable
undo dhcp relay information enable
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **dhcp relay information enable** command to enable the relay agent to support Option 82.

Use the **undo dhcp relay information enable** command to disable Option 82 support.

By default, Option 82 support is disabled on DHCP relay agent.

## Examples

```
# Enable Option 82 support on the relay agent.  
<Sysname> system-view  
[Sysname] interface vlan-interface 1  
[Sysname-Vlan-interface1] dhcp relay information enable
```

## dhcp relay information format

### Syntax

**dhcp relay information format** { **normal** | **verbose** [ **node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* } ] }

**undo dhcp relay information format** [ **verbose** **node-identifier** ]

### View

Interface view

### Default Level

2: System level

### Parameters

**normal**: Specifies the normal padding format.

**verbose**: Specifies the verbose padding format.

**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }: Specifies access node identifier. By default, the node MAC address is used as the node identifier.

- **mac** indicates using MAC address as the node identifier.
- **sysname** indicates using the device name of a node as the node identifier.
- **user-defined** *node-identifier* indicates using a specified character string as the node identifier, in which *node-identifier* is a string with 1 to 50 characters.

### Description

Use the **dhcp relay information format** command to specify a padding format for Option 82.

Use the **undo dhcp relay information format** command to restore the default padding format.

The Option 82 padding format defaults to **normal**.



## Note

- Using the **undo dhcp relay information format** command without the keyword **verbose node-identifier** restores the default **normal** padding format, or with the keyword **verbose node-identifier** restores the **mac** mode of the **verbose** padding format.
  - If configuring the handling strategy of the DHCP relay agent as **replace**, you need to configure a padding format of Option 82. If the handling strategy is **keep** or **drop**, you need not configure any padding format.
  - If sub-option 1 (node identifier) of Option 82 is padded with the device name (sysname) of a node, the device name must contain no spaces. Otherwise, the DHCP relay agent will drop the message.
- 

## Examples

```
# Specify the verbose padding format for Option 82.
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information enable
[Sysname-Vlan-interface1] dhcp relay information strategy replace
[Sysname-Vlan-interface1] dhcp relay information format verbose
```

## dhcp relay information remote-id format-type

### Syntax

```
dhcp relay information remote-id format-type { ascii | hex }
undo dhcp relay information remote-id format-type
```

### View

Interface view

### Default Level

2: System view

### Parameters

**ascii**: Specifies the code type for the remote ID sub-option as **ascii**.

**hex**: Specifies the code type for the remote ID sub-option as **hex**.

### Description

Use the **dhcp relay information remote-id format-type** command to configure the code type for the non-user-defined remote ID sub-option.

Use the **undo dhcp relay information remote-id format-type** command to restore the default.

By default, the code type for the remote ID sub-option is HEX.

Note that:

This command applies to configuring the non-user-defined remote ID sub-option only. After you configure the padding content for the remote ID sub-option using the **dhcp relay information remote-id string** command, ASCII is adopted as the code type.

## Examples

# Configure the code type for the non-user-defined remote ID sub-option as **ascii**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information remote-id format-type ascii
```

## dhcp relay information remote-id string

### Syntax

```
dhcp relay information remote-id string { remote-id | sysname }
undo dhcp relay information remote-id string
```

### View

Interface view

### Default Level

2: System level

### Parameters

*remote-id*: Padding content for the user-defined remote ID sub-option, a case sensitive string of 1 to 63 characters.

**sysname**: Specifies the device name as the padding content for the remote ID sub-option.

### Description

Use the **dhcp relay information remote-id string** command to configure the padding content for the user-defined remote ID sub-option.

Use the **undo dhcp relay information remote-id string** command to restore the default.

By default, the padding content for the remote ID sub-option depends on the padding format of Option 82.

Note that: After you configure the padding content for the remote ID sub-option using this command, ASCII is adopted as the code type.

Related commands: **dhcp relay information format**.



### Note

If you want to specify the character string **sysname** (a case-insensitive character string) as the padding content for the remote ID sub-option, you need to use quotation marks to make it take effect. For example, if you want to specify **Sysname** as the padding content for the remote ID sub-option, you need to enter the **dhcp relay information remote-id string "Sysname"** command.

---

## Examples

```
# Configure the padding content for the remote ID sub-option as device001.
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information remote-id string device001
```

## dhcp relay information strategy

### Syntax

```
dhcp relay information strategy { drop | keep | replace }
undo dhcp relay information strategy
```

### View

Interface view

### Default Level

2: System level

### Parameters

**drop**: Specifies to drop messages containing Option 82.

**keep**: Specifies to forward messages containing Option 82 without any change.

**replace**: Specifies to forward messages containing Option 82 after replacing the original Option 82 with the Option 82 padded in the specified padding format.

### Description

Use the **dhcp relay information strategy** command to configure DHCP relay agent handling strategy for messages containing Option 82.

Use the **undo dhcp relay information strategy** command to restore the default handling strategy.

The handling strategy for messages containing Option 82 defaults to **replace**.

## Examples

```
# Configure the DHCP relay agent handling strategy for messages containing Option 82 as keep.
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information enable
[Sysname-Vlan-interface1] dhcp relay information strategy keep
```

## dhcp relay release ip

### Syntax

```
dhcp relay release ip client-ip
```

### View

System view

## Default Level

2: System level

## Parameters

*client-ip*: DHCP client IP address.

## Description

Use the **dhcp relay release ip** command to request the DHCP server to release a specified client IP address.

## Examples

```
# Request the DHCP server to release the IP address 1.1.1.1.
```

```
<Sysname> system-view
```

```
[Sysname] dhcp relay release ip 1.1.1.1
```

## dhcp relay security static

### Syntax

```
dhcp relay security static ip-address mac-address [ interface interface-type interface-number ]  
undo dhcp relay security { ip-address | all | dynamic | interface interface-type interface-number | static }
```

### View

System view

## Default Level

2: System level

## Parameters

*ip-address*: Client IP address for creating a static binding.

*mac-address*: Client MAC address for creating a static binding, in the format H-H-H.

**interface** *interface-type interface-number*. Specifies a Layer 3 interface connecting to the DHCP client. *interface-type interface-number* specifies the interface type and interface number.

**all**: Specifies all client entries to be removed.

**dynamic**: Specifies dynamic client entries to be removed.

**static**: Specifies manual client entries to be removed.

## Description

Use the **dhcp relay security static** command to configure a static client entry, that is, the binding between IP address, MAC address, and Layer 3 interface on the relay agent.

Use the **undo dhcp relay security** command to remove specified client entries from the relay agent.

No manual client entry is configured on the DHCP relay agent by default.

Note that:

- When using the **dhcp relay security static** command to bind an interface to a static client entry, make sure that the interface is configured as a DHCP relay agent; otherwise, entry conflicts may occur.
- The **undo dhcp relay security interface** command is used to remove all the dynamic client entries from the interface.

Related commands: **display dhcp relay security**.

## Examples

# Bind DHCP relay interface VLAN-interface 2 to IP address 10.10.1.1 and MAC address 0005-5d02-f2b3 of the client.

```
<Sysname> system-view
[Sysname] dhcp relay security static 10.10.1.1 0005-5d02-f2b3 interface vlan-interface 2
```

## dhcp relay security tracker

### Syntax

```
dhcp relay security tracker { interval | auto }
undo dhcp relay security tracker [ interval ]
```

### View

System view

### Default Level

2: System level

### Parameters

*interval*: Refreshing interval in seconds, in the range of 1 to 120.

**auto**: Specifies the **auto** refreshing interval, which is the value of 60 seconds divided by the number of binding entries. Thus, the more entries are, the shorter interval is, but the shortest interval is no less than 500 ms.

### Description

Use the **dhcp relay security tracker** command to set a refreshing interval at which the relay agent contacts the DHCP server for refreshing dynamic bindings.

Use the **undo dhcp relay security tracker** command to restore the default interval.

The default refreshing interval is **auto**, the value of 60 seconds divided by the number of binding entries.

## Examples

# Set the refreshing interval as 100 seconds.

```
<Sysname> system-view
[Sysname] dhcp relay security tracker 100
```

## dhcp relay server-detect

### Syntax

```
dhcp relay server-detect
```

## undo dhcp relay server-detect

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **dhcp relay server-detect** command to enable unauthorized DHCP server detection.

Use the **undo dhcp relay server-detect** command to disable unauthorized DHCP server detection.

By default, unauthorized DHCP server detection is disabled.

With this function enabled, upon receiving a DHCP request, the DHCP relay agent will record the IP addresses of all DHCP servers which ever offered IP addresses to the DHCP client and the receiving interface. Each server detected is recorded only once. The administrator can get this information from logs to check out unauthorized DHCP servers.

After the information of recorded DHCP servers is cleared, the relay agent will re-record server information following this mechanism.

### Examples

# Enable unauthorized DHCP server detection.

```
<Sysname> system-view  
[Sysname] dhcp relay server-detect
```

## dhcp relay server-group

### Syntax

```
dhcp relay server-group group-id ip ip-address  
undo dhcp relay server-group group-id [ip ip-address ]
```

### View

System view

### Default Level

2: System level

### Parameters

*group-id*: DHCP server group number, in the range of 0 to 19.

**ip** *ip-address*: DHCP server IP address.

### Description

Use the **dhcp relay server-group** command to specify a DHCP server for a DHCP server group.

Use the **undo dhcp relay server-group** command to remove a DHCP server from a DHCP server group, if no **ip ip-address** is specified, all servers in the DHCP server group and the server group itself will be removed.

By default, no DHCP server is specified for a DHCP server group.

Note that:

- The IP address of any DHCP server and any interface's IP address of the DHCP relay agent cannot be in the same network segment. Otherwise, the client may fail to obtain an IP address.
- If a server group has been correlated to multiple interfaces, you need to cancel these correlations before removing the server group.

Related commands: **display dhcp relay server-group**.

## Examples

```
# Specify DHCP server 1.1.1.1 for DHCP server group 1 on the relay agent.
```

```
<Sysname> system-view
```

```
[Sysname] dhcp relay server-group 1 ip 1.1.1.1
```

## dhcp relay server-select

### Syntax

```
dhcp relay server-select group-id
```

```
undo dhcp relay server-select
```

### View

Interface view

### Default Level

2: System level

### Parameters

*group-id*: DHCP server group number to be correlated, in the range of 0 to 19.

### Description

Use the **dhcp relay server-select** command to correlate specified interface(s) to a specified DHCP server group.

Use the **undo dhcp relay server-select** command to remove a configured correlation.

By default, no DHCP server group is correlated with an interface on the relay agent.

Note that:

- A DHCP server group can correlate with one or multiple DHCP relay agent interfaces.
- A relay agent interface can only correlate with one DHCP server group, and a newly configured correlation overwrites the previous one. If the server group in the new correlation does not exist, the new configuration will not work. The interface still maintains the previous correlation.
- The DHCP server group referenced in this command should have been configured by using the **dhcp relay server-group** command.

Related commands: **dhcp relay server-group**.

## Examples

```
# Correlate VLAN-interface 1 to DHCP server group 1.
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay server-select 1
```

## dhcp select relay

### Syntax

```
dhcp select relay
undo dhcp select relay
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **dhcp select relay** command to enable the relay agent on the current interface. Upon receiving requests from an enabled interface, the relay agent will forward these requests to outside DHCP servers for IP address allocation.

Use the **undo dhcp select relay** command to restore the default.

After DHCP is enabled, the DHCP server is enabled on an interface by default. That is, upon receiving a client's request from the interface, the DHCP server allocates an IP address from the DHCP address pool to the client.

When the working mode of the interface is changed from DHCP server to DHCP relay agent, neither the IP address leases nor the authorized ARP entries will be deleted. However, these ARP entries may conflict with new ARP entries generated on the DHCP relay agent; therefore, you are recommended to delete the existing IP address leases when changing the interface working mode to DHCP relay agent.

## Examples

```
# Enable the DHCP relay agent on VLAN-interface 1.
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp select relay
```

## display dhcp relay

### Syntax

```
display dhcp relay { all | interface interface-type interface-number }
```

## View

Any view

## Default Level

1: Monitor level

## Parameters

**all**: Displays information of DHCP server groups that all interfaces correspond to.

**interface** *interface-type interface-number*: Displays information of the DHCP server group that a specified interface corresponds to.

## Description

Use the **display dhcp relay** command to display information about DHCP server groups correlated to an interface or all interfaces.

## Examples

# Display information about DHCP server groups correlated to all interfaces.

```
<Sysname> display dhcp relay all
      Interface name          Server-group
      Vlan-interface1        2
```

**Table 2-1 display dhcp relay all** command output description

Field	Description
Interface name	Interface name
Server-group	DHCP server group number correlated to the interface.

## display dhcp relay information

### Syntax

```
display dhcp relay information { all | interface interface-type interface-number }
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**all**: Displays the Option 82 configuration information of all interfaces.

**interface** *interface-type interface-number*: Displays the Option 82 configuration information of a specified interface.

## Description

Use the **display dhcp relay information** command to display Option 82 configuration information on the DHCP relay agent.

## Examples

# Display the Option 82 configuration information of all interfaces.

```
<Sysname> display dhcp relay information all
Interface: Vlan-interface100
    Status: Enable
    Strategy: Replace
    Format: Verbose
    Circuit ID format-type: HEX
    Remote ID format-type: ASCII
    Node identifier: abaci
    User defined:
        Circuit ID: company001
Interface: Vlan-interface200
    Status: Enable
    Strategy: Keep
    Format: Normal
    Circuit ID format-type: HEX
    Remote ID format-type: ASCII
    User defined:
        Remote ID: device001
```

## display dhcp relay security

### Syntax

```
display dhcp relay security [ ip-address | dynamic | static ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ip-address*: Displays the binding information of an IP address.

**dynamic**: Displays information about dynamic bindings.

**static**: Displays information about static bindings.

## Description

Use the **display dhcp relay security** command to display information about bindings of DHCP relay agents. If no parameter is specified, information about all bindings will be displayed.

## Examples

```
# Display information about all bindings.
```

```
<Sysname> display dhcp relay security
IP Address      MAC Address     Type           Interface
10.1.1.1        00e0-0000-0001 Static         Vlan1
10.1.1.5        00e0-0000-0000 Static         Vlan2
--- 2 dhcp-security item(s) found ---
```

**Table 2-2 display dhcp relay security command output description**

Field	Description
IP Address	Client IP address
MAC Address	Client MAC address
Type	Type of binding, including dynamic, static, and temporary.
Interface	Layer 3 interface connecting to the DHCP client. If no interface is recorded in the binding entry, "N/A" is displayed.

## display dhcp relay security statistics

### Syntax

```
display dhcp relay security statistics
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display dhcp relay security statistics** command to display statistics information about bindings of DHCP relay agents.

## Examples

```
# Display statistics about bindings of DHCP relay agents.
```

```
<Sysname> display dhcp relay security statistics
Static Items      :1
Dynamic Items     :0
Temporary Items   :0
All Items         :1
```

**Table 2-3** display dhcp relay security statistics command output description

Field	Description
Static Items	Static binding items
Dynamic Items	Dynamic binding items
Temporary Items	Temporary binding items
All Items	All binding items

## display dhcp relay security tracker

### Syntax

```
display dhcp relay security tracker
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display dhcp relay security tracker** command to display the interval for refreshing dynamic bindings on the relay agent.

### Examples

```
# Display the interval for refreshing dynamic bindings on the relay agent.
```

```
<Sysname> display dhcp relay security tracker  
Current tracker interval : 10s
```

The interval is 10 seconds.

## display dhcp relay server-group

### Syntax

```
display dhcp relay server-group { group-id | all }
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*group-id*: Displays the information of the specified DHCP server group numbered from 0 to 19.

**all**: Displays the information of all DHCP server groups.

## Description

Use the **display dhcp relay server-group** command to display the configuration information of a specified or all DHCP server groups.

## Examples

# Display IP addresses of DHCP servers in DHCP server group 1.

```
<Sysname> display dhcp relay server-group 1
  No.           Group IP
  ---           -
  1             1.1.1.1
  2             1.1.1.2
```

**Table 2-4** display dhcp relay server-group command output description

Field	Description
No.	Sequence number
Group IP	IP address in the server group

## display dhcp relay statistics

### Syntax

```
display dhcp relay statistics [ server-group { group-id | all } ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*group-id*: Specifies a server group number in the range of 0 to 19 about which to display DHCP packet statistics.

**all**: Specifies all server groups about which to display DHCP packet statistics. Information for each group will be displayed.

## Description

Use the **display dhcp relay statistics** command to display DHCP packet statistics related to a specified or all DHCP server groups.

Note that if no parameter (**server-group** and **all**) is specified, all DHCP packet statistics on the relay agent will be displayed.

## Examples

# Display all DHCP packet statistics on the relay agent.

```
<Sysname> display dhcp relay statistics
  Bad packets received:          0
```

```

DHCP packets received from clients:      0
  DHCPDISCOVER packets received:         0
  DHCPREQUEST packets received:          0
  DHCPINFORM packets received:           0
  DHCPRELEASE packets received:          0
  DHCPDECLINE packets received:          0
  BOOTREQUEST packets received:          0
DHCP packets received from servers:      0
  DHCPOFFER packets received:            0
  DHCPACK packets received:              0
  DHCPNAK packets received:              0
  BOOTREPLY packets received:            0
DHCP packets relayed to servers:         0
  DHCPDISCOVER packets relayed:          0
  DHCPREQUEST packets relayed:           0
  DHCPINFORM packets relayed:            0
  DHCPRELEASE packets relayed:           0
  DHCPDECLINE packets relayed:           0
  BOOTREQUEST packets relayed:           0
DHCP packets relayed to clients:         0
  DHCPOFFER packets relayed:             0
  DHCPACK packets relayed:               0
  DHCPNAK packets relayed:               0
  BOOTREPLY packets relayed:            0
DHCP packets sent to servers:            0
  DHCPDISCOVER packets sent:             0
  DHCPREQUEST packets sent:              0
  DHCPINFORM packets sent:               0
  DHCPRELEASE packets sent:              0
  DHCPDECLINE packets sent:              0
  BOOTREQUEST packets sent:              0
DHCP packets sent to clients:            0
  DHCPOFFER packets sent:                 0
  DHCPACK packets sent:                  0
  DHCPNAK packets sent:                  0
  BOOTREPLY packets sent:                0

```

**# Display DHCP packet statistics related to every server group on the relay agent.**

```
<Sysname> display dhcp relay statistics server-group all
```

```

DHCP relay server-group          #0
  Packet type                    Packet number
Client -> Server:
  DHCPDISCOVER                   0
  DHCPREQUEST                     0
  DHCPINFORM                      0
  DHCPRELEASE                     0
  DHCPDECLINE                     0
  BOOTREQUEST                     0

```

```
Server -> Client:
    DHCP OFFER          0
    DHCPACK            0
    DHCPNAK            0
    BOOTPREPLY         0
```

## reset dhcp relay statistics

### Syntax

```
reset dhcp relay statistics [ server-group group-id ]
```

### View

User view

### Default Level

1: Monitor level

### Parameters

**server-group** *group-id*: Specifies a server group ID (in the range of 0 to 19) about which to remove statistics from the relay agent.

### Description

Use the **reset dhcp relay statistics** command to remove statistics from the relay agent.

If no **server-group** is specified, all statistics will be removed from the relay agent.

Related commands: **display dhcp relay statistics**.

### Examples

```
# Remove all statistics from the DHCP relay agent.
```

```
<Sysname> reset dhcp relay statistics
```

# 3 DHCP Client Configuration Commands

---



## Note

- The DHCP client configuration is supported only on VLAN interfaces.
  - When multiple VLAN interfaces having the same MAC address use DHCP for IP address acquisition via a relay agent, the DHCP server cannot be the Windows 2000 Server or Windows 2003 Server.
  - You are not recommended to enable both the DHCP client and the DHCP snooping on the same device. Otherwise, DHCP snooping entries may fail to be generated, or the DHCP client may fail to obtain an IP address.
- 

## DHCP Client Configuration Commands

### display dhcp client

#### Syntax

```
display dhcp client [ verbose ] [ interface interface-type interface-number ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

**verbose**: Specifies verbose DHCP client information to be displayed.

**interface** *interface-type interface-number*: Specifies an interface of which to display DHCP client information.

#### Description

Use the **display dhcp client** command to display DHCP client information. If no **interface** *interface-type interface-number* is specified, DHCP client information of all interfaces will be displayed.

#### Examples

```
# Display DHCP client information of all interfaces.
```

```
<Sysname> display dhcp client
```

```
Vlan-interface1 DHCP client information:
```

```
Current machine state: BOUND
```

```

Allocated IP: 40.1.1.20 255.255.255.0
Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
DHCP server: 40.1.1.2

```

**# Display verbose DHCP client information.**

```

<Sysname> display dhcp client verbose
Vlan-interface1 DHCP client information:
Current machine state: BOUND
Allocated IP: 40.1.1.20 255.255.255.0
Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
Lease from 2005.08.13 15:37:59 to 2005.08.16 15:37:59
DHCP server: 40.1.1.2
Transaction ID: 0x1c09322d
Default router: 40.1.1.2
Classless static route:
    Destination: 1.1.0.1, Mask: 255.0.0.0, NextHop: 192.168.40.16
    Destination: 10.198.122.63, Mask: 255.255.255.255, NextHop: 192.168.40.16
DNS server: 44.1.1.11
DNS server: 44.1.1.12
Domain name: ddd.com
Boot server: 200.200.200.200 1.1.1.1
Client ID: 3030-3066-2e65-3234-
          392e-3830-3438-2d56-
          6c61-6e2d-696e-7465-
          7266-6163-6531
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.

```

**Table 3-1 display dhcp client command output description**

Field	Description
Vlan-interface1 DHCP client information	Information of the interface acting as the DHCP client
Current machine state	DHCP client current machine state
Allocated IP	The IP address allocated by the DHCP server
Allocated lease	The allocated lease time
T1	The 1/2 lease time (in seconds) of the DHCP client IP address
T2	The 7/8 lease time (in seconds) of the DHCP client IP address
Lease from....to....	The start and end time of the lease.
DHCP Server	DHCP server IP address that assigned the IP address
Transaction ID	Transaction ID, a random number chosen by the client to identify an IP address allocation.
Default router	The gateway address assigned to the client
Classless static route	Classless static routes assigned to the client
Static route	Classful static routes assigned to the client
DNS server	The DNS server address assigned to the client
Domain name	The domain name suffix assigned to the client

Field	Description
Boot server	PXE server addresses (up to 16 addresses) specified for the DHCP client, which are obtained through Option 43.
Client ID	Client ID
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.	How long the T1 (1/2 lease time) timer will timeout.

## ip address dhcp-alloc

### Syntax

**ip address dhcp-alloc** [ **client-identifier mac** *interface-type interface-number* ]

**undo ip address dhcp-alloc**

### View

Interface view

### Default Level

2: System level

### Parameters

**client-identifier mac** *interface-type interface-number*: Specifies the MAC address of an interface using which as the client ID to obtain an IP address.

### Description

Use the **ip address dhcp-alloc** command to configure an interface to use DHCP for IP address acquisition.

Use the **undo ip address dhcp-alloc** command to cancel an interface from using DHCP.

By default, an interface does not use DHCP for IP address acquisition.

Note that:

- If no parameter is specified, the client uses a character string comprised of the current interface name and MAC address as its ID for address acquisition.
- The DHCP client sends a DHCP-RELEASE message for releasing the IP address obtained via DHCP, if the interface of the client is down, the message cannot be sent.
- For a sub interface that obtained an IP address via DHCP, using the **shutdown** command on its primary interface does not make the DHCP client send a DHCP-RELEASE message for releasing the sub interface's IP address.

### Examples

# Configure VLAN-interface 1 to use DHCP for IP address acquisition.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip address dhcp-alloc
```

# 4 DHCP Snooping Configuration Commands

---



## Note

- The DHCP snooping enabled device does not work if it is between the DHCP relay agent and DHCP server, and it can work when it is between the DHCP client and relay agent or between the DHCP client and server.
  - The DHCP snooping enabled device cannot be a DHCP server or DHCP relay agent.
  - You are not recommended to enable the DHCP client, BOOTP client, and DHCP snooping on the same device. Otherwise, DHCP snooping entries may fail to be generated, or the BOOTP client/DHCP client may fail to obtain an IP address.
- 

## DHCP Snooping Configuration Commands

### dhcp-snooping

#### Syntax

**dhcp-snooping**

**undo dhcp-snooping**

#### View

System view

#### Default Level

2: System level

#### Parameters

None

#### Description

Use the **dhcp-snooping** command to enable DHCP snooping.

Use the **undo dhcp-snooping** command to disable DHCP snooping.

With DHCP snooping disabled, all ports can forward responses from any DHCP servers and does not record binding information about MAC addresses of DHCP clients and the obtained IP addresses.

By default, DHCP snooping is disabled.

Related commands: **display dhcp-snooping**.

## Examples

```
# Enable DHCP snooping.
<Sysname> system-view
[Sysname] dhcp-snooping
```

## dhcp-snooping information circuit-id format-type

### Syntax

```
dhcp-snooping information circuit-id format-type { ascii | hex }
undo dhcp-snooping information circuit-id format-type
```

### View

Layer 2 Ethernet port view

### Default Level

2: System level

### Parameters

**ascii**: Specifies the code type for the circuit ID sub-option as **ascii**.

**hex**: Specifies the code type for the circuit ID sub-option as **hex**.

### Description

Use the **dhcp-snooping information circuit-id format-type** command to configure the code type for the non-user-defined circuit ID sub-option.

Use the **undo dhcp-snooping information circuit-id format-type** command to restore the default.

By default, the code type for the circuit ID sub-option depends on the padding format of Option 82. Each field has its own code type.

Note that:

This command applies to configuring the non-user-defined circuit ID sub-option only. After you configure the padding content for the circuit ID sub-option using the **dhcp-snooping information circuit-id string** command, ASCII is adopted as the code type.

## Examples

```
# Configure the padding format for the non-user-defined circuit ID sub-option as ascii.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information circuit-id format-type ascii
```

## dhcp-snooping information circuit-id string

### Syntax

```
dhcp-snooping information [ vlan vlan-id ] circuit-id string circuit-id
undo dhcp-snooping information [ vlan vlan-id ] circuit-id string
```

## View

Layer 2 Ethernet port view

## Default Level

2: System level

## Parameters

**vlan** *vlan-id*: Specifies a VLAN ID, in the range of 1 to 4094.

*circuit-id*: Padding content for the user-defined circuit ID sub-option, a case-sensitive string of 3 to 63 characters.

## Description

Use the **dhcp-snooping information circuit-id string** command to configure the padding content for the user-defined circuit ID sub-option.

Use the **undo dhcp-snooping information circuit-id string** command to restore the default.

By default, the padding content for the circuit ID sub-option depends on the padding format of Option 82.

Note that:

- After you configure the padding content for the circuit ID sub-option using this command, ASCII is adopted as the code type.
- If a VLAN is specified, the configured circuit ID sub-option only takes effect within the VLAN; if no VLAN is specified, the configured circuit ID sub-option takes effect in all VLANs. The former case has a higher priority; that is, the circuit ID sub-option specified for a VLAN will be padded for packets within the VLAN.

Related commands: **dhcp-snooping information format**.

## Examples

```
# Configure the global padding content for the user-defined circuit ID sub-option as company001.
```

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information circuit-id string company001
```

## dhcp-snooping information enable

### Syntax

**dhcp-snooping information enable**

**undo dhcp-snooping information enable**

### View

Layer 2 Ethernet interface view

### Default Level

2: System level

## Parameters

None

## Description

Use the **dhcp-snooping information enable** command to configure DHCP snooping to support Option 82.

Use the **undo dhcp-snooping information enable** command to disable this function.

By default, DHCP snooping does not support Option 82.

## Examples

# Configure DHCP snooping to support Option 82.

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information enable
```

## dhcp-snooping information format

### Syntax

```
dhcp-snooping information format { normal | verbose [ node-identifier { mac | sysname | user-defined node-identifier } ] }
```

```
undo dhcp-snooping information format [ verbose node-identifier ]
```

### View

Layer 2 Ethernet interface view

### Default Level

2: System level

## Parameters

**normal**: Specifies the normal padding format.

**verbose**: Specifies the verbose padding format.

**node-identifier { mac | sysname | user-defined node-identifier }**: Specifies access node identifier. By default, the node MAC address is used as the node identifier.

- **mac** indicates using MAC address as the node identifier.
- **sysname** indicates using the device name of a node as the node identifier.
- **user-defined node-identifier** indicates using a specified character string as the node identifier, in which *node-identifier* is a string of 1 to 50 characters.

## Description

Use the **dhcp-snooping information format** command to specify the padding format for Option 82.

Use the **undo dhcp-snooping information format** command to restore the default.

By default, the padding format for Option 82 is **normal**.

Note that when you use the **undo dhcp-snooping information format** command, if the **verbose node-identifier** argument is not specified, the padding format will be restored to **normal**; if the **verbose**

**node-identifier** argument is specified, the padding format will be restored to **verbose** with MAC address as the node identifier.

## Examples

# Specify the padding format as **verbose** for Option 82.

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information enable
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information strategy replace
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information format verbose
```

## dhcp-snooping information remote-id format-type

### Syntax

```
dhcp-snooping information remote-id format-type { ascii | hex }
undo dhcp-snooping information remote-id format-type
```

### View

Layer 2 Ethernet port view

### Default Level

2: System level

### Parameters

**ascii**: Specifies the code type for the remote ID sub-option as **ascii**.

**hex**: Specifies the code type for the remote ID sub-option as **hex**.

### Description

Use the **dhcp-snooping information remote-id format-type** command to configure the code type for the non-user-defined remote ID sub-option.

Use the **undo dhcp-snooping information remote-id format-type** command to restore the default.

By default, the code type for the remote ID sub-option is HEX.

Note that:

This command applies to configuring a non-user-defined remote ID sub-option only. After you configure the padding content for the remote ID sub-option using the **dhcp-snooping information remote-id string** command, ASCII is adopted as the code type.

## Examples

# Configure the code type for the non-user-defined remote ID sub-option as **ascii**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information remote-id format-type ascii
```

## dhcp-snooping information remote-id string

### Syntax

```
dhcp-snooping information [ vlan vlan-id ] remote-id string { remote-id | sysname }  
undo dhcp-snooping information [ vlan vlan-id ] remote-id string
```

### View

Layer 2 Ethernet port view

### Default Level

2: System level

### Parameters

**vlan** *vlan-id*: Specifies a VLAN ID, in the range of 1 to 4094.

*remote-id*: Padding content for the user-defined circuit ID sub-option, a case-sensitive string of 1 to 63 characters.

**sysname**: Specifies the device name as the padding content for the remote ID sub-option.

### Description

Use the **dhcp-snooping information remote-id string** command to configure the padding content for the user-defined remote ID sub-option.

Use the **undo dhcp-snooping information remote-id string** command to restore the default.

By default, the padding content for the remote ID sub-option depends on the padding format of Option 82.

Note that:

- After you configure the padding content for the remote ID sub-option using this command, ASCII is adopted as the code type.
- If a VLAN is specified, the configured remote ID sub-option only takes effect within the VLAN; if no VLAN is specified, the configured remote ID sub-option takes effect in all VLANs. The former case has a higher priority; that is, the remote ID sub-option configured for a VLAN will be padded for the packets within the VLAN.

Related commands: **dhcp-snooping information format**.



#### Note

If you want to specify the character string **sysname** (a case-insensitive character string) as the padding content for the remote ID sub-option, you need to use quotation marks to make it take effect. For example, if you want to specify **Sysname** as the padding content for the remote ID sub-option, you need to enter the **dhcp relay information remote-id string "Sysname"** command.

---

### Examples

```
# Configure the padding content for the remote ID sub-option as device001.
```

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information remote-id string device001
```

## dhcp-snooping information strategy

### Syntax

```
dhcp-snooping information strategy { drop | keep | replace }
undo dhcp-snooping information strategy
```

### View

Layer 2 Ethernet interface view

### Default Level

2: System level

### Parameters

**drop:** Drops the requesting message containing Option 82.

**keep:** Forwards the requesting message containing Option 82 without changing Option 82.

**replace:** Forwards the requesting message containing Option 82 after replacing the original Option 82 with the one padded in specified format.

### Description

Use the **dhcp-snooping information strategy** command to configure the handling strategy for Option 82 in requesting messages.

Use the **undo dhcp-snooping information strategy** command to restore the default.

By default, the handling strategy for Option 82 in requesting messages is **replace**.



#### Note

Support for this command depends on the device model.

---

### Examples

# Configure the handling strategy for Option 82 in requesting messages as **keep**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information enable
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information strategy keep
```

## dhcp-snooping trust

### Syntax

```
dhcp-snooping trust [ no-user-binding ]
```

## undo dhcp-snooping trust

### View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

### Default Level

2: System level

### Parameters

**no-user-binding**: Specifies the port not to record the clients' IP-to-MAC bindings in DHCP requests it receives. The command without this keyword records the IP-to-MAC bindings of clients.

### Description

Use the **dhcp-snooping trust** command to configure a port as a trusted port.

Use the **undo dhcp-snooping trust** command to restore the default state of a port.

All ports are untrusted by default.

After enabling DHCP snooping, you need to specify the ports connected to the valid DHCP servers as trusted to ensure that DHCP clients can obtain valid IP addresses.

Related commands: **display dhcp-snooping trust**.

### Examples

# Specify GigabitEthernet 1/0/1 as a trusted port and enable it to record the IP-to-MAC bindings of clients.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping trust
```

## display dhcp-snooping

### Syntax

```
display dhcp-snooping [ ip ip-address ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**ip *ip-address***: Displays the DHCP snooping entries corresponding to the specified IP address.

### Description

Use the **display dhcp-snooping** command to display DHCP snooping entries.



## Note

Only the DHCP snooping entries containing IP-to-MAC bindings that are present both in the DHCP-ACK and DHCP-REQUEST messages are displayed by using the **display dhcp-snooping** command.

## Examples

# Display all DHCP snooping entries.

```
<Sysname> display dhcp-snooping
DHCP Snooping is enabled.
The client binding table for all untrusted ports.
Type : D--Dynamic , S--Static
Type   IP Address      MAC Address      Lease      VLAN  Interface
====  =====
D      10.1.1.1         00e0-fc00-0006  286        1     GigabiEthernet1/0/1
---  1 dhcp-snooping item(s) found  ---
```

**Table 4-1 display dhcp snooping** command output description

Field	Description
Type	Binding type
IP Address	IP address assigned to the DHCP client
MAC Address	MAC address of the DHCP client
Lease	Lease period left (in seconds)
VLAN	VLAN where the port connecting the DHCP client resides
Interface	Port to which the DHCP client is connected

## display dhcp-snooping information

### Syntax

```
display dhcp-snooping information { all | interface interface-type interface-number }
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**all**: Displays the Option 82 configuration information of all Layer 2 Ethernet interfaces.

**interface** *interface-type interface-number*: Displays the Option 82 configuration information of a specified interface.

## Description

Use the **display dhcp-snooping information** command to display Option 82 configuration information on the DHCP snooping device.

## Examples

# Display the Option 82 configuration information of all interfaces.

```
<Sysname> display dhcp-snooping information all
Interface: GigabitEthernet 1/0/1
  Status: Enable
  Strategy: Replace
  Format: Verbose
  Circuit ID format-type: HEX
  Remote ID format-type: ASCII
  Node identifier: aabbcc
  User defined:
    Circuit ID: company001
Interface: GigabitEthernet 1/0/2
  Status: Disable
  Strategy: Keep
  Format: Normal
  Circuit ID format-type: HEX
  Remote ID format-type: ASCII
  User defined:
    Circuit ID: company001
    Remote ID: device001
  VLAN 10:
    Circuit ID: vlan10@company001
  VLAN 20:
    Remote ID: device001
```

## display dhcp-snooping packet statistics

### Syntax

```
display dhcp-snooping packet statistics [ slot slot-number ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**slot** *slot-number*. Displays the DHCP packet statistics of the specified device. If the device is in an IRF stack, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF stack, the *slot-number* argument represents the device ID.

## Description

Use the **display dhcp-snooping packet statistics** command to display DHCP packet statistics on the DHCP snooping device.

On a device in IRF stack, executing the **display dhcp-snooping packet statistics** command without the **slot** keyword only displays DHCP packet statistics on the device where the command is executed.

## Examples

# Display DHCP packet statistics on the DHCP snooping device.

```
<Sysname> display dhcp-snooping packet statistics
DHCP packets received           : 100
DHCP packets sent               : 200
Packets dropped due to rate limitation : 20
Dropped invalid packets        : 0
```

## display dhcp-snooping trust

### Syntax

```
display dhcp-snooping trust
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display dhcp-snooping trust** command to display information about trusted ports.

Related commands: **dhcp-snooping trust**.

## Examples

# Display information about trusted ports.

```
<Sysname> display dhcp-snooping trust
DHCP Snooping is enabled.
DHCP Snooping trust becomes active.
Interface                               Trusted
=====                               =====
GigabitEthernet1/0/1                   Trusted
```

The above output shows that DHCP snooping is enabled, DHCP snooping trust is active, and port GigabitEthernet 1/0/1 is trusted.

## reset dhcp-snooping

### Syntax

```
reset dhcp-snooping { all | ip ip-address }
```

### View

User view

### Default Level

1: Monitor level

### Parameters

**all**: Clears all DHCP snooping entries.

**ip ip-address**: Clears the DHCP snooping entries of the specified IP address.

### Description

Use the **reset dhcp-snooping** command to clear DHCP snooping entries.

For an IRF stack, DHCP snooping entries on all devices will be cleared after you execute this command.

### Examples

```
# Clear all DHCP snooping entries.
```

```
<Sysname> reset dhcp-snooping all
```

## reset dhcp-snooping packet statistics

### Syntax

```
reset dhcp-snooping packet statistics [ slot slot-number ]
```

### View

User view

### Default Level

2: System level

### Parameters

**slot slot-number**: Clears the DHCP packet statistics of the specified device. If the device is in an IRF stack, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF stack, the *slot-number* argument represents the device ID.

### Description

Use the **reset dhcp-snooping packet statistics** command to clear DHCP packet statistics on the DHCP snooping device.

On a device in IRF stack, executing the **reset dhcp-snooping packet statistics** command without the **slot** keyword only clears DHCP packet statistics on the device where the command is executed.

## Examples

# Clear DHCP packet statistics on the DHCP snooping device.

```
<Sysname> reset dhcp-snooping packet statistics
```

# 5 BOOTP Client Configuration Commands

---



## Note

- BOOTP client configuration can only be used on VLAN interfaces.
  - If several VLAN interfaces sharing the same MAC address obtain IP addresses through a BOOTP relay agent, the BOOTP server cannot be a Windows 2000 Server or Windows 2003 Server.
  - You are not recommended to enable both the DHCP client and the DHCP snooping on the same device. Otherwise, DHCP snooping entries may fail to be generated, or the BOOTP client may fail to obtain an IP address.
- 

## BOOTP Client Configuration Commands

### display bootp client

#### Syntax

```
display bootp client [ interface interface-type interface-number ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

**interface** *interface-type interface-number*: Displays the BOOTP client information of the interface.

#### Description

Use the **display bootp client** command to display related information about a BOOTP client.

Note:

- If **interface** *interface-type interface-number* is not specified, the command will display information about BOOTP clients on all interfaces.
- If **interface** *interface-type interface-number* is specified, the command will display information about the BOOTP client on the specified interface.

#### Examples

```
# Display related information of the BOOTP client on VLAN-interface 1.
```

```
<Sysname> display bootp client interface vlan-interface 1  
Vlan-interface1 BOOTP client information:
```

Allocated IP: 169.254.0.2 255.255.0.0

Transaction ID = 0x3d8a7431

Mac Address 00e0-fc0a-c3ef

**Table 5-1 display bootp client** command output description

Field	Description
Vlan-interface1 BOOTP client information	Information of the interface serving as a BOOTP client
Allocated IP	BOOTP client's IP address allocated by the BOOTP server
Transaction ID	Value of the <b>XID</b> field in a BOOTP message, namely, a random number chosen while the BOOTP client sends a BOOTP request to the BOOTP server. It is used to match a response message from the BOOTP server. If the values of the <b>XID</b> field are different in the BOOTP response and request, the BOOTP client will drop the BOOTP response.
Mac Address	MAC address of a BOOTP client

## ip address bootp-alloc

### Syntax

```
ip address bootp-alloc  
undo ip address bootp-alloc
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **ip address bootp-alloc** command to enable an interface to obtain an IP address through BOOTP.

Use the **undo ip address bootp-alloc** command to disable the interface from obtaining an IP address through BOOTP.

By default, an interface does not obtain an IP address through BOOTP.

Related commands: **display bootp client**.

### Examples

```
# Configure VLAN-interface 1 to obtain IP address through BOOTP protocol.
```

```
<Sysname> system-view  
[Sysname] interface vlan-interface 1  
[Sysname-Vlan-interface1] ip address bootp-alloc
```

# Table of Contents

<b>1 DNS Configuration Commands</b> .....	<b>1-1</b>
DNS Configuration Commands.....	1-1
display dns domain.....	1-1
display dns dynamic-host.....	1-2
display dns server.....	1-3
display ip host.....	1-4
dns domain.....	1-4
dns proxy enable.....	1-5
dns resolve.....	1-6
dns server.....	1-6
ip host.....	1-7
reset dns dynamic-host.....	1-7

# 1 DNS Configuration Commands

---



## Note

This document only covers IPv4 DNS configuration commands. For introduction to IPv6 DNS configuration commands, refer to *IPv6 Basics Commands* in the *IP Services Volume*.

---

## DNS Configuration Commands

### display dns domain

#### Syntax

```
display dns domain [ dynamic ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

**dynamic:** Displays the domain name suffixes dynamically obtained through DHCP or other protocols.

#### Description

Use the **display dns domain** command to display the domain name suffixes.

Related commands: **dns domain**.

#### Examples

```
# Display domain name suffixes.
```

```
<Sysname> display dns domain
```

```
Type:
```

```
D:Dynamic    S:Static
```

```
No.    Type    Domain-name
```

```
1      S       com
```

**Table 1-1 display dns domain** command output description

Field	Description
No	Sequence number
Type	Type of domain name suffix: S represents a statically configured domain name suffix, and D represents a domain name suffix obtained dynamically through DHCP.
Domain-name	Domain name suffix

## display dns dynamic-host

### Syntax

**display dns dynamic-host**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display dns dynamic-host** command to display the information of the dynamic domain name resolution cache.

### Examples

# Display the information of the dynamic domain name resolution cache.

```
<Sysname> display dns dynamic-host
```

No.	Host	IP Address	TTL
1	www.baidu.com	202.108.249.134	63000
2	www.yahoo.akadns.net	66.94.230.39	24
3	www.hotmail.com	207.68.172.239	3585
4	www.eyou.com	61.136.62.70	3591

**Table 1-2 display dns dynamic-host** command output description

Field	Description
No	Sequence number
Host	Domain name
IP Address	IP address for the corresponding domain name
TTL	Time that a mapping can be stored in the cache (in seconds).



## Note

A domain name in the **display dns dynamic-host** command contains 21 characters at most. If a domain name consists of more than 21 characters, only the first 21 characters are displayed.

## display dns server

### Syntax

```
display dns server [ dynamic ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**dynamic**: Displays the DNS server information dynamically obtained through DHCP or other protocols

### Description

Use the **display dns server** command to display the DNS server information.

Related commands: **dns server**.

### Examples

```
# Display the DNS server information.
```

```
<Sysname> display dns server
```

```
Type:
```

```
  D:Dynamic   S:Static
```

```
DNS Server  Type  IP Address
    1         S    169.254.65.125
```

**Table 1-3** display dns server command output description

Field	Description
DNS Server	Sequence number of the DNS server, configured automatically by the device, starting from 1.
Type	Type of domain name server: S represents a statically configured DNS server, and D represents a DNS server obtained dynamically through DHCP.
IP Address	IP address of the DNS server

## display ip host

### Syntax

**display ip host**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display ip host** command to display the host names and corresponding IP addresses in the static domain name resolution table.

### Examples

# Display the host names and corresponding IP addresses in the static domain name resolution table.

```
<Sysname> display ip host
```

Host	Age	Flags	Address
My	0	static	1.1.1.1
Aa	0	static	2.2.2.4

**Table 1-4 display ip host command output description**

Field	Description
Host	Host name
Age	Time to live. 0 means that the static mapping will never age out. You can only manually remove the static mappings between host names and IP addresses.
Flags	Indicates the mapping type. Static represents static domain name resolution.
Address	Host IP address

## dns domain

### Syntax

**dns domain** *domain-name*

**undo dns domain** [ *domain-name* ]

### View

System view

## Default Level

2: System level

## Parameters

*domain-name*: Domain name suffix, consisting of character strings separated by a dot (for example, aabbcc.com). Each separated string contains no more than 63 characters. A domain name suffix may include case-insensitive letters, digits, hyphens (-), underscores (\_), and dots (.), with a total length of 238 characters.

## Description

Use the **dns domain** command to configure a domain name suffix. The system can automatically add the suffix to part of the domain name you entered for resolution.

Use the **undo dns domain** command to delete a domain name suffix (with a domain name suffix specified) or all domain name suffixes (with no domain name suffix specified).

No domain name suffix is configured by default, that is, only the provided domain name is resolved.

You can configure a maximum of 10 domain name suffixes.

Related commands: **display dns domain**.

## Examples

```
# Configure com as a DNS suffix.
```

```
<Sysname> system-view
```

```
[Sysname] dns domain com
```

## dns proxy enable

### Syntax

```
dns proxy enable
```

```
undo dns proxy enable
```

### View

System view

## Default Level

2: System level

## Parameters

None

## Description

Use the **dns proxy enable** command to enable DNS proxy.

Use the **undo dns proxy enable** command to disable DNS proxy.

By default, DNS proxy is disabled.

## Examples

```
# Enable DNS proxy.
```

```
<Sysname> system-view
[Sysname] dns proxy enable
```

## dns resolve

### Syntax

```
dns resolve
undo dns resolve
```

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **dns resolve** command to enable dynamic domain name resolution.

Use the **undo dns resolve** command to disable dynamic domain name resolution.

Dynamic domain name resolution is disabled by default.

### Examples

# Enable dynamic domain name resolution.

```
<Sysname> system-view
[Sysname] dns resolve
```

## dns server

### Syntax

```
dns server ip-address
undo dns server [ ip-address ]
```

### View

System view

### Default Level

2: System level

### Parameters

*ip-address*: IP address of the DNS server.

### Description

Use the **dns server** command to specify a DNS server.

Use the **undo dns server** to remove DNS server(s).

No DNS server is specified by default.

You can configure a maximum of six DNS servers, including those with IPv6 addresses.

Related commands: **display dns server**.

## Examples

```
# Specify the DNS server 172.16.1.1.
```

```
<Sysname> system-view  
[Sysname] dns server 172.16.1.1
```

## ip host

### Syntax

```
ip host hostname ip-address  
undo ip host hostname [ ip-address ]
```

### View

System view

### Default Level

2: System level

### Parameters

*hostname*: Host name, consisting of 1 to 20 characters, including case-insensitive letters, numbers, hyphens (-), underlines (\_), or dots (.). The host name must include at least one letter.

*ip-address*: IP address of the specified host in dotted decimal notation.

### Description

Use the **ip host** command to create a host name to IP address mapping in the static resolution table.

Use the **undo ip host** command to remove a mapping.

No mappings are created by default.

You can configure only one mapping for a host name. A mapping newly configured for the host name will overwrite the previous one if there is any.

Related commands: **display ip host**.

## Examples

```
# Map the IP address 10.110.0.1 to the host name aaa.
```

```
<Sysname> system-view  
[Sysname] ip host aaa 10.110.0.1
```

## reset dns dynamic-host

### Syntax

```
reset dns dynamic-host
```

## View

User view

## Default Level

2: System level

## Parameters

None

## Description

Use the **reset dns dynamic-host** command to clear the dynamic domain name resolution information.

Related commands: **display dns dynamic-host**.

## Examples

# Clear the dynamic domain name resolution information.

```
<Sysname> reset dns dynamic-host
```

# Table of Contents

<b>1 IP Performance Optimization Configuration Commands</b> .....	<b>1-1</b>
IP Performance Optimization Configuration Commands.....	1-1
display fib.....	1-1
display fib <i>ip-address</i> .....	1-3
display icmp statistics.....	1-4
display ip socket.....	1-5
display ip statistics.....	1-8
display tcp statistics.....	1-10
display tcp status.....	1-12
display udp statistics.....	1-13
ip forward-broadcast (interface view).....	1-14
ip forward-broadcast (system view).....	1-15
ip redirects enable.....	1-15
ip ttl-expires enable.....	1-16
ip unreachable enable.....	1-16
reset ip statistics.....	1-17
reset tcp statistics.....	1-17
reset udp statistics.....	1-18
tcp timer fin-timeout.....	1-18
tcp timer syn-timeout.....	1-19
tcp window.....	1-20

# 1 IP Performance Optimization Configuration

## Commands

---

### IP Performance Optimization Configuration Commands

#### display fib

##### Syntax

```
display fib [ vpn-instance vpn-instance-name ] [ | { begin | include | exclude } regular-expression |  
acl acl-number | ip-prefix ip-prefix-name ]
```

##### View

Any view

##### Default Level

1: Monitor level

##### Parameters

**vpn-instance** *vpn-instance-name*: Displays FIB entries of the specified VPN instance. The *vpn-instance-name* is a string of 1 to 31 case-sensitive characters.

**|**: Uses a regular expression to match FIB entries. For detailed information about regular expression, refer to CLI display in *Basic System Configuration* in the *System Volume*.

**begin**: Displays the first entry that matches the specified regular expression and all the FIB entries following it.

**exclude**: Displays the FIB entries that do not match the specified regular expression.

**include**: Displays the FIB entries that match the specified regular expression.

*regular-expression*: A case-sensitive string of 1 to 256 characters, excluding spaces.

**acl** *acl-number*: Displays FIB entries matching a specified ACL numbered from 2000 to 2999. If the specified ACL does not exist, all FIB entries are displayed.

**ip-prefix** *ip-prefix-name*: Displays FIB entries matching a specified IP prefix list, a string of 1 to 19 characters. If the specified IP prefix list does not exist, all FIB entries are displayed.

##### Description

Use the **display fib** command to display FIB entries. If no parameters are specified, all FIB entries will be displayed.

##### Examples

```
# Display all FIB entries.  
<Sysname> display fib  
Destination count: 4    FIB entry count: 4
```

Flag:

U:Useable G:Gateway H:Host B:Blackhole D:Dynamic S:Static  
R:Relay

Destination/Mask	Nexthop	Flag	OutInterface	InnerLabel	Token
10.2.0.0/16	10.2.1.1	U	VLAN1	Null	Invalid
10.2.1.1/32	127.0.0.1	UH	InLoop0	Null	Invalid
127.0.0.0/8	127.0.0.1	U	InLoop0	Null	Invalid
127.0.0.1/32	127.0.0.1	UH	InLoop0	Null	Invalid

#### # Display FIB information passing ACL 2000.

```
<Sysname> system-view  
[Sysname] acl number 2000  
[Sysname-acl-basic-2000] rule permit source 10.2.0.0 0.0.255.255  
[Sysname-acl-basic-2000] display fib acl 2000  
Destination count: 2 FIB entry count: 2
```

Flag:

U:Useable G:Gateway H:Host B:Blackhole D:Dynamic S:Static  
R:Relay

Destination/Mask	Nexthop	Flag	OutInterface	InnerLabel	Token
10.2.0.0/16	10.2.1.1	U	VLAN1	Null	Invalid
10.2.1.1/32	127.0.0.1	UH	InLoop0	Null	Invalid

#### # Display all entries that contain the string 127 and start from the first one.

```
<Sysname> display fib | begin 127
```

Flag:

U:Useable G:Gateway H:Host B:Blackhole D:Dynamic S:Static  
R:Relay

Destination/Mask	Nexthop	Flag	OutInterface	InnerLabel	Token
10.2.1.1/32	127.0.0.1	UH	InLoop0	Null	Invalid
127.0.0.0/8	127.0.0.1	U	InLoop0	Null	Invalid
127.0.0.1/32	127.0.0.1	UH	InLoop0	Null	Invalid

#### # Display FIB information passing the IP prefix list abc0.

```
<Sysname> system-view  
[Sysname] ip ip-prefix abc0 permit 10.2.0.0 16  
[Sysname] display fib ip-prefix abc0  
Destination count: 1 FIB entry count: 1
```

Flag:

U:Useable G:Gateway H:Host B:Blackhole D:Dynamic S:Static  
R:Relay

Destination/Mask	Nexthop	Flag	OutInterface	InnerLabel	Token
10.2.0.0/16	10.2.1.1	U	VLAN1	Null	Invalid

**Table 1-1 display fib command output description**

Field	Description
Destination count	Total number of destination addresses
FIB entry count	Total number of FIB entries
Destination/Mask	Destination address/length of mask
Nexthop	Address of next hop
Flag	Flags of routes: <ul style="list-style-type: none"> <li>• “U”—Usable route</li> <li>• “G”—Gateway route</li> <li>• “H”—Host route</li> <li>• “B”—Blackhole route</li> <li>• “D”—Dynamic route</li> <li>• “S”—Static route</li> <li>• “R”—Relay route</li> </ul>
OutInterface	Outbound interface
InnerLabel	Inner label
Token	LSP index number

## display fib ip-address

### Syntax

```
display fib [ vpn-instance vpn-instance-name ] ip-address [ mask | mask-length ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**vpn-instance** *vpn-instance-name*: Displays FIB entries of the specified VPN instance. The *vpn-instance-name* is a string of 1 to 31 case-sensitive characters. If no VPN instance is specified, FIB entries of all VPN instances are displayed.

*ip-address*: Destination IP address, in dotted decimal notation.

*mask*: IP address mask.

*mask-length*: Length of IP address mask.

### Description

Use the **display fib ip-address** command to display FIB entries that match the specified destination IP address.

If no mask or mask length is specified, the FIB entry that matches the destination IP address and has the longest mask will be displayed; if the mask is specified, the FIB entry that exactly matches the specified destination IP address will be displayed.

## Examples

```
# Display the FIB entries that match the destination IP address of 10.2.1.1.
<Sysname> display fib 10.2.1.1
Destination count: 1    FIB entry count: 1

Flag:
  U:Useable  G:Gateway  H:Host  B:Blackhole  D:Dynamic  S:Static
  R:Relay

Destination/Mask  Nexthop    Flag    OutInterface  InnerLabel  Token
10.2.1.1/32      127.0.0.1  UH      InLoop0       Null        Invalid
```

For description about the above output, refer to [Table 1-1](#).

## display icmp statistics

### Syntax

```
display icmp statistics [ slot slot-number ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**slot slot-number**: Displays the ICMP statistics on the specified device. If the device is in an IRF stack, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF stack, the *slot-number* argument represents the device ID.

### Description

Use the **display icmp statistics** command to display ICMP statistics.

Related commands: **display ip interface** (in *IP Addressing Commands of the IP Services Volume*), **reset ip statistics**.

## Examples

```
# Display ICMP statistics.
<Sysname> display icmp statistics
  Input: bad formats    0          bad checksum          0
         echo          5          destination unreachable 0
         source quench 0          redirects              0
         echo reply    10         parameter problem     0
         timestamp     0          information request    0
         mask requests 0          mask replies          0
         time exceeded 0
  Output: echo          10         destination unreachable 0
         source quench 0          redirects              0
```

```

echo reply      5           parameter problem      0
timestamp      0           information reply      0
mask requests  0           mask replies          0
time exceeded  0

```

**Table 1-2 display icmp statistics** command output description

Field	Description
bad formats	Number of input wrong format packets
bad checksum	Number of input wrong checksum packets
echo	Number of input/output echo packets
destination unreachable	Number of input/output destination unreachable packets
source quench	Number of input/output source quench packets
redirects	Number of input/output redirection packets
echo reply	Number of input/output replies
parameter problem	Number of input/output parameter problem packets
timestamp	Number of input/output time stamp packets
information request	Number of input information request packets
mask requests	Number of input/output mask requests
mask replies	Number of input/output mask replies
information reply	Number of output information reply packets
time exceeded	Number of input/output expiration packets

## display ip socket

### Syntax

```
display ip socket [ socktype sock-type ] [ task-id socket-id ] [ slot slot-number ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**socktype** *sock-type*: Displays the socket information of this type. The sock type is in the range 1 to 3, corresponding to TCP, UDP and raw IP respectively.

*task-id*: Displays the socket information of this task. Task ID is in the range 1 to 100.

*socket-id*: Displays the information of the socket. Socket ID is in the range 0 to 3072.

**slot** *slot-number*: Displays the socket information of the specified device. If the device is in an IRF stack, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF stack, the *slot-number* argument represents the device ID.

## Description

Use the **display ip socket** command to display socket information.

## Examples

# Display the TCP socket information.

```
<Sysname> display ip socket
SOCK_STREAM:
Task = VTYP(38), socketid = 1, Proto = 6,
LA = 0.0.0.0:23, FA = 0.0.0.0:0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_KEEPALIVE SO_REUSEPORT SO_SENDVFNID(3073) SO_SETKEEPALIVE,
socket state = SS_PRIV SS_ASYNC

Task = HTTP(36), socketid = 1, Proto = 6,
LA = 0.0.0.0:80, FA = 0.0.0.0:0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT,
socket state = SS_PRIV SS_NBIO

Task = ROUT(69), socketid = 10, Proto = 6,
LA = 0.0.0.0:179, FA = 192.168.1.45:0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEADDR SO_REUSEPORT SO_SENDVFNID(0),
socket state = SS_PRIV SS_ASYNC

Task = VTYP(38), socketid = 4, Proto = 6,
LA = 192.168.1.40:23, FA = 192.168.1.52:1917,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 237, rb_cc = 0,
socket option = SO_KEEPALIVE SO_OOBNLINE SO_REUSEPORT SO_SENDVFNID(0) SO_SETKEEPALIVE,
socket state = SS_ISCONNECTED SS_PRIV SS_ASYNC

Task = VTYP(38), socketid = 3, Proto = 6,
LA = 192.168.1.40:23, FA = 192.168.1.84:1503,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_KEEPALIVE SO_OOBNLINE SO_REUSEPORT SO_SENDVFNID(0) SO_SETKEEPALIVE,
socket state = SS_ISCONNECTED SS_PRIV SS_ASYNC

Task = ROUT(69), socketid = 11, Proto = 6,
LA = 192.168.1.40:1025, FA = 192.168.1.45:179,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_REUSEADDR SO_LINGER SO_SENDVFNID(0),
socket state = SS_ISCONNECTED SS_PRIV SS_ASYNC

SOCK_DGRAM:
Task = NTP(37), socketid = 1, Proto = 17,
LA = 0.0.0.0:123, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
```

socket option = SO\_UDPChecksum SO\_SENDVFNID(3073),  
socket state = SS\_PRIV

Task = AGNT(51), socketid = 1, Proto = 17,  
LA = 0.0.0.0:161, FA = 0.0.0.0:0,  
sndbuf = 9216, rcvbuf = 41600, sb\_cc = 0, rb\_cc = 0,  
socket option = SO\_UDPChecksum SO\_SENDVFNID(3073),  
socket state = SS\_PRIV SS\_NBIO SS\_ASYNC

Task = RDSO(56), socketid = 1, Proto = 17,  
LA = 0.0.0.0:1024, FA = 0.0.0.0:0,  
sndbuf = 9216, rcvbuf = 41600, sb\_cc = 0, rb\_cc = 0,  
socket option = SO\_UDPChecksum,  
socket state = SS\_PRIV

Task = TRAP(52), socketid = 1, Proto = 17,  
LA = 0.0.0.0:1025, FA = 0.0.0.0:0,  
sndbuf = 9216, rcvbuf = 0, sb\_cc = 0, rb\_cc = 0,  
socket option = SO\_UDPChecksum,  
socket state = SS\_PRIV

Task = RDSO(56), socketid = 2, Proto = 17,  
LA = 0.0.0.0:1812, FA = 0.0.0.0:0,  
sndbuf = 9216, rcvbuf = 41600, sb\_cc = 0, rb\_cc = 0,  
socket option = SO\_UDPChecksum,  
socket state = SS\_PRIV

SOCK\_RAW:

Task = ROUT(69), socketid = 8, Proto = 89,  
LA = 0.0.0.0, FA = 0.0.0.0,  
sndbuf = 262144, rcvbuf = 262144, sb\_cc = 0, rb\_cc = 0,  
socket option = SO\_SENDVFNID(0) SO\_RCVVFNID(0),  
socket state = SS\_PRIV SS\_ASYNC

Task = ROUT(69), socketid = 3, Proto = 2,  
LA = 0.0.0.0, FA = 0.0.0.0,  
sndbuf = 32767, rcvbuf = 256000, sb\_cc = 0, rb\_cc = 0,  
socket option = SO\_SENDVFNID(0) SO\_RCVVFNID(0),  
socket state = SS\_PRIV SS\_NBIO SS\_ASYNC

Task = ROUT(69), socketid = 2, Proto = 103,  
LA = 0.0.0.0, FA = 0.0.0.0,  
sndbuf = 65536, rcvbuf = 256000, sb\_cc = 0, rb\_cc = 0,  
socket option = SO\_SENDVFNID(0) SO\_RCVVFNID(0),  
socket state = SS\_PRIV SS\_NBIO SS\_ASYNC

Task = ROUT(69), socketid = 1, Proto = 65,  
LA = 0.0.0.0, FA = 0.0.0.0,

```

sndbuf = 32767, rcvbuf = 256000, sb_cc = 0, rb_cc = 0,
socket option = 0,
socket state = SS_PRIV SS_NBIO SS_ASYNC

```

```

Task = RSVP(73), socketid = 1, Proto = 46,
LA = 0.0.0.0, FA = 0.0.0.0,
sndbuf = 4194304, rcvbuf = 4194304, sb_cc = 0, rb_cc = 0,
socket option = 0,
socket state = SS_PRIV SS_NBIO SS_ASYNC

```

**Table 1-3 display ip socket** command output description

Field	Description
SOCK_STREAM	TCP socket
SOCK_DGRAM	UDP socket
SOCK_RAW	Raw IP socket
Task	Task number
socketid	Socket ID
Proto	Protocol number of the socket, indicating the protocol type that IP carries
LA	Local address and local port number
FA	Remote address and remote port number
sndbuf	Sending buffer size of the socket, in bytes
rcvbuf	Receiving buffer size of the socket, in bytes
sb_cc	Current data size in the sending buffer (It is available only for TCP that can buffer data)
rb_cc	Data size currently in the receiving buffer
socket option	Socket option
socket state	Socket state

## display ip statistics

### Syntax

```
display ip statistics [ slot slot-number ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**slot slot-number.** Displays statistics of IP packets on the specified device. If the device is in an IRF stack, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF stack, the *slot-number* argument represents the device ID.

## Description

Use the **display ip statistics** command to display statistics of IP packets.

Related commands: **display ip interface** (in *IP Addressing Commands of the IP Services Volume*), **reset ip statistics**.

## Examples

# Display statistics of IP packets.

```
<Sysname> display ip statistics
  Input:  sum          7120          local          112
         bad protocol  0           bad format     0
         bad checksum  0           bad options    0
  Output: forwarding   0           local          27
         dropped       0           no route       2
         compress fails 0
  Fragment:input      0           output         0
         dropped       0
         fragmented    0           couldn't fragment 0
  Reassembling:sum    0           timeouts       0
```

**Table 1-4 display ip statistics** command output description

	Field	Description
Input:	sum	Total number of packets received
	local	Total number of packets with destination being local
	bad protocol	Total number of unknown protocol packets
	bad format	Total number of packets with incorrect format
	bad checksum	Total number of packets with incorrect checksum
	bad options	Total number of packets with incorrect option
Output:	forwarding	Total number of packets forwarded
	local	Total number of packets sent from the local
	dropped	Total number of packets discarded
	no route	Total number of packets for which no route is available
	compress fails	Total number of packets failed to be compressed
Fragment:	input	Total number of fragments received
	output	Total number of fragments sent
	dropped	Total number of fragments dropped
	fragmented	Total number of packets successfully fragmented
	couldn't fragment	Total number of packets that failed to be fragmented
Reassembling	sum	Total number of packets reassembled
	timeouts	Total number of reassembly timeout fragments

## display tcp statistics

### Syntax

**display tcp statistics**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display tcp statistics** command to display statistics of TCP traffic.

Related commands: **display tcp status**, **reset tcp statistics**.

### Examples

# Display statistics of TCP traffic.

```
<Sysname> display tcp statistics
```

```
Received packets:
```

```
Total: 8457
```

```
packets in sequence: 3660 (5272 bytes)
```

```
window probe packets: 0, window update packets: 0
```

```
checksum error: 0, offset error: 0, short error: 0
```

```
duplicate packets: 1 (8 bytes), partially duplicate packets: 0 (0 bytes)
```

```
out-of-order packets: 17 (0 bytes)
```

```
packets of data after window: 0 (0 bytes)
```

```
packets received after close: 0
```

```
ACK packets: 4625 (141989 bytes)
```

```
duplicate ACK packets: 1702, too much ACK packets: 0
```

```
Sent packets:
```

```
Total: 6726
```

```
urgent packets: 0
```

```
control packets: 21 (including 0 RST)
```

```
window probe packets: 0, window update packets: 0
```

```
data packets: 6484 (141984 bytes) data packets retransmitted: 0 (0 bytes)
```

```
ACK-only packets: 221 (177 delayed)
```

```
Retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
```

```
Keepalive timeout: 1682, keepalive probe: 1682, Keepalive timeout, so connections  
disconnected : 0
```

Initiated connections: 0, accepted connections: 22, established connections: 22  
 Closed connections: 49 (dropped: 0, initiated dropped: 0)  
 Packets dropped with MD5 authentication: 0  
 Packets permitted with MD5 authentication: 0

**Table 1-5 display tcp statistics** command output description

	Field	Description
Received packets:	Total	Total number of packets received
	packets in sequence	Number of packets arriving in sequence
	window probe packets	Number of window probe packets received
	window update packets	Number of window update packets received
	checksum error	Number of checksum error packets received
	offset error	Number of offset error packets received
	short error	Number of received packets with length being too small
	duplicate packets	Number of completely duplicate packets received
	partially duplicate packets	Number of partially duplicate packets received
	out-of-order packets	Number of out-of-order packets received
	packets of data after window	Number of packets outside the receiving window
	packets received after close	Number of packets that arrived after connection is closed
	ACK packets	Number of ACK packets received
	duplicate ACK packets	Number of duplicate ACK packets received
	too much ACK packets	Number of ACK packets for data unsend
Sent packets:	Total	Total number of packets sent
	urgent packets	Number of urgent packets sent
	control packets	Number of control packets sent
	window probe packets	Number of window probe packets sent; in the brackets are resent packets
	window update packets	Number of window update packets sent
	data packets	Number of data packets sent
	data packets retransmitted	Number of data packets retransmitted
	ACK-only packets	Number of ACK packets sent; in brackets are delayed ACK packets
Retransmitted timeout	Number of retransmission timer timeouts	
connections dropped in retransmitted timeout	Number of connections broken due to retransmission timeouts	
Keepalive timeout	Number of keepalive timer timeouts	
keepalive probe	Number of keepalive probe packets sent	
Keepalive timeout, so connections disconnected	Number of connections broken due to timeout of the keepalive timer	

Field	Description
Initiated connections	Number of connections initiated
accepted connections	Number of connections accepted
established connections	Number of connections established
Closed connections	Number of connections closed; in brackets are connections closed accidentally (before receiving SYN from the peer) and connections closed initiatively (after receiving SYN from the peer)
Packets dropped with MD5 authentication	Number of packets dropped by MD5 authentication
Packets permitted with MD5 authentication	Number of packets permitted by MD5 authentication

## display tcp status

### Syntax

**display tcp status**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display tcp status** command to display status of all TCP connections for monitoring TCP connections.

### Examples

# Display status of all TCP connections.

```
<Sysname> display tcp status
*: TCP MD5 Connection
TCPCB      Local Add:port      Foreign Add:port      State
03e37dc4   0.0.0.0:4001        0.0.0.0:0             Listening
04217174   100.0.0.204:23      100.0.0.253:65508     Established
```

**Table 1-6 display tcp status** command output description

Field	Description
*	If the status information of a TCP connection contains *, the TCP adopts the MD5 algorithm for authentication.
TCPCB	TCP control block
Local Add:port	Local IP address and port number

Field	Description
Foreign Add:port	Remote IP address and port number
State	State of the TCP connection

## display udp statistics

### Syntax

**display udp statistics**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display udp statistics** command to display statistics of UDP packets.

Related commands: **reset udp statistics**.

### Examples

# Display statistics of UDP packets.

```
<Sysname> display udp statistics
```

Received packets:

Total: 0

checksum error: 0

shorter than header: 0, data length larger than packet: 0

unicast(no socket on port): 0

broadcast/multicast(no socket on port): 0

not delivered, input socket full: 0

input packets missing pcb cache: 0

Sent packets:

Total: 0

**Table 1-7 display udp statistics** command output description

	Field	Description
Received packets:	Total	Total number of UDP packets received
	checksum error	Total number of packets with incorrect checksum
	shorter than header	Number of packets with data shorter than head
	data length larger than packet	Number of packets with data longer than packet
	unicast(no socket on port)	Number of unicast packets with no socket on port
	broadcast/multicast(no socket on port)	Number of broadcast/multicast packets without socket on port
	not delivered, input socket full	Number of packets not delivered to an upper layer due to a full socket cache
	input packets missing pcb cache	Number of packets without matching protocol control block (PCB) cache
Sent packets:	Total	Total number of UDP packets sent

## ip forward-broadcast (interface view)

### Syntax

```
ip forward-broadcast [ acl acl-number ]  
undo ip forward-broadcast
```

### View

Interface view

### Default Level

2: System level

### Parameters

**acl** *acl-number*: Access control list number, in the range 2000 to 3999. From 2000 to 2999 are numbers for basic ACLs, and from 3000 to 3999 are numbers for advanced ACLs. Only directed broadcasts permitted by the ACL can be forwarded.

### Description

Use the **ip forward-broadcast** command to enable the interface to forward directed broadcasts to a directly-connected network.

Use the **undo ip forward-broadcast** command to disable the interface from forwarding directed broadcasts to a directly-connected network.

By default, an interface is disabled from forwarding directed broadcasts to a directly-connected network.

### Examples

```
# Enable VLAN-interface 2 to forward the directed broadcasts to a directly-connected network matching ACL 2001.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip forward-broadcast acl 2001
```

## ip forward-broadcast (system view)

### Syntax

```
ip forward-broadcast
undo ip forward-broadcast
```

### View

System view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **ip forward-broadcast** command to enable the device to receive directed broadcasts.

Use the **undo ip forward-broadcast** command to disable the device from receiving directed broadcasts.

By default, the device is disabled from receiving directed broadcasts.

### Examples

```
# Enable the device to receive directed broadcasts.
```

```
<Sysname> system-view
[Sysname] ip forward-broadcast
```

## ip redirects enable

### Syntax

```
ip redirects enable
undo ip redirects
```

### View

System view

### Default Level

2: System level

### Parameters

None

## Description

Use the **ip redirects enable** command to enable sending of ICMP redirection packets.

Use the **undo ip redirects** command to disable sending of ICMP redirection packets.

This feature is disabled by default.

## Examples

```
# Enable sending of ICMP redirect packets.
```

```
<Sysname> system-view  
[Sysname] ip redirects enable
```

## ip ttl-expires enable

### Syntax

```
ip ttl-expires enable
```

```
undo ip ttl-expires
```

### View

System view

### Default Level

2: System level

### Parameters

None

## Description

Use the **ip ttl-expires enable** command to enable the sending of ICMP timeout packets.

Use the **undo ip ttl-expires** command to disable sending ICMP timeout packets.

Sending ICMP timeout packets is enabled by default.

If the feature is disabled, the device will not send TTL timeout ICMP packets, but still send “reassembly timeout” ICMP packets.

## Examples

```
# Disable sending ICMP timeout packets.
```

```
<Sysname> system-view  
[Sysname] undo ip ttl-expires
```

## ip unreachable enable

### Syntax

```
ip unreachable enable
```

```
undo ip unreachable
```

### View

System view

## Default Level

2: System level

## Parameters

None

## Description

Use the **ip unreachable enable** command to enable the sending of ICMP destination unreachable packets.

Use the **undo ip unreachable** command to disable sending ICMP destination unreachable packets.

Sending ICMP destination unreachable packets is disabled by default.

## Examples

```
# Enable sending ICMP destination unreachable packets.
```

```
<Sysname> system-view  
[Sysname] ip unreachable enable
```

## reset ip statistics

### Syntax

```
reset ip statistics [ slot slot-number ]
```

### View

User view

### Default Level

2: System level

### Parameters

**slot slot-number**: Clears IP packet statistics on the specified device. If the device is in an IRF stack, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF stack, the *slot-number* argument represents the device ID..

### Description

Use the **reset ip statistics** command to clear statistics of IP packets.

Related commands: **display ip interface** (in *IP Addressing Commands of the IP Services Volume*), **display ip statistics**.

### Examples

```
# Clear statistics of IP packets.  
<Sysname> reset ip statistics
```

## reset tcp statistics

### Syntax

```
reset tcp statistics
```

## View

User view

## Default Level

2: System level

## Parameters

None

## Description

Use the **reset tcp statistics** command to clear statistics of TCP traffic.

Related commands: **display tcp statistics**.

## Examples

# Display statistics of TCP traffic.

```
<Sysname> reset tcp statistics
```

## reset udp statistics

### Syntax

```
reset udp statistics
```

## View

User view

## Default Level

2: System level

## Parameters

None

## Description

Use the **reset udp statistics** command to clear statistics of UDP traffic.

## Examples

# Display statistics of UDP traffic.

```
<Sysname> reset udp statistics
```

## tcp timer fin-timeout

### Syntax

```
tcp timer fin-timeout time-value
```

```
undo tcp timer fin-timeout
```

## View

System view

## Default Level

2: System level

## Parameters

*time-value*: Length of the TCP finwait timer in seconds, in the range 76 to 3,600.

## Description

Use the **tcp timer fin-timeout** command to configure the length of the TCP finwait timer.

Use the **undo tcp timer fin-timeout** command to restore the default.

By default, the length of the TCP finwait timer is 675 seconds.

Note that the actual length of the finwait timer is determined by the following formula:

Actual length of the finwait timer = (Configured length of the finwait timer – 75) + configured length of the synwait timer

Related commands: **tcp timer syn-timeout**, **tcp window**.

## Examples

# Set the length of the TCP finwait timer to 800 seconds.

```
<Sysname> system-view
[Sysname] tcp timer fin-timeout 800
```

## tcp timer syn-timeout

### Syntax

```
tcp timer syn-timeout time-value
undo tcp timer syn-timeout
```

### View

System view

## Default Level

2: System level

## Parameters

*time-value*: TCP finwait timer in seconds, in the range 2 to 600.

## Description

Use the **tcp timer syn-timeout** command to configure the length of the TCP synwait timer.

Use the **undo tcp timer syn-timeout** command to restore the default.

By default, the value of the TCP synwait timer is 75 seconds.

Related commands: **tcp timer fin-timeout**, **tcp window**.

## Examples

# Set the length of the TCP synwait timer to 80 seconds.

```
<Sysname> system-view
```

```
[Sysname] tcp timer syn-timeout 80
```

## tcp window

### Syntax

```
tcp window window-size
```

```
undo tcp window
```

### View

System view

### Default Level

2: System level

### Parameters

*window-size*: Size of the send/receive buffer in KB, in the range 1 to 32.

### Description

Use the **tcp window** command to configure the size of the TCP send/receive buffer.

Use the **undo tcp window** command to restore the default.

The size of the TCP send/receive buffer is 8 KB by default.

Related commands: **tcp timer fin-timeout**, **tcp timer syn-timeout**.

### Examples

# Configure the size of the TCP send/receive buffer as 3 KB.

```
<Sysname> system-view  
[Sysname] tcp window 3
```

# Table of Contents

<b>1 UDP Helper Configuration Commands</b> .....	<b>1-1</b>
UDP Helper Configuration Commands.....	1-1
display udp-helper server.....	1-1
reset udp-helper packet.....	1-1
udp-helper enable.....	1-2
udp-helper port.....	1-2
udp-helper server.....	1-3

# 1 UDP Helper Configuration Commands

---

## UDP Helper Configuration Commands

### display udp-helper server

#### Syntax

```
display udp-helper server [ interface interface-type interface-number ]
```

#### View

Any view

#### Default Level

2: System level

#### Parameters

**interface** *interface-type interface-number*: Displays information of forwarded UDP packets on the specified interface.

#### Description

Use the **display udp-helper server** command to display the information of forwarded UDP packets on the specified interface or all interfaces.

If *interface-type interface-number* is not specified, this command displays the information of forwarded UDP packets on all interfaces.

#### Examples

# Display the information of forwarded UDP packets on the interface VLAN-interface 1.

```
<Sysname> display udp-helper server interface vlan-interface 1
```

```
Interface name      Server address      Packets sent
```

```
Vlan-interfacel    192.1.1.2          0
```

The information above shows that the IP address of the destination server corresponding to the interface VLAN-interface 1 is 192.1.1.2, and that no packets are forwarded to the destination server.

### reset udp-helper packet

#### Syntax

```
reset udp-helper packet
```

#### View

User view

### Default Level

2: System level

### Parameters

None

### Description

Use the **reset udp-helper packet** command to clear the statistics of UDP packets forwarded.

Related commands: **display udp-helper server**.

### Examples

# Clear the statistics of the forwarded UDP packets.

```
<Sysname> reset udp-helper packet
```

## udp-helper enable

### Syntax

```
udp-helper enable
```

```
undo udp-helper enable
```

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **udp-helper enable** command to enable UDP Helper. The device enabled with UDP Helper functions as a relay agent that converts UDP broadcast packets into unicast packets and forwards them to a specified destination server.

Use the **undo udp-helper enable** command to disable UDP Helper.

By default, UDP Helper is disabled.

### Examples

# Enable UDP Helper

```
<Sysname> system-view
```

```
[Sysname] udp-helper enable
```

## udp-helper port

### Syntax

```
udp-helper port { port-number | dns | netbios-ds | netbios-ns | tacacs | tftp | time }
```

**undo udp-helper port** { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

## View

System view

## Default Level

2: System level

## Parameters

**port-number**: UDP port number with which packets need to be forwarded, in the range of 1 to 65535 (except 67 and 68).

**dns**: Forwards DNS data packets. The corresponding UDP port number is 53.

**netbios-ds**: Forwards NetBIOS data packets. The corresponding UDP port number is 138.

**netbios-ns**: Forwards NetBIOS name service data packets. The corresponding UDP port number is 137.

**tacacs**: Forwards terminal access controller access control system (TACACS) data packet. The corresponding UDP port number is 49.

**tftp**: Forwards TFTP data packets. The corresponding UDP port number is 69.

**time**: Forwards time service data packets. The corresponding UDP port number is 37.

## Description

Use the **udp-helper port** command to enable the forwarding of packets with the specified UDP port number.

Use the **undo udp-helper port** command to remove the configured UDP port numbers.

By default, no UDP port number is specified.

The specified UDP port numbers will all be removed if UDP Helper is disabled.

## Examples

```
# Forward broadcast packets with the UDP destination port number 100.
```

```
<Sysname> system-view  
[Sysname] udp-helper port 100
```

## udp-helper server

### Syntax

```
udp-helper server ip-address  
undo udp-helper server [ ip-address ]
```

### View

Interface view

### Default Level

2: System level

## Parameters

*ip-address*: IP address of the destination server, in dotted decimal notation.

## Description

Use the **udp-helper server** command to specify the destination server which UDP packets need to be forwarded to.

Use the **undo udp-helper server** command to remove the destination server.

No destination server is configured by default.

Currently, you can configure up to 20 destination servers on an interface.

Note that you will remove all the destination servers on an interface if you carry out the **undo udp-helper server** command without the *ip-address* argument.

Related commands: **display udp-helper server**.

## Examples

# Specify the IP address of the destination server as 192.1.1.2 on the interface VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] udp-helper server 192.1.1.2
```

# Table of Contents

<b>1 URPF Configuration Commands</b> .....	<b>1-1</b>
URPF Configuration Commands .....	1-1
ip urpf strict .....	1-1

# 1 URPF Configuration Commands

---

## URPF Configuration Commands

### ip urpf strict

#### Syntax

```
ip urpf strict
undo ip urpf
```

#### View

System view

#### Default Level

2: System level

#### Parameters

None.

#### Description

Use the **ip urpf strict** command to enable URPF check on the switch.

Use the **undo ip urpf** command to disable URPF check.

By default, URPF check is disabled.

#### Examples

# Enable URPF check on a switch.

```
<Sysname> system-view
[Sysname] ip urpf strict
```

# Table of Contents

<b>1 IPv6 Basics Configuration Commands</b> .....	<b>1-1</b>
IPv6 Basics Configuration Commands .....	1-1
display dns ipv6 dynamic-host .....	1-1
display dns ipv6 server .....	1-2
display ipv6 fib .....	1-3
display ipv6 host .....	1-4
display ipv6 interface .....	1-5
display ipv6 neighbors .....	1-9
display ipv6 neighbors count .....	1-10
display ipv6 pathmtu .....	1-11
display ipv6 socket .....	1-12
display ipv6 statistics .....	1-14
display tcp ipv6 statistics .....	1-17
display tcp ipv6 status .....	1-19
display udp ipv6 statistics .....	1-20
dns server ipv6 .....	1-21
ipv6 .....	1-22
ipv6 address .....	1-22
ipv6 address auto link-local .....	1-23
ipv6 address eui-64 .....	1-24
ipv6 address link-local .....	1-25
ipv6 hoplimit-expires enable .....	1-26
ipv6 host .....	1-26
ipv6 icmp-error .....	1-27
ipv6 icmpv6 multicast-echo-reply enable .....	1-28
ipv6 nd autoconfig managed-address-flag .....	1-28
ipv6 nd autoconfig other-flag .....	1-29
ipv6 nd dad attempts .....	1-29
ipv6 nd hop-limit .....	1-30
ipv6 nd ns retrans-timer .....	1-31
ipv6 nd nud reachable-time .....	1-31
ipv6 nd ra halt .....	1-32
ipv6 nd ra interval .....	1-33
ipv6 nd ra prefix .....	1-33
ipv6 nd ra router-lifetime .....	1-34
ipv6 neighbor .....	1-35
ipv6 neighbors max-learning-num .....	1-36
ipv6 pathmtu .....	1-36
ipv6 pathmtu age .....	1-37
reset dns ipv6 dynamic-host .....	1-38
reset ipv6 neighbors .....	1-38
reset ipv6 pathmtu .....	1-39
reset ipv6 statistics .....	1-39

reset tcp ipv6 statistics .....	1-40
reset udp ipv6 statistics .....	1-40
tcp ipv6 timer fin-timeout .....	1-41
tcp ipv6 timer syn-timeout .....	1-41
tcp ipv6 window .....	1-42

# 1 IPv6 Basics Configuration Commands

---

## IPv6 Basics Configuration Commands

### display dns ipv6 dynamic-host

#### Syntax

```
display dns ipv6 dynamic-host
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

None

#### Description

Use the **display dns ipv6 dynamic-host** command to display IPv6 dynamic domain name information, including the domain name, IPv6 address, and TTL of the DNS entries.

You can use the **reset dns ipv6 dynamic-host** command to clear all IPv6 dynamic domain name information from the cache.

#### Examples

```
# Display IPv6 dynamic domain name information.
```

```
<Sysname> display dns ipv6 dynamic-host
```

```
NoHost          IPv6 Address    TTL
1      aaa          2001:::2       6
```

**Table 1-1** display dns ipv6 dynamic-host command output description

Field	Description
No	Sequence number
Host	Host name
IPv6 address	IPv6 address of the host
TTL	Time within which an entry can be cached, in seconds



## Note

For a domain name displayed with the **display dns ipv6 dynamic-host** command, no more than 21 characters can be displayed. If the domain name exceeds the maximum length, the first 21 characters will be displayed.

## display dns ipv6 server

### Syntax

```
display dns ipv6 server [ dynamic ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**dynamic:** Displays IPv6 DNS server information acquired dynamically through DHCP or other protocols.

### Description

Use the **display dns ipv6 server** command to display IPv6 DNS server information.

### Examples

```
# Display IPv6 DNS server information.
```

```
<Sysname> display dns ipv6 server
```

```
Type:
```

```
  D:Dynamic   S:Static
```

```
DNS Server  Type  IPv6 Address                               (Interface Name)
   1         S    1::1
   2         S    FE80:1111:2222:3333:4444:5555:6666:7777  Vlan2
```

**Table 1-2 display dns ipv6 server** command output description

Field	Description
DNS Server	Sequence number of the DNS server, which is assigned automatically by the system, starting from 1.
Type	Type of the DNS server: "S" represents a statically configured DNS server, and "D" represents a DNS server obtained dynamically through DHCP.
IPv6 Address	IPv6 address of the DNS server
Interface Name	Interface name, which is available only for a DNS server with an IPv6 link-local address configured.

## display ipv6 fib

### Syntax

```
display ipv6 fib [ slot-number ] [ ipv6-address ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*slot-number*: Displays the IPv6 forwarding information base (FIB) entries of a specified device in an IRF stack. If no stack is formed, the IPv6 FIB entries of the current device are displayed only. The *slot-number* argument indicates the member ID of the device.

*ipv6-address*: Displays the IPv6 FIB entries for an IPv6 address.

### Description

Use the **display ipv6 fib** command to display IPv6 FIB entries. If no argument is specified, all IPv6 FIB entries will be displayed.

The device looks up a matching IPv6 FIB entry for forwarding an IPv6 packet.

### Examples

```
# Display all IPv6 FIB entries.
```

```
<Sysname> display ipv6 fib
```

```
FIB Table:
```

```
Total number of Routes : 1
```

```
Flag:
```

```
U:Useable G:Gateway H:Host B:Blackhole D:Dynamic S:Static
```

```
Destination:      ::1                PrefixLength : 128
```

```
NextHop          :      ::1                Flag          : HU
```

```
Label            :      NULL                Tunnel ID     : 0
```

```
TimeStamp        :      Date- 7/14/2008, Time- 15:17:15
```

```
Interface        :      InLoopBack0
```

**Table 1-3 display ipv6 fib command output description**

Field	Description
Total number of Routes	Total number of routes in the FIB
Destination	Destination address
PrefixLength	Prefix length of the destination address
NextHop	Next hop

Field	Description
Flag	Route flag: <ul style="list-style-type: none"> <li>• U — Usable route</li> <li>• G — Gateway route</li> <li>• H — Host route</li> <li>• B — Black hole route</li> <li>• D — Dynamic route</li> <li>• S — Static route</li> </ul>
Label	Label
Tunnel ID	ID of a tunnel
TimeStamp	Generation time of a FIB entry
Interface	Outgoing interface

## display ipv6 host

### Syntax

**display ipv6 host**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display ipv6 host** command to display the mappings between host names and IPv6 addresses in the static domain name resolution table.

Related commands: **ipv6 host**.

### Examples

# Display the mappings between host names and IPv6 addresses in the static domain name resolution table.

```
<Sysname> display ipv6 host
```

```
Host           Age           Flags           IPv6Address
aaa            0             static          2002::1
bbb            0             static          2002::2
```

**Table 1-4 display ipv6 host command output description**

Field	Description
Host	Host name
Age	Time for the entry to live. "0" is displayed in the case of static configuration.

Field	Description
Flags	Flag indicating the type of mapping between a host name and an IPv6 address. Static indicates a static mapping.
IPv6Address	IPv6 address of a host

## display ipv6 interface

### Syntax

```
display ipv6 interface [ interface-type [ interface-number ] ] [ verbose ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*interface-type*: Interface type.

*interface-number*: Interface number.

**verbose**: Displays the detailed IPv6 information of an interface.

### Description

Use the **display ipv6 interface** command to display the IPv6 information of an interface for which an IPv6 address can be configured.

If *interface-type interface-number* is not specified, the IPv6 information of all interfaces for which IPv6 addresses can be configured is displayed; if only *interface-type* is specified, the IPv6 information of the interfaces of the specified type for which IPv6 addresses can be configured is displayed; if *interface-type interface-number* is specified, the IPv6 information of the specified interface is displayed. If the **verbose** keyword is also specified, the detailed IPv6 information of the interface is displayed.

Note that:

### Examples

```
# Display the IPv6 information of VLAN-interface 2.
```

```
<Sysname> display ipv6 interface vlan-interface 2 verbose
Vlan-interface2 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::1234:56FF:FE65:4322
Global unicast address(es):
  2001::1, subnet is 2001::/64
Joined group address(es):
  FF02::1:FF00:1
  FF02::1:FF65:4322
  FF02::2
  FF02::1
MTU is 1500 bytes
```

```

ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
InReceives:                0
InTooShorts:               0
InTruncatedPkts:          0
InHopLimitExceeds:        0
InBadHeaders:              0
InBadOptions:              0
ReasmReqds:                0
ReasmOKs:                  0
InFragDrops:               0
InFragTimeouts:           0
OutFragFails:              0
InUnknownProtos:          0
InDelivers:                0
OutRequests:               0
OutForwDatagrams:         0
InNoRoutes:                0
InTooBigErrors:            0
OutFragOKs:                0
OutFragCreates:           0
InMcastPkts:              0
InMcastNotMembers:        0
OutMcastPkts:              0
InAddrErrors:              0
InDiscards:                0
OutDiscards:               0

```

**Table 1-5 display ipv6 interface verbose** command output description (on a switch)

Field	Description
Vlan-interface2 current state	Physical state of the interface: <ul style="list-style-type: none"> <li>● Administratively DOWN: Indicates that the VLAN interface is administratively down; that is, the interface is shut down using the <b>shutdown</b> command.</li> <li>● DOWN: Indicates that the VLAN interface is administratively up but its physical state is down; that is, no ports in the VLAN are up, which may be caused by a connection or link failure.</li> <li>● UP: Indicates that the administrative and physical states of the VLAN interface are both up.</li> </ul>
Line protocol current state	Link layer protocol state of the interface: <ul style="list-style-type: none"> <li>● DOWN: Indicates that the link layer protocol state of the VLAN interface is down, generally because no IP address is configured.</li> <li>● UP: Indicates that the link layer protocol state of the VLAN interface is up.</li> </ul>

Field	Description
IPv6 is enabled	IPv6 packet forwarding state of the interface (after an IPv6 address is configured for an interface, IPv6 is automatically enabled on it; IPv6 packet forwarding is enabled in the example)
link-local address	Link-local address configured for the interface
Global unicast address(es)	Aggregatable global unicast address(es) configured for the interface
Joined group address(es)	Address(es) of multicast group(s) that the interface has joined
MTU	Maximum transmission unit of the interface
ND DAD is enabled, number of DAD attempts	<p>Number of DAD attempts ( DAD is enabled).</p> <ul style="list-style-type: none"> <li>• If DAD is enabled, the number of neighbor request messages is also displayed (configured by using the <b>ipv6 nd dad attempts</b> command)</li> <li>• If DAD is disabled, “ND DAD is disabled” is displayed. (You can set the number of neighbor request messages for DAD to 0 to disable this function.)</li> </ul>
ND reachable time	Neighbor reachable time
ND retransmit interval	Interval for retransmitting a neighbor solicitation (NS) message
Hosts use stateless autoconfig for addresses	Hosts use stateless autoconfiguration mode to acquire IPv6 addresses
InReceives	All IPv6 packets received by the interface, including all types of error packets.
InTooShorts	Received IPv6 packets that are too short, with a length less than 40 bytes, for example.
InTruncatedPkts	Received IPv6 packets with a length less than that specified in the packets
InHopLimitExceeds	Received IPv6 packets with a hop count exceeding the limit
InBadHeaders	Received IPv6 packets with bad basic headers
InBadOptions	Received IPv6 packets with bad extension headers
ReasmReqds	Received IPv6 fragments
ReasmOKs	Number of packets after reassembly rather than the number of fragments
InFragDrops	IPv6 fragments discarded due to certain error
InFragTimeouts	IPv6 fragments discarded because the interval for which they had stayed in the system buffer exceeded the specified period
OutFragFails	Packets failed in fragmentation on the outbound interface
InUnknownProtos	Received IPv6 packets with unknown or unsupported protocol type
InDelivers	Received IPv6 packets that were delivered to application layer protocols (such as ICMPv6, TCP, and UDP)
OutRequests	Local IPv6 packets sent by IPv6 application protocols
OutForwDatagrams	Packets forwarded by the outbound interface.
InNoRoutes	IPv6 packets that were discarded because no matched route can be found

Field	Description
InTooBigErrors	IPv6 packets that were discarded because they exceeded the PMTU
OutFragOKs	Packets that were fragmented on the outbound interface
OutFragCreates	Number of packet fragments after fragmentation on the outbound interface
InMcastPkts	IPv6 multicast packets received on the interface
InMcastNotMembers	Incoming IPv6 multicast packets that were discarded because the interface did not belong to the corresponding multicast groups
OutMcastPkts	IPv6 multicast packets sent by the interface
InAddrErrors	IPv6 packets that were discarded due to invalid destination addresses
InDiscards	Received IPv6 packets that were discarded due to resource problems rather than packet content errors
OutDiscards	Sent packets that were discarded due to resource problems rather than packet content errors

# Display the brief IPv6 information of all interfaces for which IPv6 addresses can be configured.

```
<Sysname> display ipv6 interface
*down: administratively down
(s): spoofing
Interface                Physical    Protocol   IPv6 Address
Vlan-interface1         down       down       Unassigned
Vlan-interface2         up         up         2001::1
Vlan-interface100      up         down       Unassigned
```

**Table 1-6 display ipv6 interface** command output description

Field	Description
*down: administratively down	The interface is down, that is, the interface is closed by using the <b>shutdown</b> command.
(s): spoofing	Spoofing attribute of the interface, that is, the link protocol state of the interface is up, but the link does not exist, or the link is established on demand, instead of being permanent.
Interface	Name of the interface
Physical	Physical state of the interface: <ul style="list-style-type: none"> <li>*down: Indicates that the VLAN interface is administratively down; that is, the interface is shut down using the <b>shutdown</b> command.</li> <li>down: Indicates that the VLAN interface is administratively up but its physical state is down; that is, no port in the VLAN is up, which may be caused by a connection or link failure.</li> <li>up: Indicates that the administrative and physical states of the VLAN interface are both up.</li> </ul>
Protocol	Link protocol state of the interface: <ul style="list-style-type: none"> <li>down: Indicates that the link layer protocol state of the VLAN interface is down, generally because no IP address is configured.</li> <li>up: Indicates that the link layer protocol state of the VLAN interface is up.</li> </ul>

Field	Description
IPv6 Address	IPv6 address of the interface. Only the first of configured IPv6 addresses is displayed. (If no address is configured for the interface, "Unassigned" will be displayed.)

## display ipv6 neighbors

### Syntax

```
display ipv6 neighbors { { ipv6-address | all | dynamic | static } [ slot slot-number ] | interface
interface-type interface-number | vlan vlan-id } [ | { begin | exclude | include } regular-expression ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ipv6-address*: IPv6 address whose neighbor information is to be displayed.

**all**: Displays information of all neighbors, including neighbors acquired dynamically and configured statically.

**dynamic**: Displays information of all neighbors acquired dynamically.

**static**: Displays information of all neighbors configured statically.

**slot** *slot-number*: Displays information of the neighbors of a specified device in an IRF stack. If no stack is formed, the neighbors of the current device are displayed only. The *slot-number* argument indicates the member ID of the device.

**interface** *interface-type interface-number*: Displays information of the neighbors of a specified interface.

**vlan** *vlan-id*: Displays information of the neighbors of a specified VLAN whose ID ranges from 1 to 4094.

|: Uses a regular expression to match neighbor entries. For detailed information about regular expression, refer to CLI display in *Basic System Configuration* in the *System Volume*.

**begin**: Displays a specific neighbor entry and all the neighbor entries following it. The specific neighbor entry must match the specified regular expression.

**exclude**: Displays the neighbor entries not matching the specified regular expression.

**include**: Displays the neighbor entries matching the specified regular expression.

*regular-expression*: A case-sensitive string of 1 to 256 characters.

### Description

Use the **display ipv6 neighbors** command to display neighbor information.

You can use the **reset ipv6 neighbors** command to clear specific IPv6 neighbor information.

Related commands: **ipv6 neighbor**, **reset ipv6 neighbors**.

## Examples

# Display all neighbor information.

```
<Sysname> display ipv6 neighbors all
```

```
                Type: S-Static    D-Dynamic
IPv6 Address          Link-layer      VID  Interface    State  T  Age
FE80::200:5EFF:FE32:B800  0000-5e32-b800  N/A  GE1/0/1      REACH  S  -
```

**Table 1-7 display ipv6 neighbors command output description**

Field	Description
IPv6 Address	IPv6 address of a neighbor
Link-layer	Link layer address (MAC address of a neighbor)
VID	VLAN to which the interface connected with a neighbor belongs
Interface	Interface connected with a neighbor
State	State of a neighbor, including: <ul style="list-style-type: none"><li>• INCMP: The address is being resolved. The link layer address of the neighbor is unknown.</li><li>• REACH: The neighbor is reachable.</li><li>• STALE: The reachability of the neighbor is unknown. The device will not verify the reachability any longer unless data is sent to the neighbor.</li><li>• DELAY: The reachability of the neighbor is unknown. The device sends an NS message after a delay.</li><li>• PROBE: The reachability of the neighbor is unknown. The device sends an NS message to verify the reachability of the neighbor.</li></ul>
T	Type of neighbor information, including static configuration and dynamic acquisition.
Age	For a static entry, a hyphen "-" is displayed. For a dynamic entry, the reachable time (in seconds) elapsed is displayed, and if it is never reachable, "#" is displayed (for a neighbor acquired dynamically).

## display ipv6 neighbors count

### Syntax

```
display ipv6 neighbors { { all | dynamic | static } [ slot slot-number ] | interface interface-type  
interface-number | vlan vlan-id } count
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**all:** Displays the total number of all neighbor entries, including neighbor entries acquired dynamically and configured statically.

**dynamic:** Displays the total number of all neighbor entries acquired dynamically.

**static:** Displays the total number of neighbor entries configured statically.

**slot** *slot-number*: Displays the total number of neighbor entries of a specified device in an IRF stack. If no stack is formed, the total number of neighbor entries of the current device is displayed only. The *slot-number* argument indicates the member ID of the device.

**interface** *interface-type interface-number*: Displays the total number of neighbor entries of a specified interface.

**vlan** *vlan-id*: Displays the total number of neighbor entries of a specified VLAN whose ID ranges from 1 to 4094.

## Description

Use the **display ipv6 neighbors count** command to display the total number of neighbor entries satisfying the specified condition.

## Examples

# Display the total number of neighbor entries acquired dynamically.

```
<Sysname> display ipv6 neighbors dynamic count
Total dynamic entry(ies): 2
```

## display ipv6 pathmtu

### Syntax

```
display ipv6 pathmtu { ipv6-address | all | dynamic | static }
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ipv6-address*: IPv6 address whose PMTU information is to be displayed.

**all**: Displays all PMTU information.

**dynamic**: Displays all dynamic PMTU information.

**static**: Displays all static PMTU information.

## Description

Use the **display ipv6 pathmtu** command to display the PMTU information of IPv6 addresses.

## Examples

# Display all PMTU information.

```
<Sysname> display ipv6 pathmtu all
IPv6 Destination Address    ZoneID  PathMTU    Age    Type
fe80::12                   0       1300       40     Dynamic
2222::3                     0       1280       -      Static
```

**Table 1-8 display ipv6 pathmtu** command output description

Field	Description
IPv6 Destination Address	Destination IPv6 address
ZoneID	ID of address zone, currently invalid
PathMTU	PMTU of an IPv6 address
Age	Time for a PMTU to live. For a static PMTU, a hyphen "-" is displayed.
Type	Indicates that the PMTU is dynamically negotiated or statically configured.

## display ipv6 socket

### Syntax

```
display ipv6 socket [ socktype socket-type ] [ task-id socket-id ] [ slot slot-number ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**socktype** *socket-type*: Displays the socket information of this type. The socket type is in the range of 1 to 3. The value "1" represents a TCP socket, "2" a UDP socket, and "3" a raw IP socket.

*task-id*: Displays the socket information of the task. The task ID is in the range 1 to 100.

*socket-id*: Displays the information of the socket. The socket ID is in the range 0 to 3072.

**slot** *slot-number*: Displays the socket information of a specified device in an IRF stack. If no stack is formed, the socket information of the current device is displayed only. The *slot-number* argument indicates the member ID of the device.

### Description

Use the **display ipv6 socket** command to display socket information.

With no parameter specified, this command displays the information about all the sockets; with only the socket type specified, the command displays the information about sockets of the specified type; with the socket type, task ID and socket ID specified, the command displays the information about the specified socket.

### Examples

# Display the information of all sockets.

```
<Sysname> display ipv6 socket
SOCK_STREAM:
Task = VTYP(14), socketid = 4, Proto = 6,
LA = ::->22, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT SO_SENDFVFNID,
```

```

socket state = SS_PRIV SS_ASYNC

Task = VTYP(14), socketid = 3, Proto = 6,
LA = ::->23, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT SO_SENDFVFNID,
socket state = SS_PRIV SS_ASYNC

SOCK_DGRAM:
Task = AGNT(51), socketid = 2, Proto = 17,
LA = ::->161, FA = ::->0,
sndbuf = 9216, rcvbuf = 42080, sb_cc = 0, rb_cc = 0,
socket option = SO_REUSEPORT,
socket state = SS_PRIV SS_NBIO SS_ASYNC

Task = TRAP(52), socketid = 2, Proto = 17,
LA = ::->1024, FA = ::->0,
sndbuf = 9216, rcvbuf = 42080, sb_cc = 0, rb_cc = 0,
socket option = ,
socket state = SS_PRIV

SOCK_RAW:
Task = ROUT(86), socketid = 5, Proto = 89,
LA = ::, FA = ::,
sndbuf = 262144, rcvbuf = 262144, sb_cc = 0, rb_cc = 0,
socket option = SO_REUSEADDR,
socket state = SS_PRIV SS_ASYNC

```

**Table 1-9 display ipv6 socket** command output description

Field	Description
SOCK_STREAM	TCP socket
SOCK_DGRAM	UDP socket
SOCK_RAW	Raw IP socket
Task	Task name and ID of the created socket
socketid	ID assigned by the kernel to the created socket
Proto	Protocol ID
LA	Local address and local port number
FA	Remote address and remote port number
sndbuf	Size of the send buffer
rcvbuf	Size of the receive buffer
sb_cc	Number of bytes sent by the send buffer
rb_cc	Number of bytes received by the receive buffer

Field	Description
socket option	Socket option set by the application
socket state	State of the socket

## display ipv6 statistics

### Syntax

**display ipv6 statistics** [ slot *slot-number* ]

### View

Any view

### Default Level

1: Monitor level

### Parameters

**slot** *slot-number*: Displays statistics of IPv6 packets and ICMPv6 packets on a specified device in an IRF stack. If no stack is formed, related information of the current device is displayed only. The *slot-number* argument indicates the member ID of the device.

### Description

Use the **display ipv6 statistics** command to display statistics of IPv6 packets and ICMPv6 packets. You can use the **reset ipv6 statistics** command to clear all IPv6 and ICMPv6 packet statistics.

### Examples

# Display the statistics of IPv6 packets and ICMPv6 packets.

```
<Sysname> display ipv6 statistics
IPv6 Protocol:
```

```
Sent packets:
```

```
Total:          0
  Local sent out: 0          forwarded:          0
  raw packets:   0          discarded:         0
  routing failed: 0          fragments:         0
  fragments failed: 0
```

```
Received packets:
```

```
Total:          0
  local host:    0          hopcount exceeded: 0
  format error:  0          option error:      0
  protocol error: 0          fragments:         0
  reassembled:   0          reassembly failed: 0
  reassembly timeout: 0
```

ICMPv6 protocol:

Sent packets:

```

Total:      0
  unreachable:      0          too big:      0
  hopcount exceeded: 0          reassembly timeout: 0
  parameter problem: 0
  echo request:     0          echo replied:    0
  neighbor solicit: 0          neighbor advert: 0
  router solicit:0      router advert:    0
  redirected:       0
Send failed:
  ratelimited:     0          other errors:    0
  
```

Received packets:

```

Total:      0
  checksum error:0      too short:      0
  bad code:            0
  unreachable:        0          too big:      0
  hopcount exceeded: 0          reassembly timeout: 0
  parameter problem: 0          unknown error type: 0
  echoed:             0          echo replied:    0
  neighbor solicit: 0          neighbor advert: 0
  router solicit:0      router advert:    0
  redirected:         0          router renumbering: 0
  unknown info type: 0
Deliver failed:
  bad length:        0          ratelimited:    0
  
```

**Table 1-10 display ipv6 statistics command output description**

Field	Description
IPv6 Protocol:	Statistics of IPv6 packets
Sent packets: Total: 0 Local sent out: 0 forwarded: 0 raw packets: 0 discarded: 0 routing failed: 0 fragments: 0 fragments failed: 0	Statistics of sent IPv6 packets, including: <ul style="list-style-type: none"> <li>• Total number of locally sent packets and forwarded packets</li> <li>• Number of packets sent locally</li> <li>• Number of forwarded packets</li> <li>• Number of packets sent via raw socket</li> <li>• Number of discarded packets</li> <li>• Number of packets failing to be routed</li> <li>• Number of sent fragment packets</li> <li>• Number of fragments failing to be sent</li> </ul>

Field	Description
<p>Received packets:</p> <p>Total: 0</p> <p>local host: 0 hopcount exceeded: 0</p> <p>format error: 0 option error: 0</p> <p>protocol error: 0 fragments: 0</p> <p>reassembled: 0 reassembly failed: 0</p> <p>reassembly timeout: 0</p>	<p>Statistics of received IPv6 packets, including</p> <ul style="list-style-type: none"> <li>• Total number of received packets</li> <li>• Number of packets received locally</li> <li>• Number of packets exceeding the hop limit</li> <li>• Number of packets in an incorrect format</li> <li>• Number of packets with incorrect options</li> <li>• Number of packets with incorrect protocol</li> <li>• Number of received fragment packets</li> <li>• Number of reassembled packets</li> <li>• Number of packets failing to be reassembled</li> <li>• Number of packets whose reassembly times out</li> </ul>
<p>ICMPv6 protocol:</p>	<p>Statistics of ICMPv6 packets</p>
<p>Sent packets:</p> <p>Total: 0</p> <p>unreached: 0 too big: 0</p> <p>hopcount exceeded: 0 reassembly timeout: 0</p> <p>parameter problem: 0</p> <p>echo request: 0 echo replied: 0</p> <p>neighbor solicit: 0 neighbor advert: 0</p> <p>router solicit: 0 router advert 0</p> <p>redirected: 0</p> <p>Send failed:</p> <p>ratelimited: 0 other errors: 0</p>	<p>Statistics of sent ICMPv6 packets, including</p> <ul style="list-style-type: none"> <li>• Total number of sent packets</li> <li>• Number of packets whose destination is unreachable</li> <li>• Number of too large packets</li> <li>• Number of packets exceeding the hop limit</li> <li>• Number of packets whose fragmentation and reassembly times out</li> <li>• Number of packets with parameter errors</li> <li>• Number of request packets</li> <li>• Number of response packets</li> <li>• Number of neighbor solicitation packets</li> <li>• Number of neighbor advertisement packets</li> <li>• Number of router solicit packets</li> <li>• Number of router advertisement packets</li> <li>• Number of redirected packets</li> <li>• Number of packets failing to be sent because of rate limitation</li> <li>• Number of packets with other errors</li> </ul>

Field	Description
Received packets: Total: 0 checksum error: 0 too short: 0 bad code 0 unreached: 0 too big: 0 hopcount exceeded: 0 reassembly timeout: 0 parameter problem: 0 unknown error type: 0 echoed: 0 echo replied: 0 neighbor solicit: 0 neighbor advert: 0 router solicit: 0 router advert 0 redirected: 0 router renumbering 0 unknown info type: 0 Deliver failed: bad length: 0 ratelimited: 0	Statistics of received ICMPv6 packets, including <ul style="list-style-type: none"> <li>• Total number of received packets</li> <li>• Number of packets with checksum errors</li> <li>• Number of too small packets</li> <li>• Number of packets with error codes</li> <li>• Number of packets whose destination is unreachable</li> <li>• Number of too large packets</li> <li>• Number of packets exceeding the hop limit</li> <li>• Number of packets whose fragmentation and reassembly times out</li> <li>• Number of packets with parameter errors</li> <li>• Number of packets with unknown errors</li> <li>• Number of request packets</li> <li>• Number of response packets</li> <li>• Number of neighbor solicitation messages</li> <li>• Number of neighbor advertisement packets</li> <li>• Number of router solicitation packets</li> <li>• Number of router advertisement packets</li> <li>• Number of redirected packets</li> <li>• Number of packets recounted by the router</li> <li>• Number of unknown type of packets</li> <li>• Number of packets with a incorrect size</li> <li>• Number of packets failing to be received because of rate limitation</li> </ul>

## display tcp ipv6 statistics

### Syntax

```
display tcp ipv6 statistics
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display tcp ipv6 statistics** command to display IPv6 TCP connection statistics.

You can use the **reset tcp ipv6 statistics** command to clear statistics of all IPv6 TCP packets.

### Examples

```
# Display the statistics of IPv6 TCP connections.
```

```
<Sysname> display tcp ipv6 statistics
```

```
Received packets:
```

```

Total: 0
packets in sequence: 0 (0 bytes)
window probe packets: 0, window update packets: 0
checksum error: 0, offset error: 0, short error: 0

duplicate packets: 0 (0 bytes), partially duplicate packets: 0 (0 bytes)
out-of-order packets: 0 (0 bytes)
packets with data after window: 0 (0 bytes)
packets after close: 0

ACK packets: 0 (0 bytes)
duplicate ACK packets: 0, too much ACK packets: 0

Sent packets:
Total: 0
urgent packets: 0
control packets: 0 (including 0 RST)
window probe packets: 0, window update packets: 0

data packets: 0 (0 bytes) data packets retransmitted: 0 (0 bytes)
ACK only packets: 0 (0 delayed)

Retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
Keepalive timeout: 0, keepalive probe: 0, Keepalive timeout, so connections disconnected :
0
Initiated connections: 0, accepted connections: 0, established connections: 0
Closed connections: 0 (dropped: 0, initiated dropped: 0)

```

**Table 1-11 display tcp ipv6 statistics** command output description

Field	Description
Received packets:	Statistics of received packets, including <ul style="list-style-type: none"> <li>• Total number of received packets</li> <li>• Number of packets received in sequence</li> <li>• Number of window probe packets</li> <li>• Number of window size update packets</li> <li>• Number of packets with checksum errors</li> <li>• Number of packets with offset errors</li> <li>• Number of packets whose total length is less than specified by the packet header</li> <li>• Number of duplicate packets</li> <li>• Number of partially duplicate packets</li> <li>• Number of out-of-order packets</li> <li>• Number of packets exceeding the size of the receiving window</li> <li>• Number of packets received after the connection is closed</li> <li>• Number of ACK packets</li> <li>• Number of duplicate ACK packets</li> <li>• Number of excessive ACK packets</li> </ul>
Total: 0	
packets in sequence: 0 (0 bytes)	
window probe packets: 0	
window update packets: 0	
checksum error: 0	
offset error: 0	
short error: 0	
duplicate packets: 0 (0 bytes), partially duplicate packets: 0 (0 bytes)	
out-of-order packets: 0 (0 bytes)	
packets with data after window: 0 (0 bytes)	
packets after close: 0	
ACK packets: 0 (0 bytes)	
duplicate ACK packets: 0	
too much ACK packets: 0	

Field	Description
Sent packets: Total: 0 urgent packets: 0 control packets: 0 (including 0 RST) window probe packets: 0 window update packets: 0  data packets: 0 (0 bytes) data packets retransmitted: 0 (0 bytes) ACK only packets: 0 (0 delayed)	Statistics of sent packets, including <ul style="list-style-type: none"> <li>• Total number of packets</li> <li>• Number of packets containing an urgent indicator</li> <li>• Number of control packets</li> <li>• Number of window probe packets</li> <li>• Number of window update packets</li> <li>• Number of data packets</li> <li>• Number of retransmitted packets</li> <li>• Number of ACK packets</li> </ul>
Retransmitted timeout	Number of packets whose retransmission times out
connections dropped in retransmitted timeout	Number of connections dropped because of retransmission timeout
Keepalive timeout	Number of keepalive timeouts
keepalive probe	Number of keepalive probes
Keepalive timeout, so connections disconnected	Number of connections dropped because of keepalive response timeout
Initiated connections	Number of initiated connections
accepted connections	Number of accepted connections
established connections	Number of established connections
Closed connections	Number of closed connections
dropped	Number of dropped connections (after SYN is received from the peer)
initiated dropped	Number of initiated but dropped connections (before SYN is received from the peer)

## display tcp ipv6 status

### Syntax

```
display tcp ipv6 status
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display tcp ipv6** command to display the IPv6 TCP connection status, including IP address of

the IPv6 TCP control block, local and peer IPv6 addresses, and status of the IPv6 TCP connection.

## Examples

```
# Display the IPv6 TCP connection status.
```

```
<Sysname> display tcp ipv6 status
```

```
TCP6CB      Local Address      Foreign Address      State
045d8074    ::->21              ::->0                 Listening
```

**Table 1-12 display tcp ipv6 status** command output description

Field	Description
TCP6CB	IPv6 address of the TCP control block (hexadecimal)
Local Address	Local IPv6 address
Foreign Address	Remote IPv6 address
State	IPv6 TCP connection status, including <ul style="list-style-type: none"><li>• Closed</li><li>• Listening</li><li>• Syn_Sent</li><li>• Syn_Rcvd</li><li>• Established</li><li>• Close_Wait</li><li>• Fin_Wait1</li><li>• Closing</li><li>• Last_Ack</li><li>• Fin_Wait2</li><li>• Time_Wait</li></ul>

## display udp ipv6 statistics

### Syntax

```
display udp ipv6 statistics
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display udp ipv6 statistics** command to display the statistics of IPv6 UDP packets.

You can use the **reset udp ipv6 statistics** command to clear the statistics of all IPv6 UDP packets.

## Examples

```
# Display the statistics information of IPv6 UDP packets.
```

```

<Sysname> display udp ipv6 statistics
Received packets:
    Total: 0
    checksum error: 0
    shorter than header: 0, data length larger than packet: 0
    unicast(no socket on port): 0
    broadcast/multicast(no socket on port): 0
    not delivered, input socket full: 0
    input packets missing pcb cache: 0
Sent packets:
    Total: 0

```

**Table 1-13 display udp ipv6 statistics command output description**

Field	Description
Total	Total number of received/sent packets
checksum error	Total number of packets with a checksum error
shorter than header	Total number of IPv6 UDP packets whose total length is less than that specified by the packet header
data length larger than packet	Total number of packets whose data length exceeds that specified by the packet header
unicast(no socket on port)	Total number of received unicast packets without any socket
broadcast/multicast(no socket on port)	Total number of received broadcast/multicast packets without any socket
not delivered, input socket full	Number of packets not handled because of the receive buffer being full
input packet missing pcb cache	Number of packets failing to match the protocol control block (PCB) cache

## dns server ipv6

### Syntax

```

dns server ipv6 ipv6-address [ interface-type interface-number ]
undo dns server ipv6 ipv6-address [ interface-type interface-number ]

```

### View

System view

### Default Level

2: System level

### Parameters

*ipv6-address*: IPv6 address of a DNS server.

*interface-type interface-number*: Specifies an interface. When the IPv6 address of the DNS server is a link-local address, this argument must be specified.

## Description

Use the **dns server ipv6** command to specify a DNS server.

Use the **undo dns server ipv6** command to remove the specified DNS server.

By default, no DNS server is configured.

## Examples

```
# Specify a DNS server at 2002::1.  
<Sysname> system-view  
[Sysname] dns server ipv6 2002::1
```

## ipv6

### Syntax

```
ipv6  
undo ipv6
```

### View

System view

### Default Level

2: System level

### Parameters

None

## Description

Use the **ipv6** command to enable IPv6.

Use the **undo ipv6** command to disable IPv6.

By default, IPv6 is disabled.

## Examples

```
# Enable IPv6.  
<Sysname> system-view  
[Sysname] ipv6
```

## ipv6 address

### Syntax

```
ipv6 address { ipv6-address prefix-length | ipv6-address/prefix-length }  
undo ipv6 address [ ipv6-address prefix-length | ipv6-address/prefix-length ]
```

### View

Interface view

## Default Level

2: System level

## Parameters

*ipv6-address*: IPv6 address.

*prefix-length*: Prefix length of the IPv6 address, in the range 1 to 128.

## Description

Use the **ipv6 address** command to configure an IPv6 site-local address or aggregatable global unicast address for an interface.

Use the **undo ipv6 address** command to remove the IPv6 address from the interface.

By default, no site-local address or global unicast address is configured for an interface.

Note that except the link-local address automatically configured, all IPv6 addresses will be removed from the interface if you carry out the **undo ipv6 address** command without any parameter specified.

## Examples

```
# Set the aggregatable global IPv6 unicast address of VLAN-interface 100 to 2001::1 with prefix length 64.
```

Method I:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64
```

Method II:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1 64
```

## ipv6 address auto link-local

### Syntax

```
ipv6 address auto link-local
```

```
undo ipv6 address auto link-local
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **ipv6 address auto link-local** command to automatically generate a link-local address for an interface.

Use the **undo ipv6 address auto link-local** command to remove the automatically generated link-local address for the interface.

By default, a link-local address will automatically be generated after a site-local or global IPv6 unicast address is configured for an interface.

Note that:

- After an IPv6 site-local address or aggregatable global unicast address is configured for an interface, a link-local address is generated automatically. The automatically generated link-local address is the same as the one generated by using the **ipv6 address auto link-local** command.
- The **undo ipv6 address auto link-local** command can only remove the link-local addresses generated through the **ipv6 address auto link-local** command. Therefore, after the **undo ipv6 address auto link-local** command is used on an interface that has an IPv6 site-local address or aggregatable global unicast address configured, the interface still has a link-local address. If the interface has no IPv6 site-local address or aggregatable global unicast address configured, it will have no link-local address.
- Manual assignment takes precedence over automatic generation. That is, if you first adopt automatic generation and then manual assignment, the manually assigned link-local address will overwrite the automatically generated one. If you first adopt manual assignment and then automatic generation, the automatically generated link-local address will not take effect and the link-local address of an interface is still the manually assigned one. If you delete the manually assigned address, the automatically generated link-local address is validated. For manually assignment of an IPv6 link-local address, refer to the **ipv6 address link-local** command.

## Examples

```
# Configure VLAN-interface 100 to automatically generate a link-local address.
```

```
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] ipv6 address auto link-local
```

## ipv6 address eui-64

### Syntax

```
ipv6 address ipv6-address/prefix-length eui-64  
undo ipv6 address ipv6-address/prefix-length eui-64
```

### View

Interface view

### Default Level

2: System level

### Parameters

*ipv6-address/prefix-length*: IPv6 address and IPv6 prefix. The *ipv6-address* and *prefix-length* arguments jointly specify the prefix of an IPv6 address in the EUI-64 format.

### Description

Use the **ipv6 address eui-64** command to configure a site-local address or global unicast address in

the EUI-64 format for an interface.

Use the **undo ipv6 address eui-64** command to remove the configured site-local address or global unicast address in the EUI-64 format for the interface.

By default, no site-local or global unicast address in the EUI-64 format is configured for an interface.

An EUI-64 IPv6 address is generated based on the specified prefix and the MAC address of the local device and can be displayed by using the **display ipv6 interface** command.

Note that you cannot specify the prefix length of an IPv6 address in the EUI-64 format to be greater than 64.

## Examples

# Configure an IPv6 address in the EUI-64 format for VLAN-interface 100. The prefix length of the address is the same as that of 2001::1/64, and the interface ID is generated based on the MAC address of the device.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64 eui-64
```

## ipv6 address link-local

### Syntax

```
ipv6 address ipv6-address link-local
undo ipv6 address ipv6-address link-local
```

### View

Interface view

### Default Level

2: System level

### Parameters

*ipv6-address*: IPv6 link-local address. The first 10 bits of an address must be 1111111010 (binary), that is, the first group of hexadecimals in the address must be FE80 to FEBF.

### Description

Use the **ipv6 address link-local** command to configure a link-local address for the interface.

Use the **undo ipv6 address link-local** command to remove the configured link-local address for the interface.

Note that:

Manual assignment takes precedence over automatic generation. That is, if you first adopt automatic generation and then manual assignment, the manually assigned link-local address will overwrite the automatically generated one. If you first adopt manual assignment and then automatic generation, the automatically generated link-local address will not take effect and the link-local address of an interface is still the manually assigned one. If you delete the manually assigned address, the automatically generated link-local address is validated. For automatic generation of an IPv6 link-local address, refer to the **ipv6 address auto link-local** command.

## Examples

```
# Configure a link-local address for VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address fe80::1 link-local
```

## ipv6 hoplimit-expires enable

### Syntax

```
ipv6 hoplimit-expires enable
undo ipv6 hoplimit-expires
```

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **ipv6 hoplimit-expires enable** command to enable the sending of ICMPv6 time exceeded packets.

Use the **undo ipv6 hoplimit-expires** command to disable the sending of ICMPv6 time exceeded packets.

By default, the sending of ICMPv6 time exceeded packets is enabled.

Note that:

After you disable the sending of ICMPv6 time exceeded packets, the device will not send time-to-live count exceeded packets, but will still send fragment reassembly time exceeded packets.

## Examples

```
# Disable the sending of ICMPv6 time exceeded packets.
<Sysname> system-view
[Sysname] undo ipv6 hoplimit-expires
```

## ipv6 host

### Syntax

```
ipv6 host hostname ipv6-address
undo ipv6 host hostname [ ipv6-address ]
```

### View

System view

## Default Level

2: System level

## Parameters

*hostname*: Host name, a string of up to 20 characters. The character string can contain letters, numerals, “\_”, “-”, or “.” and must contain at least one letter.

*ipv6-address*: IPv6 address.

## Description

Use the **ipv6 host** command to configure the mappings between host names and IPv6 addresses.

Use the **undo ipv6 host** command to remove the mappings between host names and IPv6 addresses.

Each host name can correspond to only one IPv6 address.

Related commands: **display ipv6 host**.

## Examples

```
# Configure the mapping between a host name and an IPv6 address.
```

```
<Sysname> system-view  
[Sysname] ipv6 host aaa 2001::1
```

## ipv6 icmp-error

### Syntax

```
ipv6 icmp-error { bucket bucket-size | ratelimit interval } *  
undo ipv6 icmp-error
```

### View

System view

## Default Level

2: System level

## Parameters

**bucket** *bucket-size*: Number of tokens in the token bucket, in the range of 1 to 200.

**ratelimit** *interval*: Update period of the token bucket in milliseconds, in the range of 0 to 2,147,483,647. The update period “0” indicates that the number of ICMPv6 error packets sent is not restricted.

## Description

Use the **ipv6 icmp-error** command to configure the size and update period of the token bucket.

Use the **undo ipv6 icmp-error** command to restore the defaults.

By default, the size is 10 and the update period is 100 milliseconds. That is, at most 10 ICMPv6 error packets can be sent within 100 milliseconds.

## Examples

```
# Set the capacity of the token bucket to 50 and the update period to 100 milliseconds.
```

```
<Sysname> system-view
```

```
[Sysname] ipv6 icmp-error bucket 50 ratelimit 100
```

## ipv6 icmpv6 multicast-echo-reply enable

### Syntax

```
ipv6 icmpv6 multicast-echo-reply enable  
undo ipv6 icmpv6 multicast-echo-reply
```

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **ipv6 icmpv6 multicast-echo-reply enable** command to enable the sending of multicast echo replies.

Use the **undo ipv6 icmpv6 multicast-echo-reply** command to disable the sending of multicast echo replies.

By default, the device is disabled from sending multicast echo replies.

### Examples

```
# Enable the sending of multicast echo replies.  
<Sysname> system-view  
[Sysname] ipv6 icmpv6 multicast-echo-reply enable
```

## ipv6 nd autoconfig managed-address-flag

### Syntax

```
ipv6 nd autoconfig managed-address-flag  
undo ipv6 nd autoconfig managed-address-flag
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **ipv6 nd autoconfig managed-address-flag** command to set the managed address

configuration (M) flag to 1 so that the host can acquire an IPv6 address through stateful autoconfiguration (for example, from a DHCP server).

Use the **undo ipv6 nd autoconfig managed-address-flag** command to restore the default.

By default, the M flag is set to **0** so that the host can acquire an IPv6 address through stateless autoconfiguration.

## Examples

# Configure the host to acquire an IPv6 address through stateful autoconfiguration.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
```

## ipv6 nd autoconfig other-flag

### Syntax

```
ipv6 nd autoconfig other-flag
undo ipv6 nd autoconfig other-flag
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **ipv6 nd autoconfig other-flag** command to set the other stateful configuration flag (O) to 1 so that the host can acquire information other than IPv6 address through stateful autoconfiguration (for example, from a DHCP server).

Use the **undo ipv6 nd autoconfig other-flag** command to restore the default.

By default, the O flag is set to **0** so that the host can acquire other information through stateless autoconfiguration.

## Examples

# Configure the host to acquire information other than IPv6 address through stateless autoconfiguration.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo ipv6 nd autoconfig other-flag
```

## ipv6 nd dad attempts

### Syntax

```
ipv6 nd dad attempts value
```

## **undo ipv6 nd dad attempts**

### **View**

Interface view

### **Default Level**

2: System level

### **Parameters**

*value*: Number of attempts to send an NS message for DAD, in the range of 0 to 600. The default value is "1". When it is set to 0, DAD is disabled.

### **Description**

Use the **ipv6 nd dad attempts** command to configure the number of attempts to send an NS message for DAD.

Use the **undo ipv6 nd dad attempts** command to restore the default.

By default, the number of attempts to send an NS message for DAD is 1.

Related commands: **display ipv6 interface**.

### **Examples**

# Set the number of attempts to send an NS message for DAD to 20.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd dad attempts 20
```

## **ipv6 nd hop-limit**

### **Syntax**

**ipv6 nd hop-limit** *value*

**undo ipv6 nd hop-limit**

### **View**

System view

### **Default Level**

2: System level

### **Parameters**

*value*: Number of hops, in the range of 0 to 255. When it is set to 0, the Hop Limit field in RA messages sent by the device is 0. That is, the number of hops is determined by the requesting device itself.

### **Description**

Use the **ipv6 nd hop-limit** command to configure the hop limit advertised by the device.

Use the **undo ipv6 nd hop-limit** command to restore the default hop limit.

By default, the hop limit advertised by the device is 64.

## Examples

```
# Set the hop limit advertised by the device to 100.
<Sysname> system-view
[Sysname] ipv6 nd hop-limit 100
```

## ipv6 nd ns retrans-timer

### Syntax

```
ipv6 nd ns retrans-timer value
undo ipv6 nd ns retrans-timer
```

### View

Interface view

### Default Level

2: System level

### Parameters

*value*: Interval for retransmitting an NS message in milliseconds, in the range of 1,000 to 4,294,967,295.

### Description

Use the **ipv6 nd ns retrans-timer** command to set the interval for retransmitting an NS message. The local interface retransmits an NS message at intervals of this value. Furthermore, the Retrans Timer field in RA messages sent by the local interface is equal to this value.

Use the **undo ipv6 nd ns retrans-timer** command to restore the default.

By default, the local interface retransmits an NS message at intervals of 1,000 milliseconds and the Retrans Timer field in RA messages sent by the local interface is 0.

Related commands: **display ipv6 interface**.

## Examples

```
# Specify VLAN-interface 100 to retransmit NS messages at intervals of 10,000 milliseconds.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ns retrans-timer 10000
```

## ipv6 nd nud reachable-time

### Syntax

```
ipv6 nd nud reachable-time value
undo ipv6 nd nud reachable-time
```

### View

Interface view

## Default Level

2: System level

## Parameters

*value*: Neighbor reachable time in milliseconds, in the range of 1 to 3,600,000.

## Description

Use the **ipv6 nd nud reachable-time** command to configure the neighbor reachable time on an interface. This time value serves as not only the neighbor reachable time on the local interface, but also the value of the Reachable Timer field in RA messages sent by the local interface.

Use the **undo ipv6 nd nud reachable-time** command to restore the default neighbor reachable time and to specify the value of the Reachable Timer field in RA messages as 0, so that the number of hops is determined by the requesting device itself.

By default, the neighbor reachable time on the local interface is 30,000 milliseconds and the Reachable Timer field in RA messages is 0.

Related commands: **display ipv6 interface**.

## Examples

```
# Set the neighbor reachable time on VLAN-interface 100 to 10,000 milliseconds.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd nud reachable-time 10000
```

## ipv6 nd ra halt

### Syntax

```
ipv6 nd ra halt
undo ipv6 nd ra halt
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **ipv6 nd ra halt** command to enable RA message suppression.

Use the **undo ipv6 nd ra halt** command to disable RA message suppression.

By default, RA messages are suppressed.

### Examples

```
# Suppress RA messages on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra halt
```

## ipv6 nd ra interval

### Syntax

```
ipv6 nd ra interval max-interval-value min-interval-value
undo ipv6 nd ra interval
```

### View

Interface view

### Default Level

2: System level

### Parameters

*max-interval-value*: Maximum interval for advertising RA messages in seconds, in the range of 4 to 1,800.

*min-interval-value*: Minimum interval for advertising RA messages in seconds, in the range of 3 to 1,350.

### Description

Use the **ipv6 nd ra interval** command to set the maximum and minimum intervals for advertising RA messages. The device advertises RA messages at intervals of a random value between the maximum interval and the minimum interval.

Use the **undo ipv6 nd ra interval** command to restore the default.

By default, the maximum interval between RA messages is 600 seconds, and the minimum interval is 200 seconds.

Note the following:

- The minimum interval should be three-fourths of the maximum interval or less.
- The maximum interval for sending RA messages should be less than or equal to the router lifetime in RA messages.

### Examples

```
# Set the maximum interval for advertising RA messages to 1,000 seconds and the minimum interval to 700 seconds.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra interval 1000 700
```

## ipv6 nd ra prefix

### Syntax

```
ipv6 nd ra prefix { ipv6-address prefix-length | ipv6-address/prefix-length } valid-lifetime preferred-lifetime [ no-autoconfig | off-link ] *
```

**undo ipv6 nd ra prefix *ipv6-prefix***

## View

Interface view

## Default Level

2: System level

## Parameters

*ipv6-address*: IPv6 address or IPv6 address prefix.

*prefix-length*: Prefix length of the IPv6 address.

*ipv6-prefix*: IPv6 address prefix.

*valid-lifetime*: Valid lifetime of a prefix in seconds, in the range of 0 to 4,294,967,295.

*preferred-lifetime*: Preferred lifetime of a prefix used for stateless autoconfiguration in seconds, in the range of 0 to 4,294,967,295.

**no-autoconfig**: Specifies a prefix not to be used for stateless autoconfiguration. If this keyword is not provided, the prefix is used for stateless autoconfiguration.

**off-link**: Specifies the address with the prefix not to be directly reachable on the link. If this keyword is not provided, the address with the prefix is directly reachable on the link.

## Description

Use the **ipv6 nd ra prefix** command to configure the prefix information in RA messages.

Use the **undo ipv6 nd ra prefix** command to remove the prefix information from RA messages.

By default, no prefix information is configured in RA messages and the IPv6 address of the interface sending RA messages is used as the prefix information.

## Examples

```
# Configure the prefix information for RA messages on VLAN-interface 100.
```

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 100
```

```
[Sysname-Vlan-interface100] ipv6 nd ra prefix 2001:10::100/64 100 10
```

## ipv6 nd ra router-lifetime

### Syntax

**ipv6 nd ra router-lifetime *value***

**undo ipv6 nd ra router-lifetime**

### View

Interface view

### Default Level

2: System level

## Parameters

*value*: Router lifetime in seconds, in the range of 0 to 9,000. When it is set to 0, the device does not serve as the default router.

## Description

Use the **ipv6 nd ra router-lifetime** command to configure the router lifetime in RA messages.

Use the **undo ipv6 nd ra router-lifetime** command to restore the default.

By default, the router lifetime in RA messages is 1,800 seconds.

Note that the router lifetime in RA messages should be greater than or equal to the advertising interval.

## Examples

```
# Set the router lifetime in RA messages on VLAN-interface 100 to 1,000 seconds.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra router-lifetime 1000
```

## ipv6 neighbor

### Syntax

```
ipv6 neighbor ipv6-address mac-address { vlan-id port-type port-number | interface interface-type interface-number }
```

```
undo ipv6 neighbor ipv6-address interface-type interface-number
```

### View

System view

### Default Level

2: System level

### Parameters

*ipv6-address*: IPv6 address of the static neighbor entry.

*mac-address*: MAC address of the static neighbor entry (48 bits long, in the format of H-H-H).

*vlan-id*: VLAN ID of the static neighbor entry, in the range of 1 to 4094.

*port-type port-number*: Type and number of a Layer 2 port of the static neighbor entry.

**interface** *interface-type interface-number*: Type and number of a Layer 3 interface of the static neighbor entry.

### Description

Use the **ipv6 neighbor** command to configure a static neighbor entry.

Use the **undo ipv6 neighbor** command to remove a static neighbor entry.

You can use a Layer 3 VLAN interface or a Layer 2 port in the VLAN to configure a static neighbor entry.

- If the first method is used, the neighbor entry is in the INCMP state. After the device obtains the corresponding Layer 2 port information through resolution, the neighbor entry will go into the REACH state.

- If the second method is used, the corresponding VLAN interface must exist and the port specified by *port-type port-number* must belong to the VLAN specified by *vlan-id*. After the static neighbor entry is configured, the device will relate the VLAN interface with the IPv6 address to identify the static neighbor entry uniquely and the entry will be in the REACH state.

To remove a static neighbor entry, you only need to specify the corresponding VLAN interface and the neighbor address.

Related commands: **display ipv6 neighbors**.

## Examples

# Configure a static neighbor entry for Layer 2 port GigabitEthernet1/0/1 of VLAN 100.

```
<Sysname> system-view
[Sysname] ipv6 neighbor 2000::1 fe-e0-89 100 gigabitethernet 1/0/1
```

## ipv6 neighbors max-learning-num

### Syntax

```
ipv6 neighbors max-learning-num number
undo ipv6 neighbors max-learning-num
```

### View

Interface view

### Default Level

2: System level

### Parameters

*number*: Maximum number of neighbors that can be dynamically learned by the interface, in the range 1 to 4096.

### Description

Use the **ipv6 neighbors max-learning-num** command to configure the maximum number of neighbors that can be dynamically learned on the interface.

Use the **undo ipv6 neighbors max-learning-num** command to restore the default.

By default, the maximum number of neighbors that can be dynamically learned on the interface is 4096.

## Examples

# Set the maximum number of neighbors that can be dynamically learned on VLAN-interface 100 to 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 neighbors max-learning-num 10
```

## ipv6 pathmtu

### Syntax

```
ipv6 pathmtu ipv6-address [ value ]
undo ipv6 pathmtu ipv6-address
```

## View

System view

## Default Level

2: System level

## Parameters

*ipv6-address*: IPv6 address.

*value*: PMTU of a specified IPv6 address in bytes. It ranges from 1280 to 10000.

## Description

Use the **ipv6 pathmtu** command to configure a static PMTU for a specified IPv6 address.

Use the **undo ipv6 pathmtu** command to remove the PMTU configuration for a specified IPv6 address.

By default, no static PMTU is configured.

## Examples

# Configure a static PMTU for a specified IPv6 address.

```
<Sysname> system-view  
[Sysname] ipv6 pathmtu fe80::12 1300
```

## ipv6 pathmtu age

### Syntax

**ipv6 pathmtu age** *age-time*

**undo ipv6 pathmtu age**

### View

System view

### Default Level

2: System level

### Parameters

*age-time*: Aging time for PMTU in minutes, in the range of 10 to 100.

### Description

Use the **ipv6 pathmtu age** command to configure the aging time for a dynamic PMTU.

Use the **undo ipv6 pathmtu age** command to restore the default.

By default, the aging time is 10 minutes.

Note that the aging time is invalid for a static PMTU.

Related commands: **display ipv6 pathmtu**.

### Examples

# Set the aging time for a dynamic PMTU to 40 minutes.

```
<Sysname> system-view
```

## reset dns ipv6 dynamic-host

### Syntax

```
reset dns ipv6 dynamic-host
```

### View

User view

### Default Level

2: System level

### Parameters

None

### Description

Use the **reset dns ipv6 dynamic-host** command to clear IPv6 dynamic domain name cache information.

You can use the **display dns ipv6 dynamic-host** command to display the current IPv6 dynamic domain name cache information.

### Examples

```
# Clear IPv6 dynamic domain name cache information.
```

```
<Sysname> reset dns ipv6 dynamic-host
```

## reset ipv6 neighbors

### Syntax

```
reset ipv6 neighbors { all | dynamic | interface interface-type interface-number | slot slot-number | static }
```

### View

User view

### Default Level

2: System level

### Parameters

**all**: Clears static and dynamic neighbor information on all interfaces.

**dynamic**: Clears dynamic neighbor information on all interfaces.

**interface** *interface-type interface-number*: Clears dynamic neighbor information on a specified interface.

**slot** *slot-number*: Clears dynamic neighbor information on a specified device in an IRF stack. If no stack is formed, only the dynamic neighbor information of the current device is cleared. The *slot-number* argument indicates the member ID of the device.

**static:** Clears static neighbor information on all interfaces.

## Description

Use the **reset ipv6 neighbors** command to clear IPv6 neighbor information.

You can use the **display ipv6 neighbors** command to display the current IPv6 neighbor information.

## Examples

# Clear neighbor information on all interfaces.

```
<Sysname> reset ipv6 neighbors all
```

# Clear dynamic neighbor information on all interfaces.

```
<Sysname> reset ipv6 neighbors dynamic
```

# Clear all neighbor information on VLAN-interface 1.

```
<Sysname> reset ipv6 neighbors interface vlan-interface 1
```

## reset ipv6 pathmtu

### Syntax

```
reset ipv6 pathmtu { all | static | dynamic }
```

### View

User view

### Default Level

2: System level

### Parameters

**all:** Clears all PMTUs.

**static:** Clears all static PMTUs.

**dynamic:** Clears all dynamic PMTUs.

### Description

Use the **reset ipv6 pathmtu** the command to clear the PMTU information.

### Examples

# Clear all PMTUs.

```
<Sysname> reset ipv6 pathmtu all
```

## reset ipv6 statistics

### Syntax

```
reset ipv6 statistics [ slot slot-number ]
```

### View

User view

## Default Level

2: System level

## Parameters

**slot** *slot number*: Clears the statistics of IPv6 packets and ICMPv6 packets on a specified device in an IRF stack. If no stack is formed, related information on the current device is cleared only. The *slot-number* argument indicates the member ID of the device.

## Description

Use the **reset ipv6 statistics** command to clear the statistics of IPv6 packets and ICMPv6 packets.

You can use the **display ipv6 statistics** command to display the statistics of IPv6 and ICMPv6 packets.

## Examples

```
# Clear the statistics of IPv6 packets and ICMPv6 packets.
```

```
<Sysname> reset ipv6 statistics
```

## reset tcp ipv6 statistics

### Syntax

```
reset tcp ipv6 statistics
```

### View

User view

## Default Level

2: System level

## Parameters

None

## Description

Use the **reset tcp ipv6 statistics** command to clear the statistics of all IPv6 TCP connections.

You can use the **display tcp ipv6 statistics** command to display the statistics of IPv6 TCP connections.

## Examples

```
# Clear the statistics of all IPv6 TCP connections.
```

```
<Sysname> reset tcp ipv6 statistics
```

## reset udp ipv6 statistics

### Syntax

```
reset udp ipv6 statistics
```

### View

User view

## Default Level

2: System level

## Parameters

None

## Description

Use the **reset udp ipv6 statistics** command to clear the statistics of all IPv6 UDP packets.

You can use the **display udp ipv6 statistics** command to display the statistics of IPv6 UDP packets.

## Examples

```
# Clear the statistics of all IPv6 UDP packets.
```

```
<Sysname> reset udp ipv6 statistics
```

## tcp ipv6 timer fin-timeout

### Syntax

```
tcp ipv6 timer fin-timeout wait-time
```

```
undo tcp ipv6 timer fin-timeout
```

### View

System view

## Default Level

2: System level

## Parameters

*wait-time*: Length of the finwait timer for IPv6 TCP connections in seconds, in the range of 76 to 3,600.

## Description

Use the **tcp ipv6 timer fin-timeout** command to set the finwait timer for IPv6 TCP connections.

Use the **undo tcp ipv6 timer fin-timeout** command to restore the default.

By default, the length of the finwait timer is 675 seconds.

## Examples

```
# Set the finwait timer length of IPv6 TCP connections to 800 seconds.
```

```
<Sysname> system-view
```

```
[Sysname] tcp ipv6 timer fin-timeout 800
```

## tcp ipv6 timer syn-timeout

### Syntax

```
tcp ipv6 timer syn-timeout wait-time
```

```
undo tcp ipv6 timer syn-timeout
```

## View

System view

## Default Level

2: System level

## Parameters

*wait-time*: Length of the synwait timer for IPv6 TCP connections in seconds, in the range of 2 to 600.

## Description

Use the **tcp ipv6 timer syn-timeout** command to set the synwait timer for IPv6 TCP connections

Use the **undo tcp ipv6 timer syn-timeout** command to restore the default.

By default, the length of the synwait timer of IPv6 TCP connections is 75 seconds.

## Examples

```
# Set the synwait timer length of IPv6 TCP connections to 100 seconds.
```

```
<Sysname> system-view
```

```
[Sysname] tcp ipv6 timer syn-timeout 100
```

## tcp ipv6 window

### Syntax

```
tcp ipv6 window size
```

```
undo tcp ipv6 window
```

### View

System view

### Default Level

2: System level

### Parameters

*size*: Size of the IPv6 TCP send/receive buffer in KB (kilobyte), in the range of 1 to 32.

### Description

Use the **tcp ipv6 window** command to set the size of the IPv6 TCP send/receive buffer.

Use the **undo tcp ipv6 window** command to restore the default.

By default, the size of the IPv6 TCP send/receive buffer is 8 KB.

### Examples

```
# Set the size of the IPv6 TCP send/receive buffer to 4 KB.
```

```
<Sysname> system-view
```

```
[Sysname] tcp ipv6 window 4
```

# Table of Contents

<b>1 Tunneling Configuration Commands</b> .....	<b>1-1</b>
Tunnel Configuration Commands .....	1-1
destination .....	1-1
display interface tunnel .....	1-2
display ipv6 interface tunnel .....	1-3
interface tunnel .....	1-7
service-loopback-group .....	1-7
source .....	1-8
tunnel-protocol .....	1-9

# 1 Tunneling Configuration Commands

---



## Note

The tunnel interface number is in the A/B/C format, where A, B, and C represent the stack member device ID, the sub-slot number, and the tunnel interface number respectively. The value ranges of A and B vary with devices. C is in the range of 0 to 126.

---

## Tunnel Configuration Commands

### destination

#### Syntax

**destination** *ip-address*

**undo destination**

#### View

Tunnel interface view

#### Default Level

2: System level

#### Parameters

*ip-address*: Tunnel destination IPv4 address.

#### Description

Use the command **destination** to specify the destination address for the tunnel interface.

Use the **undo destination** command to remove the configured tunnel destination address.

By default, no tunnel destination address is configured.

Note that:

- The tunnel destination address is the address of the peer interface receiving packets and should be configured as the source address of the peer tunnel interface.
- Two or more tunnel interfaces using the same encapsulation protocol must have different source and destination addresses.

Related commands: **interface tunnel**, **source**.

## Examples

# Set the interface VLAN-interface 100 (193.101.1.1) of Sysname 1 and the interface VLAN-interface 100 (192.100.1.1) of Sysname 2 as the source and destination interfaces of a tunnel between the two devices, respectively.

```
<Sysname1> system-view
[Sysname1] interface tunnel 1/0/0
[Sysname1-Tunnel1/0/0] source 193.101.1.1
[Sysname1-Tunnel1/0/0] destination 192.100.1.1
<Sysname2> system-view
[Sysname2] interface tunnel 1/0/1
[Sysname2-Tunnel1/0/1] source 192.100.1.1
[Sysname2-Tunnel1/0/1] destination 193.101.1.1
```

## display interface tunnel

### Syntax

```
display interface tunnel [ number ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*number*: Tunnel interface number. If the *number* argument is not specified, the information of all tunnel interfaces will be displayed.

### Description

Use the **display interface tunnel** command to display related information of a specified tunnel interface, such as source address, destination address, and encapsulation mode.

Related commands: **interface tunnel**, **source**, **destination**, **tunnel-protocol**.

## Examples

# Display the information of the interface tunnel 1/0/0.

```
<Sysname> display interface tunnel 1/0/0
Tunnel1/0/0 current state: DOWN
Line protocol current state: DOWN
Description: Tunnel1/0/0 Interface
The Maximum Transmit Unit is 64000
Internet Address is 1.1.1.1/24 Primary
Encapsulation is TUNNEL, service-loopback-group ID not set.
Tunnel source unknown, destination unknown
Tunnel protocol/transport IPv6/IP
    Last 300 seconds input:  0 bytes/sec, 0 packets/sec
    Last 300 seconds output: 0 bytes/sec, 0 packets/sec
```

```

0 packets input, 0 bytes
0 input error
0 packets output, 0 bytes
0 output error

```

**Table 1-1 display interface tunnel** command output description

Field	Description
Tunnel1/0/0 current state	The physical-layer connectivity of the tunnel interface.
Line protocol current state	The link-layer connectivity of the tunnel interface.
Description	Descriptive information of the tunnel interface
Tunnel1/0/0 Interface	Tunnel interface number
Maximum Transmit Unit	Maximum transmission unit (MTU) in the tunnel
Encapsulation is TUNNEL	The encapsulation protocol is tunnel.
service-loopback-group ID	Service loopback group referenced by the tunnel.
Tunnel source	Tunnel source address
destination	Tunnel destination address
Tunnel protocol/transport	Tunnel protocol and transport protocol.
Last 300 seconds input	Number of bytes and packets input per second in the last five minutes.
Last 300 seconds output	Number of bytes and packets output per second in the last five minutes.
packets input	Total number of input packets.
input error	Number of error packets among all input packets.
packets output	Total number of output packets.
output error	Number of error packets in all output packets

## display ipv6 interface tunnel

### Syntax

```
display ipv6 interface tunnel [ number ] [ verbose ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*number*: Tunnel interface number.

**verbose**: Displays the detailed configuration and IPv6 packet statistics of the specified tunnel interface.

## Description

Use the **display ipv6 interface tunnel** command to display the configuration and IPv6 packet statistics of a tunnel interface or all tunnel interfaces.

Note that:

- If no tunnel interface is specified, information about all tunnel interfaces is displayed.
- If the **verbose** keyword is not specified, summary tunnel interface information is displayed.

## Examples

# Display the detailed information of interface tunnel 1/0/0.

```
<Sysname> display ipv6 interface tunnel 1/0/0 verbose
Tunnell1/0/0 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::202:201
Global unicast address(es):
  3000::1, subnet is 3000::/64
Joined group address(es):
  FF02::1:FF02:201
  FF02::1:FF00:1
  FF02::1:FF00:0
  FF02::2
  FF02::1
MTU is 1480 bytes
ND reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
InReceives:                45
InTooShorts:                0
InTruncatedPkts:          0
InHopLimitExceeds:        0
InBadHeaders:              0
InBadOptions:              0
ReasmReqds:                0
ReasmOKs:                  0
InFragDrops:               0
InFragTimeouts:           0
OutFragFails:              0
InUnknownProtos:          0
InDelivers:                45
OutRequests:               45
OutForwDatagrams:          0
InNoRoutes:                0
InTooBigErrors:            0
OutFragOKs:                0
OutFragCreates:            0
InMcastPkts:               0
InMcastNotMembers:         0
```

```

OutMcastPkts:      0
InAddrErrors:     0
InDiscards:       0
OutDiscards:      0

```

**Table 1-2 display interface tunnel** command output description

Field	Description
Tunnel1/0/0 current state	The physical-layer state of the tunnel interface
Line protocol current state	The link-layer protocol state of the tunnel interface
IPv6 is enabled	IPv6 forwarding state of the tunnel interface (IPv6 is enabled on the tunnel interface in this example)
link-local address	Link-local address of the tunnel interface
Global unicast address(es)	Aggregatable global unicast address of the tunnel interface.
Joined group address(es)	Multicast address of the tunnel interface.
MTU is 1480 bytes	Size of the MTU in the tunnel.
ND reachable time	Neighbor reachable time
ND retransmit interval	Interval for retransmitting a neighbor discovery request message.
Hosts use stateless autoconfig for addresses	Hosts use the stateless auto-configuration mode to acquire IPv6 addresses.
InReceives	All IPv6 packets received on the tunnel interface, including error packets.
InTooShorts	IPv6 packets that are too short in length received on the tunnel interface, such as a packet with a length less than 40 bytes.
InTruncatedPkts	IPv6 packets received on the tunnel interface, with a length less than that specified in the packet header.
InHopLimitExceeds	IPv6 packets having exceeded the hop limit received on the tunnel interface
InBadHeaders	IPv6 packets with wrong basic headers received on the tunnel interface
InBadOptions	IPv6 packets with wrong extension headers received on the tunnel interface
ReasmReqds	IPv6 fragments received on the tunnel interface
ReasmOKs	Number of IPv6 datagrams reassembled on the tunnel interface.
InFragDrops	Wrong IPv6 fragments discarded on the tunnel interface
InFragTimeouts	IPv6 fragments discarded on the interface because they had stayed in the cache longer than the specified time.
OutFragFails	IPv6 Packets that failed to be fragmented on the outbound tunnel interface
InUnknownProtos	IPv6 packets received on the tunnel interface, with an unknown or unsupported protocol type.
InDelivers	IPv6 packets delivered to the upper-layer IPv6 protocols (such as ICMPv6, TCP, or UDP) from the tunnel interface

Field	Description
OutRequests	Local IPv6 packets from the upper-layer IPv6 protocols
OutForwDatagrams	IPv6 packets forwarded by the outbound tunnel interface
InNoRoutes	IPv6 packets discarded on the interface because no matching route is found
InTooBigErrors	IPv6 packets discarded while being forwarded on the interface due to exceeding MTU values
OutFragOKs	Packets that are successfully fragmented on the outbound interface
OutFragCreates	Fragments on the outbound interface
InMcastPkts	IPv6 multicast packets received on the interface
InMcastNotMembers	IPv6 multicast packets discarded on the interface because the interface does not belong to the corresponding multicast groups
OutMcastPkts	IPv6 multicast packets sent on the interface
InAddrErrors	IPv6 packets discarded on the interface due to illegal destination addresses
InDiscards	IPv6 packets received but then discarded on the interface due to resource problems rather than packet content errors
OutDiscards	IPv6 packets sent on the interface but then discarded due to resource problems rather than packet content errors

# Display the summary IPv6 information of the interface tunnel 1/0/0.

```
<Sysname> display ipv6 interface tunnel 1/0/0
*down: administratively down
(s): spoofing
Interface                Physical   Protocol   IPv6 Address
Tunnell1/0/0             up        up         3000::1
```

**Table 1-3** display ipv6 interface tunnel command output description

Field	Description
*down	The tunnel interface is in administrative down state, meaning the interface is shut down using the <b>shutdown</b> command.
(s)	Spoofing feature of the tunnel interface. That is, although the link-layer protocol state of the interface is up, no such link exists, or the link is not a permanent one and can only be established as needed.
Interface	Name of the tunnel interface
Physical	Physical state of the tunnel interface
Protocol	Link-layer protocol state of the tunnel interface
IPv6 Address	IPv6 address of the tunnel interface. Only the first configured IPv6 address is displayed

## interface tunnel

### Syntax

```
interface tunnel number  
undo interface tunnel number
```

### View

System view

### Default Level

2: System level

### Parameters

*number*: Tunnel interface number.

### Description

Use the **interface tunnel** command to create a tunnel interface and enter tunnel interface view.

Use the **undo interface tunnel** command to remove the specified tunnel interface.

By default, there is no tunnel interface on the device.

- Executing the **interface tunnel** command enters interface view of a specified tunnel. If no tunnel interface is created, executing this command first creates a tunnel and then enters the tunnel interface view.
- A tunnel interface number has only local significance, and therefore, the same interface number or different interface numbers can be set at both ends of a tunnel.

Related commands: **display interface tunnel**, **source**, **destination**, **tunnel-protocol**.

### Examples

```
# Create the interface tunnel 1/0/3.  
<Sysname> system-view  
[Sysname] interface tunnel 1/0/3  
[Sysname-Tunnel1/0/3]
```

## service-loopback-group

### Syntax

```
service-loopback-group number  
undo service-loopback-group
```

### View

Tunnel interface view

### Default Level

2: System level

### Parameters

*number*: Service loopback group ID, in the range of 1 to 1024.

## Description

Use the **service-loopback-group** command to reference a service loopback group on the tunnel interface.

Use the **undo service-loopback-group** command to remove the referenced service loopback group from the tunnel interface.

By default, no service loopback group is referenced on a tunnel interface.

The service loopback group to be referenced must have been configured and have the service type set to tunnel in system view.

One tunnel interface can reference only one service loopback group.

Related commands: **service-loopback group** in *Service Loopback Group Commands* in the *Access Volume*.

## Examples

# Create service loopback group 1 of tunnel type.

```
<Sysname> system-view
[Sysname] service-loopback group 1 type tunnel
```

# Add a Layer 2 GE interface to service loopback group 1.

```
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] undo stp enable
[Sysname-GigabitEthernet1/0/1] port service-loopback group 1
[Sysname-GigabitEthernet1/0/1] quit
```

# Reference service loopback group 1 on interface tunnel 1/0/2.

```
[Sysname] interface tunnel 1/0/2
[Sysname-Tunnel1/0/2] service-loopback-group 1
```

## source

### Syntax

**source** { *ip-address* | *interface-type interface-number* }

**undo source**

### View

Tunnel interface view

### Default Level

2: System level

### Parameters

*ip-address*: Tunnel source IPv4 address.

*interface-type interface-number*: Specifies an interface. The interface types include Vlan-interface, tunnel, and loopback.

## Description

Use the **source** command to specify the source address or interface of the tunnel interface.

Use the **undo source** command to remove the configured source address or interface of the tunnel interface.

By default, no source address or interface is specified for the tunnel interface.

Note that:

- The tunnel source address is the address of the interface sending packets and should be configured as the destination address of the peer tunnel interface.
- Two or more tunnel interfaces using the same encapsulation protocol must have different source addresses and destination addresses.

Related commands: **interface tunnel**, **destination**.

## Examples

# Set the tunnel source address to 192.100.1.1 (or the interface VLAN-interface 100) on the interface Tunnel 1/0/5.

```
<Sysname> system-view
[Sysname] interface tunnel 1/0/5
[Sysname-Tunnel1/0/5] source 192.100.1.1
```

Or

```
<Sysname> system-view
[Sysname] interface tunnel 1/0/5
[Sysname-Tunnel1/0/5] source vlan-interface 100
```

## tunnel-protocol

### Syntax

```
tunnel-protocol ipv6-ipv4 [ 6to4 | isatap ]
undo tunnel-protocol
```

### View

Tunnel interface view

### Default Level

2: System level

### Parameters

**ipv6-ipv4**: Sets the tunnel to an IPv6 over IPv4 manual tunnel.

**ipv6-ipv4 6to4**: Sets the tunnel to IPv6 over IPv4 6to4 tunnel.

**ipv6-ipv4 isatap**: Sets the tunnel to an IPv6 over IPv4 ISATAP tunnel.

### Description

Use the **tunnel-protocol** command to configure the tunnel mode.

Use the **undo tunnel-protocol** to restore the default tunnel mode.

By default, the tunnel is an IPv6 over IPv4 manual tunnel.

Note that:

- A proper tunnel mode can be selected for packet encapsulation according to the network topology and application. The same tunnel mode must be configured at both ends of the tunnel. Otherwise, packet delivery will fail.
- Only one automatic tunnel can be configured at the same tunnel source.

### Examples

# Specify the tunnel mode as IPv6 over IPv4 6to4 tunnel.

```
<Sysname> system-view  
[Sysname] interface tunnel 1/0/2  
[Sysname-Tunnel1/0/2] tunnel-protocol ipv6-ipv4 6to4
```

# Table of Contents

<b>1 sFlow Configuration Commands</b> .....	<b>1-1</b>
sFlow Configuration Commands .....	1-1
display sflow .....	1-1
sflow agent ip .....	1-2
sflow collector ip .....	1-3
sflow enable .....	1-3
sflow interval .....	1-4
sflow sampling-mode .....	1-5
sflow sampling-rate .....	1-5

# 1 sFlow Configuration Commands

---

## sFlow Configuration Commands

### display sflow

#### Syntax

**display sflow** [*slot slot-number*]

#### View

Any view

#### Default Level

2: System level

#### Parameters

**slot slot-number**: Displays the sFlow configuration information on a specified member device in an IRF stack. If no stack is formed, the sFlow configuration information of the current device are displayed only. The *slot-number* argument indicates the member device ID.

#### Description

Use the **display sflow** command to display the sFlow configuration information.

#### Examples

# Display the sFlow configuration information of member device 1 in an IRF stack.

```
<Sysname> display sflow slot 1
sFlow Version: 5
sFlow Global Information:
Agent          IP:10.10.10.1
Collector     IP:10.10.10.2  Port:6343
IP:10.10.10.3  Port:6555
Interval(s): 20
sFlow Port Information:
Interface          Direction      Rate      Mode      Status
GigabitEthernet1/0/1  Out           5000     Random    Active
```

**Table 1-1** display sflow command output description

Field	Description
sFlow Version	Currently, sFlow has the following versions: <ul style="list-style-type: none"><li>• 4: sFlow version 4.</li><li>• 5: sFlow version 5.</li></ul>
sFlow Global Information	sFlow global configuration information

Field	Description
Agent	IP address of the sFlow agent
Collector	IP address and port number of each sFlow collector
Interval(s)	Counter sampling interval (sFlow interval)
sFlow Port Information	Information of the ports enabled with sFlow
Interface	sFlow enabled interface
Direction	Packet sampling direction: <ul style="list-style-type: none"> <li>• In: Samples inbound packets.</li> <li>• Out: Samples outbound packets.</li> <li>• In/Out: Samples inbound and outbound packets.</li> </ul>
Rate	Packet sampling rate
Mode	Packet sampling mode: <ul style="list-style-type: none"> <li>• Determine: Samples a fixed number of packets.</li> <li>• Random: Samples a random number of packets.</li> </ul>
Status	Status of the sFlow enabled port: <ul style="list-style-type: none"> <li>• Suspend: Indicates the port is suspended, and it stops sampling.</li> <li>• Active: Indicates the port is active and performs sampling.</li> </ul>

## sflow agent ip

### Syntax

**sflow agent ip** *ip-address*

**undo sflow agent ip**

### View

System view

### Default Level

2: System level

### Parameters

*ip-address*: IP address of the sFlow agent.

### Description

Use the **sflow agent ip** command to configure the IP address of the sFlow agent.

Use the **undo sflow agent ip** command to remove the configured IP address.

By default, no IP address is configured for the sFlow agent.

Note that:

- The sFlow agent and sFlow collector must not have the same IP address.
- Currently, a device supports only one sFlow agent.
- sFlow does not work if the sFlow agent has no IP address configured, or if you execute the **undo sflow agent ip** command.

## Examples

```
# Configure the IP address of the sFlow agent.
<Sysname> system-view
[Sysname] sflow agent ip 10.10.10.1
```

## sflow collector ip

### Syntax

```
sflow collector ip ip-address [ port portnum ]
undo sflow collector ip ip-address
```

### View

System view

### Default Level

2: System level

### Parameters

*ip-address*: IP address of the sFlow collector.

**port** *portnum*: Port number of the sFlow Collector, which is in the range 1 to 65535 and defaults to 6343.

### Description

Use the **sflow collector ip** command to specify the IP address and port number of an sFlow collector.

Use the **undo sflow collector ip** command to remove an sFlow collector.

By default, no sFlow collector is specified.

Note that:

- The sFlow collector and sFlow agent must not have the same IP address.
- Currently, you can specify at most two sFlow collectors, with one as the backup sFlow collector.
- sFlow does not work if no sFlow collector is specified.
- If only one sFlow collector is specified, sFlow does not work after you use the **undo sflow collector ip** command to disable it.

## Examples

```
# Specify the IP address and port number of an sFlow collector.
<Sysname> system-view
[Sysname] sflow collector ip 10.10.10.2 port 6343
```

## sflow enable

### Syntax

```
sflow enable { inbound | outbound }
undo sflow enable { inbound | outbound }
```

### View

Layer 2 Ethernet interface view

## Default Level

2: System level

## Parameters

**inbound:** Samples inbound packets.

**outbound:** Samples outbound packets.

## Description

Use the **sflow enable** command to enable sFlow in the inbound or outbound direction on the port.

Use the **undo sflow enable** command to disable sFlow in the inbound or outbound direction on the port.

sFlow is disabled by default.

Note that:

This command is supported on physical Ethernet interfaces only, instead of logical interfaces (Ethernet subinterfaces and VLAN interfaces) and network management interfaces. If you want to enable sFlow on an aggregation group, you need to enable sFlow on each member port.

## Examples

```
# Enable sFlow in the outbound direction on GigabitEthernet 1/0/1.
```

```
<Sysname> system-view
```

```
[Sysname] interface GigabitEthernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] sflow enable outbound
```

## sflow interval

### Syntax

**sflow interval** *interval-time*

**undo sflow interval**

### View

System view

## Default Level

2: System level

## Parameters

*interval-time:* Counter sampling interval in seconds, in the range 2 to 200.

## Description

Use the **sflow interval** command to set the counter sampling interval at which the sFlow agent collects the statistics of all sFlow enabled ports.

Use the **undo sflow interval** command to restore the default interval.

By default, the sampling interval is 20 seconds.

## Examples

```
# Configure the counter sampling interval as 50 seconds.
<Sysname> system-view
[Sysname] sflow interval 50
```

## sflow sampling-mode

### Syntax

```
sflow sampling-mode { determine | random }
undo sflow sampling-mode
```

### View

Layer 2 Ethernet interface view

### Default Level

2: System level

### Parameters

**determine**: Sample a fixed number of packets.

**random**: Sample packets randomly.

### Description

Use the **sflow sampling-mode** command to specify the packet sampling mode.

Use the **undo sflow sampling-mode** command to restore the default.

By default, the packet sampling mode is **random**.

Note that this command should be used after sFlow is enabled on the current port.



#### Note

Currently, the **determine** mode is not supported on 3Com Switch 4800G.

---

## Examples

```
# Configure the interface to sample a fixed number of inbound packets.
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] sflow enable inbound
[Sysname-GigabitEthernet1/0/1] sflow sampling-mode determine
```

## sflow sampling-rate

### Syntax

```
sflow sampling-rate rate
```

## **undo sflow sampling-rate**

### **View**

Interface view

### **Default Level**

2: System level

### **Parameters**

*rate*: Number of packets, in the range of 1000 to 500000.

### **Description**

Use the **sflow sampling-rate** command to specify the number of packets out of which the interface will sample a packet.

Use the **undo sflow sampling-rate** command to restore the default.

By default, the packet sampling rate is 200000.

Note that this command should be used after sFlow is enabled on the current port.

### **Examples**

# Specify the interface to sample a packet out of 100000 inbound packets.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] sflow enable inbound
[Sysname-GigabitEthernet1/0/1] sflow sampling-rate 100000
```

# IP Routing Volume Organization

---

## Manual Version

6W100-20090120

## Product Version

Release 2202

## Organization

The IP Routing Volume is organized as follows:

Features	Description
IP Routing Overview	This document describes: <ul style="list-style-type: none"><li>• Introduction to IP routing and routing table</li><li>• Routing protocol overview</li></ul>
Static Routing	A static route is manually configured by the administrator. The proper configuration and usage of static routes can improve network performance and ensure bandwidth for important network applications. This document describes: <ul style="list-style-type: none"><li>• Static route configuration</li><li>• Detecting Reachability of the Static Route's Nexthop</li></ul>
RIP	Routing Information Protocol (RIP) is a simple Interior Gateway Protocol (IGP), mainly used in small-sized networks. This document describes: <ul style="list-style-type: none"><li>• RIP basic functions configuration</li><li>• RIP advanced functions configuration</li><li>• RIP network optimization configuration</li></ul>
OSPF	Open Shortest Path First (OSPF) is an Interior Gateway Protocol based on the link state developed by IETF. This document describes: <ul style="list-style-type: none"><li>• Enabling OSPF</li><li>• Configuring OSPF Areas</li><li>• Configuring OSPF Network Types</li><li>• Configuring OSPF Route Control</li><li>• Configuring OSPF Sham Link</li><li>• Configuring OSPF Network Optimization</li><li>• Configuring OSPF Graceful Restart</li></ul>

Features	Description
IS-IS	<p>Intermediate System-to-Intermediate System (IS-IS) is a link state protocol, which uses the shortest path first (SPF) algorithm. This document describes:</p> <ul style="list-style-type: none"> <li>• Configuring IS-IS Basic Functions</li> <li>• Configuring IS-IS Routing Information Control</li> <li>• Tuning and Optimizing IS-IS Networks</li> <li>• Configuring IS-IS Authentication</li> <li>• Configuring System ID to Host Name Mappings</li> <li>• Configuring IS-IS GR</li> <li>• Enabling the Logging of Neighbor State Changes</li> <li>• Enabling IS-IS SNMP Trap</li> </ul>
BGP	<p>Border gateway protocol (BGP) is an inter-autonomous system (inter-AS) dynamic route discovery protocol. This document describes:</p> <ul style="list-style-type: none"> <li>• Configuring BGP Basic Functions</li> <li>• Controlling Route Generation</li> <li>• Controlling Route Distribution and Reception</li> <li>• Configuring BGP Route Attributes</li> <li>• Tuning and Optimizing BGP Networks</li> <li>• Configuring a Large Scale BGP Network</li> <li>• Configuring BGP GR</li> <li>• Enabling Trap</li> <li>• Enabling Logging of Peer State Changes</li> </ul>
IPv6 Static Routing	<p>Static routes are special routes that are manually configured by network administrators. Similar to IPv4 static routes, IPv6 static routes work well in simple IPv6 network environments. This document describes:</p> <ul style="list-style-type: none"> <li>• IPv6 static route configuration</li> </ul>
IPv6 RIPng	<p>RIP next generation (RIPng) is an extension of RIP-2 for IPv4. RIPng for IPv6 is IPv6 RIPng. This document describes:</p> <ul style="list-style-type: none"> <li>• Configuring RIPng Basic Functions</li> <li>• Configuring RIPng Route Control</li> <li>• Tuning and Optimizing the RIPng Network</li> </ul>
IPv6 OSPFv3	<p>OSPFv3 is OSPF version 3 for short, supporting IPv6 and compliant with RFC2740 (OSPF for IPv6). This document describes:</p> <ul style="list-style-type: none"> <li>• Enabling OSPFv3</li> <li>• Configuring OSPFv3 Area Parameters</li> <li>• Configuring OSPFv3 Network Types</li> <li>• Configuring OSPFv3 Routing Information Control</li> <li>• Tuning and Optimizing OSPFv3 Networks</li> </ul>
IPv6 IS-IS	<p>The IS-IS routing protocol supports multiple network protocols, including IPv6. IS-IS with IPv6 support is called IPv6 IS-IS dynamic routing protocol. This document describes:</p> <ul style="list-style-type: none"> <li>• Configuring IPv6 IS-IS Basic Functions</li> <li>• Configuring IPv6 IS-IS Routing Information Control</li> </ul>

Features	Description
IPv6 BGP	<p>To support multiple network layer protocols, IETF extended BGP-4 by introducing IPv6 BGP. This document describes:</p> <ul style="list-style-type: none"> <li>• Configuring IPv6 BGP Basic Functions</li> <li>• Controlling Route Distribution and Reception</li> <li>• Configuring IPv6 BGP Route Attributes</li> <li>• Tuning and Optimizing IPv6 BGP Networks</li> <li>• Configuring a Large Scale IPv6 BGP Network</li> </ul>
Routing Policy	<p>Routing policy is used on the router for route inspection, filtering, attributes modifying when routes are received, advertised, or redistributed. This document describes:</p> <ul style="list-style-type: none"> <li>• Defining Filters</li> <li>• Route policy configuration</li> </ul>
BFD	<p>Bidirectional forwarding detection (BFD) provides a single mechanism to quickly detect and monitor the connectivity of links in networks.</p> <ul style="list-style-type: none"> <li>• Configuring BFD Basic Functions</li> <li>• Configuring Protocol-based BFD</li> <li>• Enabling Trap</li> </ul>
MCE	<p>Multi-CE (MCE) enables a switch to function as the CEs of multiple VPN instances in a BGP/MPLS VPN network, thus reducing the investment on network equipment.</p> <ul style="list-style-type: none"> <li>• Configuring a VPN Instance</li> <li>• Configuring Route Exchange between a MCE and a Site</li> <li>• Configuring Route Exchange between a MCE and a PE</li> </ul>

# Table of Contents

<b>1 IP Routing Table Commands</b> .....	<b>1-1</b>
IP Routing Table Commands.....	1-1
display ip routing-table.....	1-1
display ip routing-table acl.....	1-4
display ip routing-table <i>ip-address</i> .....	1-7
display ip routing-table ip-prefix.....	1-9
display ip routing-table protocol.....	1-10
display ip routing-table statistics.....	1-11
display ipv6 routing-table.....	1-12
display ipv6 routing-table acl.....	1-13
display ipv6 routing-table <i>ipv6-address</i> .....	1-14
display ipv6 routing-table <i>ipv6-address1 ipv6-address2</i> .....	1-15
display ipv6 routing-table ipv6-prefix.....	1-16
display ipv6 routing-table protocol.....	1-17
display ipv6 routing-table statistics.....	1-18
display ipv6 routing-table verbose.....	1-19
display router id.....	1-20
router id.....	1-20
reset ip routing-table statistics protocol.....	1-21
reset ipv6 routing-table statistics.....	1-22

# 1 IP Routing Table Commands

---



## Note

The term “router” in this document refers to a router in a generic sense or a Layer 3 switch.

---

## IP Routing Table Commands

### display ip routing-table

#### Syntax

```
display ip routing-table [ vpn-instance vpn-instance-name ] [ verbose | { begin | exclude | include }  
regular-expression ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

**vpn-instance** *vpn-instance-name*: Displays routing table information for a VPN instance. The *vpn-instance-name* argument represents the instance name and is a string of 1 to 31 case-sensitive characters.

**verbose**: Displays detailed routing table information, including that for inactive routes. With this keyword absent, the command displays only brief information about active routes.

**]**: Uses a regular expression to filter output information. For details about regular expressions, refer to the section *CLI Display in Basic System Configuration* in the *System Volume*.

**begin**: Displays route entries starting from the one specified by the regular expression.

**exclude**: Displays route entries not matching the regular expression.

**include**: Displays route entries matching the regular expression.

*regular-expression*: Regular expression, a string of 1 to 256 case-sensitive characters used for specifying routing entries.

#### Description

Use the **display ip routing-table** command to display brief information about active routes in the routing table.

This command displays brief information about a routing table, with a routing entry contained in one line. The information displayed includes destination IP address/mask length, protocol, priority, cost, next hop and outbound interface. This command only displays the routes currently in use, that is, the optimal routes.

Use the **display ip routing-table verbose** command to display detailed information about all routes in the routing table.

This command displays detailed information about all active and inactive routes, including the statistics of the entire routing table and information for each route.

## Examples

# Display brief information about active routes in the routing table.

```
<Sysname> display ip routing-table
Routing Tables: Public
          Destinations : 4          Routes : 4
Destination/Mask    Proto  Pre  Cost           NextHop           Interface
127.0.0.0/8         Direct 0    0              127.0.0.1         InLoop0
127.0.0.1/32        Direct 0    0              127.0.0.1         InLoop0
192.168.80.0/24     Direct 0    0              192.168.80.10    Vlan1
192.168.80.10/32    Direct 0    0              127.0.0.1         InLoop0
```

**Table 1-1 display ip routing-table** command output description

Field	Description
Destinations	Number of destination addresses
Routes	Number of routes
Destination/Mask	Destination address/mask length
Proto	Protocol that presents the route
Pre	Priority of the route
Cost	Cost of the route
NextHop	Address of the next hop on the route
Interface	Outbound interface for packets to be forwarded along the route

# Display detailed information about all routes in the routing table.

```
<Sysname> display ip routing-table verbose
Routing Table : Public
          Destinations : 4          Routes : 4

Destination: 10.1.1.0/24
  Protocol: Direct                Process ID: 0
Preference: 0                    Cost: 0
  NextHop: 10.1.1.1              Interface: Vlan-interface1
RelyNextHop: 0.0.0.0             Neighbour: 0.0.0.0
Tunnel ID: 0x0                   Label: NULL
  State: Active Adv              Age: 04h00m30s
Tag: 0
```

```

Destination: 10.1.1.1/32
  Protocol: Direct          Process ID: 0
  Preference: 0             Cost: 0
  NextHop: 127.0.0.1       Interface: InLoopBack0
  RelyNextHop: 0.0.0.0     Neighbour: 0.0.0.0
  Tunnel ID: 0x0           Label: NULL
  State: Active NoAdv      Age: 04h00m30s
  Tag: 0

Destination: 127.0.0.0/8
  Protocol: Direct          Process ID: 0
  Preference: 0             Cost: 0
  NextHop: 127.0.0.1       Interface: InLoopBack0
  RelyNextHop: 0.0.0.0     Neighbour: 0.0.0.0
  Tunnel ID: 0x0           Label: NULL
  State: Active NoAdv      Age: 04h00m36s
  Tag: 0

Destination: 127.0.0.1/32
  Protocol: Direct          Process ID: 0
  Preference: 0             Cost: 0
  NextHop: 127.0.0.1       Interface: InLoopBack0
  RelyNextHop: 0.0.0.0     Neighbour: 0.0.0.0
  Tunnel ID: 0x0           Label: NULL
  State: Active NoAdv      Age: 04h00m36s
  Tag: 0

```

Displayed first are statistics for the whole routing table, followed by detailed description of each route (in sequence).

**Table 1-2** display ip routing-table verbose command output description

Field	Description
Destination	Destination address/mask length
Protocol	Protocol that presents the route
Process ID	Process ID
Preference	Priority of the route
Cost	Cost of the route
NextHop	Address of the next hop on the route
Interface	Outbound interface for packets to be forwarded along the route
BkNextHop	Backup next hop
BkInterface	Backup outbound interface
RelyNextHop	The next hop address obtained through routing recursion
Neighbour	Neighboring address determined by Routing Protocol
Tunnel ID	Tunnel ID
Label	Label

Field	Description
	Route status:
Active	This is an active unicast route.
Adv	This route can be advertised.
Delete	This route is deleted.
Gateway	This is an indirect route.
Holddown	Number of holddown routes. Holddown is a route advertisement policy used in some distance vector (D-V) routing protocols, such as RIP, to avoid the propagation of some incorrect routes. It distributes a Holddown route during a period regardless of whether a new route to the same destination is found. For details, refer to corresponding routing protocols.
Int	The route was discovered by an Interior Gateway Protocol (IGP).
NoAdv	The route is not advertised when the router advertises routes based on policies.
NotInstall	Normally, among routes to a destination, the route with the highest priority is installed into the core routing table and advertised, while a NotInstall route cannot be installed into the core routing table but may be advertised.
Reject	The packets matching a Reject route will be dropped. Besides, the router sends ICMP unreachable messages to the sources of the dropped packets. The Reject routes are usually used for network testing.
Static	A static route is not lost when you perform the save operation and then restart the router. Routes configured manually are marked as <b>static</b> .
Unicast	Unicast routes
Inactive	Inactive routes
Invalid	Invalid routes
WaitQ	The route is the WaitQ during route recursion.
TunE	Tunnel
GotQ	The route is in the GotQ during route recursion.
Age	Time for which the route has been in the routing table, in the sequence of hour, minute, and second from left to right.
Tag	Route tag

## display ip routing-table acl

### Syntax

```
display ip routing-table acl acl-number [ verbose ]
```

### View

Any view

## Default Level

1: Monitor level

## Parameters

**acl-number:** Basic ACL number, in the range of 2000 to 2999.

**verbose:** Displays detailed routing table information, including that for inactive routes. With this argument absent, the command displays only brief information about active routes.

## Description

Use the **display ip routing-table acl** command to display information about routes permitted by a specified basic ACL.

This command is intended for the follow-up display of routing policies.

For more information about routing policy, refer to *Routing Policy Configuration* in the *IP Routing Volume*.



### Note

If the specified ACL does not exist or it has no rules configured, the entire routing table is displayed.

---

## Examples

# Define basic ACL 2000 and set the route filtering rules.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.1.0.0 0.0.255.255
[Sysname-acl-basic-2000] rule deny source any
```

# Display brief information about active routes permitted by basic ACL 2000.

```
[Sysname-acl-basic-2000] display ip routing-table acl 2000
Routes Matched by Access list : 2000
Summary Count : 6
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.1.1.0/24	Direct	0	0	10.1.1.2	Vlan1
10.1.1.2/32	Direct	0	0	127.0.0.1	InLoop0
10.1.2.0/24	Direct	0	0	10.1.2.1	Vlan2
10.1.2.1/32	Direct	0	0	127.0.0.1	InLoop0
10.1.3.0/24	Direct	0	0	10.1.3.1	Vlan3
10.1.3.1/32	Direct	0	0	127.0.0.1	InLoop0

For detailed description of the above output, see [Table 1-1](#).

# Display detailed information about both active and inactive routes permitted by basic ACL 2000.

```
<Sysname> display ip routing-table acl 2000 verbose
Routes Matched by Access list : 2000
```

Summary Count: 6

Destination: 10.1.1.0/24

Protocol: Direct	Process ID: 0
Preference: 0	Cost: 0
NextHop: 10.1.1.2	Interface: Vlan-interface1
RelyNextHop: 0.0.0.0	Neighbour: 0.0.0.0
Tunnel ID: 0x0	Label: NULL
State: Active Adv	Age: 00h25m32s
Tag: 0	

Destination: 10.1.1.2/32

Protocol: Direct	Process ID: 0
Preference: 0	Cost: 0
NextHop: 127.0.0.1	Interface: InLoopBack0
RelyNextHop: 0.0.0.0	Neighbour: 0.0.0.0
Tunnel ID: 0x0	Label: NULL
State: Active NoAdv	Age: 00h41m34s
Tag: 0	

Destination: 10.1.2.0/24

Protocol: Direct	Process ID: 0
Preference: 0	Cost: 0
NextHop: 10.1.2.1	Interface: Vlan-interface2
RelyNextHop: 0.0.0.0	Neighbour: 0.0.0.0
Tunnel ID: 0x0	Label: NULL
State: Active Adv	Age: 00h05m42s
Tag: 0	

Destination: 10.1.2.1/32

Protocol: Direct	Process ID: 0
Preference: 0	Cost: 0
NextHop: 127.0.0.1	Interface: InLoopBack0
RelyNextHop: 0.0.0.0	Neighbour: 0.0.0.0
Tunnel ID: 0x0	Label: NULL
State: Active NoAdv	Age: 00h05m42s
Tag: 0	

Destination: 10.1.3.0/24

Protocol: Direct	Process ID: 0
Preference: 0	Cost: 0
NextHop: 10.1.3.1	Interface: Vlan-interface3
RelyNextHop: 0.0.0.0	Neighbour: 0.0.0.0
Tunnel ID: 0x0	Label: NULL
State: Active Adv	Age: 00h05m31s
Tag: 0	

Destination: 10.1.3.1/32

```

    Protocol: Direct          Process ID: 0
Preference: 0                Cost: 0
    NextHop: 127.0.0.1      Interface: InLoopBack0
RelyNextHop: 0.0.0.0        Neighbour: 0.0.0.0
    Tunnel ID: 0x0          Label: NULL
    State: Active NoAdv     Age: 00h05m32s
    Tag: 0

```

For the description of the command output above, see [Table 1-2](#).

## display ip routing-table *ip-address*

### Syntax

```

display ip routing-table ip-address [ mask-length | mask ] [ longer-match ] [ verbose ]
display ip routing-table ip-address1 { mask-length | mask } ip-address2 { mask-length | mask }
[ verbose ]

```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ip-address*: Destination IP address, in dotted decimal format.

*mask-length*: IP address mask length in the range 0 to 32.

*mask*: IP address mask in dotted decimal format.

**longer-match**: Displays the route with the longest mask.

**verbose**: Displays detailed routing table information, including both active and inactive routes. With this argument absent, the command displays only brief information about active routes.

### Description

Use the **display ip routing-table** *ip-address* command to display information about routes to a specified destination address.

Executing the command with different parameters yields different output:

- **display ip routing-table** *ip-address*

The system ANDs the input destination IP address with the subnet mask in each route entry; and ANDs the destination IP address in each route entry with its corresponding subnet mask.

If the two operations yield the same result for an entry and this entry is active, it is displayed.

- **display ip routing-table** *ip-address mask*

The system ANDs the input destination IP address with the input subnet mask; and ANDs the destination IP address in each route entry with the input subnet mask.

If the two operations yield the same result for an entry and the entry is active with a subnet mask less than or equal to the input subnet mask, the entry is displayed.

Only route entries that exactly match the input destination address and mask are displayed.

- **display ip routing-table *ip-address* longer-match**

The system ANDs the input destination IP address with the subnet mask in each route entry; and ANDs the destination IP address in each route entry with its corresponding subnet mask.

If the two operations yield the same result for multiple entries that are active, the one with longest mask length is displayed.

- **display ip routing-table *ip-address* mask longer-match**

The system ANDs the input destination IP address with the input subnet mask; and ANDs the destination IP address in each route entry with the input subnet mask.

If the two operations yield the same result for multiple entries with a mask less than or equal to the input subnet mask, the one that is active with longest mask length is displayed.

Use the **display ip routing-table *ip-address1* { *mask-length* | *mask* } *ip-address2* { *mask-length* | *mask* }** command to display route entries with destination addresses within a specified range.

## Examples

# Display route entries for the destination IP address 11.1.1.1.

```
<Sysname> display ip routing-table 11.1.1.1
Routing Table : Public
Summary Count : 4
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/0	Static	60	0	0.0.0.0	NULL0
11.0.0.0/8	Static	60	0	0.0.0.0	NULL0
11.1.0.0/16	Static	60	0	0.0.0.0	NULL0
11.1.1.0/24	Static	60	0	0.0.0.0	NULL0

For detailed description about the output, see [Table 1-1](#).

# Display route entries by specifying a destination IP address and the **longer-match** keyword.

```
[Sysname] display ip routing-table 11.1.1.1 longer-match
Routing Table : Public
Summary Count : 1
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
11.1.1.0/24	Static	60	0	0.0.0.0	NULL0

# Display route entries by specifying a destination IP address and mask.

```
[Sysname] display ip routing-table 11.1.1.1 24
Routing Table : Public
Summary Count : 3
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
11.0.0.0/8	Static	60	0	0.0.0.0	NULL0
11.1.0.0/16	Static	60	0	0.0.0.0	NULL0
11.1.1.0/24	Static	60	0	0.0.0.0	NULL0

# Display route entries by specifying a destination IP address and mask and the **longer-match** keyword.

```
[Sysname] display ip routing-table 11.1.1.1 24 longer-match
Routing Table : Public
Summary Count : 1
Destination/Mask    Proto  Pre  Cost           NextHop           Interface
11.1.1.0/24         Static 60   0              0.0.0.0           NULL0
```

For detailed description of the above output, see [Table 1-1](#).

# Display route entries for destination addresses in the range 1.1.1.0 to 5.5.5.0.

```
<Sysname> display ip routing-table 1.1.1.0 24 5.5.5.0 24
Routing Table : Public

Destination/Mask    Proto  Pre  Cost           NextHop           Interface
1.1.1.0/24          Direct 0    0              1.1.1.1           Vlan1
1.1.1.1/32          Direct 0    0              127.0.0.1         InLoop0
2.2.2.0/24          Direct 0    0              2.2.2.1           Vlan2
2.2.2.1/32          Direct 0    0              127.0.0.1         InLoop0
```

## display ip routing-table ip-prefix

### Syntax

```
display ip routing-table ip-prefix ip-prefix-name [ verbose ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ip-prefix-name*: IP prefix list name, a string of 1 to 19 characters.

**verbose**: Displays detailed routing table information, including that for inactive routes. With this argument absent, the command displays only brief information about active routes.

### Description

Use the **display ip routing-table ip-prefix** command to display information about routes permitted by a specified prefix list.

This command is intended for the follow-up display of routing policies. If the specified prefix list is not configured, detailed information about all routes (with the **verbose** keyword) or brief information about all active routes (without the **verbose** keyword) is displayed.

### Examples

# Configure a prefix list named **test**, permitting routes with a prefix of 2.2.2.0 and a mask length between 24 and 32.

```
<Sysname> system-view
[Sysname] ip ip-prefix test permit 2.2.2.0 24 less-equal 32
```

# Display brief information about active routes permitted by the prefix list **test**.

```
[Sysname] display ip routing-table ip-prefix test
Routes Matched by Prefix list : test
Summary Count : 2
Destination/Mask  Proto  Pre  Cost      NextHop      Interface
2.2.2.0/24        Direct  0    0         2.2.2.1      Vlan2
2.2.2.1/32        Direct  0    0         127.0.0.1    InLoop0
```

For detailed description of the above output, see [Table 1-1](#).

# Display detailed information about both active and inactive routes permitted by IP prefix list **test**.

```
[Sysname] display ip routing-table ip-prefix test verbose
Routes Matched by Prefix list  test :
Summary Count : 2

Destination: 2.2.2.0/24
  Protocol: Direct                Process ID: 0
  Preference: 0                   Cost: 0
  NextHop: 2.2.2.1                Interface: Vlan-interface2
  RelyNextHop: 0.0.0.0            Neighbour: 0.0.0.0
  Tunnel ID: 0x0                  Label: NULL
  State: Active Adv               Age: 00h20m52s
  Tag: 0

Destination: 2.2.2.1/32
  Protocol: Direct                Process ID: 0
  Preference: 0                   Cost: 0
  NextHop: 127.0.0.1              Interface: InLoopBack0
  RelyNextHop: 0.0.0.0            Neighbour: 0.0.0.0
  Tunnel ID: 0x0                  Label: NULL
  State: Active NoAdv             Age: 00h20m52s
  Tag: 0
```

For detailed description of the above output, see [Table 1-2](#).

## display ip routing-table protocol

### Syntax

```
display ip routing-table protocol protocol [ inactive | verbose ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*protocol*: Routing protocol. It can be **bgp4**, **direct**, **isis**, **ospfv2**, **rip**, or **static**.

**inactive:** Displays information about only inactive routes. With this argument absent, the command displays information about both active and inactive routes.

**verbose:** Displays detailed routing table information. With this argument absent, the command displays brief routing table information.

## Description

Use the **display ip routing-table protocol** command to display routing information of a specified routing protocol.

## Examples

# Display brief information about direct routes.

```
<Sysname> display ip routing-table protocol direct
```

```
Public Routing Table : Direct
```

```
Summary Count : 4
```

```
Direct Routing table Status : < Active>
```

```
Summary Count : 4
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
2.2.2.0/24	Direct	0	0	2.2.2.1	Vlan2
2.2.2.2/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

```
Direct Routing table Status : < Inactive>
```

```
Summary Count : 0
```

# Display brief information about static routes.

```
<Sysname> display ip routing-table protocol static
```

```
Public Routing Table : Static
```

```
Summary Count : 1
```

```
Static Routing table Status : < Active>
```

```
Summary Count : 0
```

```
Static Routing table Status : < Inactive>
```

```
Summary Count : 1
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
1.2.3.0/24	Static	60	0	1.2.4.5	Vlan10

For detailed description of the above output, see [Table 1-1](#).

## display ip routing-table statistics

### Syntax

```
display ip routing-table [ vpn-instance vpn-instance-name ] statistics
```

## View

Any view

## Default Level

1: Monitor level

## Parameters

**vpn-instance** *vpn-instance-name*: Displays routing table statistics for a VPN instance. The VPN instance name is a string of 1 to 31 case-sensitive characters.

## Description

Use the **display ip routing-table statistics** command to display the route statistics of the public network routing table or the VPN routing table.

## Examples

# Display route statistics in the routing table.

```
<Sysname> display ip routing-table statistics
```

Proto	route	active	added	deleted	freed
DIRECT	24	4	25	1	0
STATIC	4	1	4	0	0
RIP	0	0	0	0	0
OSPF	0	0	0	0	0
IS-IS	0	0	0	0	0
BGP	0	0	0	0	0
Total	28	5	29	1	0

**Table 1-3** display ip routing-table statistics command output description

Field	Description
Proto	Origin of the routes.
route	Number of routes from the origin
active	Number of active routes from the origin
added	Number of routes added into the routing table since the router started up or the routing table was last cleared
deleted	Number of routes marked as deleted, which will be freed after a period.
freed	Number of routes that got freed, that is, got removed permanently.
Total	Total number

## display ipv6 routing-table

### Syntax

```
display ipv6 routing-table
```

### View

Any view

## Default Level

1: Monitor level

## Parameters

None

## Description

Use the **display ipv6 routing-table** command to display brief routing table information, including destination IP address and prefix, protocol type, priority, metric, next hop and outbound interface.

The command displays only active routes, namely, the brief information about the current optimal routes.

## Examples

```
# Display brief routing table information
```

```
<Sysname> display ipv6 routing-table
```

```
Routing Table :
```

```
Destinations : 1          Routes : 1
```

```
Destination : ::1/128          Protocol      : Direct
NextHop      : ::1             Preference    : 0
Interface    : InLoop0         Cost          : 0
```

**Table 1-4 display ipv6 routing-table** command output description

Field	Description
Destination	IPv6 address of the destination network/host
NextHop	Nexthop address
Preference	Route priority
Interface	Outbound interface
Protocol	Routing protocol
Cost	Route cost

## display ipv6 routing-table acl

### Syntax

```
display ipv6 routing-table acl acl6-number [ verbose ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*acl6-number*: Basic IPv6 ACL number, in the range 2000 to 2999.

**verbose:** Displays both active and inactive verbose routing information permitted by the ACL. Without this keyword, only brief active routing information is displayed.

## Description

Use the **display ipv6 routing-table acl** command to display routing information permitted by the IPv6 ACL.

If the specified IPv6 ACL is not available, all routing information is displayed.

## Examples

```
# Display brief routing information permitted by ACL 2000.
```

```
<Sysname> display ipv6 routing-table acl 2000
```

```
Routes Matched by Access list 2000 :
```

```
Summary Count : 2
```

```
Destination : ::1/128                Protocol : Direct
NextHop      : ::1                    Preference : 0
Interface    : InLoop0                Cost      : 0
Destination : 1:1::/64                Protocol  : Static
NextHop      : ::                      Preference : 60
Interface    : NULL0                   Cost      : 0
```

Refer to [Table 1-4](#) for description about the above output.

## display ipv6 routing-table ipv6-address

### Syntax

```
display ipv6 routing-table ipv6-address prefix-length [ longer-match ] [ verbose ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ipv6-address*: Destination IPv6 address.

*prefix-length*: Prefix length, in the range 0 to 128.

**longer-match**: Displays the matched route having the longest prefix length.

**verbose**: Displays both active and inactive verbose routing information. Without this keyword, only brief active routing information is displayed.

## Description

Use the **display ipv6 routing-table ipv6-address** command to display routing information about the specified destination IPv6 address.

Executing the command with different parameters yields different output:

- **display ipv6 routing-table ipv6-address prefix-length**

The system ANDs the input destination IPv6 address with the input prefix length, and ANDs the destination IPv6 address in each route entry with the input prefix length.

If the two operations yield the same result for an entry and the entry is active with a prefix length less than or equal to the input prefix length, the entry is displayed.

Only route entries that exactly match the input destination address and prefix length are displayed.

- **display ipv6 routing-table *ipv6-address prefix-length longer-match***

The system ANDs the input destination IPv6 address with the input prefix length; and ANDs the destination IPv6 address in each route entry with the input prefix length.

If the two operations yield the same result for multiple entries with a prefix length less than or equal to the input prefix length, the one that is active with the longest prefix length is displayed.

## Examples

# Display brief information about the route matching the specified destination IPv6 address.

```
<Sysname> display ipv6 routing-table 10::1 127
```

```
Routing Table:
```

```
Summary Count: 3
```

```
Destination: 10::/64                                Protocol : Static
NextHop      : ::                                    Preference: 60
Interface   : NULL0                                  Cost      : 0
```

```
Destination: 10::/68                                Protocol : Static
NextHop      : ::                                    Preference: 60
Interface   : NULL0                                  Cost      : 0
```

```
Destination: 10::/120                               Protocol : Static
NextHop      : ::                                    Preference: 60
Interface   : NULL0                                  Cost      : 0
```

# Display brief information about the matched route with the longest prefix length.

```
<Sysname> display ipv6 routing-table 10:: 127 longer-match
```

```
Routing Tables:
```

```
Summary Count : 1
```

```
Destination: 10::/120                               Protocol : Static
NextHop      : ::                                    Preference: 60
Interface   : NULL0                                  Cost      : 0
```

Refer to [Table 1-4](#) for description about the above output.

## **display ipv6 routing-table *ipv6-address1 ipv6-address2***

### Syntax

```
display ipv6 routing-table ipv6-address1 prefix-length1 ipv6-address2 prefix-length2 [ verbose ]
```

### View

Any view

## Default Level

1: Monitor level

## Parameters

*ipv6-address1/ipv6-address2*: An IPv6 address range from IPv6 address1 to IPv6 address2.

*prefix-length1/prefix-length2*: Prefix length, in the range 0 to 128.

**verbose**: Displays both active and inactive verbose routing information. Without this keyword, only brief active routing information is displayed.

## Description

Use the **display ipv6 routing-table** *ipv6-address1 ipv6-address2* command to display routes with destinations falling into the specified IPv6 address range.

## Examples

# Display routes with destinations falling into the IPv6 address range.

```
<Sysname> display ipv6 routing-table 100:: 64 300:: 64
```

```
Routing Table :
```

```
Summary Count : 3
```

```
Destination: 100::/64                Protocol : Static
NextHop      : ::                     Preference: 60
Interface    : NULL0                  Cost      : 0
```

```
Destination: 200::/64                Protocol : Static
NextHop      : ::                     Preference: 60
Interface    : NULL0                  Cost      : 0
```

```
Destination: 300::/64                Protocol : Static
NextHop      : ::                     Preference: 60
Interface    : NULL0                  Cost      : 0
```

Refer to [Table 1-4](#) for description about the above output.

## display ipv6 routing-table ipv6-prefix

### Syntax

```
display ipv6 routing-table ipv6-prefix ipv6-prefix-name [ verbose ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ipv6-prefix-name*: Name of the IPv6 prefix list, in the range 1 to 19 characters.

**verbose:** Displays both active and inactive verbose routing information. Without this keyword, only brief active routing information is displayed.

## Description

Use the **display ipv6 routing-table ipv6-prefix** command to display routes permitted by the IPv6 prefix list.

## Examples

# Display brief active routing information permitted by the IPv6 prefix list **test2**.

```
<Sysname> display ipv6 routing-table ipv6-prefix test2
```

```
Routes Matched by Prefix list test2 :
```

```
Summary Count : 1
```

```
Destination: 100::/64
```

```
Protocol : Static
```

```
NextHop : ::
```

```
Preference: 60
```

```
Interface : NULL0
```

```
Cost : 0
```

Refer to [Table 1-4](#) for description about the above output.

## display ipv6 routing-table protocol

### Syntax

```
display ipv6 routing-table protocol protocol [ inactive | verbose ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*protocol:* Displays routes of a routing protocol, which can be **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng** and **static**.

**inactive:** Displays only inactive routes. Without the keyword, all active and inactive routes are displayed.

**verbose:** Displays both active and inactive verbose routing information. Without this keyword, only brief active routing information is displayed.

## Description

Use the **display ipv6 routing-table protocol** command to display routes of a specified routing protocol.

## Examples

# Display brief information about all direct routes.

```
<Sysname> display ipv6 routing-table protocol direct
```

```
Direct Routing Table :
```

```
Summary Count : 1
```

Direct Routing Table's Status : < Active >

Summary Count : 1

Destination: ::1/128

Protocol : Direct

NextHop : ::1

Preference: 0

Interface : InLoop0

Cost : 0

Direct Routing Table's Status : < Inactive >

Summary Count : 0

Refer to [Table 1-4](#) for description about the above output.

## display ipv6 routing-table statistics

### Syntax

**display ipv6 routing-table statistics**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display ipv6 routing-table statistics** command to display routing statistics, including total route number, added route number and deleted route number.

### Examples

# Display routing statistics.

```
<Sysname> display ipv6 routing-table statistics
```

Protocol	route	active	added	deleted	freed
DIRECT	1	1	1	0	0
STATIC	3	0	3	0	0
RIPng	0	0	0	0	0
OSPFv3	0	0	0	0	0
IS-ISv6	0	0	0	0	0
BGP4+	0	0	0	0	0
Total	4	1	4	0	0

**Table 1-5** display ipv6 routing-table statistics command output description

Field	Description
Protocol	Routing protocol
route	Route number of the protocol
active	Number of active routes

Field	Description
added	Routes added after the last startup of the router
deleted	Deleted routes, which will be released after a specified time
freed	Released (totally removed from the routing table) route number
Total	Total number of routes

## display ipv6 routing-table verbose

### Syntax

**display ipv6 routing-table verbose**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display ipv6 routing-table verbose** command to display detailed information about all active and inactive routes, including the statistics of the entire routing table and information for each route.

### Examples

# Display detailed information about all active and inactive routes.

```
<Sysname> display ipv6 routing-table verbose
```

```
Routing Table :
```

```
Destinations : 1          Routes : 1
```

```

Destination : ::1          PrefixLength : 128
NextHop     : ::1          Preference   : 0
RelayNextHop : ::          Tag          : 0H
Neighbour   : ::          ProcessID    : 0
Interface   : InLoopBack0 Protocol     : Direct
State       : Active NoAdv Cost         : 0
Tunnel ID   : 0x0          Label       : NULL
Age         : 22161sec
```

**Table 1-6** display ipv6 routing-table verbose command output description

Field	Description
Destination	Destination IPv6 address
PrefixLength	Prefix length of the address
Nexthop	Next hop

Field	Description
Preference	Route priority
RelayNextHop	Recursive next hop
Tag	Tag of the route
Neighbour	Neighbor address
ProcessID	Process ID
Interface	Outbound interface
Protocol	Routing protocol
State	State of the route, Active, Inactive, Adv (advertised), or NoAdv (not advertised)
Cost	Cost of the route
Tunnel ID	Tunnel ID
Label	Label
Age	Time that has elapsed since the route was generated

## display router id

### Syntax

```
display router id
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display router id** command to display the router ID.

### Examples

```
# Display the router ID.
```

```
<Sysname> display router id
    Configured router ID is 1.1.1.1
```

## router id

### Syntax

```
router id router-id
```

```
undo router id
```

## View

System view

## Default Level

2: System level

## Parameters

*router-id*: Router ID, expressed as an IPv4 address.

## Description

Use the **router id** command to configure a router ID.

Use the **undo router id** command to remove the router ID.

By default, no router ID is configured.

Some routing protocols use a router ID to identify a routing device. A router ID is selected in the following sequence:

- Select the router ID configured with the **router id** command;
- Select the highest IP address among loopback interfaces as the router ID;
- If no loopback interface IP address is available, the highest IP address among physical interfaces is selected as the router ID (regardless of the interface state).
- If the interface whose IP address is the router ID is removed or modified, a new router ID is selected. Other events, (the interface goes down; after a physical interface's IP address is selected as the router ID, an IP address is configured for a loopback interface; a higher interface IP address is configured) will not trigger a router ID re-selection.

A VPN instance selects a router ID among interfaces belonging to it according to the preceding procedure.

When a master/backup switchover occurs, the backup device selects a router ID according to the preceding procedure.

After a router ID is changed, you need to use the **reset** command to make it effective.

## Examples

```
# Configure a router ID.  
<Sysname> system-view  
[Sysname] router id 1.1.1.1
```

## reset ip routing-table statistics protocol

### Syntax

```
reset ip routing-table statistics protocol [ vpn-instance vpn-instance-name ] { protocol | all }
```

### View

User view

### Default Level

2: System level

## Parameters

*vpn-instance-name*: VPN instance name, a string of 1 to 31 case-sensitive characters.

*protocol*: Clears statistics for the IPv4 routing protocol, which can be **bgp**, **direct**, **isis**, **ospf**, **rip**, or **static**.

**all**: Clears statistics for all IPv4 routing protocols.

## Description

Use the **reset ip routing-table statistics protocol** command to clear routing statistics for the routing table or VPN routing table.

## Examples

# Clear routing statistics for the VPN instance **Sysname1**.

```
<Sysname> reset ip routing-table statistics protocol vpn-instance Sysname1 all
```

## reset ipv6 routing-table statistics

### Syntax

```
reset ipv6 routing-table statistics protocol { protocol | all }
```

### View

User view

### Default Level

2: System level

## Parameters

*protocol*: Clears statistics for the routing protocol, which can be **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng**, or **static**.

**all**: Clears statistics for all IPv6 routing protocols.

## Description

Use the **reset ipv6 routing-table statistics** command to clear the route statistics of the routing table.

## Examples

# Clear statistics for all routing protocols.

```
<Sysname> reset ipv6 routing-table statistics protocol all
```

# Table of Contents

<b>1 Static Routing Configuration Commands</b> .....	<b>1-1</b>
Static Routing Configuration Commands.....	1-1
delete static-routes all.....	1-1
ip route-static .....	1-2
ip route-static default-preference.....	1-4

# 1 Static Routing Configuration Commands

---



## Note

The term “router” in this document refers to a router in a generic sense or a Layer 3 switch.

---

## Static Routing Configuration Commands

### delete static-routes all

#### Syntax

```
delete [ vpn-instance vpn-instance-name ] static-routes all
```

#### View

System view

#### Default Level

2: System level

#### Parameters

*vpn-instance-name*: Name of a VPN instance, a string of 1 to 31 case-sensitive characters.

#### Description

Use the **delete static-routes all** command to delete all static routes.

When you use this command to delete static routes, the system will prompt you to confirm the operation before deleting all the static routes.

Related commands: **ip route-static** and **display ip routing-table** in *IP Routing Table Display Commands* in the *IP Routing Volume*.

#### Examples

```
# Delete all static routes on the router.
```

```
<Sysname> system-view
```

```
[Sysname] delete static-routes all
```

```
This will erase all ipv4 static routes and their configurations, you must reconfigure all static routes
```

```
Are you sure?[Y/N]:Y
```

## ip route-static

### Syntax

```
ip route-static dest-address { mask | mask-length } { next-hop-address [ track track-entry-number ] | interface-type interface-number next-hop-address [ bfd { control-packet | echo-packet } ] | vpn-instance d-vpn-instance-name next-hop-address [ track track-entry-number ] } [ preference preference-value ] [ tag tag-value ] [ description description-text ]
```

```
undo ip route-static dest-address { mask | mask-length } [ next-hop-address | interface-type interface-number [ next-hop-address ] | vpn-instance d-vpn-instance-name next-hop-address ] [ preference preference-value ]
```

```
ip route-static vpn-instance s-vpn-instance-name&<1-6> dest-address { mask | mask-length } { next-hop-address [ track track-entry-number ] [ public ] | interface-type interface-number next-hop-address [ bfd { control-packet | echo-packet } ] | vpn-instance d-vpn-instance-name next-hop-address [ track track-entry-number ] } [ preference preference-value ] [ tag tag-value ] [ description description-text ]
```

```
undo ip route-static vpn-instance s-vpn-instance-name&<1-6> dest-address { mask | mask-length } [ next-hop-address [ public ] | interface-type interface-number [ next-hop-address ] | vpn-instance d-vpn-instance-name next-hop-address ] [ preference preference-value ]
```

### View

System view

### Default Level

2: System level

### Parameters

**vpn-instance** *s-vpn-instance-name*&<1-6>: Specifies the VPN instance name, which is a string of 1 to 31 case-sensitive characters. &<1-6> indicates the argument before it can be entered up to 6 times. Each VPN instance has its own routing table, and the configured static route is installed in the routing tables of the specified VPN instances.

*dest-address*: Destination IP address of the static route, in dotted decimal notation.

*mask*: Mask of the IP address, in dotted decimal notation.

*mask-length*: Mask length, in the range 0 to 32.

*next-hop-address*: IP address of the next hop, in dotted decimal notation.

*interface-type interface-number*: Specifies the output interface by its type and number.

**vpn-instance** *d-vpn-instance-name*: Name of the destination VPN instance, case-sensitive. If a destination VPN instance name is specified, the router will search the output interface in the destination VPN instance based on the configured *next-hop-address*.

*next-hop-address* **public**: Indicates that the specified *next-hop-address* is a public network address, rather than a VPN instance address.

**preference** *preference-value*: Specifies the preference of the static route, which is in the range of 1 to 255 and defaults to 60.

**tag** *tag-value*: Sets a tag value for the static route from 1 to 4294967295. The default is 0. Tags of routes are used in routing policies to control routing.

**description** *description-text*: Configures a description for the static route, which consists of 1 to 60 characters, including special characters like space, but excluding ?.

**bfd**: Enable the BFD (bidirectional forwarding detection) function to detect reachability of the static route's next hop. Once the next hop is unreachable, the system will switch to a backup route.

**control-packet**: Implements BFD in the control packet mode.

**echo-packet**: Implements BFD in the echo packet mode.

**track** *track-entry-number*: Associates the static route with a track entry. Use the *track-entry-number* argument to specify a track entry number, in the range 1 to 1024.

## Description

Use the **ip route-static** command to configure a unicast static route.

Use the **undo ip route-static** command to delete a unicast static route.

When configuring a unicast static route, note that:

- 1) If the destination IP address and the mask are both 0.0.0.0, the configured route is a default route. If routing table searching fails, the router will use the default route for packet forwarding.
- 2) Different route management policies can be implemented for different route preference configurations. For example, specifying the same preference for different routes to the same destination address enables load sharing, while specifying different preferences for these routes enables route backup.
- 3) When configuring a static route, Note that the next hop address must not be the IP address of the local interface; otherwise, the route configuration will not take effect. When specifying the output interface, note that:
  - For a Null 0 or loopback interface, if the output interface has already been configured, there is no need to configure the next hop address.
  - To implement BFD with the **control-packet** mode, the remote end must create a BFD session; otherwise the BFD function cannot work. To implement BFD with the **echo-packet** mode, the BFD function can work without the remote end needing to create any BFD session.

Related commands: **display ip routing-table**, **ip route-static default-preference**.



## Note

- The static route does not take effect if you specify its next hop address first and then configure the address as the IP address of a local interface. For details about BFD, refer to *BFD Configuration* in the *IP Routing Volume*.
- If route oscillation occurs, enabling BFD may worsen the oscillation. Be cautious for use of this feature. For details about BFD, refer to *BFD Configuration* in the *IP Routing Volume*.
- To configure track monitoring for an existing static route, simply associate the static route with a track entry. For a non-existent static route, configure it and associate it with a Track entry.
- If the track module uses NQA to detect the reachability of the private network static route's nexthop, the VPN instance number of the static route's nexthop must be identical to that configured in the NQA test group.
- If a static route needs route recursion, the associated track entry must monitor the nexthop of the recursive route instead of that of the static route; otherwise, a valid route may be mistakenly considered invalid.

## Examples

# Configure a static route, whose destination address is 1.1.1.1/24, next hop address is 2.2.2.2, tag value is 45, and description information is **for internet & intranet**.

```
<Sysname> system-view
```

```
[Sysname] ip route-static 1.1.1.1 24 2.2.2.2 tag 45 description for internet & intranet
```

# Configure a static route for a VPN instance named **vpn1**: the destination address is 1.1.1.1/16 and the next hop address is 1.1.1.2, which is the address of this VPN instance.

```
<Sysname> system-view
```

```
[Sysname] ip route-static vpn-instance vpn1 1.1.1.1 16 vpn-instance vpn1 1.1.1.2
```

# Configure a static route: the destination address is 1.1.1.1/24, the output interface is Vlan-interface 1, and the next hop address is 2.2.2.2, and enable BFD with the echo packet mode.

```
<Sysname> system-view
```

```
[Sysname] ip route-static 1.1.1.1 24 Vlan-interface 1 2.2.2.2 bfd echo-packet
```

## ip route-static default-preference

### Syntax

```
ip route-static default-preference default-preference-value
```

```
undo ip route-static default-preference
```

### View

```
System view
```

### Default Level

```
2: System level
```

### Parameters

*default-preference-value*: Default preference for static routes, which is in the range of 1 to 255.

## Description

Use the **ip route-static default-preference** command to configure the default preference for static routes.

Use the **undo ip route-static default-preference** command to restore the default.

By default, the default preference of static routes is 60.

Note that:

- If no preference is specified when configuring a static route, the default preference is used.
- When the default preference is re-configured, it applies to newly added static routes only.

Related commands: **ip route-static** and **display ip routing-table** in *IP Routing Table Display Commands* in the *IP Routing Volume*.

## Examples

# Set the default preference of static routes to 120.

```
<Sysname> system-view
```

```
[Sysname] ip route-static default-preference 120
```

# Table of Contents

<b>1 RIP Configuration Commands</b> .....	<b>1-1</b>
RIP Configuration Commands .....	1-1
checkzero .....	1-1
default cost (RIP view).....	1-2
default-route .....	1-2
display rip .....	1-3
display rip database.....	1-5
display rip interface.....	1-6
display rip route .....	1-7
filter-policy export (RIP view).....	1-9
filter-policy import (RIP view).....	1-10
host-route .....	1-11
import-route (RIP view).....	1-11
maximum load-balancing (RIP view).....	1-13
network .....	1-13
output-delay.....	1-14
peer.....	1-15
preference .....	1-15
reset rip statistics.....	1-16
rip.....	1-16
rip authentication-mode.....	1-17
rip default-route .....	1-18
rip input.....	1-19
rip metricin .....	1-20
rip metricout.....	1-21
rip mib-binding .....	1-21
rip output.....	1-22
rip poison-reverse.....	1-23
rip split-horizon .....	1-23
rip summary-address.....	1-24
rip version .....	1-25
silent-interface (RIP view).....	1-26
summary.....	1-26
timers .....	1-27
validate-source-address .....	1-28
version .....	1-29

# 1 RIP Configuration Commands

---



## Note

The term “router” in this document refers to a router in a generic sense or a Layer 3 switch.

---

## RIP Configuration Commands

### checkzero

#### Syntax

```
checkzero
undo checkzero
```

#### View

RIP view

#### Default Level

2: System level

#### Parameters

None

#### Description

Use the **checkzero** command to enable the zero field check on RIPv1 messages.

Use the **undo checkzero** command to disable the zero field check.

The zero field check is enabled by default.

After the zero field check is enabled, the router discards RIPv1 messages in which zero fields are non-zero. If all messages are trustworthy, you can disable this feature to reduce the processing time of the CPU.

#### Examples

```
# Disable the zero field check on RIPv1 messages for RIP process 100.
```

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] undo checkzero
```

## default cost (RIP view)

### Syntax

```
default cost value  
undo default cost
```

### View

RIP view

### Default Level

2: System level

### Parameters

*value*: Default metric of redistributed routes, in the range of 0 to 16.

### Description

Use the **default cost** command to configure the default metric for redistributed routes.

Use the **undo default cost** command to restore the default.

By default, the default metric of redistributed routes is 0.

When you use the **import-route** command to redistribute routes from other protocols without specifying a metric, the metric specified by the **default cost** command applies.

Related command: **import-route**.

### Examples

# Configure the default metric for redistributed routes to 3.

```
<Sysname> system-view  
[Sysname] rip 100  
[Sysname-rip-100] default cost 3
```

## default-route

### Syntax

```
default-route { only | originate } [ cost cost ]  
undo default-route
```

### View

RIP view

### Default Level

2: System level

### Parameters

**only**: Advertises only a default route.

**originate**: Advertises both a default route and other routes.

*cost*: Cost of the default route, in the range of 1 to 15.

## Description

Use the **default-route originate cost** command to configure all the interfaces under the RIP process to advertise a default route with the specified metric to RIP neighbors.

Use the **undo default-route** command to disable all the interfaces under the RIP process from sending a default route.

By default, no default route is sent to RIP neighbors.

The RIP router with this feature configured will not receive any default routes from RIP neighbors.

Related commands: **rip default-route**.

## Examples

# Configure all the interfaces under RIP process 1 to send only a default route with a metric of 2 to RIP neighbors.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] default-route only cost 2
```

## display rip

### Syntax

```
display rip [ process-id | vpn-instance vpn-instance-name ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*process-id*: RIP process ID, in the range of 1 to 65535.

**vpn-instance** *vpn-instance-name*: Specifies a VPN instance name, a string of 1 to 31 characters.

## Description

Use the **display rip** command to display the current status and configuration information of the specified RIP process.

- If *process-id* is not specified, information about all configured RIP processes is displayed.
- If *vpn-instance-name* is specified, the RIP configuration of the specified VPN instance is displayed.

## Examples

# Display the current status and configuration information of all configured RIP processes.

```
<Sysname> display rip
Public VPN-instance name :

RIP process : 1
RIP version : 1
Preference : 100
```

```

Checkzero : Enabled
Default-cost : 0
Summary : Enabled
Hostroutes : Enabled
Maximum number of balanced paths : 8
Update time : 30 sec(s) Timeout time : 180 sec(s)
Suppress time : 120 sec(s) Garbage-collect time : 120 sec(s)
update output delay : 20(ms) output count : 3
TRIP retransmit time : 5 sec(s)
TRIP response packets retransmit count : 36
Silent interfaces : None
Default routes : Only Default route cost : 3
Verify-source : Enabled
Networks :
    192.168.1.0
Configured peers : None
Triggered updates sent : 0
Number of routes changes : 0
Number of replies to queries : 0

```

**Table 1-1 display rip command output description**

Field	Description
Public VPN-instance name (or Private VPN-instance name)	The RIP process runs under a public VPN instance/The RIP process runs under a private VPN instance
RIP process	RIP process ID
RIP version	RIP version 1 or 2
Preference	RIP route priority
Checkzero	Indicates whether the zero field check is enabled for RIPv1 messages.
Default-cost	Default cost of the redistributed routes
Summary	Indicates whether route summarization is enabled
Hostroutes	Indicates whether to receive host routes
Maximum number of balanced paths	Maximum number of load balanced routes
Update time	RIP update interval
Timeout time	RIP timeout time
Suppress time	RIP suppress interval
update output delay	RIP packet sending interval
output count	Maximum number of RIP packets sent at each interval
Garbage-collect time	RIP garbage collection interval
TRIP retransmit time	TRIP retransmit interval for sending update requests and responses.
TRIP response packets retransmit count	Maximum retransmit times for update requests and responses

Field	Description
Silent interfaces	Number of silent interfaces, which do not periodically send updates
Default routes	Indicates whether a default route is sent to RIP neighbors <ul style="list-style-type: none"> <li>• <b>only</b> means only a default route is advertised.</li> <li>• <b>originate</b> means a default route is advertised along with other routes.</li> <li>• <b>disable</b> means no default route is advertised.</li> </ul>
Default route cost	Cost of the default route
Verify-source	Indicates whether the source IP address is checked on the received RIP routing updates
Networks	Networks enabled with RIP
Configured peers	Configured neighbors
Triggered updates sent	Number of sent triggered updates
Number of routes changes	Number of changed routes in the database
Number of replies to queries	Number of RIP responses

## display rip database

### Syntax

**display rip** *process-id* **database**

### View

Any view

### Default Level

1: Monitor level

### Parameters

*process-id*: RIP process ID, in the range of 1 to 65535.

### Description

Use the **display rip database** command to display active routes in the database of the specified RIP process, which are sent in normal RIP routing updates.

### Examples

# Display the active routes in the database of RIP process 100.

```
<Sysname> display rip 100 database
 10.0.0.0/8, cost 1, ClassfulSumm
 10.0.0.0/24, cost 1, nexthop 10.0.0.1, Rip-interface
 11.0.0.0/8, cost 1, ClassfulSumm
 11.0.0.0/24, cost 1, nexthop 10.0.0.1, Imported
```

**Table 1-2 display rip database** command output description

Field	Description
X.X.X.X/X	Destination address and subnet mask
cost	Cost of the route
classful-summ	Indicates the route is a RIP summary route.
Nexthop	Address of the next hop
Rip-interface	Routes learnt from a RIP-enabled interface
imported	Routes redistributed from other routing protocols

## display rip interface

### Syntax

**display rip process-id interface** [ *interface-type interface-number* ]

### View

Any view

### Default Level

1: Monitor level

### Parameters

*process-id*: RIP process ID, in the range of 1 to 65535.

*interface-type interface-number*: Specifies an interface.

### Description

Use the **display rip interface** command to display the RIP interface information of the RIP process.

If no interface is specified, information about all RIP interfaces of the RIP process is displayed.

### Examples

# Display all the interface information of RIP process 1.

```
<Sysname> display rip 1 interface
```

```
Interface-name: Vlan-interface1
```

```
Address/Mask:1.1.1.1/24      Version:RIPv1
```

```
MetricIn:5      MetricIn route policy:123
```

```
MetricOut:5     MetricOut route policy:234
```

```
Split-horizon/Poison-reverse:on/off      Input/Output:on/on
```

```
Default route:off
```

```
Current packets number/Maximum packets number:234/2000
```

**Table 1-3 display rip interface** command output description

Field	Description
Interface-name	The name of an interface running RIP
Address/Mask	IP address and mask of the interface

Field	Description
Version	RIP version running on the interface
MetricIn	Additional routing metric added to the incoming routes
MetricIn route policy	Name of the routing policy used to add the additional routing metric for the incoming routes. If no routing policy is referenced, the field displays <b>Not designated</b> .
MetricOut	Additional routing metric added to the outgoing routes
MetricOut route policy	Name of the routing policy used to add the additional routing metric for the outgoing routes. If no routing policy is referenced, the field displays <b>Not designated</b> .
Split-horizon	Indicates whether split-horizon is enabled (ON: enabled, OFF: disabled)
Poison-reverse	Indicates whether poison-reverse is enabled (ON: enabled, OFF: disabled)
Input/Output	Indicates if the interface is allowed to receive (Input) or send (Output) RIP messages (on means it is allowed, off means it is not allowed)
Current packets number/Maximum packets number	Packets to be sent/Maximum packets that can be sent on the interface

## display rip route

### Syntax

```
display rip process-id route [ ip-address { mask | mask-length } | peer ip-address | statistics ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*process-id*: RIP process ID, in the range of 1 to 65535.

*ip-address* { *mask* | *mask-length* }: Displays route information about a specified IP address.

**peer** *ip-address*: Displays all routing information learned from a specified neighbor.

**statistics**: Displays the route statistics, including total number of routes and number of routes of each neighbor.

### Description

Use the **display rip route** command to display the routing information of a specified RIP process.

### Examples

```
# Display all routing information of RIP process 1.
```

```
<Sysname> display rip 1 route
```

```
Route Flags: R-RIP, T-TRIP
```

P-Permanent, A-Aging, S-Suppressed, G-Garbage-collect

```
-----
Peer 21.0.0.23 on Vlan-interface1
Destination/Mask    NextHop    Cost     Tag     Flags    Sec
56.0.0.0/8         21.0.0.23    1        0       RA       102
34.0.0.0/8         21.0.0.23    1        0       RA       23
```

# Display routing information for network 56.0.0.0/8 of RIP process 1.

```
<Sysname> display rip 1 route 56.0.0.0 8
Route Flags: R-RIP, T-TRIP
                P-Permanent, A-Aging, S-Suppressed, G-Garbage-collect
-----
```

```
Peer 21.0.0.23 on Vlan-interface1
Destination/Mask    NextHop    Cost     Tag     Flags    Sec
56.0.0.0/8         21.0.0.23    1        0       RA       102
```

# Display RIP process1 routing information learned from the specified neighbor.

```
<Sysname> display rip 1 route peer 21.0.0.23
Route Flags: R-RIP, T-TRIP
                P-Permanent, A-Aging, S-Suppressed, G-Garbage-collect
-----
```

```
Peer 21.0.0.23 on Vlan-interface1
Destination/Mask    NextHop    Cost     Tag     Flags    Sec
56.0.0.0/8         21.0.0.23    1        0       RA       102
34.0.0.0/8         21.0.0.23    1        0       RA       23
```

**Table 1-4 display rip route command output description**

Field	Description
Route Flags	R — RIP route T — TRIP route P — The route never expires A — The route is aging S — The route is suppressed G — The route is in Garbage-collect state
Peer 21.0.0.23 on Vlan-interface1	Routing information learned on a RIP interface from the specified neighbor
Destination/Mask	Destination IP address and subnet mask
NextHop	Next hop of the route
Cost	Cost of the route
Tag	Route tag
Flags	Indicates the route state
Sec	Remaining time of the timer corresponding to the route state

# Display the routing statistics of RIP process 1.

```
<Sysname> display rip 1 route statistics
Peer      Aging      Permanent  Garbage
```

21.0.0.23	2	0	3
21.0.0.12	2	0	4
Total	4	0	7

**Table 1-5** display rip route statistics command output description

Field	Description
Peer	IP address of a neighbor
Aging	Total number of aging routes learned from the specified neighbor
Permanent	Total number of permanent routes learned from the specified neighbor
Garbage	Total number of routes in the garbage-collection state learned from the specified neighbor
Total	Total number of routes learned from all RIP neighbors

## filter-policy export (RIP view)

### Syntax

**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [ *protocol* [ *process-id* ] | *interface-type* *interface-number* ]

**undo filter-policy export** [ *protocol* [ *process-id* ] | *interface-type* *interface-number* ]

### View

RIP view

### Default Level

2: System level

### Parameters

*acl-number*: Number of an ACL used to filter outbound routes, in the range of 2000 to 3999.

**ip-prefix** *ip-prefix-name*: Name of an IP prefix list used to filter outbound routes, a string of 1 to 19 characters.

*protocol*: Filters outbound routes redistributed from a specified routing protocol, which can be **bgp**, **direct**, **isis**, **ospf**, **rip**, and **static**.

*process-id*: Process ID of the specified routing protocol, in the range of 1 to 65535. You need to specify a process ID when the routing protocol is **rip**, **ospf**, or **isis**.

*interface-type interface-number*: Specifies an interface.

### Description

Use the **filter-policy export** command to configure the filtering of RIP outgoing routes. Only routes not filtered out can be advertised.

Use the **undo filter-policy export** command to remove the filtering.

By default, RIP does not filter outbound routes.

Note that:

- If *protocol* is specified, RIP filters only the outgoing routes redistributed from the specified routing protocol. Otherwise, RIP filters all routes to be advertised.
- If *interface-type interface-number* is specified, RIP filters only the routes advertised by the specified interface. Otherwise, RIP filters routes advertised by all RIP interfaces.

Related commands: **acl**, **import-route**, and **ip ip-prefix**.

## Examples

```
# Reference ACL 2000 to filter outbound routes.
```

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] filter-policy 2000 export
```

```
# Reference IP prefix list abc to filter outbound routes on Vlan-interface1.
```

```
[Sysname-rip-1] filter-policy ip-prefix abc export Vlan-interface 1
```

## filter-policy import (RIP view)

### Syntax

```
filter-policy { acl-number | gateway ip-prefix-name | ip-prefix ip-prefix-name [ gateway
ip-prefix-name ] } import [ interface-type interface-number ]
undo filter-policy import [ interface-type interface-number ]
```

### View

RIP view

### Default Level

2: System level

### Parameters

*acl-number*: Number of the ACL used for filtering incoming routes, in the range of 2000 to 3999.

**ip-prefix** *ip-prefix-name*: References an IP prefix list to filter incoming routes. The *ip-prefix-name* is a string of 1 to 19 characters.

**gateway** *ip-prefix-name*: References an IP prefix list to filter routes from the gateway. *ip-prefix-name* is a string of 1 to 19 characters.

*interface-type interface-number*: Specifies an interface by its interface type and interface number.

### Description

Use the **filter-policy import** command to configure RIP to filter the incoming routes.

Use the **undo filter-policy import** command to restore the default.

By default, RIP does not filter incoming routes.

Related commands: **acl** and **ip ip-prefix**.

## Examples

```
# Reference ACL 2000 to filter incoming routes.
```

```
<Sysname> system-view
[Sysname] rip 1
```

```
[Sysname-rip-1] filter-policy 2000 import
# Reference IP prefix list abc on Vlan-interface1 to filter all received RIP routes.
[Sysname-rip-1] filter-policy ip-prefix abc import Vlan-interface 1
```

## host-route

### Syntax

```
host-route
undo host-route
```

### View

RIP view

### Default Level

2: System level

### Parameters

None

### Description

Use the **host-route** command to enable host route reception.

Use the **undo host-route** command to disable host route reception.

By default, receiving host routes is enabled.

In some cases, a router may receive many host routes from the same network segment. These routes are not helpful for routing and occupy a large amount of network resources. You can use the **undo host-route** command to disable receiving of host routes.



#### Note

RIPv2 can be disabled from receiving host routes, but RIPv1 cannot.

---

### Examples

```
# Disable RIP from receiving host routes.
```

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] undo host-route
```

## import-route (RIP view)

### Syntax

```
import-route protocol [ process-id | all-processes | allow-ibgp ] [ cost cost | route-policy route-policy-name | tag tag ] *
```

**undo import-route** *protocol* [*process-id*]

## View

RIP view

## Default Level

2: System level

## Parameters

*protocol*: Specifies a routing protocol from which to redistribute routes. At present, it can be **bgp**, **direct**, **isis**, **ospf**, **rip**, or **static**.

*process-id*: Process ID, in the range of 1 to 65535. The default is 1. It is available only when the protocol is **isis**, **rip**, or **ospf**.

**all-processes**: Enables route redistribution from all the processes of a protocol. This keyword takes effect only when the protocol is **rip**, **ospf**, or **isis**.

**allow-ibgp**: When the *protocol* argument is set to **bgp**, **allow-ibgp** is an optional keyword. The **import-route bgp** command only redistributes eBGP routes, while the **import-route bgp allow-ibgp** command additionally redistributes iBGP routes, which may cause routing loops. Be cautious when using it.

*cost*: Cost for redistributed routes, in the range of 0 to 16. If *cost* is not specified, the default cost specified by the **default cost** command applies.

*tag*: Tag marking redistributed routes, in the range of 0 to 65,535. The default is 0.

**route-policy** *route-policy-name*: Specifies a routing policy with 1 to 19 characters.

## Description

Use the **import-route** command to enable route redistribution from another routing protocol.

Use the **undo import-route** command to disable route redistribution.

By default, RIP does not redistribute routes from other routing protocols.

Note that:

- Only active routes can be redistributed. You can use the **display ip routing-table protocol** command to display route state information.
- You can specify a routing policy using the keyword **route-policy** to redistribute only the specified routes.
- You can configure a cost for redistributed routes using the keyword **cost**.
- You can configure a tag value for redistributed routes using the keyword **tag**.

Related commands: **default cost**.

## Examples

# Redistribute static routes, and set the cost to 4.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] import-route static cost 4
```

# Configure the default cost for redistributed routes to 3.

```
[Sysname-rip-1] default cost 3
```

```
# Redistribute OSPF routes with the cost being the default cost.
```

```
[Sysname-rip-1] import-route ospf
```

## maximum load-balancing (RIP view)

### Syntax

```
maximum load-balancing number
```

```
undo maximum load-balancing
```

### View

RIP view

### Default Level

2: System level

### Parameters

*number*: Maximum number of load balanced routes, in the range 1 to 4. .

### Description

Use the **maximum load-balancing** command to specify the maximum number of load balanced routes in load sharing mode.

Use the **undo maximum load-balancing** command to restore the default.

By default, the maximum number of load balanced routes is 4.

### Examples

```
# Specify the maximum number of load balanced routes as 2.
```

```
<Sysname> system-view
```

```
[Sysname] rip
```

```
[Sysname-rip-1] maximum load-balancing 2
```

## network

### Syntax

```
network network-address
```

```
undo network network-address
```

### View

RIP view

### Default Level

2: System level

### Parameters

*network-address*: IP address of a network segment, which can be the IP network address of any interface.

## Description

Use the **network** command to enable RIP on the interface attached to the specified network.

Use the **undo network** command to disable RIP on the interface attached to the specified network.

RIP is disabled on an interface by default.

Note that:

- RIP runs only on the interfaces attached to the specified network. For an interface not on the specified network, RIP neither receives/sends routes on it nor forwards interface route through it. Therefore, you need to specify the network after enabling RIP to validate RIP on a specific interface.
- For a single process, you can use the **network 0.0.0.0** command to enable RIP on all interfaces, while the command is not applicable in case of multi-process.

## Examples

```
# Enable RIP on the interface attached to the network 129.102.0.0.
```

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] network 129.102.0.0
```

## output-delay

### Syntax

```
output-delay time count count
```

```
undo output-delay
```

### View

RIP view

### Default Level

2: System level

### Parameters

*time*: RIP packet sending interval, in milliseconds. It is in the range 10 to 100.

*count*: Maximum number of RIP packets sent at each interval. It is in the range 1 to 20.

## Description

Use the **output-delay** command to configure the maximum RIP packets that can be sent at the specified interval for all interfaces under the RIP process.

Use the **undo output-delay** command to restore the default.

By default, an interface sends up to three RIP packets every 20 milliseconds.

## Examples

```
# Configure all the interfaces under RIP process 1 to send up to 10 RIP packets every 30 milliseconds.
```

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-1] output-delay 30 output-count 10
```

## peer

### Syntax

```
peer ip-address  
undo peer ip-address
```

### View

RIP view

### Default Level

2: System level

### Parameters

*ip-address*: IP address of a RIP neighbor, in dotted decimal format.

### Description

Use the **peer** command to specify the IP address of a neighbor in the non-broadcast multi-access (NBMA) network, where routing updates destined for the peer are unicast, rather than multicast or broadcast.

Use the **undo peer** command to remove the IP address of a neighbor.

By default, no neighbor is specified.

Note that you need not use the **peer ip-address** command when the neighbor is directly connected; otherwise the neighbor may receive both the unicast and multicast (or broadcast) of the same routing information.

### Examples

```
# Specify to send unicast updates to peer 202.38.165.1.  
<Sysname> system-view  
[Sysname] rip 1  
[Sysname-rip-1] peer 202.38.165.1
```

## preference

### Syntax

```
preference [ route-policy route-policy-name ] value  
undo preference [ route-policy ]
```

### View

RIP view

### Default Level

2: System level

### Parameters

*route-policy-name*: Routing policy name with 1 to 19 characters.

*value*: Priority for RIP route, in the range of 1 to 255. The smaller the value, the higher the priority.

## Description

Use the **preference** command to specify the RIP route priority.

Use the **undo preference route-policy** command to restore the default.

By default, the priority of a RIP route is 100.

You can specify a routing policy using the keyword **route-policy** to set the specified priority to routes matching the routing policy.

- If a priority is set for matched routes in the routing policy, the priority applies to these routes. The priority of other routes is the one set by the **preference** command.
- If no priority is set for matched routes in the routing policy, the priority of all routes is the one set by the **preference** command.

## Examples

```
# Set the RIP route priority to 120.
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] preference 120
```

## reset rip statistics

### Syntax

```
reset rip process-id statistics
```

### View

User view

### Default Level

2: System level

### Parameters

*process-id*: RIP process ID, in the range of 1 to 65535.

## Description

Use the **reset rip statistics** command to clear the statistics of the specified RIP process. This command can be used to clear the statistics for debugging.

## Examples

```
# Clear statistics in RIP process 100.
<Sysname> reset rip 100 statistics
```

## rip

### Syntax

```
rip [ process-id ] [ vpn-instance vpn-instance-name ]
undo rip [ process-id ] [ vpn-instance vpn-instance-name ]
```

## View

System view

## Default Level

2: System level

## Parameters

*process-id*: RIP process ID, in the range of 1 to 65535. The default is 1.

**vpn-instance** *vpn-instance-name*: Specifies a VPN instance name, a string of 1 to 31 case-sensitive characters.

## Description

Use the **rip** command to create a RIP process and enter RIP view.

Use the **undo rip** command to disable a RIP process.

By default, no RIP process runs.

Note that:

- If no VPN instance is specified, the RIP process will run under public network instance.
- You must create a VPN instance before you apply a RIP process to it. For related configuration, refer to the **ip vpn-instance** command.
- You must enable the RIP process before configuring the global parameters. This limitation is not for configuration of interface parameters.
- The configured interface parameters become invalid after you disable the RIP process.

## Examples

```
# Create a RIP process and enter RIP process view.
```

```
<Sysname> system-view  
[Sysname] rip  
[Sysname-rip-1]
```

## rip authentication-mode

### Syntax

```
rip authentication-mode { md5 { rfc2082 key-string key-id | rfc2453 key-string } | simple password }  
undo rip authentication-mode
```

## View

Interface view

## Default Level

2: System level

## Parameters

**md5**: MD5 authentication mode.

**rfc2453**: Uses the message format defined in RFC 2453 (IETF standard).

**rfc2082**: Uses the message format defined in RFC 2082.

*key-id*: MD5 key number, in the range of 1 to 255.

*key-string*: MD5 key string with 1 to 16 characters in plain text format, or 1 to 24 characters in cipher text format. When the **display current-configuration** command is used to display system information, a 24-character cipher string is displayed as the MD5 key string.

**simple**: Plain text authentication mode.

*password*: Plain text authentication string with 1 to 16 characters.

## Description

Use the **rip authentication-mode** command to configure RIPv2 authentication mode and parameters.

Use the **undo rip authentication-mode** command to cancel authentication.

Note that the key string you configured can overwrite the old one if there is any.

Related commands: **rip version**.

## Examples

# Configure MD5 authentication on VLAN-interface 10 with the key string being **rose** in the format defined in RFC 2453.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip version 2
[Sysname-Vlan-interface10] rip authentication-mode md5 rfc2453 rose
```

## rip default-route

### Syntax

**rip default-route** { { **only** | **originate** } [ **cost** *cost* ] | **no-originate** }

**undo rip default-route**

### View

Interface view

### Default Level

2: System level

### Parameters

**only**: Advertises only a default route.

**originate**: Advertises a default route and other routes.

*cost*: Cost of the default route, in the range 1 to 15.

**no-originate**: Advertises routes other than a default route.

## Description

Use the **rip default-route** command to configure the RIP interface to advertise a default route with the specified metric.

Use the **undo rip default-route** command to disable the RIP interface from sending a default route.

By default, a RIP interface can advertise a default route if the RIP process is configured with default route advertisement.



#### Note

A RIP router configured to advertise a default route will not receive any default routes from RIP neighbors.

---

Related commands: **default-route**.

### Examples

# Configure VLAN-interface 10 to advertise only a default route with a metric of 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip default-route only cost 2
```

### rip input

#### Syntax

```
rip input
undo rip input
```

#### View

Interface view

#### Default Level

2: System level

#### Parameters

None

#### Description

Use the **rip input** command to enable the interface to receive RIP messages.

Use the **undo rip input** command to disable the interface from receiving RIP messages.

By default, an interface is enabled to receive RIP messages.

Related commands: **rip output**.

### Examples

# Disable VLAN-interface 10 from receiving RIP messages.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] undo rip input
```

## rip metricin

### Syntax

```
rip metricin [ route-policy route-policy-name ] value
undo rip metricin
```

### View

Interface view

### Default Level

2: System level

### Parameters

**route-policy** *route-policy-name*: Specifies the name of a routing policy used to add an additional metric for the routes matching it. The name is a string of 1 to 19 characters

*value*: Additional metric added to received routes, in the range of 0 to 16.

### Description

Use the **rip metricin** command to configure the interface to add a metric to the routes it receives.

Use the **undo rip metricin** command to restore the default.

By default, the additional metric of a received route is 0.

When a valid RIP route is received, the system adds a metric to it and then installs it into the routing table. Therefore, the metric of the route received on the configured interface is increased. If the sum of the additional metric and the original metric is greater than 16, the metric of the route will be 16.

If a routing policy is referenced with the **route-policy** keyword:

- Routes matching the policy is added with the metric specified in the **apply cost** command configured in the policy, while routes not matching it is added with the metric specified in the **rip metricout** command. Note that, the **rip metricout** command does not support the **+** or **-** keyword (used to add or reduce a metric) specified in the **apply cost** command. For details about the **apply cost** command, refer to *Routing Policy Commands* in the *IP Routing Volume*.
- If the **apply cost** command is not configured in the policy, all the advertised routes is added with the metric specified in the **rip metricout** command.

Related commands: **rip metricout**.

### Examples

# Configure VLAN-interface 10 to add a metric of 6 for incoming route 1.0.0.0/8 and to add a metric of 2 for other incoming routes.

```
<Sysname> system-view
[Sysname] ip ip-prefix 123 permit 1.0.0.0 8
[Sysname] route-policy abc permit node 0
[Sysname-route-policy] if-match ip-prefix 123
[Sysname-route-policy] apply cost 6
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip metricin route-policy abc 2
```

## rip metricout

### Syntax

```
rip metricout [ route-policy route-policy-name ] value
undo rip metricout
```

### View

Interface view

### Parameters

*value*: Additional metric of sent routes, in the range of 1 to 16.

### Description

Use the **rip metricout** command to add a metric to sent routes.

Use the **undo rip metricout** command to restore the default.

By default, the additional metric for sent routes is 1.

With the command configured on an interface, the metric of RIP routes sent on the interface will be increased.

If a routing policy is referenced with the **route-policy** keyword:

- Routes matching the policy is added with the metric specified in the **apply cost** command configured in the policy, while routes not matching it is added with the metric specified in the **rip metricout** command. Note that, the **rip metricout** command does not support the **+** or **-** keyword (used to add or reduce a metric) specified in the **apply cost** command. For details about the **apply cost** command, refer to *Routing Policy Commands* in the *IP Routing Volume*.
- If the **apply cost** command is not configured in the policy, all the advertised routes is added with the metric specified in the **rip metricout** command.

Related commands: **rip metricin**.

### Examples

```
# Configure VLAN-interface 10 to add a metric of 6 for the outgoing route 1.0.0.0/8 and to add a metric of 2 for other outgoing routes.
```

```
<Sysname> system-view
[Sysname] ip ip-prefix 123 permit 1.0.0.0 8
[Sysname] route-policy abc permit node 0
[Sysname-route-policy] if-match ip-prefix 123
[Sysname-route-policy] apply cost 6
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip metricout route-policy abc 2
```

## rip mib-binding

### Syntax

```
rip mib-binding process-id
undo rip mib-binding
```

## View

System view

## Default Level

2: System level

## Parameters

*process-id*: RIP process ID, in the range of 1 to 65535.

## Description

Use the **rip mib-binding** command to bind MIB operations with a specified RIP process, so that the RIP process can receive SNMP requests.

Use the **undo rip mib-binding** command to restore the default.

By default, MIB operations are bound to RIP process 1, that is, RIP process 1 is enabled to receive SNMP requests.

## Examples

# Enable RIP process 100 to receive SNMP requests.

```
<Sysname> system-view  
[Sysname] rip mib-binding 100
```

# Restore the default.

```
[Sysname] undo rip mib-binding
```

## rip output

### Syntax

```
rip output  
undo rip output
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **rip output** command to enable the interface to send RIP messages.

Use the **undo rip output** command to disable the interface from sending RIP messages.

Sending RIP messages is enabled on an interface by default.

Related commands: **rip input**.

## Examples

```
# Disable VLAN-interface 10 from receiving RIP messages.  
<Sysname> system-view  
[Sysname] interface vlan-interface 10  
[Sysname-Vlan-interface10] undo rip output
```

## rip poison-reverse

### Syntax

```
rip poison-reverse  
undo rip poison-reverse
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **rip poison-reverse** command to enable the poison reverse function.

Use the **undo rip poison-reverse** command to disable the poison reverse function.

By default, the poison reverse function is disabled.

## Examples

```
# Enable the poison reverse function for RIP routing updates on VLAN-interface 10.  
<Sysname> system-view  
[Sysname] interface vlan-interface 10  
[Sysname-Vlan-interface10] rip poison-reverse
```

## rip split-horizon

### Syntax

```
rip split-horizon  
undo rip split-horizon
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

## Description

Use the **rip split-horizon** command to enable the split horizon function.

Use the **undo rip split-horizon** command to disable the split horizon function.

The split horizon function is enabled by default.

- The split horizon function is necessary for preventing routing loops. Therefore, you are not recommended to disable it.
- In special cases, make sure it is necessary to disable the split horizon function.



### Note

Only the poison reverse function takes effect if both the split horizon and poison reverse functions are enabled.

---

## Examples

```
# Enable the split horizon function on VLAN-interface 10.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip split-horizon
```

## rip summary-address

### Syntax

```
rip summary-address ip-address { mask | mask-length }
undo rip summary-address ip-address { mask | mask-length }
```

### View

Interface view

### Default Level

2: System level

### Parameters

*ip-address*: Destination IP address of summary route.

*mask*: Subnet mask of summary route, in dotted decimal format.

*mask-length*: Subnet mask length of summary route, in the range 0 to 32.

## Description

Use the **rip summary-address** command to configure RIPv2 to advertise a summary route through the interface.

Use the **undo rip summary-address** command to remove the configuration.

Note that the summary address is valid only when the automatic summarization is disabled.

Related commands: **summary**.

## Examples

```
# Advertise a local summary address on VLAN-interface 10.  
<Sysname> system-view  
[Sysname] interface vlan-interface 10  
[Sysname-Vlan-interface10] rip summary-address 10.0.0.0 255.255.255.0
```

## rip version

### Syntax

```
rip version { 1 | 2 [ broadcast | multicast ] }  
undo rip version
```

### View

Interface view

### Default Level

2: System level

### Parameters

1: RIP version 1.

2: RIP version 2.

**broadcast**: Sends RIPv2 messages in broadcast mode.

**multicast**: Sends RIPv2 messages in multicast mode.

### Description

Use the **rip version** command to specify a RIP version for the interface.

Use the **undo rip version** command to remove the specified RIP version.

By default, no RIP version is configured for an interface, which uses the global RIP version. If the global RIP version is not configured, the interface can only send RIPv1 broadcasts and can receive RIPv1 broadcasts and unicasts, and RIPv2 broadcasts, multicasts and unicasts.

If RIPv2 is specified with no sending mode configured, RIPv2 messages will be sent in multicast mode.

When RIPv1 runs on an interface, the interface will:

- Send RIPv1 broadcast messages
- Receive RIPv1 broadcast messages
- Receive RIPv1 unicast messages

When RIPv2 runs on the interface in broadcast mode, the interface will:

- Send RIPv2 broadcast messages
- Receive RIPv1 broadcast messages
- Receive RIPv1 unicast messages
- Receive RIPv2 broadcast messages
- Receive RIPv2 multicast messages
- Receive RIPv2 unicast messages

When RIPv2 runs on the interface in multicast mode, the interface will:

- Send RIPv2 multicast messages

- Receive RIPv2 broadcast messages
- Receive RIPv2 multicast messages
- Receive RIPv2 unicast messages

## Examples

# Configure VLAN-interface 10 to broadcast RIPv2 messages.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip version 2 broadcast
```

## silent-interface (RIP view)

### Syntax

```
silent-interface { interface-type interface-number | all }
undo silent-interface { interface-type interface-number | all }
```

### View

RIP view

### Default Level

2: System level

### Parameters

*interface-type interface-number*: Specifies an interface by its type and number.

**all**: Silents all interfaces.

### Description

Use the **silent-interface** command to disable an interface or all interfaces from sending routing updates. That is, the interface only receives but does not send RIP messages.

Use the **undo silent-interface** command to restore the default.

By default, all interfaces are allowed to send routing updates.

## Examples

# Configure all VLAN interfaces to work in the silent state, and activate VLAN-interface 10.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] silent-interface all
[Sysname-rip-100] undo silent-interface vlan-interface 10
[Sysname-rip-100] network 131.108.0.0
```

## summary

### Syntax

**summary**

**undo summary**

## View

RIP view

## Default Level

2: System level

## Parameters

None

## Description

Use the **summary** command to enable automatic RIPv2 summarization. Natural masks are used to advertise summary routes so as to reduce the size of routing tables.

Use the **undo summary** command to disable automatic RIPv2 summarization so that all subnet routes can be broadcast.

By default, automatic RIPv2 summarization is enabled.

Enabling automatic RIPv2 summarization can reduce the size of the routing table to enhance the scalability and efficiency of large networks.

Related commands: **rip version**.

## Examples

# Disable RIPv2 automatic summarization.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1] undo summary
```

## timers

### Syntax

```
timers { garbage-collect garbage-collect-value | suppress suppress-value | timeout timeout-value | update update-value }*
```

```
undo timers { garbage-collect | suppress | timeout | update } *
```

## View

RIP view

## Default Level

2: System level

## Parameters

*garbage-collect-value*: Garbage-collect timer time in seconds, in the range of 1 to 3600.

*suppress-value*: Suppress timer time in seconds, in the range of 0 to 3600.

*timeout-value*: Timeout timer time in seconds, in the range of 1 to 3600.

*update-value*: Update timer time in seconds, in the range of 1 to 3600.

## Description

Use the **timers** command to configure RIP timers. By adjusting RIP timers, you can improve network performance.

Use the **undo timers** command to restore the default.

By default, the garbage-collect timer is 120 seconds, the suppress timer 120 seconds, the timeout timer 180 seconds, and the update timer 30 seconds.

RIP is controlled by the above four timers.

- The update timer defines the interval between routing updates.
- The timeout timer defines the route aging time. If no routing update related to a route is received after the aging time, the metric of the route is set to 16 in the routing table.
- The suppress timer defines how long a RIP route stays in the suppressed state. When the metric of a route is 16, the route enters the suppressed state. In the suppressed state, only routes which come from the same neighbor and whose metric is less than 16 will be received by the router to replace unreachable routes.
- The garbage-collect timer defines the interval from when the metric of a route becomes 16 to when it is deleted from the routing table. During the Garbage-Collect timer length, RIP advertises the route with the routing metric set to 16. If no routing update is announced for that route after the Garbage-Collect timer expires, the route will be deleted from the routing table.

Note that:

- Generally, you are not recommended to change the default values of these timers.
- The time lengths of these timers must be kept consistent on all routers and access servers in the network.

## Examples

# Specifies the update, timeout, suppress, and garbage-collect timers as 5, 15, 15 and 30 respectively.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] timers update 5 timeout 15 suppress 15 garbage-collect 30
```

## validate-source-address

### Syntax

```
validate-source-address
undo validate-source-address
```

### View

RIP view

### Default Level

2: System level

### Parameters

None

## Description

Use the **validate-source-address** command to enable the source IP address validation on incoming RIP routing updates.

Use the **undo validate-source-address** command to disable the source IP address validation.

The source IP address validation is enabled by default.

RIP checks whether the source IP address of the packet is on the same network segment as the interface IP address; if not, the packet is discarded.

Generally, disabling the validation is not recommended.

## Examples

```
# Disable the source IP address validation on incoming RIP routing updates.
```

```
<Sysname> system-view
[Sysname-rip] rip 100
[Sysname-rip-100] undo validate-source-address
```

## version

### Syntax

```
version { 1 | 2 }
```

```
undo version
```

### View

RIP view

### Default Level

2: System level

### Parameters

- 1: Specifies the RIP version as RIPv1.
- 2: Specifies the RIP version as RIPv2. RIPv2 messages are multicast.

## Description

Use the **version** command to specify a global RIP version.

Use the **undo version** command to remove the configured global RIP version.

By default, if an interface has a RIP version specified, the RIP version takes effect; if it has no RIP version specified, it can send RIPv1 broadcasts, and receive RIPv1 broadcasts, RIPv1 unicasts, RIPv2 broadcasts, RIPv2 multicasts, and RIPv2 unicasts.

Note that:

- If an interface has an RIP version specified, the RIP version takes precedence over the global RIP version.
- If no RIP version is specified for the interface and the global version is RIPv1, the interface inherits RIPv1, and it can send RIPv1 broadcasts, and receive RIPv1 broadcasts and unicasts.

- If no RIP version is specified for the interface and the global version is RIPv2, the interface operates in the RIPv2 multicast mode, and it can send RIPv2 multicasts, and receive RIPv2 broadcasts, multicasts and unicasts.

### Examples

# Specify RIPv2 as the global RIP version.

```
<Sysname> system-view  
[Sysname] rip 100  
[Sysname-rip-100] version 2
```

# Table of Contents

<b>1 OSPF Configuration Commands</b> .....	<b>1-1</b>
OSPF Configuration Commands .....	1-1
abr-summary (OSPF area view).....	1-1
area (OSPF view).....	1-2
asbr-summary.....	1-2
authentication-mode.....	1-3
bandwidth-reference (OSPF view) .....	1-4
default.....	1-5
default-cost (OSPF area view) .....	1-5
default-route-advertise (OSPF view) .....	1-6
description (OSPF/OSPF area view).....	1-7
display ospf abr-asbr .....	1-8
display ospf asbr-summary .....	1-9
display ospf brief.....	1-10
display ospf cumulative .....	1-13
display ospf error.....	1-15
display ospf interface.....	1-16
display ospf lsdb.....	1-18
display ospf nexthop.....	1-20
display ospf peer .....	1-21
display ospf peer statistics .....	1-24
display ospf request-queue .....	1-25
display ospf retrans-queue .....	1-26
display ospf routing.....	1-27
display ospf sham-link .....	1-28
display ospf vlink .....	1-29
enable link-local-signaling .....	1-30
enable log.....	1-31
enable out-of-band-resynchronization.....	1-32
filter.....	1-32
filter-policy export (OSPF view).....	1-33
filter-policy import (OSPF view).....	1-34
graceful-restart (OSPF view).....	1-35
graceful-restart help.....	1-36
graceful-restart interval (OSPF view) .....	1-37
host-advertise .....	1-37
import-route (OSPF view).....	1-38
ip binding vpn-instance.....	1-39
log-peer-change .....	1-40
lsa-arrival-interval .....	1-41
lsa-generation-interval .....	1-41
lsdb-overflow-limit.....	1-42
maximum load-balancing (OSPF view) .....	1-43

maximum-routes	1-43
network (OSPF area view)	1-44
nssa	1-45
opaque-capability enable	1-46
ospf	1-46
ospf authentication-mode	1-47
ospf cost	1-49
ospf dr-priority	1-49
ospf mib-binding	1-50
ospf mtu-enable	1-51
ospf network-type	1-51
ospf packet-process prioritized-treatment	1-52
ospf timer dead	1-53
ospf timer hello	1-54
ospf timer poll	1-55
ospf timer retransmit	1-55
ospf trans-delay	1-56
peer	1-57
preference	1-58
reset ospf counters	1-59
reset ospf process	1-59
reset ospf redistribution	1-60
rfc1583 compatible	1-60
route-tag	1-61
sham-link	1-62
silent-interface (OSPF view)	1-63
snmp-agent trap enable ospf	1-64
spf-schedule-interval	1-65
stub (OSPF area view)	1-66
stub-router	1-67
transmit-pacing	1-67
vlink-peer (OSPF area view)	1-68

# 1 OSPF Configuration Commands

---

## OSPF Configuration Commands

### abr-summary (OSPF area view)

#### Syntax

```
abr-summary ip-address { mask | mask-length } [ advertise | not-advertise ] [ cost cost ]  
undo abr-summary ip-address { mask | mask-length }
```

#### View

OSPF area view

#### Default Level

2: System level

#### Parameters

*ip-address*: Destination IP address of the summary route, in dotted decimal format.

*mask*: Mask of the IP address in dotted decimal format.

*mask-length*: Mask length, in the range 0 to 32 bits.

**advertise** | **not-advertise**: Advertises the summary route or not. By default, the summary route is advertised.

**cost cost**: Specifies the cost of the summary route, in the range 1 to 16777215. The default cost is the largest cost value among routes that are summarized.

#### Description

Use the **abr-summary** command to configure a summary route on the area border router.

Use the **undo abr-summary** command to remove a summary route.

By default, no route summarization is configured on an ABR.

You can enable advertising the summary route or not, and specify a route cost.

This command is usable only on an ABR. Multiple contiguous networks may be available in an area, where you can summarize them into one network on the ABR for advertisement. The ABR advertises only the summary route to other areas.

With the **undo abr-summary** command used, summarized routes will be advertised.

#### Examples

```
# Summarize networks 36.42.10.0/24 and 36.42.110.0/24 in Area 1 into 36.42.0.0/16.
```

```
<Sysname> system-view  
[Sysname] ospf 100  
[Sysname-ospf-100] area 1
```

```
[Sysname-ospf-100-area-0.0.0.1] network 36.42.10.0 0.0.0.255
[Sysname-ospf-100-area-0.0.0.1] network 36.42.110.0 0.0.0.255
[Sysname-ospf-100-area-0.0.0.1] abr-summary 36.42.0.0 255.255.0.0
```

## area (OSPF view)

### Syntax

```
area area-id
undo area area-id
```

### View

OSPF view

### Default Level

2: System level

### Parameters

*area-id*: ID of an area, a decimal integer in the range 0 to 4294967295 that is translated into the IP address format by the system, or an IP address.

### Description

Use the **area** command to create an area and enter area view.

Use the **undo area** command to remove a specified area.

No OSPF area is created by default.

### Examples

```
# Create Area 0 and enter Area 0 view
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0]
```

## asbr-summary

### Syntax

```
asbr-summary ip-address { mask | mask-length } [ cost cost | not-advertise | tag tag ] *
undo asbr-summary ip-address { mask | mask-length }
```

### View

OSPF view

### Default Level

2: System level

### Parameters

*ip-address*: IP address of the summary route in dotted decimal notation.

*mask*: Summary route mask, in dotted decimal notation.

*mask-length*: Length of summary route mask, in the range 0 to 32 bits.

**cost cost**: Specifies the cost of the summary route, in the range 1 to 16777214. For Type-1 external routes, the cost defaults to the largest cost among routes that are summarized. For Type-2 external routes, the cost defaults to the largest cost among routes that are summarized plus 1.

**not-advertise**: Disables advertising the summary route. If the keyword is not specified, the route is advertised.

**tag tag**: Specifies a tag value for the summary route, used by a route policy to control summary route advertisement, in the range 0 to 4294967295. The default is 1.

## Description

Use the **asbr-summary** command to configure a summary route.

Use the **undo asbr-summary** command to remove a summary route.

No ASBR route summarization is configured by default.

With the **asbr-summary** command configured on an ASBR, it summarizes redistributed routes that fall into the specified address range into a single route. If the ASBR resides in an NSSA area, it advertises the summary route in a Type-7 LSA into the area.

With the **asbr-summary** command configured on an NSSA ABR, it summarizes routes described by Type-5 LSAs translated from Type-7 LSAs into a single route and advertises the summary route to other areas. This command does not take effect on non NSSA ABRs.

With the **undo asbr-summary** command used, summarized routes will be advertised.

Related command: **display ospf asbr-summary**.

## Examples

# Summarize redistributed routes into a single route, specifying a tag value of 2 and a cost of 100 for the summary route.

```
<Sysname> system-view
[Sysname] ip route-static 10.2.1.0 24 null 0
[Sysname] ip route-static 10.2.2.0 24 null 0
[Sysname] ospf 100
[Sysname-ospf-100] import-route static
[Sysname-ospf-100] asbr-summary 10.2.0.0 255.255.0.0 tag 2 cost 100
```

## authentication-mode

### Syntax

**authentication-mode { md5 | simple }**

**undo authentication-mode**

### View

OSPF area view

### Default Level

2: System level

## Parameters

**md5**: Specifies the MD5 ciphertext authentication mode.

**simple**: Specifies the simple authentication mode.

## Description

Use the **authentication-mode** command to specify an authentication mode for the OSPF area.

Use the **undo authentication-mode** command to remove the authentication mode.

By default, no authentication mode is configured for an OSPF area.

Routers that reside in the same area must have the same authentication mode: non-authentication, simple, or MD5.

Related commands: **ospf authentication-mode**.

## Examples

# Configure OSPF area 0 to use the MD5 ciphertext authentication mode.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0] authentication-mode md5
```

## bandwidth-reference (OSPF view)

### Syntax

**bandwidth-reference** *value*

**undo bandwidth-reference**

### View

OSPF view

### Default Level

2: System level

### Parameters

*value*: Bandwidth reference value for link cost calculation, in the range 1 to 2147483648 Mbps.

### Description

Use the **bandwidth-reference** command to specify a reference bandwidth value for link cost calculation.

Use the **undo bandwidth-reference** command to restore the default value.

The default value is 100 Mbps.

When links have no cost values configured, OSPF calculates their cost values: Cost=Reference bandwidth value / Link bandwidth. If the calculated cost is greater than 65535, the value of 65535 is used.

### Examples

# Specify the reference bandwidth value as 1000 Mbps.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] bandwidth-reference 1000
```

## default

### Syntax

```
default { cost cost | limit limit | tag tag | type type } *
undo default { cost | limit | tag | type } *
```

### View

OSPF view

### Default Level

2: System level

### Parameters

*cost*: Specifies the default cost for redistributed routes, in the range 0 to 16777214.

*limit*: Specifies the default upper limit of routes redistributed per time, in the range 1 to 2147483647.

*tag*: Specifies the default tag for redistributed routes, in the range 0 to 4294967295.

*type*: Specifies the default type for redistributed routes: 1 or 2.

### Description

Use the **default** command to configure default parameters for redistributed routes.

Use the **undo default** command to restore default values.

The cost, route type, tag, and the upper limit are 1, 2, 1 and 1000 by default.

Related commands: **import-route**.

### Examples

# Configure the default cost, upper limit, tag and type as 10, 20000, 100 and 2 respectively for redistributed external routes.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] default cost 10 limit 20000 tag 100 type 2
```

## default-cost (OSPF area view)

### Syntax

```
default-cost cost
undo default-cost
```

### View

OSPF area view

## Default Level

2: System level

## Parameters

*cost*: Specifies a cost for the default route advertised to the Stub or NSSA area, in the range 0 to 16777214.

## Description

Use the **default-cost** command to configure a cost for the default route advertised to the stub or NSSA area.

Use the **undo default-cost** command to restore the default value.

The cost defaults to 1.

This command is only applicable to the ABR of a stub area or the ABR/ASBR of an NSSA area.

Related commands: **stub**, **nssa**.

## Examples

# Configure Area 1 as a stub area, and specify the cost of the default route advertised to the stub area as 20.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] stub
[Sysname-ospf-100-area-0.0.0.1] default-cost 20
```

## default-route-advertise (OSPF view)

### Syntax

```
default-route-advertise [ [ always | cost cost | route-policy route-policy-name | type type ] * | summary cost cost ]
```

```
undo default-route-advertise
```

### View

OSPF view

### Default Level

2: System level

### Parameters

**always**: Generates a default route in an ASE LSA into the OSPF routing domain regardless of whether a default route exists in the routing table. Without this keyword used, the command can distribute a default route in a Type-5 LSA into the OSPF routing domain only when a default route exists in the routing table.

**cost** *cost*: Specifies a cost for the default route, in the range 0 to 16777214. If no *cost* is specified, the default cost specified by the **default cost** command applies..

**route-policy** *route-policy-name*: Specifies a route policy name, a string of 1 to 19 characters. If the default route matches the specified route policy, the route policy modifies some values in the ASE LSA.

**type** *type*: Specifies a type for the ASE LSA: 1 or 2. If *type* is not specified, the default type for the ASE LSA specified by the **default type** command applies.

**summary**: Advertises the Type-3 summary LSA of the specified default route.

## Description

Use the **default-route-advertise** command to generate a default route into the OSPF routing domain.

Use the **undo default-route-advertise** command to disable OSPF from distributing a default external route.

By default, no default route is distributed.

Using the **import-route** command cannot redistribute a default route. To do so, use the **default-route-advertise** command. If no default route exists in the router's routing table, use the **default-route-advertise always** command to generate a default route in a Type-5 LSA.

The **default-route-advertise summary cost** command is applicable only to VPNs, and the default route is redistributed in a Type-3 LSA. The PE router advertises the redistributed default route to the CE router.

Related commands: **import-route**, **default**.

## Examples

# Generate a default route in an ASE LSA into the OSPF routing domain (no default route configured on the router), regardless of whether the default route is available in the routing table.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] default-route-advertise always
```

## description (OSPF/OSPF area view)

### Syntax

**description** *description*

**undo description**

### View

OSPF view/OSPF area view

### Default Level

2: System level

### Parameters

*description*: Configures a description for the OSPF process in OSPF view, or for the OSPF area in OSPF area view. *description* is a string of up to 80 characters.

## Description

Use the **description** command to configure a description for an OSPF process or area.

Use the **undo description** command to remove the description.

No description is configured by default.

Use of this command is only for the identification of an OSPF process or area. The description has no special meaning.

## Examples

# Describe the OSPF process 100 as **abc**.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] description abc
```

# Describe the OSPF area0 as **bone area**.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0] description bone area
```

## display ospf abr-asbr

### Syntax

```
display ospf [ process-id ] abr-asbr
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*process-id*: OSPF process ID, in the range 1 to 65535. Use this argument to display information about the routes to the ABR/ASBR under the specified OSPF process.

### Description

Use the **display ospf abr-asbr** command to display information about the routes to OSPF ABR/ASBR.

If you use this command on routers in a stub area, no ASBR information is displayed.

## Examples

# Display information about the routes to the OSPF ABR and ASBR.

```
<Sysname> display ospf abr-asbr
```

```
OSPF Process 1 with Router ID 192.168.1.2
Routing Table to ABR and ASBR
```

Type	Destination	Area	Cost	NextHop	RtType
Inter	3.3.3.3	0.0.0.0	3124	10.1.1.2	ASBR
Intra	2.2.2.2	0.0.0.0	1562	10.1.1.2	ABR

**Table 1-1 display ospf abr-asbr command output description**

Field	Description
Type	Type of the route to the ABR or ASBR: <ul style="list-style-type: none"><li>• Intra: intra-area route</li><li>• Inter: Inter-area route</li></ul>
Destination	Router ID of an ABR/ASBR
Area	ID of the area of the next hop
Cost	Cost from the router to the ABR/ASBR
Nexthop	Next hop address
RtType	Router type: ABR, ASBR

## display ospf asbr-summary

### Syntax

```
display ospf [ process-id ] asbr-summary [ ip-address { mask | mask-length } ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*process-id*: OSPF process ID, in the range 1 to 65535.

*ip-address*: IP address, in dotted decimal format.

*mask*: IP address mask, in dotted decimal format.

*mask-length*: Mask length, in the range 0 to 32 bits.

### Description

Use the **display ospf asbr-summary** command to display information about the redistributed routes that are summarized.

If no OSPF process is specified, related information of all OSPF processes is displayed.

If no IP address is specified, information about all summarized redistributed routes will be displayed.

Related commands: **asbr-summary**.

### Examples

# Display information about all summarized redistributed routes.

```
<Sysname> display ospf asbr-summary
```

```
OSPF Process 1 with Router ID 2.2.2.2
```

```
Summary Addresses
```

Total Summary Address Count: 1

#### Summary Address

Net : 30.1.0.0  
Mask : 255.255.0.0  
Tag : 20  
Status : Advertise  
Cost : 10 (Configured)  
The Count of Route is : 2

Destination	Net Mask	Proto	Process	Type	Metric
30.1.2.0	255.255.255.0	OSPF	1	2	1
30.1.1.0	255.255.255.0	OSPF	1	2	1

**Table 1-2 display ospf asbr-summary command output description**

Field	Description
Total Summary Address Count	Total summary route number
Net	The address of the summary route
Mask	The mask of the summary route address
Tag	The tag of the summary route
Status	The advertisement status of the summary route
Cost	The cost to the summary net
The Count of Route	The count of routes that are summarized
Destination	Destination address of a summarized route
Net Mask	Network mask of a summarized route
Proto	Routing protocol
Process	Process ID of routing protocol
Type	Type of a summarized route
Metric	Metric of a summarized route

## display ospf brief

### Syntax

**display ospf [ *process-id* ] brief**

### View

Any view

### Default Level

1: Monitor level

## Parameters

*process-id*: OSPF process ID, in the range 1 to 65535.

## Description

Use the **display ospf brief** command to display OSPF brief information. If no OSPF process is specified, brief information about all OSPF processes is displayed.

## Examples

# Display OSPF brief information.

```
<Sysname> display ospf brief
```

```
OSPF Process 1 with Router ID 192.168.1.2
```

```
OSPF Protocol Information
```

```
RouterID: 192.168.1.2      Border Router:  NSSA
```

```
Route Tag: 0
```

```
Multi-VPN-Instance is not enabled
```

```
Applications Supported: MPLS Traffic-Engineering
```

```
SPF-schedule-interval: 5 0 5000
```

```
LSA generation interval: 5 0 5000
```

```
LSA arrival interval: 1000
```

```
Transmit pacing: Interval: 20 Count: 3
```

```
Default ASE parameters: Metric: 1 Tag: 1 Type: 2
```

```
Route Preference: 10
```

```
ASE Route Preference: 150
```

```
SPF Computation Count: 22
```

```
RFC 1583 Compatible
```

```
Area Count: 1  Nssa Area Count: 1
```

```
ExChange/Loading Neighbors: 0
```

```
Area: 0.0.0.1      (MPLS TE not enabled)
```

```
Authtype: None Area flag: NSSA
```

```
SPF Scheduled Count: 5
```

```
ExChange/Loading Neighbors: 0
```

```
Interface: 192.168.1.2 (Vlan-interfaces)
```

```
Cost: 1      State: DR      Type: Broadcast      MTU: 1500
```

```
Priority: 1
```

```
Designated Router: 192.168.1.2
```

```
Backup Designated Router: 192.168.1.1
```

```
Timers: Hello 10 , Dead 40 , Poll 40 , Retransmit 5 , Transmit Delay 1
```

**Table 1-3 display ospf brief command output description**

Field	Description
OSPF Process 1 with Router ID 192.168.1.2	OSPF process ID and OSPF router ID
RouterID	Router ID
Border Router	Whether the router is a boarder router: <ul style="list-style-type: none"> <li>• ABR</li> <li>• ASBR</li> <li>• NSSA ABR</li> </ul>
Route Tag	The tag of redistributed routes
Multi-VPN-Instance is not enabled	The OSPF process does not support multi-VPN-instance.
Applications Supported	Applications supported. <b>MPLS Traffic-Engineering</b> means MPLS TE is supported.
SPF-schedule-interval	Interval for SPF calculations
LSA generation interval	LSA generation interval
LSA arrival interval	Minimum LSA repeat arrival interval
Transmit pacing	LSU packet transmit rate of the interface: <ul style="list-style-type: none"> <li>• <b>Interval</b> indicates the LSU transmit interval of the interface.</li> <li>• <b>Count</b> indicates the maximum number of LSU packets sent at each interval.</li> </ul>
Default ASE Parameter	Default ASE Parameters: metric, tag, route type.
Route Preference	Internal route priority
ASE Route Preference	External route priority
SPF Computation count	SPF computation count of the OSPF process
RFC1583 Compatible	Compatible with routing rules defined in RFC1583
Area Count	Area number of the current process
Nssa Area Count	NSSA area number of the current process
ExChange/Loading Neighbors	Neighbors in ExChange/Loading state
Area	Area ID in the IP address format
Authtype	Authentication type of the area: <ul style="list-style-type: none"> <li>• None: No authentication</li> <li>• Simple: simple authentication</li> <li>• MD5: MD5 authentication</li> </ul>
Area flag	The type of the area
SPF scheduled Count	SPF calculation count in the OSPF area
Interface	Interface in the area
Cost	Interface cost
State	Interface state
Type	Interface network type
MTU	Interface MTU

Field	Description
Priority	Router priority
Designated Router	The Designated Router
Backup Designated Router	The Backup Designated Router
Timers	Intervals of timers: hello, dead, poll, retransmit, and transmit delay

## display ospf cumulative

### Syntax

**display ospf** [ *process-id* ] **cumulative**

### View

Any view

### Default Level

1: Monitor level

### Parameters

*process-id*: OSPF process ID, in the range 1 to 65535.

### Description

Use the **display ospf cumulative** command to display OSPF statistics.

Use of this command is helpful for troubleshooting.

### Examples

# Display OSPF statistics.

```
<Sysname> display ospf cumulative
      OSPF Process 1 with Router ID 2.2.2.2
      Cumulations

      IO Statistics
            Type      Input      Output
      Hello          61         122
      DB Description    2          3
      Link-State Req    1          1
      Link-State Update 3          3
      Link-State Ack    3          2

      LSAs originated by this router
      Router: 4
      Network: 0
      Sum-Net: 0
      Sum-Asbr: 0
      External: 0
```

NSSA: 0  
 Opq-Link: 0  
 Opq-Area: 0  
 Opq-As: 0

LSAs Originated: 4 LSAs Received: 7

Routing Table:

Intra Area: 2 Inter Area: 3 ASE/NSSA: 0

**Table 1-4 display ospf cumulative** command output description

Field	Description
IO statistics	Statistics about input/output packets and LSAs
Type	OSPF packet type
Input	Packets received
Output	Packets sent
Hello	Hell packet
DB Description	Database Description packet
Link-State Req	Link-State Request packet
Link-State Update	Link-State Update packet
Link-State Ack	Link-State Acknowledge packet
LSAs originated by this router	LSAs originated by this router
Router	Number of Type-1 LSAs originated
Network	Number of Type-2 LSAs originated
Sum-Net	Number of Type-3 LSAs originated
Sum-Asbr	Number of Type-4 LSAs originated
External	Number of Type-5 LSAs originated
NSSA	Number of Type-7 LSAs originated
Opq-Link	Number of Type-9 LSAs originated
Opq-Area	Number of Type-10 LSAs originated
Opq-As	Number of Type-11 LSAs originated
LSA originated	Number of LSAs originated
LSA Received	Number of LSAs received
Routing Table	Routing table information
Intra Area	Intra-area route number
Inter Area	Inter-area route number
ASE	ASE route number

## display ospf error

### Syntax

```
display ospf [ process-id ] error
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*process-id*: OSPF process ID, in the range 1 to 65535.

### Description

Use the **display ospf error** command to display OSPF error information.

If no process is specified, the OSPF error information of all OSPF processes is displayed.

### Examples

```
# Display OSPF error information.
```

```
<Sysname> display ospf error
```

```
OSPF Process 1 with Router ID 192.168.80.100
OSPF Packet Error Statistics

0   : OSPF Router ID confusion      0   : OSPF bad packet
0   : OSPF bad version              0   : OSPF bad checksum
0   : OSPF bad area ID              0   : OSPF drop on unnumber interface
0   : OSPF bad virtual link         0   : OSPF bad authentication type
0   : OSPF bad authentication key   0   : OSPF packet too small
0   : OSPF Neighbor state low       0   : OSPF transmit error
0   : OSPF interface down           0   : OSPF unknown neighbor
0   : HELLO: Netmask mismatch       0   : HELLO: Hello timer mismatch
0   : HELLO: Dead timer mismatch    0   : HELLO: Extern option mismatch
0   : HELLO: NBMA neighbor unknown 0   : DD: MTU option mismatch
0   : DD: Unknown LSA type          0   : DD: Extern option mismatch
0   : LS ACK: Bad ack               0   : LS ACK: Unknown LSA type
0   : LS REQ: Empty request         0   : LS REQ: Bad request
0   : LS UPD: LSA checksum bad      0   : LS UPD: Received less recent LSA
0   : LS UPD: Unknown LSA type
```

**Table 1-5 display ospf error** command output description

Field	Description
OSPF Router ID confusion	Packets with duplicate route ID
OSPF bad packet	Packets illegal
OSPF bad version	Packets with wrong version

Field	Description
OSPF bad checksum	Packets with wrong checksum
OSPF bad area ID	Packets with invalid area ID
OSPF drop on unnumber interface	Packets dropped on the unnumbered interface
OSPF bad virtual link	Packets on wrong virtual links
OSPF bad authentication type	Packets with invalid authentication type
OSPF bad authentication key	Packets with invalid authentication key
OSPF packet too small	Packets too small in length
OSPF Neighbor state low	Packets received in low neighbor state
OSPF transmit error	Packets with error when being transmitted
OSPF interface down	Shutdown times of the interface
OSPF unknown neighbor	Packets received from unknown neighbors
HELLO: Netmask mismatch	Hello packets with mismatched mask
HELLO: Hello timer mismatch	Hello packets with mismatched hello timer
HELLO: Dead timer mismatch	Hello packets with mismatched dead timer
HELLO: Extern option mismatch	Hello packets with mismatched option field
HELLO: NBMA neighbor unknown	Hello packets received from unknown NBMA neighbors
DD: MTU option mismatch	DD packets with mismatched MTU
DD: Unknown LSA type	DD packets with unknown LSA type
DD: Extern option mismatch	DD packets with mismatched option field
LS ACK: Bad ack	Bad LSAck packets for LSU packets
LS ACK: Unknown LSA type	LSAck packets with unknown LSA type
LS REQ: Empty request	LSR packets with no request information
LS REQ: Bad request	Bad LSR packets
LS UPD: LSA checksum bad	LSU packets with wrong LSA checksum
LS UPD: Received less recent LSA	LSU packets without latest LSA
LS UPD: Unknown LSA type	LSU packets with unknown LSA type

## display ospf interface

### Syntax

```
display ospf [ process-id ] interface [ interface-type interface-number | all ]
```

### View

Any view

### Default Level

1: Monitor level

## Parameters

*process-id*: OSPF process ID, in the range 1 to 65535.

*interface-type interface-number*: Interface type and interface number.

**all**: Displays the OSPF information of all interfaces.

## Description

Use the **display ospf interface** command to display OSPF interface information.

If no OSPF process is specified, the OSPF interface information of all OSPF processes is displayed.

## Examples

# Display OSPF interface information.

```
<Sysname> display ospf interface
```

```
OSPF Process 1 with Router ID 192.168.1.1
      Interfaces

Area: 0.0.0.0
IP Address      Type          State      Cost  Pri  DR           BDR
192.168.1.1    PTP           P-2-P     1562  1   0.0.0.0     0.0.0.0

Area: 0.0.0.1
IP Address      Type          State      Cost  Pri  DR           BDR
172.16.0.1     Broadcast    DR         1     1   172.16.0.1  0.0.0.0
```

**Table 1-6** display ospf interface command output description

Field	Description
Area	Area ID of the interface
IP address	Interface IP address (regardless of whether TE is enabled or not)
Type	Interface network type: PTP, PTMP, Broadcast, or NBMA
State	Interface state defined by interface state machine: <ul style="list-style-type: none"><li>• DOWN: In this state, no protocol traffic will be sent or received on the interface.</li><li>• Waiting: Means the interface starts sending and receiving Hello packets and the router is trying to determine the identity of the (Backup) designated router for the network.</li><li>• p-2-p: Means the interface will send Hello packets at the interval of HelloInterval, and try to establish an adjacency with the neighbor.</li><li>• DR: Means the router itself is the designated router on the attached network.</li><li>• BDR: Means the router itself is the backup designated router on the attached network.</li><li>• DROther: Means the interface is on a network on which another router has been selected as the designated router.</li></ul>
Cost	Interface cost
Pri	Router priority

Field	Description
DR	The DR on the interface's network segment
BDR	The BDR on the interface's network segment

## display ospf lsdb

### Syntax

```
display ospf [ process-id ] lsdb [ brief | [ { asbr | ase | network | nssa | opaque-area | opaque-as | opaque-link | router | summary } [ link-state-id ] ] [ originate-router advertising-router-id | self-originate ] ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*process-id*: OSPF process ID, in the range 1 to 65535.

**brief**: Displays brief LSDB information.

**asbr**: Displays Type-4 LSA (ASBR Summary LSA) information in the LSDB.

**ase**: Displays Type-5 LSA (AS External LSA) information in the LSDB.

**network**: Displays Type-2 LSA (Network LSA) information in the LSDB.

**nssa**: Displays Type-7 LSA (NSSA External LSA) information in the LSDB.

**opaque-area**: Displays Type-10 LSA (Opaque-area LSA) information in the LSDB.

**opaque-as**: Displays Type-11 LSA (Opaque-AS LSA) information in the LSDB.

**opaque-link**: Displays Type-9 LSA (Opaque-link LSA) information in the LSDB.

**router**: Displays Type-1 LSA (Router LSA) information in the LSDB.

**summary**: Displays Type-3 LSA (Network Summary LSA) information in the LSDB.

*link-state-id*: Link state ID, in the IP address format.

**originate-router** *advertising-router-id*: Displays information about LSAs originated by the specified router.

**self-originate**: Displays information about self-originated LSAs.

### Description

Use the **display ospf lsdb** command to display LSDB information.

If no OSPF process is specified, LSDB information of all OSPF processes is displayed.

### Examples

# Display OSPF LSDB information.

```
<Sysname> display ospf lsdb
```

```
OSPF Process 1 with Router ID 192.168.0.1
```

Link State Database

```

Area: 0.0.0.0
Type      LinkState ID   AdvRouter      Age  Len  Sequence  Metric
Router    192.168.0.2     192.168.0.2   474  36   80000004   0
Router    192.168.0.1     192.168.0.1   21   36   80000009   0
Network   192.168.0.1     192.168.0.1   321  32   80000003   0
Sum-Net   192.168.1.0     192.168.0.1   321  28   80000002   1
Sum-Net   192.168.2.0     192.168.0.2   474  28   80000002   1

Area: 0.0.0.1
Type      LinkState ID   AdvRouter      Age  Len  Sequence  Metric
Router    192.168.0.1     192.168.0.1   21   36   80000005   0
Sum-Net   192.168.2.0     192.168.0.1   321  28   80000002   2
Sum-Net   192.168.0.0     192.168.0.1   321  28   80000002   1

```

**Table 1-7 display ospf lsdb command output description**

Field	Description
Area	LSDB information of the area
Type	LSA type
LinkState ID	Linkstate ID
AdvRouter	The router that advertised the LSA
Age	Age of the LSA
Len	Length of the LSA
Sequence	Sequence number of the LSA
Metric	Cost of the LSA

# Display Type2 LSA (Network LSA) information in the LSDB.

```
<Sysname> display ospf 1 lsdb network
```

```

OSPF Process 1 with Router ID 192.168.1.1
Area: 0.0.0.0
Link State Database

Type      : Network
LS ID     : 192.168.0.2
Adv Rtr   : 192.168.2.1
LS Age    : 922
Len       : 32
Options   : E
Seq#      : 80000003
Chksum    : 0x8d1b
Net Mask  : 255.255.255.0
Attached Router 192.168.1.1
Attached Router 192.168.2.1
Area: 0.0.0.1

```

```

Link State Database
Type      : Network
LS ID     : 192.168.1.2
Adv Rtr   : 192.168.1.2
LS Age    : 782
Len       : 32
Options   : NP
Seq#      : 80000003
Chksum    : 0x2a77
Net Mask  : 255.255.255.0
  Attached Router 192.168.1.1
  Attached Router 192.168.1.2

```

**Table 1-8 display ospf 1 lsdb network** command output description

Field	Description
Type	LSA type
LS ID	DR IP address
Adv Rtr	Router that advertised the LSA
LS Age	LSA age time
Len	LSA length
Options	LSA options: O: Opaque LSA advertisement capability E: AS External LSA reception capability EA: External extended LSA reception capability DC: On-demand link support N: NSSA external LSA support P: Capability of an NSSA ABR to translate Type-7 LSAs into Type-5 LSAs.
Seq#	LSA sequence number
Chksum	LSA checksum
Net Mask	Network mask
Attached Router	ID of the router that established adjacency with the DR, and ID of the DR itself

## display ospf nexthop

### Syntax

```
display ospf [ process-id ] nexthop
```

### View

Any view

### Default Level

1: Monitor level

## Parameters

*process-id*: OSPF process ID, in the range 1 to 65535.

## Description

Use the **display ospf nexthop** command to display OSPF next hop information.

If no OSPF process is specified, the next hop information of all OSPF processes is displayed.

## Examples

# Display OSPF next hop information.

```
<Sysname> display ospf nexthop
      OSPF Process 1 with Router ID 192.168.0.1
      Routing Nexthop Information

Next Hops:
Address          Refcount  IntfAddr      Intf Name
-----
192.168.0.1     1         192.168.0.1  Vlan-interface1
192.168.0.2     1         192.168.0.1  Vlan-interface1
192.168.1.1     1         192.168.1.1  Vlan-interface10
```

**Table 1-9 display ospf nexthop** command output description

Field	Description
Next hops	Information about Next hops
Address	Next hop address
Refcount	Reference count, namely, routes that reference the next hop
IntfAddr	Outbound interface address
Intf Name	Outbound interface name

## display ospf peer

### Syntax

```
display ospf [ process-id ] peer [ verbose | [ interface-type interface-number ] [ neighbor-id ] ]
```

### View

Any view

### Default Level

1: Monitor level

## Parameters

*process-id*: OSPF process ID, in the range 1 to 65535.

**verbose**: Displays detailed neighbor information.

*interface-type interface-number*: Interface type and interface number.

*neighbor-id*: Neighbor router ID.

## Description

Use the **display ospf peer** command to display information about OSPF neighbors.

Note that:

If no OSPF process is specified, OSPF neighbor information of all OSPF processes is displayed.

If an interface is specified, the neighbor on the interface is displayed.

If a neighbor ID is specified, detailed information about the neighbor is displayed,

If neither interface nor neighbor ID is specified, brief information about neighbors of the specified OSPF process or all OSPF processes is displayed.

## Examples

# Display detailed OSPF neighbor information.

```
<Sysname> display ospf peer verbose
```

```
OSPF Process 1 with Router ID 1.1.1.1
Neighbors
```

```
Area 0.0.0.0 interface 1.1.1.1(Vlan-interfaces)'s neighbors
```

```
Router ID: 1.1.1.2          Address: 1.1.1.2          GR State: Normal
```

```
State: Full  Mode: Nbr is Master  Priority: 1
```

```
DR: 1.1.1.2  BDR: 1.1.1.1  MTU: 0
```

```
Dead timer due in 33 sec
```

```
Neighbor is up for 02:03:35
```

```
Authentication Sequence: [ 0 ]
```

```
Neighbor state change count: 6
```

**Table 1-10 display ospf peer verbose** command output description

Field	Description
Area <i>areaID</i> interface <i>IPAddress(InterfaceName)</i> 's neighbors	Neighbor information of the interface in the specified area: <ul style="list-style-type: none"><li>• <i>areaID</i>: Area to which the neighbor belongs.</li><li>• <i>IPAddress</i>: Interface IP address</li><li>• <i>InterfaceName</i>: Interface name</li></ul>
interface	Interface attached with the neighbor
Router ID	Neighbor router ID
Address	Neighbor router address
GR State	GR state

Field	Description
State	<p>Neighbor state:</p> <ul style="list-style-type: none"> <li>• Down: This is the initial state of a neighbor conversation.</li> <li>• Init: In this state, the router has seen a Hello packet from the neighbor. However, the router has not established bidirectional communication with the neighbor (the router itself did not appear in the neighbor's hello packet).</li> <li>• Attempt: Available only in an NBMA network, Under this state, the OSPF router has not received any information from a neighbor for a period but can send Hello packets at a longer interval to keep neighbor relationship.</li> <li>• 2-Way: In this state, communication between the two routers is bidirectional. The router itself appears in the neighbor's Hello packet.</li> <li>• Exstart: The goal of this state is to decide which router is the master, and to decide upon the initial Database Description (DD) sequence number.</li> <li>• Exchange: In this state, the router is sending DD packets to the neighbor, describing its entire link-state database.</li> <li>• Loading: In this state, the router sends Link State Request packets to the neighbor, requesting more recent LSAs.</li> <li>• Full: In this state, the neighboring routers are fully adjacent.</li> </ul>
Mode	<p>Neighbor mode for LSDB synchronization:</p> <ul style="list-style-type: none"> <li>• Nbr is Master: Means the neighboring router is the master.</li> <li>• Nbr is Slave: Means the neighboring router is the slave.</li> </ul>
Priority	Neighboring router priority
DR	The DR on the interface's network segment
BDR	The BDR on the interface's network segment
MTU	Interface MTU
Dead timer due in 33 sec	Dead timer times out in 33 seconds
Neighbor is up for 02:03:35	The neighbor has been up for 02:03:35.
Authentication Sequence	Authentication sequence number
Neighbor state change count	Count of neighbor state changes

# Display brief OSPF neighbor information.

```
<Sysname> display ospf peer
```

```

OSPF Process 1 with Router ID 1.1.1.1
Neighbor Brief Information

Area: 0.0.0.0
Router ID      Address      Pri Dead-Time Interface      State
1.1.1.2       1.1.1.2     1   40          Vlan1          Full/DR

```

**Table 1-11 display ospf peer command output description**

Field	Description
Area	Neighbor area
Router ID	Neighbor router ID
Address	Neighbor interface address
Pri	Neighboring router priority
Dead time(s)	Dead interval remained
Interface	Interface connected to the neighbor
State	Neighbor state: Down, Init, Attempt, 2-Way, Exstart, Exchange, Loading or Full

## display ospf peer statistics

### Syntax

**display ospf [ *process-id* ] peer statistics**

### View

Any view

### Default Level

1: Monitor level

### Parameters

*process-id*: OSPF process ID, in the range 1 to 65535.

### Description

Use the **display ospf peer statistics** command to display OSPF neighbor statistics.

If no OSPF process is specified, OSPF neighbor statistics of all OSPF processes is displayed.

### Examples

# Display OSPF neighbor statistics.

```
<Sysname> display ospf peer statistics
      OSPF Process 1 with Router ID 10.3.1.1
      Neighbor Statistics
Area ID      Down Attempt Init 2-Way ExStart Exchange Loading Full Total
0.0.0.0      0    0      0    0    0      0      0      1    1
0.0.0.2      0    0      0    0    0      0      0      1    1
Total        0    0      0    0    0      0      0      2    2
```

**Table 1-12** display ospf peer statistics command output description

Field	Description
Area ID	Area ID. The state statistics information of all the routers in the area to which the router belongs is displayed.
Down	Number of neighboring routers in the Down state in the same area
Attempt	Number of neighboring routers in the Attempt state in the same area
Init	Number of neighboring routers in the Init state in the same area
2-Way	Number of neighboring routers in the 2-Way state in the same area
ExStart	Number of neighboring routers in the ExStart state in the same area
Exchange	Number of neighboring routers in the Exchange state in the same area
Loading	Number of neighboring routers in the Loading state in the same area
Full	Number of neighboring routers in the Full state in the same area
Total	Total number of neighbors under the same state, namely, Down, Attempt, Init, 2-Way, ExStart, Loading, or Full.

## display ospf request-queue

### Syntax

```
display ospf [ process-id ] request-queue [ interface-type interface-number ] [ neighbor-id ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*process-id*: OSPF process ID, in the range 1 to 65535.

*interface-type interface-number*: Interface type and number.

*neighbor-id*: Neighbor's router ID.

### Description

Use the **display ospf request-queue** command to display OSPF request queue information.

If no OSPF process is specified, the OSPF request queue information of all OSPF processes is displayed.

### Examples

```
# Display OSPF request queue information.
```

```
<Sysname> display ospf request-queue
```

```
OSPF Process 1 with Router ID 1.1.1.1
OSPF Request List
```

```

The Router's Neighbor is Router ID 2.2.2.2          Address 10.1.1.2
Interface 10.1.1.1          Area 0.0.0.0
Request list:
  Type      LinkState ID      AdvRouter      Sequence      Age
  Router    2.2.2.2            1.1.1.1        80000004     1
  Network   192.168.0.1        1.1.1.1        80000003     1
  Sum-Net   192.168.1.0        1.1.1.1        80000002     2

```

**Table 1-13 display ospf request queue command output description**

Field	Description
The Router's Neighbor is Router ID	Neighbor router ID
Address	Neighbor interface IP address
Interface	Local interface IP address
Area	Area ID
Request list	Request list information
Type	LSA type
LinkState ID	Link state ID
AdvRouter	Advertising router
Sequence	LSA sequence number
Age	LSA age

## display ospf retrans-queue

### Syntax

```
display ospf [ process-id ] retrans-queue [ interface-type interface-number ] [ neighbor-id ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*process-id*: OSPF process ID, in the range 1 to 65535.

*interface-type interface-number*: Interface type and interface number.

*neighbor-id*: Neighbor's router ID.

### Description

Use the **display ospf retrans-queue** command to display retransmission queue information.

If no OSPF process is specified, the retransmission queue information of all OSPF processes is displayed.

## Examples

```
# Display OSPF retransmission queue information.
```

```
<Sysname> display ospf retrans-queue
```

```
OSPF Process 1 with Router ID 1.1.1.1
      OSPF Retransmit List

The Router's Neighbor is Router ID 2.2.2.2      Address 10.1.1.2
Interface 10.1.1.1          Area 0.0.0.0
Retransmit list:
  Type      LinkState ID      AdvRouter      Sequence      Age
  Router    2.2.2.2              2.2.2.2        80000004      1
  Network   12.18.0.1            2.2.2.2        80000003      1
  Sum-Net   12.18.1.0            2.2.2.2        80000002      2
```

**Table 1-14** display ospf retrans-queue command output description

Field	Description
The Router's Neighbor is Router ID	Neighbor router ID
Address	Neighbor interface IP address
Interface	Interface address of the router
Area	Area ID
Retrans List	Retransmission list
Type	LSA type
LinkState ID	Link state ID
AdvRouter	Advertising router
Sequence	LSA sequence number
Age	LSA age

## display ospf routing

### Syntax

```
display ospf [ process-id ] routing [ interface interface-type interface-number ] [ nexthop nexthop-address ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*process-id*: OSPF process ID, in the range 1 to 65535.

**interface** *interface-type interface-number*: Displays OSPF routing information advertised via the interface.

**nexthop** *nexthop-address*: Displays OSPF routing information with the specified next hop.

## Description

Use the **display ospf routing** command to display OSPF routing information.

If no OSPF process is specified, the routing information of all OSPF processes is displayed.

## Examples

# Display OSPF routing information.

```
<Sysname> display ospf routing
```

```
OSPF Process 1 with Router ID 192.168.1.2
Routing Tables

Routing for Network
Destination          Cost  Type          NextHop          AdvRouter          Area
192.168.1.0/24      1562  Stub          192.168.1.2     192.168.1.2       0.0.0.0
172.16.0.0/16       1563  Inter         192.168.1.1     192.168.1.1       0.0.0.0

Total Nets: 2
Intra Area: 1  Inter Area: 1  ASE: 0  NSSA: 0
```

**Table 1-15 display ospf routing** command output description

Field	Description
Destination	Destination network
Cost	Cost to destination
Type	Route type: intra-area, transit, stub, inter-area, type1 external, type2 external.
NextHop	Next hop address
AdvRouter	Advertising router
Area	Area ID
Total Nets	Total networks
Intra Area	Total intra-area routes
Inter Area	Total inter-area routes
ASE	Total ASE routes
NSSA	Total NSSA routes

## display ospf sham-link

### Syntax

```
display ospf [ process-id ] sham-link [ area area-id ]
```

## View

Any view

## Default Level

1: Monitor level

## Parameters

*process-id*: OSPF process ID, in the range 1 to 65535.

*area-id*: OSPF area ID. It can be an integer in the range 0 to 4294967295 or in the format of an IPv4 address.

## Description

Use the **display ospf sham-link** command to display information about sham links.

With neither process ID nor area ID specified, the command displays information about all configured sham links.

Related commands: **sham-link**.

## Examples

# Display information about all OSPF sham links.

```
<Sysname> display ospf sham-link
      OSPF Process 100 with Router ID 100.1.1.2
Sham Link:
Area      NeighborId      Source-IP      Destination-IP  State Cost
0.0.0.1   100.1.1.2      3.3.3.3       5.5.5.5        Down  1
```

**Table 1-16 display ospf sham-link** command output description

Field	Description
Area	OSPF area to which the sham link belongs
NeighborId	Neighbor ID of the sham link
Source-IP	Source IP address of the sham link
Destination-IP	Destination IP address of the sham link
State	Status of the sham link interface
Cost	Cost of the sham link

## display ospf vlink

### Syntax

```
display ospf [ process-id ] vlink
```

### View

Any view

## Default Level

1: Monitor level

## Parameters

*process-id*: OSPF process ID, in the range 1 to 65535.

## Description

Use the **display ospf vlink** command to display OSPF virtual link information.

If no OSPF process is specified, the OSPF virtual link information of all OSPF processes is displayed.

## Examples

# Display OSPF virtual link information.

```
<Sysname> display ospf vlink
      OSPF Process 1 with Router ID 3.3.3.3
          Virtual Links

Virtual-link Neighbor-ID -> 2.2.2.2, Neighbor-State: Full
Interface: 10.1.2.1 (Vlan-interface1)
Cost: 1562  State: P-2-P  Type: Virtual
Transit Area: 0.0.0.1
Timers: Hello 10 , Dead 40 , Retransmit 5 , Transmit Delay 1
```

**Table 1-17 display ospf vlink** command output description

Field	Description
Virtual-link Neighbor-id	ID of the neighbor connected to the router via the virtual link
Neighbor-State	Neighbor State: Down, Init, 2-Way, ExStart, Exchange, Loading, Full.
Interface	Local interface's IP address and name of the virtual link
Cost	Interface route cost
State	Interface state
Type	Type: virtual link
Transit Area	Transit area ID
Timers	Values of timers: hello, dead, poll (NBMA), retransmit, and interface transmission delay

## enable link-local-signaling

### Syntax

**enable link-local-signaling**

**undo enable link-local-signaling**

### View

OSPF view

## Default Level

2: System level

## Parameters

None

## Description

Use the **enable link-local-signaling** command to enable the OSPF link-local signaling (LLC) capability.

Use the **undo enable link-local-signaling** command to disable the OSPF link-local signaling capability.

By default, this capability is disabled.

## Examples

```
# Enable link-local signaling for OSPF process 1.  
<Sysname> system-view  
[Sysname] ospf 1  
[Sysname-ospf-1] enable link-local-signaling
```

## enable log

### Syntax

```
enable log [ config | error | state ]  
undo enable log [ config | error | state ]
```

### View

OSPF view

## Default Level

2: System level

## Parameters

**config**: Enables configuration logging.

**error**: Enables error logging.

**state**: Enables state logging.

## Description

Use the **enable** command to enable specified OSPF logging.

Use the **undo enable** command to disable specified OSPF logging.

OSPF logging is disabled by default.

If no keyword is specified, all logging is enabled.

## Examples

```
# Enable OSPF logging.  
<Sysname> system-view
```

```
[Sysname] ospf 100
[Sysname-ospf-100] enable log
```

## enable out-of-band-resynchronization

### Syntax

```
enable out-of-band-resynchronization
undo enable out-of-band-resynchronization
```

### View

OSPF view

### Default Level

2: System level

### Parameters

None

### Description

Use the **enable out-of-band-resynchronization** command to enable the OSPF out-of-band resynchronization (OOB-Resynch) capability.

Use the **undo enable out-of-band-resynchronization** command to disable the OSPF out-of-band resynchronization capability.

By default, the capability is disabled.

### Examples

```
# Enable the out-of-band resynchronization capability for OSPF process 1.
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] enable link-local-signaling
[Sysname-ospf-1] enable out-of-band-resynchronization
```

## filter

### Syntax

```
filter { acl-number | ip-prefix ip-prefix-name } { export | import }
undo filter { export | import }
```

### View

OSPF area view

### Default Level

2: System level

### Parameters

*acl-number*: ACL number, in the range 2000 to 3999.

*ip-prefix-name*: IP prefix list name, a string of up to 19 characters. For details about IP prefix lists, see *Route Policy Configuration* in the *IP Routing Volume*.

**export**: Filters Type-3 LSAs advertised to other areas.

**import**: Filters Type-3 LSAs advertised into the area.

## Description

Use the **filter** command to configure incoming/outgoing Type-3 LSAs filtering on an ABR.

Use the **undo filter** command to disable Type-3 LSA filtering.

By default, Type-3 LSAs filtering is disabled.



### Note

This command is only available on an ABR.

---

## Examples

# Apply IP prefix list **my-prefix-list** to filter inbound Type-3 LSAs, and apply ACL 2000 to filter outbound Type-3 LSAs in OSPF Area 1.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] filter ip-prefix my-prefix-list import
[Sysname-ospf-100-area-0.0.0.1] filter 2000 export
```

## filter-policy export (OSPF view)

### Syntax

```
filter-policy { acl-number | ip-prefix ip-prefix-name } export [ protocol [ process-id ] ]
undo filter-policy export [ protocol [ process-id ] ]
```

### View

OSPF view

### Default Level

2: System level

### Parameters

*acl-number*: Number of an ACL used to filter redistributed routes, in the range 2000 to 3999.

*ip-prefix-name*: Name of an IP prefix list used to filter redistributed routes, a string of up to 19 characters.

*protocol*: Specifies a protocol from which to filter redistributed routes. The protocol can be **direct**, **static**, **rip**, **ospf**, **isis** or **bgp**. If no protocol is specified, all redistributed routes are filtered.

*process-id*: Process ID, which is required when the *protocol* is **rip**, **ospf** or **isis**, in the range 1 to 65535.

## Description

Use the **filter-policy export** command to configure the filtering of redistributed routes.

Use the **undo filter-policy export** command to disable the filtering.

By default, the filtering of redistributed routes is not configured.

You can use this command to filter redistributed routes as needed.

Related commands: **import-route**.

## Examples

# Filter redistributed routes using ACL2000.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] filter-policy 2000 export
```

## filter-policy import (OSPF view)

### Syntax

```
filter-policy { acl-number [ gateway ip-prefix-name ] | gateway ip-prefix-name | ip-prefix ip-prefix-name [ gateway ip-prefix-name ] | route-policy route-policy-name } import
```

```
undo filter-policy import
```

### View

OSPF view

### Default Level

2: System level

### Parameters

*acl-number*: Number of an ACL used to filter incoming routes, in the range 2000 to 3999.

**gateway** *ip-prefix-name*: Name of an IP address prefix list used to filter routes based on the next hop of the routing information, a string of up to 19 characters.

**ip-prefix** *ip-prefix-name*: Name of an IP address prefix list used to filter incoming routes based on destination IP address, a string of up to 19 characters. For details about IP prefix lists, refer to *Route Policy Configuration* in the *IP Routing Volume*.

**route-policy** *route-policy-name*: Name of a route policy used to filter incoming routes based on route policy, a string of up to 19 characters. For details about route policy, refer to *Route Policy Configuration* in the *IP Routing Volume*.

## Description

Use the **filter-policy import** command to configure the filtering of routes calculated from received LSAs.

Use the **undo filter-policy import** command to disable the filtering.

By default, the filtering is not configured.

## Examples

```
# Filter incoming routes using ACL2000.
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 192.168.10.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] ospf 100
[Sysname-ospf-100] filter-policy 2000 import
```

## graceful-restart (OSPF view)

### Syntax

```
graceful-restart [ ietf | nonstandard ]
undo graceful-restart
```

### View

OSPF view

### Default Level

2: System level

### Parameters

**ietf**: Enables the IETF GR capability.

**nonstandard**: Enables the non-IETF GR capability.

### Description

Use the **graceful-restart** command to enable OSPF Graceful Restart capability.

Use the **undo graceful-restart** command to disable OSPF Graceful Restart capability.

By default, OSPF Graceful Restart capability is disabled.

Note the following:

- Enable Opaque LSA advertisement and reception with the **opaque-capability enable** command before enabling the IETF GR capability for OSPF.
- Before enabling non-IETF GR capability for OSPF, enable OSPF LLS (link local signaling) with the **enable link-local-signaling** command and OOB (out of band resynchronization) with the **enable out-of-band-resynchronization** command.
- If the keywords **nonstandard** and **ietf** are not specified when OSPF GR is enabled, **nonstandard** is the default.

Related commands: **enable link-local-signaling**, **enable out-of-band-resynchronization**, **opaque-capability enable**.

## Examples

```
# Enable IETF Graceful Restart for OSPF process 1.
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] opaque-capability enable
```

```
[Sysname-ospf-1] graceful-restart ietf
# Enable non-IETF Graceful Restart for OSPF process 1.
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] enable link-local-signaling
[Sysname-ospf-1] enable out-of-band-resynchronization
[Sysname-ospf-1] graceful-restart nonstandard
```

## graceful-restart help

### Syntax

```
graceful-restart help { acl-number | prefix prefix-list }
undo graceful-restart help
```

### View

OSPF view

### Default Level

2: System level

### Parameters

*acl-number*: Basic or advanced ACL number, in the range 2000 to 3999.

*prefix-list*: Name of the specified IP prefix list, a string of 1 to 19 characters.

### Description

Use the **graceful-restart help** command to configure for which OSPF neighbors the current router can serve as a GR Helper. (The neighbors are specified by the ACL or the IP prefix list.)

Use the **undo graceful-restart help** command to restore the default.

By default, the router can serve as a GR Helper for any OSPF neighbor.

### Examples

# Enable IETF standard GR for OSPF process 1 and configure the router as a GR Helper for OSPF neighbors defined in the ACL 2001.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] opaque-capability enable
[Sysname-ospf-1] graceful-restart help 2001
```

# Enable non IETF standard GR for OSPF process 1 and configure the router as a GR Helper for OSPF neighbors defined in the ACL 2001.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] enable link-local-signaling
[Sysname-ospf-1] enable out-of-band-resynchronization
[Sysname-ospf-1] graceful-restart help 2001
```

## graceful-restart interval (OSPF view)

### Syntax

**graceful-restart interval** *interval-value*

**undo graceful-restart interval**

### View

OSPF view

### Default Level

2: System level

### Parameters

*interval-value*: Specifies the Graceful Restart interval, in the range 40 to 1,800 seconds.

### Description

Use the **graceful-restart interval** command to configure the Graceful Restart interval.

Use the **undo graceful-restart interval** command to restore the default Graceful Restart interval.

By default, the Graceful Restart interval is 120 seconds.

Note that the Graceful Restart interval of OSPF cannot be less than the maximum value of dead intervals on all OSPF interfaces; otherwise, the Graceful Restart of OSPF may fail.

Related commands: **ospf timer dead**.

### Examples

# Configure the Graceful Restart interval for OSPF process 1 as 100 seconds.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] graceful-restart interval 100
```

## host-advertise

### Syntax

**host-advertise** *ip-address cost*

**undo host-advertise** *ip-address*

### View

OSPF area view

### Default Level

2: System level

### Parameters

*ip-address*: IP address of a host

*cost*: Cost of the route, in the range 1 to 65535.

## Description

Use the **host-advertise** command to advertise a host route.

Use the **undo host-advertise** command to remove a host route.

No host route is advertised by default.

## Examples

# Advertise route 1.1.1.1 with a cost of 100.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0]host-advertise 1.1.1.1 100
```

## import-route (OSPF view)

### Syntax

**import-route** *protocol* [ *process-id* | **all-processes** | **allow-ibgp** ] [ **cost** *cost* | **type** *type* | **tag** *tag* | **route-policy** *route-policy-name* ] \*

**undo import-route** *protocol* [ *process-id* | **all-processes** ]

### View

OSPF view

### Default Level

2: System level

### Parameters

*protocol*: Redistributes routes from the specified protocol, which can be **bgp**, **direct**, **isis**, **ospf**, **rip**, or **static**.

*process-id*: Process ID, in the range 1 to 65535. The default is 1. It is available only when the *protocol* is **rip**, **ospf**, or **isis**.

**all-processes**: Redistributes routes from all the processes of the specified routing protocol. This keyword takes effect only when the protocol is **rip**, **ospf**, or **isis**.

**allow-ibgp**: Allows IBGP routes redistribution. It is optional only when the *protocol* is **bgp**.

**cost** *cost*: Specifies a route cost, in the range 0 to 16777214. The default is 1.

**type** *type*: Specifies a cost type, 1 or 2. The default is 2.

**tag** *tag*: Specifies a tag for external LSAs. The default is 1.

**route-policy** *route-policy-name*: Specifies a route policy to redistribute qualified routes only. A Route policy name is a string of up to 19 characters.

## Description

Use the **import-route** command to redistribute routes from another protocol.

Use the **undo import-route** command to disable route redistribution from a protocol.

Route redistribution from another protocol is not configured by default.

OSPF prioritize routes as follows:

- Intra-area route
- Inter-area route
- Type1 External route
- Type2 External route

An intra-area route is a route in an OSPF area. An inter-area route is between any two OSPF areas. Both of them are internal routes.

An external route is a route to a destination outside the OSPF AS.

A Type-1 external route is an IGP route, such as RIP or STATIC, which has high reliability and whose cost is comparable with the cost of OSPF internal routes. Therefore, the cost from an OSPF router to a Type-1 external route's destination equals the cost from the router to the corresponding ASBR plus the cost from the ASBR to the external route's destination.

A Type-2 external route is an EGP route, which has low credibility, so OSPF considers the cost from the ASBR to a Type-2 external route is much bigger than the cost from the ASBR to an OSPF internal router. Therefore, the cost from an internal router to a Type-2 external route's destination equals the cost from the ASBR to the Type-2 external route's destination.

Related commands: **default-route-advertise**.



#### Note

- The **import-route** command cannot redistribute default routes.
- Use the **import-route bgp allow-ibgp** command with care, because it redistributes both EBGP and IBGP routes that may cause routing loops.
- Only active routes can be redistributed. You can use the **display ip routing-table protocol** command to display route state information.

## Examples

# Redistribute routes from RIP process 40 and specify the type, tag, and cost as 2, 33 and 50 for redistributed routes.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] import-route rip 40 type 2 tag 33 cost 50
```

## ip binding vpn-instance

### Syntax

```
ip binding vpn-instance vpn-instance-name
undo ip binding vpn-instance vpn-instance-name
```

### View

Interface view

### Default Level

2: System level

## Parameters

*vpn-instance-name*: Name of the VPN instance to be associated, a case-insensitive string of 1 to 31 characters.

## Description

Use the **ip binding vpn-instance** command to associate an interface with a VPN instance.

Use the **undo ip binding vpn-instance** command to remove the association.

By default, an interface is associated with no VPN instance; it belongs to the public network.

When configured on an interface, the **ip binding vpn-instance** command clears the IP address of the interface. Therefore, you must re-configure the IP address of the interface after configuring the command.

## Examples

```
# Associate interface VLAN-interface 1 with VPN instance vpn1.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip binding vpn-instance vpn1
```

## log-peer-change

### Syntax

**log-peer-change**

**undo log-peer-change**

### View

OSPF view

### Default Level

2: System level

### Parameters

None

### Description

Use the **log-peer-change** command to enable the logging of OSPF neighbor state changes.

Use the **undo log-peer-change** command to disable the logging.

The logging is enabled by default.

With this feature enabled, information about neighbor state changes is displayed on the terminal until the feature is disabled.

### Examples

```
# Disable the logging of neighbor state changes for OSPF process 100.
```

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] undo log-peer-change
```

## Isa-arrival-interval

### Syntax

```
Isa-arrival-interval interval  
undo Isa-arrival-interval
```

### View

OSPF view

### Default Level

2: System level

### Parameters

*interval*: Specifies the minimum LSA repeat arrival interval in milliseconds, in the range 0 to 60000.

### Description

Use the **Isa-arrival-interval** command to specify the minimum LSA repeat arrival interval.

Use the **undo Isa-arrival-interval** command to restore the default.

The interval defaults to 1000 milliseconds.

If an LSA that has the same LSA type, LS ID, originating router ID with the previous LSA is received within the interval, the LSA will be discarded. This feature helps protect routers and bandwidth from being over-consumed due to frequent network changes.

It is recommended the interval set with the **Isa-arrival-interval** command is smaller or equal to the initial interval set with the **Isa-generation-interval** command.

Related commands: **Isa-generation-interval**.

### Examples

```
# Set the LSA minimum repeat arrival interval to 200 milliseconds.
```

```
<Sysname> system-view  
[Sysname] ospf 100  
[Sysname-ospf-100] lsa-arrival-interval 200
```

## Isa-generation-interval

### Syntax

```
Isa-generation-interval maximum-interval [ initial-interval [ incremental-interval ] ]  
undo Isa-generation-interval
```

### View

OSPF view

### Default Level

2: System level

## Parameters

*maximum-interval*: Maximum LSA generation interval in seconds, in the range 1 to 60.

*initial-interval*: Minimum LSA generation interval in milliseconds, in the range 10 to 60000. The default is 0, that is, the LSA generation interval is not limited.

*incremental-interval*: LSA generation incremental interval in milliseconds, in the range 10 to 60000. The default is 5000 milliseconds.

## Description

Use the **lsa-generation-interval** command to configure the OSPF LSA generation interval.

Use the **undo lsa-generation-interval** command to restore the default.

The LSA generation interval defaults to 5 seconds.

With this command configured, when network changes are not frequent, LSAs are generated at the *initial-interval*. If network changes become frequent, LSA generation interval is incremented by a specified value each time a generation happens, up to the *maximum-interval*.

Related commands: **lsa-arrival-interval**.

## Examples

# Configure the maximum LSA generation interval as 2 seconds, minimum interval as 100 milliseconds and incremental interval as 100 milliseconds.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsa-generation-interval 2 100 100
```

## lsdb-overflow-limit

### Syntax

**lsdb-overflow-limit** *number*

**undo lsdb-overflow-limit**

### View

OSPF view

### Default Level

2: System level

## Parameters

*number*: Specifies the upper limit of external LSAs in the LSDB, in the range 1 to 1000000.

## Description

Use the **lsdb-overflow-limit** command to specify the upper limit of external LSAs in the LSDB.

Use the **undo lsdb-overflow-limit** command to restore the default.

External LSAs in the LSDB are not limited by default.

## Examples

# Specify the upper limit of external LSAs as 400000.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsdbs-overflow-limit 400000
```

## maximum load-balancing (OSPF view)

### Syntax

```
maximum load-balancing maximum
undo maximum load-balancing
```

### View

OSPF view

### Default Level

2: System level

### Parameters

*maximum*: Maximum number of equal cost routes for load balancing., in the range 1 to 4.No load balancing is available when the number is set to 1.

### Description

Use the **maximum load-balancing** command to specify the maximum number of equal cost routes for load balancing.

Use the **undo maximum load-balancing** command to restore the default.

By default, the maximum number of equal cost routes is 4.

### Examples

# Specify the maximum number of equal cost routes for load balancing as 2.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] maximum load-balancing 2
```

## maximum-routes

### Syntax

```
maximum-routes { external | inter | intra } number
undo maximum-routes { external | inter | intra }
```

### View

OSPF view

### Default Level

2: System level

### Parameters

**external**: Specifies the maximum number of external routes.

**inter:** Specifies the maximum number of inter-area routes.

**intra:** Specifies the maximum number of intra-area routes.

*number:* Maximum route number.

- **external:** Ranges from 0 to 12288.
- **inter:** Ranges from 0 to 10240.
- **Intra:** Ranges from 0 to 1024.

## Description

Use the **maximum-routes** command to specify the maximum route number of a specified type, inter-area, intra-area or external.

Use the **undo maximum-routes** command to restore the default route maximum value of a specified type.

By default, the maximum number of AS external routes, inter-area routes and intra-area routes is 12288, 10240 and 1024, respectively.

## Examples

```
# Specify the maximum number of intra-area routes as 500.
```

```
<Sysname> system-view  
[Sysname] ospf 100  
[Sysname-ospf-100] maximum-routes intra 500
```

## network (OSPF area view)

### Syntax

```
network ip-address wildcard-mask
```

```
undo network ip-address wildcard-mask
```

### View

OSPF area view

### Default Level

2: System level

### Parameters

*ip-address:* IP address of a network.

*wildcard-mask:* Wildcard mask of the IP address. For example, the wildcard mask of mask 255.0.0.0 is 0.255.255.255.

## Description

Use the **network** command to enable OSPF on the interface attached to the specified network in the area.

Use the **undo network** command to disable OSPF for the interface attached to the specified network in the area.

By default, an interface neither belongs to any area nor runs OSPF.

You can configure one or multiple interfaces in an area to run OSPF. Note that the interface's primary IP address must fall into the specified network segment to make the interface run OSPF. If only the interface's secondary IP address falls into the network segment, the interface cannot run OSPF.

Related commands: **ospf**.

## Examples

# Specify the interface whose primary IP address falls into 131.108.20.0/24 to run OSPF in Area 2.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 2
[Sysname-ospf-100-area-0.0.0.2] network 131.108.20.0 0.0.0.255
```

## nssa

### Syntax

**nssa [ default-route-advertise | no-import-route | no-summary ] \***

**undo nssa**

### View

OSPF area view

### Default Level

2: System level

### Parameters

**default-route-advertise:** Usable on an NSSA ABR or an ASBR only. If it is configured on an NSSA ABR, the ABR generates a default route in a Type-7 LSA into the NSSA regardless of whether the default route is available. If it is configured on an ASBR, only a default route is available on the ASBR can it generates the default route in a Type-7 LSA into the attached area.

**no-import-route:** Usable only on an NSSA ABR that is also the ASBR of the OSPF routing domain to disable redistributing routes in Type7 LSAs into the NSSA area, making sure that routes can be redistributed correctly.

**no-summary:** Usable only on an NSSA ABR to advertise only a default route in a Type-3 summary LSA into the NSSA area. In this way, all the other summary LSAs are not advertised into the area. Such an area is known as an NSSA totally stub area.

### Description

Use the **nssa** command to configure the current area as an NSSA area.

Use the **undo nssa** command to restore the default.

By default, no NSSA area is configured.

All routers attached to an NSSA area must be configured with the **nssa** command in area view.

Related commands: **default-cost**.

## Examples

# Configure Area 1 as an NSSA area.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] nssa
```

## opaque-capability enable

### Syntax

```
opaque-capability enable
undo opaque-capability
```

### View

OSPF view

### Default Level

2: System level

### Parameters

None

### Description

Use the **opaque-capability enable** command to enable opaque LSA advertisement and reception. With the command configured, the OSPF device can receive and advertise the Type-9, Type-10 and Type-11 opaque LSAs.

Use the **undo opaque-capability** command to restore the default.

The feature is disabled by default.

### Examples

```
# Enable advertising and receiving opaque LSAs.
```

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100]opaque-capability enable
```

## ospf

### Syntax

```
ospf [ process-id | router-id router-id | vpn-instance instance-name ] *
undo ospf [ process-id ]
```

### View

System view

### Default Level

2: System level

## Parameters

*process-id*: OSPF process ID, in the range 1 to 65535.

*router-id*: OSPF Router ID, in dotted decimal format.

*instance-name*: VPN instance name, a string of 1 to 31 characters.

## Description

Use the **ospf** command to enable an OSPF process.

Use the **undo ospf** command to disable an OSPF process.

No OSPF process is enabled by default.

You can enable multiple OSPF processes on a router and specify different Router IDs for these processes.

Enabling OSPF first is required before performing other tasks.

## Examples

```
# Enable OSPF process 100 and specify Router ID 10.10.10.1.
```

```
<Sysname> system-view  
[Sysname] ospf 100 router-id 10.10.10.1  
[Sysname-ospf-100]
```

## ospf authentication-mode

### Syntax

For MD5/HMAC-MD5 authentication:

```
ospf authentication-mode { hmac-md5 | md5 } key-id [ cipher | plain ] password
```

```
undo ospf authentication-mode { hmac-md5 | md5 } key-id
```

For simple authentication:

```
ospf authentication-mode simple [ cipher | plain ] password
```

```
undo ospf authentication-mode simple
```

### View

Interface view

### Default Level

2: System level

## Parameters

**hmac-md5**: HMAC-MD5 authentication.

**md5**: MD5 authentication.

**simple**: Simple authentication.

*key-id*: Authentication key ID, in the range 1 to 255.

**cipher** | **plain**: Plain or cipher password. If **plain** is specified, only plain password is supported and displayed upon displaying the configuration file. If **cipher** is specified, both plain and cipher are supported, but only cipher password is displayed when displaying the configuration file. If no keyword is

specified, the cipher type is the default for the MD5/HMAC-MD5 authentication mode, and the plain type is the default for the simple authentication mode.

*password*: Password. Simple authentication: For plain type password, a plain password is a string of up to 8 characters; for cipher type password, a plain password is a string of up to 8 characters, and a cipher password is a string of up to 24 characters. MD5/HMAC-MD5 authentication: For plain type password, a plain password is a string of up to 16 characters; for cipher type password, a plain password is a string of up to 16 characters, and a cipher password is a string of up to 24 characters.

## Description

Use the **ospf authentication-mode** command to set the authentication mode and key ID on an interface.

Use the **undo ospf authentication-mode** command to remove specified configuration.

By default, no authentication is available on an interface.

Interfaces attached to the same network segment must have the same authentication password and mode.

This configuration is not supported on the null interface.

Related commands: **authentication-mode**.

## Examples

# Configure the network 131.119.0.0/16 in Area 1 to support MD5 cipher authentication, and set the interface key ID to 15, authentication password to **abc**, and password type to cipher.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] network 131.119.0.0 0.0.255.255
[Sysname-ospf-100-area-0.0.0.1] authentication-mode md5
[Sysname-ospf-100-area-0.0.0.1] quit
[Sysname-ospf-100] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf authentication-mode md5 15 cipher abc
```

# Configure the network 131.119.0.0/16 in Area 1 to support simple authentication, and set for the interface the authentication password to **abc**, and password type to cipher.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] network 131.119.0.0 0.0.255.255
[Sysname-ospf-100-area-0.0.0.1] authentication-mode simple
[Sysname-ospf-100-area-0.0.0.1] quit
[Sysname-ospf-100] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf authentication-mode simple cipher abc
```

## ospf cost

### Syntax

```
ospf cost value  
undo ospf cost
```

### View

Interface view

### Default Level

2: System level

### Parameters

*value*: OSPF cost, in the range 0 to 65535 for a loopback interface and 1 to 65535 for other interfaces.

### Description

Use the **ospf cost** command to set an OSPF cost for the interface.

Use the **undo ospf cost** command to restore the default.

By default, the OSPF cost for a loopback interface is 0, and an OSPF interface calculates its cost with the formula: interface default OSPF cost=100 Mbps/interface bandwidth(Mbps). Default OSPF costs of some interfaces are:

- 1785 for the 56 kbps serial interface
- 1562 for the 64 kbps serial interface
- 48 for the E1 (2.048 Mbps) interface
- 1 for the Ethernet (100 Mbps) interface

You can use the **ospf cost** command to set an OSPF cost for an interface manually.



#### Note

This configuration is not supported on null interfaces.

---

### Examples

```
# Set the OSPF cost for the interface to 65.  
<Sysname> system-view  
[Sysname] interface vlan-interface 10  
[Sysname-Vlan-interface10] ospf cost 65
```

## ospf dr-priority

### Syntax

```
ospf dr-priority priority  
undo ospf dr-priority
```

## View

Interface view

## Default Level

2: System level

## Parameters

*priority*: DR Priority of the interface, in the range 0 to 255.

## Description

Use the **ospf dr-priority** command to set the priority for DR/BDR election on an interface.

Use the **undo ospf dr-priority** command to restore the default value.

By default, the priority is 1.

The bigger the value, the higher the priority. If a device has a priority of 0, it will not be elected as a DR or BDR.

The DR priority configuration is not supported on the null and loopback interfaces.

## Examples

# Set the DR priority on the current interface to 8.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf dr-priority 8
```

## ospf mib-binding

### Syntax

**ospf mib-binding** *process-id*

**undo ospf mib-binding**

### View

System view

### Default Level

2: System level

### Parameters

*process-id*: OSPF process ID, in the range 1 to 65535.

### Description

Use the **ospf mib-binding** command to bind an OSPF process to MIB operation for responding SNMP requests.

Use the **undo ospf mib-binding** command to restore the default.

By default, MIB operation is bound to the first enabled OSPF process.

## Examples

```
# Bind OSPF process 100 to MIB operation.
```

```
<Sysname> system-view  
[Sysname] ospf mib-binding 100
```

```
# Restore the default, that is, bind the first enabled OSPF process to MIB operation.
```

```
<Sysname> system-view  
[Sysname] undo ospf mib-binding
```

## ospf mtu-enable

### Syntax

```
ospf mtu-enable
```

```
undo ospf mtu-enable
```

### View

```
Interface view
```

### Default Level

```
2: System level
```

### Parameters

```
None
```

### Description

Use the **ospf mtu-enable** command to enable an interface to add the real MTU into DD packets.

Use the **undo ospf mtu-enable** command to restore the default.

By default, an interface adds a MTU of 0 into DD packets, that is, no real MTU is added.

Note that:

- After a virtual link is established via a Tunnel, two devices on the link from different vendors may have different MTU values. To make them consistent, set the attached interfaces' default MTU to 0.
- This configuration is not supported on the null interface.
- After you configure this command, upon receiving a DD packet, the interface checks whether the MTU in the packet is greater than that of its own; if yes, the interface discards the packet.

## Examples

```
# Enable the interface to add the real MTU value into DD packets.
```

```
<Sysname> system-view  
[Sysname] interface vlan-interface 10  
[Sysname-Vlan-interface10] ospf mtu-enable
```

## ospf network-type

### Syntax

```
ospf network-type { broadcast | nbma | p2mp | p2p }
```

```
undo ospf network-type
```

## View

Interface view

## Default Level

2: System level

## Parameters

**broadcast**: Specifies the network type as Broadcast.

**nbma**: Specifies the network type as NBMA.

**p2mp**: Specifies the network type as P2MP.

**p2p**: Specifies the network type as P2P.

## Description

Use the **ospf network-type** command to set the network type for an interface.

Use the **undo ospf network-type** command to restore the default network type for an interface.

By default, the network type is broadcast.

Note that:

- If a router on a broadcast network does not support multicast, you can configure the interface's network type as NBMA.
- If any two routers on an NBMA network are directly connected via a virtual link, that is, the network is fully meshed, you can configure the network type as NBMA; otherwise you need to configure it as P2MP for two routers having no direct link to exchange routing information via another router.
- When the network type of an interface is NBMA, you need to use the **peer** command to specify a neighbor.
- If only two routers run OSPF on a network segment, you can configure associated interfaces' network type as P2P.

Related commands: **ospf dr-priority**.



### Note

This command is not supported on the null or loopback interfaces.

---

## Examples

# Configure the interface's network type as NBMA.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf network-type nbma
```

## ospf packet-process prioritized-treatment

### Syntax

**ospf packet-process prioritized-treatment**

## **undo ospf packet-process prioritized-treatment**

### **View**

System view

### **Default Level**

2: System level

### **Parameters**

None

### **Description**

Use the **ospf packet-process prioritized-treatment** command to enable OSPF to give priority to receiving and processing Hello packets.

Use the **undo ospf packet-process prioritized-treatment** command to restore the default.

By default, this function is not enabled.

### **Examples**

# Enable OSPF to give priority to receiving and processing Hello packets.

```
<Sysname> system-view  
[Sysname] ospf packet-process prioritized-treatment
```

## **ospf timer dead**

### **Syntax**

**ospf timer dead** *seconds*

**undo ospf timer dead**

### **View**

Interface view

### **Default Level**

2: System level

### **Parameters**

*seconds*: Dead interval in seconds, in the range 1 to 2147483647.

### **Description**

Use the **ospf timer dead** command to set the dead interval.

Use the **undo ospf timer dead** command to restore the default.

The dead interval defaults to 40s for Broadcast, P2P interfaces and defaults to 120s for P2MP and NBMA interfaces.

If an interface receives no hello packet from the neighbor within the dead interval, the interface considers the neighbor down. The dead interval on an interface is at least four times the hello interval. Any two routers attached to the same segment must have the same dead interval.



#### Note

This configuration is not supported on the null interface.

---

Related commands: **ospf timer hello**.

### Examples

# Configure the dead interval on the current interface as 60 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf timer dead 60
```

### ospf timer hello

#### Syntax

**ospf timer hello** *seconds*

**undo ospf timer hello**

#### View

Interface view

#### Default Level

2: System level

#### Parameters

*seconds*: Hello interval in seconds, in the range 1 to 65535.

#### Description

Use the **ospf timer hello** command to set the hello interval on an interface.

Use the **undo ospf timer hello** command to restore the default hello interval on an interface.

The hello interval defaults to 10s for P2P and Broadcast interfaces, and defaults to 30s for P2MP and NBMA interfaces.

The shorter the hello interval is, the faster the topology converges and the more resources are consumed. Make sure the hello interval on two neighboring interfaces is the same.



#### Note

This configuration is not supported on the null interface.

---

Related commands: **ospf timer dead**.

## Examples

```
# Configure the hello interval on the current interface as 20 seconds.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf timer hello 20
```

## ospf timer poll

### Syntax

```
ospf timer poll seconds
undo ospf timer poll
```

### View

Interface view

### Default Level

2: System level

### Parameters

*seconds*: Poll interval in seconds, in the range 1 to 2147483647.

### Description

Use the **ospf timer poll** command to set the poll interval on an NBMA interface.

Use the **undo ospf timer poll** command to restore the default value.

By default, the poll interval is 120s.

When an NBMA interface finds its neighbor is down, it will send hello packets at the poll interval.

Note that:

- The poll interval is at least four times the hello interval.
- This configuration is not supported on the null interface.

Related commands: **ospf timer hello**.

## Examples

```
# Set the poll timer interval on the current interface to 130 seconds.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf timer poll 130
```

## ospf timer retransmit

### Syntax

```
ospf timer retransmit interval
undo ospf timer retransmit
```

### View

Interface view

## Default Level

2: System level

## Parameters

*interval*: LSA retransmission interval in seconds, in the range 1 to 3600.

## Description

Use the **ospf timer retransmit** command to set the LSA retransmission interval on an interface.

Use the **undo ospf timer retransmit** command to restore the default.

The interval defaults to 5s.

After sending an LSA, an interface waits for an acknowledgement packet. If the interface receives no acknowledgement within the retransmission interval, it will retransmit the LSA.

The retransmission interval should not be so small to avoid unnecessary retransmissions.



### Note

This configuration is not supported on the null interface.

---

## Examples

```
# Set the LSA retransmission interval to 8 seconds.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf timer retransmit 8
```

## ospf trans-delay

### Syntax

**ospf trans-delay** *seconds*

**undo ospf trans-delay**

### View

Interface view

### Default Level

2: System level

### Parameters

*seconds*: LSA transmission delay in seconds, in the range 1 to 3600.

### Description

Use the **ospf trans-delay** command to set the LSA transmission delay on an interface.

Use the **undo ospf trans-delay** command to restore the default.

The delay defaults to 1s.

Each LSA in the LSDB has an age that is incremented by 1 every second, but the age does not change during transmission. It is necessary to add a transmission delay into its age time, which is important for low speed networks.



#### Note

This configuration is not supported on the null interface.

---

## Examples

# Set the LSA transmission delay to 3 seconds on the current interface.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf trans-delay 3
```

## peer

### Syntax

```
peer ip-address [ dr-priority dr-priority ]
undo peer ip-address
```

### View

OSPF view

### Default Level

2: System level

### Parameters

*ip-address*: Neighbor IP address.

*dr-priority*: Neighbor DR priority, in the range 0 to 255.

### Description

Use the **peer** command to specify a neighbor, and the DR priority of the neighbor.

Use the **undo peer** command to remove the configuration.

On NBMA network, you can configure mappings to make the network fully meshed (any two routers have a direct link in between), so OSPF can handle DR/BDR election as it does on a broadcast network. However, since routers on the network cannot find neighbors via broadcasting hello packets, you need to specify neighbors and neighbor DR priorities on the routers.

After startup, a router sends a hello packet to neighbors with DR priorities higher than 0. When the DR and BDR are elected, the DR will send hello packets to all neighbors for adjacency establishment.

A router uses the priority set with the **peer** command to determine whether to send a hello packet to the neighbor rather than for DR election. The DR priority set with the **ospf dr-priority** command is used for DR election.

Related commands: **ospf dr-priority**.

## Examples

```
# Specify the neighbor 1.1.1.1.
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] peer 1.1.1.1
```

## preference

### Syntax

```
preference [ ase ] [ route-policy route-policy-name ] value
undo preference [ ase ]
```

### View

OSPF view

### Default Level

2: System level

### Parameters

**ase**: Sets a priority for ASE routes. If the keyword is not specified, using the command sets a priority for OSPF internal routes.

**route-policy** *route-policy-name*: References a route policy to set priorities for specified routes. A *route-policy-name* is a string of 1 to 19 characters.

*value*: Priority value, in the range 1 to 255. A smaller value represents a higher priority.

### Description

Use the **preference** command to set the priority of OSPF routes.

Use the **undo preference** command to restore the default.

The priority of OSPF internal routes defaults to 10, and the priority of OSPF external routes defaults to 150.

If a route policy is specified, priorities defined by the route policy will apply to matching routes, and the priorities set with the **preference** command apply to OSPF routes not matching the route policy.

A router may run multiple routing protocols. When several routing protocols find routes to the same destination, the router uses the route found by the protocol with the highest priority.

## Examples

```
# Set a priority of 200 for OSPF external routes.
```

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] preference ase 200
```

## reset ospf counters

### Syntax

```
reset ospf [ process-id ] counters [ neighbor [ interface-type interface-number ] [ router-id ] ]
```

### View

User view

### Default Level

2: System level

### Parameters

*process-id*: Clears the statistics information of the specified OSPF process, which is in the range 1 to 65535.

**neighbor**: Clears neighbor statistics.

*interface-type interface-number*: Clears the statistics information of the neighbor connected to the specified interface.

*router-id*: Clears the statistics information of the specified neighbor.

### Description

Use the **reset ospf counters** command to clear OSPF statistics information.

### Examples

```
# Reset OSPF counters.
```

```
<Sysname> reset ospf counters
```

## reset ospf process

### Syntax

```
reset ospf [ process-id ] process [ graceful-restart ]
```

### View

User view

### Default Level

2: System level

### Parameters

*process-id*: OSPF process ID, in the range 1 to 65535.

**graceful-restart**: Starts GR for the OSPF process.

### Description

Use the **reset ospf process** command to reset all OSPF processes or a specified process.

Using the **reset ospf process** command will:

- Clear all invalid LSAs without waiting for their timeouts;
- Make a newly configured Router ID take effect;

- Start a new round of DR/BDR election;
- Not remove any previous OSPF configurations.

The system prompts whether to reset OSPF process upon execution of this command.

## Examples

```
# Reset all OSPF processes.
<Sysname> reset ospf process
Warning : Reset OSPF process? [Y/N]:Y

# Reset the OSPF GR process.
<Sysname> reset ospf process graceful-restart
Warning : Reset OSPF process? [Y/N]:Y
```

## reset ospf redistribution

### Syntax

```
reset ospf [ process-id ] redistribution
```

### View

User view

### Default Level

2: System level

### Parameters

*process-id*: OSPF process ID, in the range 1 to 65535.

### Description

Use the **reset ospf redistribution** command to restart route redistribution. If no process ID is specified, using the command restarts route redistribution for all OSPF processes.

### Examples

```
# Restart route redistribution.
<Sysname> reset ospf redistribution
```

## rfc1583 compatible

### Syntax

```
rfc1583 compatible
undo rfc1583 compatible
```

### View

OSPF view

### Default Level

2: System level

## Parameters

None

## Description

Use the **rfc1583 compatible** command to make routing rules defined in RFC1583 compatible.

Use the **undo rfc1583 compatible** command to disable the function.

By default, RFC1583 routing rules are compatible.

RFC1583 and RFC2328 have different routing rules on selecting the best route when multiple AS external LSAs describe routes to the same destination. Using this command can make them compatible. If RFC1583 is made compatible with RFC 2328, the routes in the backbone area are preferred; if not, the routes in the non-backbone area are preferred to reduce the burden of the backbone area.

## Examples

```
# Disable making RFC1583 routing rules compatible.
```

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] undo rfc1583 compatible
```

## route-tag

### Syntax

**route-tag** *tag-value*

**undo route-tag**

### View

OSPF view

### Default Level

2: System level

## Parameters

*tag-value*: Tag for identifying injected VPN routes, in the range 0 to 4294967295.

## Description

Use the **route-tag** command to configure the tag for identifying injected VPN routes.

Use the **undo route-tag** command to restore the default.

The first two octets of the default tag is always 0xD000, while the last two octets is the AS number of the local BGP. For example, if the local BGP AS number is 100, the default tag is 3489661028 in decimal.

An OSPF instance-related VPN instance on a PE is usually configured with a VPN route tag, which must be included in Type 5/7 LSAs. PEs in the same AS are recommended to have the same route tag. The route tag is local significant and can be configured and take effect on only PEs receiving BGP routes and generating OSPF LSAs; it is not transferred in any BGP extended community attribute. Different OSPF processes can have the same route tag.

Tags configured with different commands have different priorities:

- A tag configured with the **import-route** command has the highest priority.

- A tag configured with the **route-tag** command has the second highest priority.
- A tag configured with the **default tag** command has the lowest priority.

A received Type 5 or Type 7 LSA is neglected in route calculation if its tag is the same as the local one.



### Note

A configured route tag takes effect after you issue the **reset ospf** command.

## Examples

```
# Configure the route tag for OSPF process 100 as 100.
```

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] route-tag 100
```

## sham-link

### Syntax

```
sham-link source-ip-address destination-ip-address [ cost cost | dead dead-interval | hello hello-interval | retransmit retrans-interval | trans-delay delay | simple [ cipher | plain ] password1 | { md5 | hmac-md5 } key-id [ cipher | plain ] password2 ] *
```

```
undo sham-link source-ip-address destination-ip-address [ cost | dead | hello | retransmit | trans-delay | simple | { md5 | hmac-md5 } key-id ] *
```

### View

OSPF area view

### Default Level

2: System level

### Parameters

*source-ip-address*: Source IP address for the sham link.

*destination-ip-address*: Destination IP address for the sham link.

*cost*: Cost for the sham link. It ranges from 1 to 65,535 and defaults to 1.

*dead-interval*: Dead Interval in seconds. It ranges from 1 to 32,768 and defaults to 40. It must be equal to the dead interval of the router on the other end of the virtual link and be at least four times the hello interval.

*hello-interval*: Interval at which the interface sends Hello packets. It ranges from 1 to 8,192 seconds and defaults to 10 seconds. It must be equal to the hello interval of the router on the other end of the virtual link.

*retrans-interval*: Interval at which the interface retransmits LSAs. It ranges from 1 to 8,192 seconds and defaults to 5 seconds.

*delay*: Delay interval before the interface sends an LSA. It ranges from 1 to 8,192 seconds and defaults to 1 second.

**simple** [ **cipher** | **plain** ] *password1*: Uses simple authentication. If you specify neither the **cipher** nor the **plain** keyword, the *password1* argument is a string of 1 to 8 characters. For the plain mode, the *password1* argument is a string of 1 to 8 characters. For the cipher mode, the *password1* argument can be either a string of 1 to 8 characters in plain text, or a string of 24 characters in cipher text.

**md5**: Uses MD5 algorithm for authentication.

**hmac-md5**: Uses HMAC-MD5 algorithm for authentication.

*key-id*: Authentication key ID of the interface, in the range 1 to 255. It must be the same as that of the peer.

**cipher**: Uses cipher text.

**plain**: Uses plain text.

*password2*: Password string, case-sensitive. If you specify neither the **cipher** nor the **plain** keyword, it is a string of 1 to 16 characters in plain text or a string of 24 characters in cipher text. For the plain mode, it is a string of 1 to 16 characters. For the cipher mode, it can be either a string of 1 to 16 characters in plain text, or a string of 24 characters in cipher text.

## Description

Use the **sham link** command to configure a sham link.

Use the **undo sham link** command with no optional keyword to remove a sham link.

Use the **undo sham link** command with optional keywords to restore the defaults of the parameters for a sham link.

If two PEs belong to the same AS and a backdoor link is present, a sham link can be established between them.

For plain text authentication, the default authentication key type is plain. For authentication using MD5 algorithm or HMAC-MD5 algorithm, the default authentication key type is cipher.

## Examples

```
# Create a sham link with the source address of 1.1.1.1 and the destination address of 2.2.2.2.
```

```
<Sysname> system-view
[Sysname] ospf
[Sysname-ospf-1] area 0
[Sysname-ospf-1-area-0.0.0.1] sham-link 1.1.1.1 2.2.2.2
```

## silent-interface (OSPF view)

### Syntax

```
silent-interface { all | interface-type interface-number }
```

```
undo silent-interface { all | interface-type interface-number }
```

### View

OSPF view

## Default Level

2: System level

## Parameters

**all**: Disables all interfaces from sending OSPF packets.

*interface-type interface-number*: Disables the specified interface from sending OSPF packets

## Description

Use the **silent-interface** command to disable an interface or all interfaces from sending OSPF packets.

Use the **undo silent-interface** command to restore the default.

By default, an interface sends OSPF packets.

A disabled interface is a passive interface, which cannot send any hello packet.

To make no routing information obtained by other routers on a network segment, you can use this command to disable the interface from sending OSPF packets.

## Examples

# Disable an interface from sending OSPF packets.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] silent-interface vlan-interface 10
```

## snmp-agent trap enable ospf

### Syntax

```
snmp-agent trap enable ospf [ process-id ] [ ifauthfail | ifcfgerror | ifrxbadpkt | ifstatechange |
iftxretransmit | Isdbapproachoverflow | Isdboverflow | maxagelsa | nbrstatechange | originatelsa
| vifcfgerror | virifauthfail | virifrxbadpkt | virifstatechange | viriftxretransmit | virnbrstatechange ]
*
```

```
undo snmp-agent trap enable ospf [ process-id ] [ ifauthfail | ifcfgerror | ifrxbadpkt | ifstatechange
| iftxretransmit | Isdbapproachoverflow | Isdboverflow | maxagelsa | nbrstatechange |
originatelsa | vifcfgerror | virifauthfail | virifrxbadpkt | virifstatechange | viriftxretransmit |
virnbrstatechange ] *
```

### View

System view

## Default Level

3: Manage level

## Parameters

*process-id*: OSPF process ID, in the range 1 to 65535.

**ifauthfail**: Interface authentication failure information.

**ifcfgerror**: Interface configuration error information.

**ifrxbadpkt**: Information about error packets received.

**ifstatechange**: Interface state change information.

**iftxretransmit**: Packet receiving and forwarding information.

**lsdbapproachoverflow**: Information about cases approaching LSDB overflow.

**lsdboverflow**: LSDB overflow information.

**maxagelsa**: LSA max age information.

**nbrstatechange**: Neighbor state change information.

**originatelsa**: Information about LSAs originated locally.

**vifauthfail**: Virtual interface authentication failure information.

**vifcfgerror**: Virtual interface configuration error information.

**virifauthfail**: Virtual interface authentication failure information.

**virifrxbadpkt**: Information about error packets received by virtual interfaces.

**virifstatechange**: Virtual interface state change information.

**viriftxretransmit**: Virtual interface packet retransmission information.

**virnbrstatechange**: Virtual interface neighbor state change information.

## Description

Use the **snmp-agent trap enable ospf** command to enable the sending of SNMP traps for a specified OSPF process. If no process is specified, the feature is enabled for all processes.

Use the **undo snmp-agent trap enable ospf** command to disable the feature.

By default, this feature is enabled.

Refer to *SNMP Commands* in the *System Volume* for related information.

## Examples

```
# Enable the sending of SNMP traps for OSPF process 1.
```

```
<Sysname> system-view  
[Sysname] snmp-agent trap enable ospf 1
```

## spf-schedule-interval

### Syntax

```
spf-schedule-interval maximum-interval [ minimum-interval [ incremental-interval ] ]
```

```
undo spf-schedule-interval
```

### View

OSPF view

### Default Level

2: System level

### Parameters

*maximum-interval*: Maximum OSPF route calculation interval in seconds, in the range 1 to 60.

*minimum-interval*: Minimum OSPF route calculation interval in milliseconds, in the range 10 to 60000, which defaults to 0.

*incremental-interval*: Incremental value in milliseconds, in the range 10 to 60000, which defaults to 5000.

## Description

Use the **spf-schedule-interval** command to set the OSPF SPF calculation interval.

Use the **undo spf-schedule-interval** command to restore the default.

The interval defaults to 5 seconds.

Based on its LSDB, an OSPF router calculates the shortest path tree with itself being the root, and uses it to determine the next hop to a destination. Through adjusting the SPF calculation interval, you can protect bandwidth and router resources from being over-consumed due to frequent network changes.

With this command configured, when network changes are not frequent, SPF calculation applies at the *minimum-interval*. If network changes become frequent, the SPF calculation interval is incremented by the *incremental-interval* each time a calculation happens, up to the *maximum-interval*.

## Examples

```
# Configure the SPF calculation maximum interval as 10 seconds, minimum interval as 500 milliseconds and incremental interval as 200 milliseconds.
```

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] spf-schedule-interval 10 500 200
```

## stub (OSPF area view)

### Syntax

```
stub [ no-summary ]
```

```
undo stub
```

### View

```
OSPF area view
```

### Default Level

```
2: System level
```

### Parameters

**no-summary**: Usable only on a stub ABR. With it configured, the ABR advertises only a default route in a Summary LSA into the stub area (such a stub area is known as a totally stub area).

## Description

Use the **stub** command to configure an area as a stub area.

Use the **undo stub** command to remove the configuration.

No area is stub area by default.

Note that, to cancel the **no-summary** configuration on the ABR, simply execute the **stub** command again to overwrite it.

To configure an area as a stub area, all routers attached to it must be configured with this command.

Related commands: **default-cost**.

## Examples

```
# Configure Area1 as a stub area.
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] stub
```

## stub-router

### Syntax

```
stub-router
undo stub-router
```

### View

OSPF view

### Default Level

2: System level

### Parameters

None

### Description

Use the **stub-router** command to configure the router as a stub router.

Use the **undo stub-router** command to restore the default.

By default, no router is configured as a stub router.

The router LSAs from the stub router may contain different link type values. A value of 3 means a link to the stub network, so the cost of the link remains unchanged. A value of 1, 2 or 4 means a point-to-point link, a link to a transit network or a virtual link; in such cases, a maximum cost value of 65535 is used. Thus, other neighbors find the links to the stub router have such big costs, they will not send packets to the stub router for forwarding as long as there is a route with a smaller cost.

## Examples

```
# Configure a stub router.
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] stub-router
```

## transmit-pacing

### Syntax

```
transmit-pacing interval interval count count
undo transmit-pacing
```

## View

OSPF view

## Default Level

2: System level

## Parameters

*interval*: Interval at which an interface sends LSU packets, in milliseconds. Its value is in the range 10 to 1000. If the router has a number of OSPF interfaces, you are recommended to increase this interval to reduce the total numbers of LSU packets sent by the router every second.

*count*: Maximum number of LSU packets sent by an interface at each interval. It is in the range 1 to 200. If the router has a number of OSPF interfaces, you are recommended to decrease this interval to reduce the total numbers of LSU packets sent by the router every second.

## Description

Use the **transmit-pacing** command to configure the maximum number of LSU packets that can be sent every the specified interval.

Use the **undo transmit-pacing** command to restore the default.

By default, an OSPF interface sends up to three LSU packets every 20 milliseconds.

## Examples

```
# Configure all the interfaces under OSPF process 1 to send up to 10 LSU packets every 30 milliseconds.
```

```
<Sysname> system-view  
[Sysname-ospf-1] transmit-pacing interval 30 count 10
```

## vlink-peer (OSPF area view)

### Syntax

```
vlink-peer router-id [ hello seconds | retransmit seconds | trans-delay seconds | dead seconds | simple [ plain | cipher ] password | { md5 | hmac-md5 } key-id [ plain | cipher ] password ] *
```

```
undo vlink-peer router-id [ hello | retransmit | trans-delay | dead | [ simple | { md5 | hmac-md5 } key-id ] ] *
```

## View

OSPF area view

## Default Level

2: System level

## Parameters

*router-id*: Router ID of the neighbor on the virtual link.

**hello** *seconds*: Hello interval in seconds, in the range 1 to 8192. The default is 10. It must be identical to the hello interval on its virtual link neighbor.

**retransmit** *seconds*: Retransmission interval in seconds, in the range 1 to 3600, which defaults to 5.

**trans-delay** *seconds*: Transmission delay interval in seconds, in the range 1 to 3600, which defaults to 1.

**dead** *seconds*: Dead interval in seconds, in the range 1 to 32768, which defaults to 40 and is identical to the value on its virtual link neighbor. The dead interval is at least four times the hello interval.

**md5**: MD5 authentication.

**hmac-md5**: HMAC-MD5 authentication.

**simple**: Simple authentication.

*key-id*: Key ID for MD5 or HMAC-MD5 authentication, in the range 1 to 255.

**plain** | **cipher**: Plain or cipher type. If plain is specified, only plain password is supported and displayed upon displaying the configuration file. If cipher is specified, both plain and cipher are supported, but only cipher password is displayed when displaying the configuration file. By default, MD5 and HMAC-MD5 support cipher password, and simple authentication supports plain password.

*password*: Plain or cipher password. Simple authentication: For plain type, a plain password is a string of up to 8 characters. For cipher type, a plain password is a string of up to 8 characters, and a cipher password is a string of up to 24 characters. MD5/HMAC-MD5 authentication: For plain type, a plain password is a string of up to 16 characters. For cipher type, a plain password is a string of up to 16 characters, and a cipher password is a string of up to 24 characters.

## Description

Use the **vlink-peer** command to configure a virtual link.

Use the **undo vlink-peer** command to remove a virtual link.

As defined in RFC2328, all non-backbone areas must maintain connectivity to the backbone. You can use the **vlink-peer** command to configure a virtual link to connect an area to the backbone.

Considerations on parameters:

- The smaller the hello interval is, the faster the network converges and the more network resources are consumed.
- A so small retransmission interval will lead to unnecessary retransmissions. A big value is appropriate for a low speed link.
- You need to specify an appropriate transmission delay with the **trans-delay** keyword.

The authentication mode at the non-backbone virtual link end follows the one at the backbone virtual link end. The two authentication modes (MD5 or Simple) are independent, and you can specify neither of them.

Related commands: **authentication-mode**, **display ospf**.

## Examples

```
# Configure a virtual link to the neighbor with router ID 1.1.1.1.
```

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 2
[Sysname-ospf-100-area-0.0.0.2] vlink-peer 1.1.1.1
```

# Table of Contents

<b>1 IS-IS Configuration Commands</b> .....	<b>1-1</b>
IS-IS Configuration Commands .....	1-1
area-authentication-mode .....	1-1
auto-cost enable .....	1-2
bandwidth-reference (IS-IS view) .....	1-3
circuit-cost .....	1-3
cost-style .....	1-4
default-route-advertise (IS-IS view) .....	1-5
display isis brief .....	1-6
display isis debug-switches .....	1-7
display isis graceful-restart status .....	1-8
display isis interface .....	1-9
display isis license .....	1-11
display isis lsdb .....	1-13
display isis mesh-group .....	1-15
display isis name-table .....	1-16
display isis peer .....	1-17
display isis route .....	1-20
display isis spf-log .....	1-23
display isis statistics .....	1-24
domain-authentication-mode .....	1-25
filter-policy export (IS-IS view) .....	1-27
filter-policy import (IS-IS view) .....	1-27
flash-flood .....	1-28
graceful-restart (IS-IS view) .....	1-29
graceful-restart interval (IS-IS view) .....	1-30
graceful-restart suppress-sa .....	1-30
import-route (IS-IS view) .....	1-31
import-route isis level-2 into level-1 .....	1-32
import-route limit (IS-IS view) .....	1-33
isis .....	1-34
isis authentication-mode .....	1-34
isis circuit-level .....	1-36
isis circuit-type p2p .....	1-36
isis cost .....	1-37
isis dis-name .....	1-38
isis dis-priority .....	1-39
isis enable .....	1-40
isis mesh-group .....	1-41
isis mib-binding .....	1-42
isis silent .....	1-42
isis small-hello .....	1-43
isis timer csnp .....	1-44

isis timer hello	1-44
isis timer holding-multiplier	1-45
isis timer lsp	1-46
isis timer retransmit	1-47
is-level	1-48
is-name	1-49
is-name map	1-49
is-snmp-traps enable	1-50
log-peer-change (IS-IS view)	1-51
lsp-fragments-extend	1-51
lsp-length originate	1-52
lsp-length receive	1-53
maximum load-balancing (IS-IS view)	1-53
network-entity	1-54
preference (IS-IS view)	1-55
reset isis all	1-55
reset isis peer	1-56
set-overload	1-57
summary (IS-IS view)	1-58
timer lsp-generation	1-59
timer lsp-max-age	1-60
timer lsp-refresh	1-61
timer spf	1-61
virtual-system	1-63

# 1 IS-IS Configuration Commands

---



The “router” in this document refers to a generic router or an Ethernet switch running routing protocols.

---

## IS-IS Configuration Commands

### area-authentication-mode

#### Syntax

```
area-authentication-mode { md5 | simple } password [ ip | osi ]  
undo area-authentication-mode
```

#### View

IS-IS view

#### Default Level

2: System level

#### Parameters

**md5**: Specifies the MD5 authentication mode.

**simple**: Specifies the simple authentication mode.

*password*: Password. For **simple** authentication mode, the *password* must be plain text. For **md5** authentication mode, the password can be either plain text or cipher text. A plaintext password can be a string of up to 16 characters, such as **user918**. A cipher password must be a ciphertext string of 24 characters, such as **(TT8F]Y5SQ=^Q`MAF4<1!!**.

**ip**: Checks IP related fields in LSPs.

**osi**: Checks OSI related fields in LSPs.



Whether a password should use **ip** or **osi** is not affected by the actual network environment.

---

## Description

Use the **area-authentication-mode** command to specify the area authentication mode and a password.

Use the **undo area-authentication-mode** command to restore the default.

No area authentication is configured by default.

The password in the specified mode is inserted into all outgoing Level-1 packets (LSP, CSNP and PSNP) and is used for authenticating the incoming Level-1 packets.

With area authentication configured, IS-IS discards incoming routes from untrusted routers.

Note that:

- Routers in a common area must have the same authentication mode and password.
- If neither **ip** nor **osi** is specified, OSI related fields are checked.

Related commands: **reset isis all**, **domain-authentication-mode**, **isis authentication-mode**

## Examples

# Set the area authentication password to ivg, and the authentication mode to simple.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] area-authentication-mode simple ivg
```

## auto-cost enable

### Syntax

**auto-cost enable**

**undo auto-cost enable**

### View

IS-IS view

### Default Level

2: System level

### Parameters

None

## Description

Use the **auto-cost enable** command to enable automatic link cost calculation.

Use the **undo auto-cost enable** command to disable the function.

This function is disabled by default.

After automatic link cost calculation is enabled, the link cost is automatically calculated based on the bandwidth reference value of an interface. When the **cost-style** is **wide** or **wide-compatible**, the cost value of an interface is calculated by using the formula: Cost = (reference bandwidth value/link bandwidth) × 10.

Related commands: **bandwidth-reference**, **cost-style**.

## Examples

```
# Enable automatic link cost calculation.
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] auto-cost enable
```

## bandwidth-reference (IS-IS view)

### Syntax

```
bandwidth-reference value
undo bandwidth-reference
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

**value:** Bandwidth reference value in Mbps, ranging from 1 to 2147483648.

### Description

Use the **bandwidth-reference** command to set the bandwidth reference value for automatic link cost calculation.

Use the **undo bandwidth-reference** command to restore the default.

By default, the bandwidth reference value is 100 Mbps.

Related commands: **auto-cost enable**.

## Examples

```
# Configure the bandwidth reference of IS-IS process 1 as 200 Mbps.
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] bandwidth-reference 200
```

## circuit-cost

### Syntax

```
circuit-cost value [ level-1 | level-2 ]
undo circuit-cost [ level-1 | level-2 ]
```

### View

IS-IS view

### Default Level

2: System level

## Parameters

*value*: Link cost value. The value range varies with cost styles.

- For styles **narrow**, **narrow-compatible** and **compatible**, the cost value ranges from 0 to 63.
- For styles **wide** and **wide-compatible**, the cost value ranges from 0 to 16777215.

**level-1**: Applies the link cost to Level-1.

**level-2**: Applies the link cost to Level-2.

## Description

Use the **circuit-cost** command to set a global IS-IS link cost.

Use the **undo circuit-cost** command to restore the default.

By default, no global link cost is configured.

If no level is specified, the specified cost applies to both Level-1 and Level-2.

Related commands: **isis cost**, **cost-style**.

## Examples

```
# Set the global Level-1 link cost of IS-IS process 1 to 11.
```

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] circuit-cost 11 level-1
```

## cost-style

### Syntax

```
cost-style { narrow | wide | wide-compatible | { compatible | narrow-compatible }
[ relax-spf-limit ] }
undo cost-style
```

### View

IS-IS view

### Default Level

2: System level

## Parameters

**narrow**: Receives and sends only narrow cost style packets (The narrow cost ranges from 0 to 63).

**wide**: Receives and sends only wide cost style packets (The wide cost ranges from 0 to 16777215).

**compatible**: Receives and sends both wide and narrow cost style packets.

**narrow-compatible**: Receives both narrow and wide cost style packets, but sends only narrow cost style packets.

**wide-compatible**: Receives both narrow and wide cost style packets, but sends only wide cost style packets.

**relax-spf-limit**: Allows receiving routes with a cost greater than 1023. If this keyword is not specified, any route with a cost bigger than 1023 will be discarded. This keyword is only available when **compatible** or **narrow-compatible** is included.

## Description

Use the **cost-style** command to set a cost style.

Use the **undo cost-style** command to restore the default.

Only narrow cost style packets can be received and sent by default.

Related commands: **isis cost**, **circuit-cost**.

## Examples

```
# Configure the router to send only narrow cost style packets, but receive both narrow and wide cost style packets.
```

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] cost-style narrow-compatible
```

## default-route-advertise (IS-IS view)

### Syntax

```
default-route-advertise [ route-policy route-policy-name | [ level-1 | level-2 | level-1-2 ] ] *
undo default-route-advertise [ route-policy route-policy-name ]
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

*route-policy-name*: Specifies the name of a routing policy, a string of 1 to 19 characters.

**level-1**: Advertises a Level-1 default route.

**level-2**: Advertises a Level-2 default route.

**level-1-2**: Advertises both Level-1 and Level-2 default routes.

## Description

Use the **default-route-advertise** command to advertise a default route of 0.0.0.0/0.

Use the **undo default-route-advertise** command to disable default route advertisement.

Default route advertisement is disabled by default.

Note that:

- If no level is specified, a Level-2 default route is advertised.
- The Level-1 default route is advertised to other routers in the same area, while the Level-2 default route is advertised to all the Level-2 and Level-1-2 routers.
- Using the **apply isis level-1** command in routing policy view will generate a default route in a Level-1 LSP. Using the **apply isis level-2** command in routing policy view will generate a default route in a Level-2 LSP. Using the **apply isis level-1-2** command in routing policy view will generate a default route in a Level-1 LSP and Level-2 LSP respectively.

## Examples

```
# Advertise a Level-2 default route.
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] default-route-advertise
```

## display isis brief

### Syntax

```
display isis brief [ process-id | vpn-instance vpn-instance-name ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*process-id*: Displays IS-IS brief configuration information for the IS-IS process. The process ID is in the range 1 to 65535.

**vpn-instance** *vpn-instance-name*: Displays IS-IS brief configuration information for the VPN instance. The VPN instance name is a string of 1 to 31 characters.

### Description

Use the **display isis brief** command to view IS-IS brief configuration information.

### Examples

```
# Display IS-IS brief configuration information.
```

```
<Sysname> display isis brief
```

```
ISIS (1) Protocol Brief Information :
```

```
network-entity:
  10.0000.0000.0001.00
is-level :level-1-2
cost-style: narrow
preference : 15
Lsp-length receive : 1497
Lsp-length originate : level-1 1497
                      level-2 1497
maximum imported routes number : 10000
Timers:
  lsp-max-age: 1200
  lsp-refresh: 900
  Interval between SPF: 10
```

**Table 1-1 display isis brief** command output description

Field		Description
network-entity		Network entity name
is-level		IS-IS Routing level
cost-style		Cost style
preference		Preference
Lsp-length receive		Maximum LSP that can be received
Lsp-length originate		Maximum LSP that can be generated
maximum imported routes number		Maximum number of redistributed Level-1/Level-2 IPv4 routes
Timers	lsp-max-age	Maximum life period of LSP
	lsp-refresh	Refresh interval of LSP
	Interval between SPFs	Interval between SPF calculations

## display isis debug-switches

### Syntax

**display isis debug-switches** { *process-id* | **vpn-instance** *vpn-instance-name* }

### View

Any view

### Default Level

1: Monitor level

### Parameters

*process-id*: Displays the IS-IS debugging switch state for the IS-IS process. The ID is in the range of 1 to 65535.

*vpn-instance-name*: Displays the IS-IS debugging switch state for the VPN instance. The name is a string of 1 to 31 characters.

### Description

Use the **display isis debug-switches** command to display IS-IS debugging switch state.

### Examples

# Display the debugging switch state of IS-IS process 1.

```
<Sysname> display isis debug-switches 1
```

```
IS-IS - Debug settings.
```

```
IS-IS SPF Triggering Events debugging is on
```

## display isis graceful-restart status

### Syntax

```
display isis graceful-restart status [ level-1 | level-2 ] [ process-id | vpn-instance  
vpn-instance-name ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**level-1**: Displays the IS-IS Level-1 Graceful Restart state.

**level-2**: Displays the IS-IS Level-2 Graceful Restart state.

*process-id*: IS-IS Process ID, in the range 1 to 65535.

**vpn-instance** *vpn-instance-name*: Name of a VPN instance, a string of 1 to 31 characters.

### Description

Use the **display isis graceful-restart status** command to display IS-IS Graceful Restart status.

### Examples

# Display IS-IS Graceful Restart status.

```
<Sysname> display isis graceful-restart status  
Restart information for IS-IS(1)
```

-----

```
IS-IS(1) Level-1 Restart Status
```

```
Restart Interval: 150
```

```
SA Bit Supported
```

```
Total Number of Interfaces = 1
```

```
Restart Status: RESTARTING
```

```
Number of LSPs Awaited: 3
```

```
T3 Timer Status:
```

```
Remaining Time: 140
```

```
T2 Timer Status:
```

```
Remaining Time: 59
```

```
IS-IS(1) Level-2 Restart Status
```

```
Restart Interval: 150
```

```
SA Bit Supported
```

```
Total Number of Interfaces = 1
```

```
Restart Status: RESTARTING
```

```
Number of LSPs Awaited: 3
```

```
T3 Timer Status:
```

```
Remaining Time: 140
```

```
T2 Timer Status:
```

```
Remaining Time: 59
```

**Table 1-2** display isis graceful-restart status command output description

Field	Description
Restart Interval	Graceful Restart interval
SA Bit Supported	The SA bit is set
Total Number of Interfaces = 1	The current IS-IS interface number
Restart Status	Graceful Restart status
Number of LSPs Awaited	Number of LSPs not obtained by the GR restarter from GR helpers during LSDB synchronization
T3 Timer Status	Remaining time of T3 timer
T2 Timer Status	Remaining time of T2 Timer

## display isis interface

### Syntax

```
display isis interface [ statistics | [ interface-type interface-number ] [ verbose ] ] [ process-id | vpn-instance vpn-instance-name ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**statistics**: Displays IS-IS interface statistics information.

*interface-type interface-number*: IS-IS interface whose statistics information is to be displayed.

**verbose**: Displays detailed IS-IS interface information.

*process-id*: Displays the IS-IS interface information of the IS-IS process. The ID is in the range of 1 to 65535.

*vpn-instance-name*: Displays the IS-IS interface information of the VPN instance. The name is a string of 1 to 31 characters.

### Description

Use the **display isis interface** command to display IS-IS interface information.

### Examples

```
# Display brief IS-IS interface information.
```

```
<Sysname> display isis interface
                Interface information for ISIS(1)
                -----
Interface: Vlan-interfaces
Id      IPV4.State      IPV6.State      MTU      Type      DIS
001     Up              Down            1497     L1/L2     No/No
```

# Display detailed IS-IS interface information.

```
<Sysname> display isis interface verbose
```

```

Interface information for ISIS(1)
-----

Interface: Vlan-interface999
Id      IPV4.State      IPV6.State      MTU  Type  DIS
001     Up             Down           1497 L1/L2 No/No
SNPA Address      : 000f-e237-c6e0
IP Address       : 192.168.1.48
Secondary IP Address(es) :
IPv6 Link Local Address :
IPv6 Global Address(es) :
Csnp Timer Value : L1 10 L2 10
Hello Timer Value : L1 10 L2 10
Hello Multiplier Value : L1 3 L2 3
Lsp Timer Value   : L12 33
Cost              : L1 10 L2 10
Priority          : L1 64 L2 64
Retransmit Timer Value : L12 5
BFD              : Disabled

```

**Table 1-3 display isis interface command output description**

Field	Description
Interface	Interface type and number
Id	Circuit ID
IPV4.State	IPv4 state
IPV6.State	IPv6 state
MTU	Interface MTU
Type	Interface link adjacency type
DIS	Whether the interface is elected as the DIS or not
SNPA Address	Subnet access point address
IP Address	Primary IP address
Secondary IP Address(es)	Secondary IP addresses
IPv6 Link Local Address	IPv6 link local address
IPv6 Global Address(es)	IPv6 global address
Csnp Timer Value	Interval for sending CSNP packets
Hello Timer Value	Interval for sending Hello packets
Hello Multiplier Value	Number of invalid Hello packets
Lsp Timer Value	Minimum interval for sending LSP packets
Cost	Cost of the interface

Field	Description
Priority	DIS priority
Retransmit Timer Value	LSP retransmission interval over the point-to-point link
BFD	Whether BFD is enabled on the interface

# Display IS-IS interface statistics information.

```
<sysname> display isis interface statistics
                Interface Statistics information for ISIS(1)
                -----
Type           IPv4 Up/Down           IPv6 Up/Down
LAN            0/1                          -/-
P2P           4/0                          -/-
```

**Table 1-4** display isis interface statistics command output description

Field	Description
Type	Network type of the interface: <ul style="list-style-type: none"> <li>• LAN for broadcast network.</li> <li>• P2P for point-to-point network.</li> </ul>
IPv4 UP	Number of IS-IS interfaces in up state
IPv4 DOWN	Number of IS-IS interfaces in down state
IPv6 UP	Number of IS-ISv6 interfaces in up state. A value of "-" means IPv6 is not enabled.
IPv6 DOWN	Number of IS-ISv6 interfaces in down state. A value of "-" means IPv6 is not enabled.

## display isis license

### Syntax

```
display isis license
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display isis license** command to display the information of the IS-IS license.

### Examples

```
# Display the information of the IS-IS license.
```

<Sysname> display isis license

ISIS Shell License Values

---

Feature Name	Active	Controllable
ISIS Protocol	YES	NO
IPV6	YES	NO
RESTART	YES	NO
TE	NO	NO
MI	YES	NO

Resource Name	MinVal	MaxVal	CurrVal	Controllable
Max Processes Resource	1	1024	500	0
Max Paths Resource	1	6	3	0
Max IPv4 Rt Resource	400000	400000	400000	0
Max IPv6 Rt Resource	400000	400000	400000	0

ISIS Core License Values

---

Feature Name	Active
ISIS Protocol	YES
IPV6	YES
RESTART	YES
TE	NO
MI	YES

Resource Name	Current Value
Max Processes Resource	64
Max Paths Resource	4
Max IPv4 Rt Resource	12288
Max IPv6 Rt Resource	6144

**Table 1-5 display isis license command output description**

Field	Description
ISIS Shell License Values	License values of IS-IS shell
Feature Name	Feature name
Active	Whether the state is active.
Controllable	Whether support reading configuration through License file.
ISIS Protocol	IS-IS Protocol
IPV6	Whether IPv6 is active or not.
RESTART	Graceful Restart (GR)
TE	Traffic Engineering
MI	Multi-instance

Field	Description
Resource Name	Resource name
MinVal	Minimum value
MaxVal	Maximum value
CurrVal	Current value
ISIS Core License Values	License values of IS-IS Core
Max Processes Resource	Maximum number of processes supported
Max Paths Resource	Maximum equal cost paths
Max IPv4 Rt Resource	Maximum IPv4 routes supported
Max IPv6 Rt Resource	Maximum IPv6 routes supported

## display isis lsdb

### Syntax

```
display isis lsdb [ [ I1 | I2 | level-1 | level-2 ] | [ lsp-id lspid | lsp-name lspname ] | local | verbose ] *
[ process-id | vpn-instance vpn-instance-name ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**I1, level-1:** Displays the level-1 LSDB.

**I2, level-2:** Displays the level-2 LSDB.

*lspid*: LSP ID, in the form of sysID. Pseudo ID-fragment num, where sysID represents the originating node or pseudo node.

*lspname*: LSP name, in the form of Symbolic name.[Pseudo ID]-fragment num.

**local:** Displays LSP information generated locally.

**verbose:** Displays LSDB detailed information.

*process-id*: Displays the LSDB of the IS-IS process. The ID is in the range of 1 to 65535.

*vpn-instance-name*: Displays the LSDB of the VPN instance. The VPN instance name is a string of 1 to 31 characters.

### Description

Use the **display isis lsdb** command to display IS-IS link state database.

If no level is specified, both Level-1 and Level-2 link state databases are displayed.

### Examples

```
# Display brief Level-1 LSDB information.
```

<Sysname> display isis lsdb level-1

Level-1 Link State Database

LSPID	Seq Num	Checksum	Holdtime	Length	ATT/P/OL
1111.1111.1111.00-00	0x00000004	0xa76	563	68	0/0/0
1111.1111.1112.00-00*	0x00000006	0x498d	578	84	0/0/0
1111.1111.1112.01-00*	0x00000001	0x4c0e	556	55	0/0/0

\*-Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload

# Display detailed Level-1 LSDB information.

<Sysname> display isis lsdb level-1 verbose

Database information for ISIS(1)

Level-1 Link State Database

LSPID	Seq Num	Checksum	Holdtime	Length	ATT/P/OL
1111.1111.1111.00-00	0x00000005	0x877	1090	68	0/0/0
SOURCE	1111.1111.1111.00				
NLPID	IPV4				
AREA ADDR	10				
INTF ADDR	3.1.1.2				
NBR ID	1111.1111.1112.01	COST: 10			
IP-Internal	3.1.1.0	255.255.255.0	COST: 10		
1111.1111.1112.00-00*	0x00000007	0x478e	1120	84	0/0/0
SOURCE	1111.1111.1112.00				
NLPID	IPV4				
AREA ADDR	10				
INTF ADDR	3.1.1.1				
INTF ADDR	2.1.2.2				
NBR ID	1111.1111.1112.01	COST: 10			
IP-Internal	3.1.1.0	255.255.255.0	COST: 10		
IP-Internal	2.1.2.0	255.255.255.0	COST: 10		
1111.1111.1112.01-00*	0x00000002	0x4a0f	1118	55	0/0/0
SOURCE	1111.1111.1112.01				
NLPID	IPV4				
NBR ID	1111.1111.1112.00	COST: 0			
NBR ID	1111.1111.1111.00	COST: 0			

**Table 1-6 display isis lsdb** command output description

Field	Description
LSPID	Link state packet ID
Seq Num	LSP sequence number
Checksum	LSP checksum
Holdtime	LSP lifetime which decreases as time elapses
Length	LSP length
ATT/P/OL	Attach bit (ATT) Partition bit (P) Overload bit (OL) 1 means the bit is set and 0 means the bit is not set.
SOURCE	System ID of the originating router
NLPID	Network layer protocol the originating router runs
AREA ADDR	Area address of the originating router
INTF ADDR	IP address of the originating router's IS-IS interface
INTF ADDR V6	IPv6 address of the originating router's IS-ISv6 interface
NBR ID	Neighbor ID of the originating router
IP-Internal	Internal IP address and mask of the originating router
IP-External	External IP address and mask of the originating router
IP-Extended	Extended IP address and mask of the originating router
COST	Cost
HOST NAME	Dynamic host name of the originating router
ORG ID	Original system ID of the virtual system ID of the originating router
Auth	Authentication information of the originating router
IPV6	Internal IPv6 address and prefix of the originating router
IPV6-Ext	External IPv6 address and prefix of the originating router

## display isis mesh-group

### Syntax

**display isis mesh-group** [ *process-id* | **vpn-instance** *vpn-instance-name* ]

### View

Any view

### Default Level

1: Monitor level

## Parameters

*process-id*: Displays IS-IS mesh-group configuration information for the IS-IS process. The ID is in the range of 1 to 65535.

*vpn-instance-name*: Displays IS-IS mesh-group configuration information for the VPN instance. The VPN instance name is a string of 1 to 31 characters.

## Description

Use the **display isis mesh-group** command to display IS-IS mesh-group configuration information.

## Examples

# Configure VLAN-interface 10 and VLAN-interface 20 to belong to mesh-group 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis mesh-group 100
[Sysname-Vlan-interface10] interface vlan-interface 20
[Sysname-Vlan-interface20] isis mesh-group 100
```

# Display the configuration information of IS-IS mesh-group.

```
[Sysname-Vlan-interface20] display isis mesh-group

                Mesh Group information for ISIS(1)
                -----
Interface      Status
Vlan10        100
Vlan20        100
```

**Table 1-7 display isis mesh-group** command output description

Field	Description
Interface	Interface name
Status	Mesh-group the interface belongs to

## display isis name-table

### Syntax

```
display isis name-table [ process-id | vpn-instance vpn-instance-name ]
```

### View

Any view

### Default Level

1: Monitor level

## Parameters

*process-id*: Displays the host name-to-system ID mapping table for the IS-IS process. The ID is in the range of 1 to 65535.

*vpn-instance-name*: Displays the host name-to-system ID mapping table for the VPN instance. The VPN instance name is a string of 1 to 31 characters.

## Description

Use the **display isis name-table** command to display the host name-to-system ID mapping table.

## Examples

```
# Configure a name for the local IS system.
```

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] is-name RUTA
```

```
# Configure a static mapping for the remote IS system (system ID 0000.0000.0041, host name RUTB).
```

```
[Sysname-isis-1] is-name map 0000.0000.0041 RUTB
```

```
# Display the IS-IS host name-to-system ID mapping table.
```

```
[Sysname-isis-1] display isis name-table
      Name table information for ISIS(1)
-----
System ID          Hostname          Type
6789.0000.0001    RUTA              DYNAMIC
0000.0000.0041    RUTB              STATIC
```

**Table 1-8 display isis name-table** command output description

Field	Description
System ID	System ID
Hostname	Hostname name
Type	Mapping type (static or dynamic)

## display isis peer

### Syntax

```
display isis peer [ statistics | verbose ] [ process-id | vpn-instance vpn-instance-name ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**statistics**: Displays IS-IS neighbor statistics information.

**verbose**: Displays detailed IS-IS neighbor information. Without the keyword, the command displays brief IS-IS neighbor information.

*process-id*: Displays the IS-IS neighbor information of the IS-IS process. The ID is in the range of 1 to 65535.

*vpn-instance-name*: Displays the IS-IS neighbor information of the VPN instance. The *vpn-instance-name* is a string of 1 to 31 characters.

## Description

Use the **display isis peer** command to display IS-IS neighbor information.

## Examples

# Display brief IS-IS neighbor information.

```
<Sysname> display isis peer
```

```
Peer information for ISIS(1)
-----

System Id: 1111.1111.1111
Interface: Vlan-interface1      Circuit Id: 1111.1111.1112.01
State: Up      HoldTime: 23s      Type: L1(L1L2)      PRI: 64

System Id: 1111.1111.1111
Interface: Vlan-interface1      Circuit Id: 1111.1111.1112.01
State: Up      HoldTime: 23s      Type: L2(L1L2)      PRI: 64
```

# Display detailed IS-IS neighbor information.

```
<Sysname>display isis peer verbose
```

```
Peer information for ISIS(1)
-----

System Id: 1111.1111.1111
Interface: Vlan-interface1      Circuit Id: 1111.1111.1112.01
State: Up      HoldTime: 27s      Type: L1(L1L2)      PRI: 64
Area Address(es):10
Peer IP Address(es): 3.1.1.2
Uptime: 00:38:15
Adj Protocol:  IPV4

System Id: 1111.1111.1111
Interface: Vlan-interface1      Circuit Id: 1111.1111.1112.01
State: Up      HoldTime: 28s      Type: L2(L1L2)      PRI: 64
Area Address(es):10
Peer IP Address(es): 3.1.1.2
Uptime: 00:38:15
Adj Protocol:  IPV4
```

**Table 1-9 display isis peer command output description**

Field	Description
System Id	System ID of the neighbor
Interface	Interface connecting to the neighbor
Circuit Id	Circuit ID
State	Circuit state
HoldTime	Holdtime Within the holdtime if no hellos are received from the neighbor, the neighbor is considered down. If a hello is received, the holdtime is reset to the initial value.
Type	Circuit type L1 means the circuit type is Level-1 and the neighbor is a Level-1 router. L2 means the circuit type is Level-2 and the neighbor is a Level-2 router. L1(L1L2) means the circuit type is Level-1 and the neighbor is a Level-1-2 router. L2(L1L2) means the circuit type is Level-2 and the neighbor is a Level-1-2 router.
PRI	DIS priority of the neighbor
Area Address(es)	The neighbor's area address
Peer IP Address(es)	IP address of the neighbor
Uptime	Time that elapsed since the neighbor relationship was formed.
Adj Protocol	Adjacency protocol

# Display IS-IS neighbor statistics information.

```
<Sysname> display isis peer statistics
```

```

Peer Statistics information for ISIS(1)
-----
Type          IPv4 Up/Init          IPv6 Up/Init
LAN Level-1   0/0                   0/0
LAN Level-2   0/0                   0/0
P2P           3/0                   0/0

```

**Table 1-10 display isis peer statistics command output description**

Field	Description
Type	Neighbor type: <ul style="list-style-type: none"> <li>LAN Level-1: Number of Level-1 neighbors whose network type is broadcast.</li> <li>LAN Level-2: Number of Level-2 neighbors whose network type is broadcast.</li> <li>P2P: Number of neighbors whose network type is P2P.</li> </ul>
IPv4 Up	Number of IPv4 neighbors in up state
IPv4 Init	Number of IPv4 neighbors in init state

Field	Description
IPv6 Up	Number of IPv6 neighbors in up state
IPv6 Init	Number of IPv6 neighbors in init state

## display isis route

### Syntax

```
display isis route [ ipv4 ] [ [ level-1 | level-2 ] | verbose ] * [ process-id | vpn-instance
vpn-instance-name ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**ipv4**: Displays IS-IS IPv4 routing information (the default).

**verbose**: Displays detailed IS-IS IPv4 routing information.

*process-id*: Displays the IS-IS IPv4 routing information of the IS-IS process. The ID is in the range of 1 to 65535.

*vpn-instance-name*: Displays the IS-IS IPv4 routing information of the VPN instance. The *vpn-instance-name* is a string of 1 to 31 characters.

**level-1**: Displays Level-1 IS-IS routes.

**level-2**: Displays Level-2 IS-IS routes.

### Description

Use the **display isis route** command to display IS-IS IPv4 routing information.

If no level is specified, both Level-1 and Level-2 routing information will be displayed.

### Examples

# Display IS-IS IPv4 routing information.

```
<Sysname> display isis route 1
```

```

                                Route information for ISIS(1)
                                -----

                                ISIS(1) IPv4 Level-1 Forwarding Table
                                -----

IPv4 Destination      IntCost    ExtCost  ExitInterface  NextHop      Flags
-----
1.1.1.0/16           20         NULL     Vlan10         1.2.1.1      R/L/-

```

```
1.2.0.0/16          10          NULL    Vlan10      Direct      D/L/-
```

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

ISIS(1) IPv4 Level-2 Forwarding Table

```
-----
```

IPv4 Destination	IntCost	ExtCost	ExitInterface	NextHop	Flags
1.1.0.0/16	20	NULL			
1.2.0.0/16	10	NULL	Vlan10	Direct	D/L/-

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

**Table 1-11 display isis route command output description**

Field	Description
Route information for ISIS(1)	Route information for IS-IS process 1
ISIS(1) IPv4 Level-1 Forwarding Table	IS-IS IPv4 routing information for Level-1
ISIS(1) IPv4 Level-2 Forwarding Table	IS-IS IPv4 routing information for Level-2
IPv4 Destination	IPv4 destination address
IntCost	Interior routing cost
ExtCost	Exterior routing cost
ExitInterface	Exit interface
NextHop	Next hop
Flags	Routing state flag D: Direct route. R: The route has been added into the routing table. L: The route has been advertised in an LSP. U: A route's penetration flag. Setting it to UP can prevent an LSP sent from L2 to L1 from being sent back to L2.

# Display detailed IS-IS IPv4 routing information.

```
<Sysname>display isis route verbose
      Route information for ISIS(1)
      -----

      ISIS(1) IPv4 Level-1 Forwarding Table
      -----

      IPv4 Dest  : 1.1.0.0/16          Int. Cost : 20          Ext. Cost : NULL
      Admin Tag  : -                  Src Count  : 2          Flag      : R/L/-
      NextHop    :                    Interface   :                    ExitIndex :
      1.2.1.1    :                    Vlan10     :                    0x00000008
```

```

IPv4 Dest   : 1.2.0.0/16           Int. Cost : 10           Ext. Cost : NULL
Admin Tag   : -                     Src Count  : 2           Flag      : D/L/-
NextHop     :                       Interface  :                   ExitIndex :
Direct      :                       Vlan10      :                   0x00000000

```

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

ISIS(1) IPv4 Level-2 Forwarding Table

-----

```

IPv4 Dest   : 1.1.0.0/16           Int. Cost : 20           Ext. Cost : NULL
Admin Tag   : -                     Src Count  : 2           Flag      : -/-/-
NextHop     :                       Interface  :                   ExitIndex :
Direct      :                       Vlan10      :                   0x00000000

```

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

**Table 1-12 display isis route verbose command output description**

Field	Description
Route information for ISIS(1)	Route information for IS-IS process 1
ISIS(1) IPv4 Level-1 Forwarding Table	IS-IS IPv4 routing information for Level-1
ISIS(1) IPv4 Level-2 Forwarding Table	IS-IS IPv4 routing information for Level-2
IPv4 Dest	IPv4 destination
Int. Cost	Internal route cost
Ext. Cost	External route cost
Admin Tag	Tag
Src Count	Count of advertising sources
Flag	Route state flag R: Indicates the route have been installed into the routing table. L: The route has been flooded in an LSP. U: Route leaking flag. If it is UP, routes from L2 to L1 cannot be advertised back to L2.
Next Hop	Next hop
Interface	Outgoing interface
ExitIndex	Index of the outgoing interface

## display isis spf-log

### Syntax

```
display isis spf-log [ process-id | vpn-instance vpn-instance-name ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*process-id*: Displays IS-IS SPF log information for the IS-IS process. The ID is in the range of 1 to 65535.

*vpn-instance-name*: Displays IS-IS SPF log information for the VPN instance. The name is a string of 1 to 31 characters.

### Description

Use the **display isis spf-log** command to display IS-IS SPF log information.

### Examples

```
# Display IS-IS SPF log information.
```

```
<Sysname> display isis spf-log
                SPF Log information for ISIS(1)
                -----
                Level      Trig.Event                No.Nodes  Duration  StartTime
                L2         IS_SPFTRIG_PERIODIC      2          0         13:3:24
                L1         IS_SPFTRIG_PERIODIC      2          0         13:18:8
                L2         IS_SPFTRIG_PERIODIC      2          0         13:18:8
                L1         IS_SPFTRIG_PERIODIC      2          0         13:32:28
                L2         IS_SPFTRIG_PERIODIC      2          0         13:32:28
                L1         IS_SPFTRIG_PERIODIC      2          0         13:44:0
                L2         IS_SPFTRIG_PERIODIC      2          0         13:44:0
                L1         IS_SPFTRIG_PERIODIC      2          0         13:55:43
                -->L2      IS_SPFTRIG_PERIODIC      2          0         13:55:43
                L1         IS_SPFTRIG_PERIODIC      2          0         11:54:12
                L2         IS_SPFTRIG_PERIODIC      2          0         11:54:12
                L1         IS_SPFTRIG_PERIODIC      2          0         12:7:24
                L2         IS_SPFTRIG_PERIODIC      2          0         12:7:24
                L1         IS_SPFTRIG_PERIODIC      2          0         12:21:24
                L2         IS_SPFTRIG_PERIODIC      2          0         12:21:24
                L1         IS_SPFTRIG_PERIODIC      2          0         12:35:24
                L2         IS_SPFTRIG_PERIODIC      2          0         12:35:24
                L1         IS_SPFTRIG_PERIODIC      2          0         12:49:24
                L2         IS_SPFTRIG_PERIODIC      2          0         12:49:24
                L1         IS_SPFTRIG_PERIODIC      2          0         13:3:24
```

**Table 1-13 display isis spf-log command output description**

Field	Description
SPF Log information for ISIS(1)	SPF log information for IS-IS process 1
Level	SPF calculation level
Trig.Event	SPF triggered event
No.Nodes	Number of SPF calculation nodes
Duration	SPF calculation duration
StartTime	SPF calculation start time

## display isis statistics

### Syntax

```
display isis statistics [ level-1 | level-2 | level-1-2 ] [ process-id | vpn-instance vpn-instance-name ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**level-1**: Displays IS-IS Level-1 statistics.

**level-2**: Displays IS-IS Level-2 statistics.

**level-1-2**: Displays IS-IS Level-1-2 statistics.

*process-id*: Displays IS-IS statistics for the IS-IS process. The ID is in the range of 1 to 65535.

*vpn-instance-name*: Displays IS-IS statistics for the VPN instance. The name is a string of 1 to 31 characters.

### Description

Use the **display isis statistics** command to display IS-IS statistics.

### Examples

```
# Display IS-IS statistics.
```

```
<Sysname> display isis statistics
```

```
Statistics information for ISIS(1)
```

```
-----
```

```
Level-1 Statistics
```

```
-----
```

```
Learnt routes information:
```

```
Total IPv4 Learnt Routes in IPv4 Routing Table: 1
```

Total IPv6 Learnt Routes in IPv6 Routing Table: 0

Imported routes information:

IPv4 Imported Routes:

```

Static: 0      Direct: 0
ISIS:   0      BGP:    0
RIP:    0      OSPF:   0

```

IPv6 Imported Routes:

```

Static: 0      Direct: 0
ISISv6: 0     BGP4+: 0
RIPng:  0     OSPFv3: 0

```

Lsp information:

```

LSP Source ID:      No. of used LSPs
0000.0000.0003      002

```

**Table 1-14 display isis statistics** command output description

Field		Description
Statistics information for ISIS( <i>processid</i> )		Statistics for the IS-IS process
Level-1 Statistics		Level-1 Statistics
Level-2 Statistics		Level-2 Statistics
Learnt routes information		Number of learnt IPv4 routes Number of learnt IPv6 routes
Imported routes information	IPv4 Imported Routes	Redistributed IPv4 routes <ul style="list-style-type: none"> <li>• Static</li> <li>• Direct</li> <li>• IS-IS</li> <li>• BGP</li> <li>• RIP</li> <li>• OSPF</li> </ul>
	IPv6 Imported Routes	Redistributed IPv6 routes <ul style="list-style-type: none"> <li>• Static</li> <li>• Direct</li> <li>• IS-ISv6</li> <li>• BGP4+</li> <li>• RIPng</li> <li>• OSPFv3</li> </ul>
Lsp information		LSP information <ul style="list-style-type: none"> <li>• LSP Source ID: ID of the source system</li> <li>• No. of used LSPs: number of used LSPs</li> </ul>

## domain-authentication-mode

### Syntax

**domain-authentication-mode** { md5 | simple } password [ ip | osi ]

## undo domain-authentication-mode

### View

IS-IS view

### Default Level

2: System level

### Parameters

**md5**: Specifies the MD5 authentication mode.

**simple**: Specifies the simple authentication mode.

*password*: Specifies a password. For **simple** authentication mode, the *password* must be plain text. For **md5** authentication mode, the password can be either plain text or cipher text. A plain text password can be a string of up to 16 characters, such as **user918**. A cipher password must be a string of 24 characters, such as **\_(TT8F]Y!5SQ=^Q`MAF4<1!!**.

**ip**: Checks IP related fields in LSPs.

**osi**: Checks OSI related fields in LSPs.



#### Note

Whether a password should use **ip** or **osi** is not affected by the actual network environment.

---

### Description

Use the **domain-authentication-mode** command to specify the routing domain authentication mode and a password.

Use the **undo domain-authentication-mode** command to restore the default.

No routing domain authentication is configured by default

The configured password in the specified mode is inserted into all outgoing Level-2 packets (LSP, CSNP and PSNP) and is used for authenticating the incoming Level-2 packets.

Note that:

- All the backbone routers must have the same authentication mode and password.
- If neither **ip** nor **osi** is specified, the OSI related fields in LSPs are checked.

Related commands: **area-authentication-mode**, **isis authentication-mode**.

### Examples

# Specify the routing domain authentication mode as **simple** and password as **123456**.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] domain-authentication-mode simple 123456
```

## filter-policy export (IS-IS view)

### Syntax

```
filter-policy { acl-number | ip-prefix ip-prefix-name | route-policy route-policy-name } export  
[ protocol [ process-id ] ]  
undo filter-policy export [ protocol [ process-id ] ]
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

*acl-number*: Specifies the number of an ACL that is used to filter redistributed routes, ranging from 2000 to 3999. For ACL configuration information, refer to *ACL Commands* in the *Security Volume*.

**ip-prefix** *ip-prefix-name*: Specifies the name of an IP prefix list that is used to filter redistributed routes, a string of 1 to 19 characters. For IP prefix list configuration information, refer to *Routing Policy Commands* in the *IP Routing Volume*.

**route-policy** *route-policy-name*: Specifies the name of a routing policy that is used to filter redistributed routes, a string of 1 to 19 characters. For routing policy configuration information, refer to *Routing Policy Commands* in the *IP Routing Volume*.

*protocol*: Filters routes redistributed from the routing protocol, which can be BGP, direct, IS-IS, OSPF, RIP or static.

*process-id*: Process ID, in the range of 1 to 65535. It is optional only when the protocol is IS-IS, OSPF or RIP.

### Description

Use the **filter-policy export** command to configure IS-IS to filter redistributed routes.

Use the **undo filter-policy export** command to disable IS-IS from filtering redistributed routes.

IS-IS does not filter redistributed routes by default.

Related commands: **filter-policy import**.

### Examples

```
# Reference ACL 2000 to filter redistributed routes.
```

```
<Sysname> system-view  
[Sysname] isis  
[Sysname-isis-1] filter-policy 2000 export
```

## filter-policy import (IS-IS view)

### Syntax

```
filter-policy { acl-number | ip-prefix ip-prefix-name | route-policy route-policy-name } import  
undo filter-policy import
```

## View

IS-IS view

## Default Level

2: System level

## Parameters

**acl-number**: Specifies the number of an ACL that is used to filter routes calculated from received LSPs, ranging from 2000 to 3999. For ACL configuration information, refer to *ACL Commands* in the *Security Volume*.

**ip-prefix ip-prefix-name**: Specifies the name of an IP prefix list that is used to filter routes calculated from received LSPs, a string of 1 to 19 characters. For IP prefix list configuration information, refer to *Routing Policy Commands* in the *IP Routing Volume*.

**route-policy route-policy-name**: Specifies the name of a routing policy that is used to filter routes calculated from received LSPs, a string of 1 to 19 characters. For routing policy configuration information, refer to *Routing Policy Commands* in the *IP Routing Volume*.

## Description

Use the **filter-policy import** command to configure IS-IS to filter routes calculated from received LSPs.

Use the **undo filter-policy import** command to disable IS-IS from filtering routes calculated from received LSPs.

IS-IS does not filter routes calculated from received LSPs by default.

Related commands: **filter-policy export**.

## Examples

```
# Reference ACL 2000 to filter routes calculated from received LSPs.
```

```
<Sysname> system-view  
[Sysname] isis  
[Sysname-isis-1] filter-policy 2000 import
```

## flash-flood

### Syntax

```
flash-flood [  flood-count flooding-count |  max-timer-interval flooding-interval | [  level-1 |  level-2 ] ] *  
undo flash-flood [  level-1 |  level-2 ]
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

**flood-count** *flooding-count*: Specifies the maximum number of LSPs to be flooded before the next SPF calculation, ranging from 1 to 15. The default is 5.

**max-timer-interval** *flooding-interval*: Specifies the delay (in milliseconds) of the flash flooding, ranging from 10 to 50000. The default is 10.

**level-1**: Enables flash flooding for **level-1**.

**level-2**: Enables fast-flooding for **level-2**.

### Description

Use the **flash-flood** command to enable IS-IS LSP flash flooding.

Use the **undo flash-flood** command to disable IS-IS LSP flash flooding.

IS-IS LSP flash flooding is disabled by default.

If no level is specified, the command enables IS-IS LSP flash flooding for both Level-1 and Level-2.

### Examples

# Enable fast flooding and configure the maximum LSPs be sent as 10 and the delay time as 100 milliseconds.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] flash-flood flood-count 10 max-timer-interval 100
```

## graceful-restart (IS-IS view)

### Syntax

**graceful-restart**

**undo graceful-restart**

### View

IS-IS view

### Default Level

2: System level

### Parameters

None

### Description

Use the **graceful-restart** command to enable IS-IS Graceful Restart capability.

Use the **undo graceful-restart** command to disable IS-IS Graceful Restart capability.

By default, IS-IS Graceful Restart capability is disabled.

### Examples

# Enable the Graceful Restart capability for IS-IS process 1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] graceful-restart
```

## graceful-restart interval (IS-IS view)

### Syntax

```
graceful-restart interval interval-value  
undo graceful-restart interval
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

*interval-value*: Graceful Restart interval, in the range 30 to 1800 seconds.

### Description

Use the **graceful-restart interval** command to configure the Graceful Restart interval.

Use the **undo graceful-restart interval** command to restore the default Graceful Restart interval.

By default, the Graceful Restart interval is 300 seconds.

### Examples

```
# Configure the Graceful Restart interval for IS-IS process 1 as 120 seconds.
```

```
<Sysname> system-view  
[Sysname] isis 1  
[Sysname-isis-1] graceful-restart interval 120
```

## graceful-restart suppress-sa

### Syntax

```
graceful-restart suppress-sa  
undo graceful-restart suppress-sa
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

None

### Description

Use the **graceful-restart suppress-sa** command to suppress the SA (Suppress-Advertisement) bit during restart.

Use the **undo graceful-restart suppress-sa** command to set the SA bit.

By default, the SA bit is set during restart.

Suppressing the SA bit is mainly for avoiding black hole route. If a router starts or reboots without keeping the local forwarding table, sending packets to the router may result in a severe packet loss. To avoid this, you can set the SA bit of the hello packet sent by the GR Restarter to 1. Upon receiving such hello packets, the GR Helpers will not advertise the GR Restarter through LSP.

## Examples

```
# Suppress the SA bit during Graceful Restart.
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] graceful-restart suppress-sa
```

## import-route (IS-IS view)

### Syntax

```
import-route protocol [ process-id | all-processes | allow-ibgp ] [ cost cost | cost-type { external | internal } ] [ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ] *
undo import-route protocol [ process-id | all-processes ]
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

*protocol*: Redistributes routes from a routing protocol, which can be BGP, direct, IS-IS, OSPF, RIP or static.

*process-id*: Process ID, in the range of 1 to 65535. It is available only when the protocol is IS-IS, OSPF or RIP.

**all-processes**: Redistributes routes from all the processes of the specified routing protocol. This keyword takes effect only when the protocol is **rip**, **ospf**, or **isis**.

**allow-ibgp**: Allows redistribution of IBGP routes. It is available when the protocol is BGP.

*cost*: Specifies a cost for redistributed routes.

The range of the cost depends on its style:

- For the styles of narrow, narrow-compatible and compatible, the cost ranges from 0 to 63.
- For the styles of wide, wide-compatible, the cost ranges from 0 to 16777215.

**cost-type** { **external** | **internal** }: Specifies the cost type. The **internal** type indicates internal routes, and the **external** type indicates external routes. If **external** is specified, the cost of a redistributed route to be advertised is added by 64 to make internal routes take priority over external routes. The type is **external** by default. The keywords are available only when the cost type is **narrow**, **narrow-compatible** or **compatible**.

**level-1**: Redistributes routes into the Level-1 routing table.

**level-2**: Redistributes routes into the Level-2 routing table. If no level is specified, the routes are redistributed into the Level-2 routing table by default.

**level-1-2**: Redistributes routes into both Level-1 and Level-2 routing tables.

**route-policy** *route-policy-name*: Redistributes only routes satisfying the matching conditions of a routing policy, the name of which is a string of 1 to 19 characters.

**tag** *tag*: Specifies a tag value for redistributed routes from 1 to 4294967295.

## Description

Use the **import-route** command to redistribute routes from another routing protocol or another IS-IS process.

Use the **undo import-route** command to disable route redistribution from another routing protocol or another IS-IS process.

No route redistribution is configured by default.

IS-IS takes all the redistributed routes as external routes to destinations outside the IS-IS routing domain.

Related commands: **import-route isis level-2 into level-1**.



### Caution

- Using the **import-route bgp** command redistributes only EBGP routes. Using the **import-route bgp allow-ibgp** command redistributes both EBGP and IBGP routes, but this may cause routing loops; be cautious with this command.
  - Only active routes can be redistributed. You can use the **display ip routing-table protocol** command to display route state information.
- 

## Examples

# Redistribute static routes and set the cost to 15.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] import-route static cost 15
```

## import-route isis level-2 into level-1

### Syntax

```
import-route isis level-2 into level-1 [ filter-policy { acl-number | ip-prefix ip-prefix-name | route-policy route-policy-name } | tag tag ] *
```

```
undo import-route isis level-2 into level-1
```

### View

IS-IS view

### Default Level

2: System level

## Parameters

**acl-number**: Specifies the number of an ACL that is used to filter routes from Level-2 to Level-1, ranging from 2000 to 3999. For ACL configuration information, refer to *ACL Commands* in the *Security Volume*.

**ip-prefix ip-prefix-name**: Specifies the name of an IP prefix list that is used to filter routes from Level-2 to Level-1, a string of 1 to 19 characters. For IP prefix list configuration information, refer to *Routing Policy Commands* in the *IP Routing Volume*.

**route-policy route-policy-name**: Specifies the name of a routing policy that is used to filter routes from Level-2 to Level-1, a string of 1 to 19 characters. For routing policy configuration information, refer to *Routing Policy Commands* in the *IP Routing Volume*.

**tag tag**: Specifies a tag value from 1 to 4294967295 for redistributed routes.

## Description

Use the **import-route isis level-2 into level-1** command to enable route leaking from Level-2 to Level-1.

Use the **undo import-route isis level-2 into level-1** command to disable routing leaking.

No route leaking is configured by default.

Note that:

- You can specify a routing policy in the **import-route isis level-2 into level-1** command to filter routes from Level-2 to Level-1. Other routing policies specified for route reception and redistribution does not affect the route leaking.
- If a filter policy is configured, only routes passing it can be advertised into the Level-1 area.

Related commands: **import-route**.

## Examples

```
# Enable route leaking from Level-2 to Level-1.
```

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] import-route isis level-2 into level-1
```

## import-route limit (IS-IS view)

### Syntax

```
import-route limit number
```

```
undo import-route limit
```

### View

```
IS-IS view
```

### Default Level

```
2: System level
```

### Parameters

**number**: Maximum number of redistributed Level 1/Level 2 IPv4 routes. in the range 1 to 12288.

## Description

Use the **import-route limit** command to configure the maximum number of redistributed Level 1/Level 2 IPv4 routes.

Use the **undo import-route limit** command to restore the default.

By default, the maximum number of redistributed Level 1/Level 2 IPv4 routes is 12288.

## Examples

# Configure IS-IS process 1 to redistribute up to 1000 Level 1/Level 2 IPv4 routes.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] import-route limit 1000
```

## isis

### Syntax

```
isis [ process-id ] [ vpn-instance vpn-instance-name ]
undo isis [ process-id ]
```

### View

System view

### Default Level

2: System level

### Parameters

*process-id*: Process ID, ranging from 1 to 65535. The default is 1.

*vpn-instance-name*: VPN instance name, a string of 1 to 31 characters.

## Description

Use the **isis** command to enable an IS-IS process and specify an associated VPN instance and/or enter IS-IS view.

Use the **undo isis** command to disable an IS-IS process.

Related commands: **isis enable**, **network-entity**.

## Examples

# Enable IS-IS routing process 1, with the system ID being 0000.0000.0002, and area ID being 01.0001.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] network-entity 01.0001.0000.0000.0002.00
```

## isis authentication-mode

### Syntax

```
isis authentication-mode { md5 | simple } password [ level-1 | level-2 ] [ ip | osi ]
```

**undo isis authentication-mode [ level-1 | level-2 ]**

## View

Interface view

## Default Level

2: System level

## Parameters

**md5**: Specifies the MD5 authentication mode.

**simple**: Specifies the simple authentication mode.

*password*: Specifies a password. For **simple** authentication mode, the *password* must be plain text. For **md5** authentication mode, the password can be either plain text or ciphertext. A plain text password can be a string of up to 16 characters, such as **user918**. A cipher password must be a string of 24 characters, such as **\_(TT8F]Y5SQ=^Q`MAF4<1!!**.

**level-1**: Sets the password for Level-1.

**level-2**: Sets the password for Level-2.

**ip**: Checks IP related fields in LSPs and SNPs.

**osi**: Checks OSI related fields in LSPs and SNPs.



### Note

- This command is not available in loopback interface view.
  - Whether a password should use **ip** or **osi** is not affected by the actual network environment.
- 

## Description

Use the **isis authentication-mode** command to set the IS-IS authentication mode and password for an interface.

Use the **undo isis authentication-mode** command to restore the default.

No neighbor relationship authentication is configured by default.

The password in the specified mode is inserted into all outgoing hello packets and is used for authenticating the incoming hello packets. Only the authentication succeeds can the neighbor relationship be formed.

Note that:

- For two routers to become neighbors, the same authentication mode and password must be specified at both ends.
- If you set a password without specifying a level, the password applies to both Level-1 and Level-2.
- If neither **ip** nor **osi** is specified, the OSI related fields in LSPs are checked.
- The **level-1** and **level-2** keywords are available only on the VLAN interfaces of switches after IS-IS is enabled on the interfaces with the **isis enable** command.

Related commands: **area-authentication-mode**, **domain authentication-mode**.

## Examples

```
# Set the plain text password tangshi for VLAN-interface 10.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis authentication-mode simple tangshi level-1
```

## isis circuit-level

### Syntax

```
isis circuit-level [ level-1 | level-1-2 | level-2 ]
undo isis circuit-level
```

### View

Interface view

### Default Level

2: System level

### Parameters

**level-1**: Sets the circuit level to Level-1.  
**level-1-2**: Sets the circuit level to Level-1-2.  
**level-2**: Sets the circuit level to Level-2.

### Description

Use the **isis circuit-level** command to set the circuit level for the interface.

Use the **undo isis circuit-level** command to restore the default.

An interface can establish either the Level-1 or Level-2 adjacency by default.

Note that:

For a Level-1 (Level-2) router, the circuit level can only be Level-1 (Level-2). For a Level-1-2 router, you need to specify a circuit level for a specific interface to form only the specified level neighbor relationship.

Related commands: **is-level**.

## Examples

```
# VLAN-interface 10 is connected to a non backbone router in the same area. Configure the circuit level
of VLAN-interface 10 as Level-1 to prevent sending and receiving Level-2 Hello packets.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis enable
[Sysname-Vlan-interface10] isis circuit-level level-1
```

## isis circuit-type p2p

### Syntax

```
isis circuit-type p2p
```

## undo isis circuit-type

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **isis circuit-type p2p** command to configure the network type for an interface as P2P.

Use the **undo isis circuit-type** command to cancel the configuration.

By default, the network type of a switch's VLAN interface is broadcast.

Interfaces with different network types operate differently. For example, broadcast interfaces on a network need to elect a DIS and flood CSNP packets to synchronize the LSDBs, while P2P interfaces on a network need not elect a DIS and have a different LSP synchronization mechanism.

If there are only two routers on a broadcast network, you can configure the network type of attached interfaces as P2P to avoid DIS election and CSNP flooding, saving network bandwidth and speeding up network convergence.



#### Note

- You can perform this configuration only for a broadcast network with only two attached routers.
  - This command is not supported in loopback interface view.
- 

### Examples

# Configure the network type of VLAN-interface 10 as P2P.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis enable
[Sysname-Vlan-interface10] isis circuit-type p2p
```

### isis cost

#### Syntax

**isis cost** *value* [ **level-1** | **level-2** ]

**undo isis cost** [ **level-1** | **level-2** ]

#### View

Interface view

## Default Level

2: System level

## Parameters

*value*: Specifies an IS-IS cost for the interface. The cost range differs with cost styles.

- For cost styles **narrow**, **narrow-compatible** and **compatible**, the cost ranges from 1 to 63.
- For cost styles **wide** and **wide-compatible**, the cost ranges from 1 to 16777215.

**level-1**: Applies the cost to Level-1.

**level-2**: Applies the cost to Level-2.

## Description

Use the **isis cost** command to set the IS-IS cost of an interface.

Use the **undo isis cost** command to restore the default.

No cost is configured by default.

If neither **level-1** nor **level-2** is included, the cost applies to both **level-1** and **level-2**.

You are recommended to configure a proper IS-IS cost for each interface to guarantee correct route calculation.

Relate command: **circuit-cost**.

## Examples

```
# Configure the Level-2 IS-IS cost as 5 for VLAN-interface10.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis cost 5 level-2
```

## isis dis-name

### Syntax

```
isis dis-name symbolic-name
```

```
undo isis dis-name
```

### View

Interface view

## Default Level

2: System level

## Parameters

*symbolic-name*: Specifies a DIS name, a string of 1 to 64 characters.

## Description

Use the **isis dis-name** command to configure a name for a DIS to represent the pseudo node on a broadcast network.

Use the **undo isis dis-name** command to remove the configuration.

No name is configured for the DIS by default.

Note that this command takes effect only on a router that must have dynamic system ID to host name mapping enabled. This command is not supported on a Point-to-Point interface.



#### Note

This command is not available in loopback interface view.

---

## Examples

```
# Configure the DIS name as LOCALAREA.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis dis-name LOCALAREA
```

## isis dis-priority

### Syntax

```
isis dis-priority value [ level-1 | level-2 ]
undo isis dis-priority [ level-1 | level-2 ]
```

### View

Interface view

### Default Level

2: System level

### Parameters

*value*: Specifies a DIS priority for the interface, ranging from 0 to 127.

**level-1**: Applies the DIS priority to Level-1.

**level-2**: Applies the DIS priority to level-2.

### Description

Use the **isis dis-priority** command to specify a DIS priority at a specified level for an interface.

Use the **undo isis dis-priority** command to restore the default priority of 64 for Level-1 and Level-2.

If neither level-1 nor level-2 is specified in this command, the DIS priority applies to both Level-1 and Level-2.

On an IS-IS broadcast network, a router should be elected as the DIS at each routing level. You can specify a DIS priority at a level for an interface. The greater the interface's priority is, the more likelihood it becomes the DIS. If multiple routers in the broadcast network have the same highest DIS priority, the router with the highest SNPA (Subnetwork Point of Attachment) address (SNPA addresses are MAC addresses on a broadcast network) becomes the DIS.

There is no backup DIS in IS-IS and the router with a priority of 0 can also participate in DIS election.

---



This command is not available in loopback interface view.

---

## Examples

# Configure the level-2 DIS priority as 127 for VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis dis-priority 127 level-2
```

## isis enable

### Syntax

```
isis enable [ process-id ]
undo isis enable
```

### View

Interface view

### Default Level

2: System level

### Parameters

*process-id*: Specifies a IS-IS process ID, ranging from 1 to 65535. The default is 1.

### Description

Use the **isis enable** command to enable an IS-IS process on the interface.

Use the **undo isis enable** command to disable IS-IS.

No IS-IS routing process is enabled on an interface by default.

Related commands: **isis**, **network-entity**.

## Examples

# Create IS-IS routing process 1, and enable the IS-IS routing process on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
[Sysname-isis-1] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis enable 1
```

## isis mesh-group

### Syntax

```
isis mesh-group { mesh-group-number | mesh-blocked }  
undo isis mesh-group
```

### View

Interface view

### Default Level

2: System level

### Parameters

*mesh-group-number*: Mesh group number, ranging from 1 to 4294967295.

**mesh-blocked**: Blocks the interface, which sends LSPs only after receiving LSP requests.

### Description

Use the **isis mesh-group** command to add the interface into a specified mesh group or block the interface.

Use the **undo isis mesh-group** command to restore the default.

By default, an interface does not belong to any mesh group.

For an interface not in a mesh group, it follows the normal process to flood the received LSPs to other interfaces. For the NBMA network with high connectivity and multiple point-to-point links, this will cause repeated LSP flooding and bandwidth waste.

After an interface is added to a mesh group, it will only flood a received LSP or a generated LSP to interfaces not belonging to the same mesh group.

If you block an interface, the interface can send LSPs only after receiving LSP requests.



#### Note

- The mesh-group feature is only available for a point-to-point link interface.
  - This command is not available in loopback interface view.
- 

### Examples

```
# Add IS-IS enabled VLAN-interface 10 to the mesh-group 3. .  
<Sysname> system-view  
[Sysname] interface vlan-interface 10  
[Sysname-Vlan-interface10] isis mesh-group 3
```

## isis mib-binding

### Syntax

```
isis mib-binding process-id  
undo isis mib-binding
```

### View

System view

### Default Level

2: System level

### Parameters

*process-id*: IS-IS process ID, in the range 1 to 65535.

### Description

Use the **isis mib-binding** command to bind MIBs with an IS-IS process.

Use the **undo isis mib-binding** command to restore the default.

By default, MIBs are bound with IS-IS process 1.

### Examples

```
# Bind MIBs with IS-IS process 100.  
<Sysname> system-view  
[Sysname] isis mib-binding 100
```

## isis silent

### Syntax

```
isis silent  
undo isis silent
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **isis silent** command to disable the interface from sending and receiving IS-IS packets.

Use the **undo isis silent** command to restore the default.

By default, an interface is not disabled from sending and receiving IS-IS packets.



#### Note

The feature is not supported on the loopback interface.

---

### Examples

```
# Disable VLAN-interface 10 from sending and receiving IS-IS packets.
<Sysname> system-view
[Sysname] interface vlan-interface10
[Sysname-Vlan-interface10] isis silent
```

### isis small-hello

#### Syntax

```
isis small-hello
undo isis small-hello
```

#### View

Interface view

#### Default Level

2: System level

#### Parameters

None

#### Description

Use the **isis small-hello** command to configure the interface to send small hello packets without CLVs.

Use the **undo isis small-hello** command to restore the default.

An interface sends standard hello packets by default.



#### Note

This command is not available in loopback interface view.

---

### Examples

```
# Configure VLAN-interface 10 to send small Hello packets.
<Sysname> system-view
[Sysname] interface vlan-interface10
[Sysname-Vlan-interface10] isis small-hello
```

## isis timer csnp

### Syntax

```
isis timer csnp seconds [ level-1 | level-2 ]  
undo isis timer csnp [ level-1 | level-2 ]
```

### View

Interface view

### Default Level

2: System level

### Parameters

*seconds*: Specifies on the DIS of a broadcast network the interval in seconds for sending CSNP packets, ranging from 1 to 600.

**level-1**: Applies the interval to Level-1.

**level-2**: Applies the interval to Level-2.

### Description

Use the **isis timer csnp** command to specify on the DIS of a broadcast network the interval for sending CSNP packets.

Use the **undo isis timer csnp** command to restore the default.

The default CSNP interval is 10 seconds.



#### Note

- If no level is specified, the CSNP interval applies to both Level-1 and Level-2.
  - This command only applies to the DIS of a broadcast network, which sends CSNP packets periodically for LSDB synchronization.
  - This command is not supported in loopback interface view.
- 

### Examples

```
# Configure Level-2 CSNP packets to be sent every 15 seconds over VLAN-interface 10.
```

```
<Sysname> system-view  
[Sysname] interface vlan-interface 10  
[Sysname-Vlan-interface10] isis timer csnp 15 level-2
```

## isis timer hello

### Syntax

```
isis timer hello seconds [ level-1 | level-2 ]  
undo isis timer hello [ level-1 | level-2 ]
```

## View

Interface view

## Default Level

2: System level

## Parameters

**seconds**: Specifies the interval in seconds for sending hello packets, ranging from 3 to 255.

**level-1**: Specifies the interval for sending Level-1 hello packets.

**level-2**: Specifies the interval for sending Level-2 hello packets.

## Description

Use the **isis timer hello** command to specify the interval for sending hello packets.

Use the **undo isis timer hello** command to restore the default.

The default hello interval is 10 seconds.



### Note

- Level-1 and Level-2 hello packets are sent independently on a broadcast network, so you need to specify an interval for the two levels respectively. On a P2P link, Level-1 and Level-2 packets are both sent in P2P hello packets, and you need not specify an interval for two levels respectively.
  - As the shorter the interval is, the more system resources will be occupied, you should configure a proper interval as needed.
  - If no level is specified, the hello interval applies to both Level-1 and Level-2.
  - This command is not supported in loopback interface view.
- 

Related commands: **isis timer holding-multiplier**.

## Examples

# Configure Level-2 Hello packets to be sent every 20 seconds over VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis timer hello 20 level-2
```

## isis timer holding-multiplier

### Syntax

**isis timer holding-multiplier** *value* [ **level-1** | **level-2** ]

**undo isis timer holding-multiplier** [ **level-1** | **level-2** ]

### View

Interface view

## Default Level

2: System level

## Parameters

*value*: Number of hello intervals, in the range of 3 to 1000.

**level-1**: Applies the number to the Level-1 IS-IS neighbor.

**level-2**: Applies the number to the Level-2 IS-IS neighbor.



### Note

This command is not available in loopback interface view.

---

## Description

Use the **isis timer holding-multiplier** command to specify the IS-IS hello multiplier.

Use the **undo isis timer holding-multiplier** command to restore the default.

The default IS-IS hello multiplier is 3.

If no level is specified, the hello multiplier applies to the current level.

With the IS-IS hello multiplier configured, a router can use hello packets to notify its neighbor router of the adjacency hold time (hello multiplier times hello interval). If the neighbor router receives no hello packets from this router within the hold time, it declares the adjacency down. You can adjust the adjacency hold time by changing the hello multiplier or the hello interval on an interface.

Level-1 and Level-2 hello packets are sent independently on a broadcast network, so you need to specify a hello multiplier for the two levels respectively. On a P2P link, Level-1 and Level-2 packets are both sent in P2P hello packets, and you need not specify Level-1 or Level-2.

Related commands: **isis timer hello**.

## Examples

# Configure the number of Level-2 Hello intervals as 6 for interface VLAN-interface, that is, if no Hello packet is received from the interface within 6 hello intervals, the IS-IS neighbor is considered dead.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis timer holding-multiplier 6
```

## isis timer lsp

### Syntax

**isis timer lsp** *time* [ **count** *count* ]

**undo isis timer lsp**

### View

Interface view

## Default Level

2: System level

## Parameters

*time*: Specifies the minimum interval in milliseconds for sending link-state packets, ranging from 1 to 1000.

*count*: Specifies the maximum number of link-state packets to be sent at one time, in the range of 1 to 1000. The default is 5.

## Description

Use the **isis timer lsp** command to configure the minimum interval for sending LSPs on the interface and specify the maximum LSPs that can be sent per time.

Use the **undo isis timer lsp** command to restore the default of 33ms.

Related commands: **isis timer retransmit**.



### Note

This command is not available in loopback interface view.

---

## Examples

# Configure the interval as 500 milliseconds for sending LSPs on interface VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis timer lsp 500
```

## isis timer retransmit

### Syntax

**isis timer retransmit** *seconds*

**undo isis timer retransmit**

### View

Interface view

## Default Level

2: System level

## Parameters

*seconds*: Specifies the interval in seconds for retransmitting LSP packets, ranging from 1 to 300.

## Description

Use the **isis timer retransmit** command to configure the interval for retransmitting LSP packets over a point-to-point link.

Use the **undo isis timer retransmit** command to restore the default.

By default, the retransmission interval is 5 seconds.

A P2P link requires a response to a sent LSP. If no response is received within the retransmission interval, the LSP is retransmitted.

You need not use this command over a broadcast link where CNSPs are broadcast periodically.

Related commands: **isis timer lsp**.

---



#### Note

- This command is not available in loopback interface view.
  - Configure a proper retransmission interval to avoid unnecessary retransmissions.
  - Perform this configuration only when the link layer protocol is PPP.
- 

## Examples

```
# Configure the LSP retransmission interval as 10 seconds for Vlan-interface 10.
```

```
<Sysname> system-view
[Sysname] interface Vlan-interface 10
[Sysname-Vlan-interface10] isis timer retransmit 10
```

## is-level

### Syntax

```
is-level { level-1 | level-1-2 | level-2 }
```

```
undo is-level
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

**level-1**: Configures the router to work on Level-1, which means it only calculates routes within the area, and maintains the L1 LSDB.

**level-1-2**: Configures the router to work on Level-1-2, which means it calculates routes and maintains the LSDBs for both L1 and L2.

**level-2**: Configures the router to work on Level-2, which means it calculates routes and maintains the LSDB for L2 only.

### Description

Use the **is-level** command to specify the IS level.

Use the **undo is-level** command to restore the default.

The default IS level is **level-1-2**.

You can configure all the routers as either Level-1 or Level-2 if there is only one area, because there is no need for all routers to maintain two identical databases at the same time. If the only area is an IP network, you are recommended to configure all the routers as Level-2 for scalability.

Related commands: **isis circuit-level**.

## Examples

```
# Configure the router to work in Level-1.
```

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] is-level level-1
```

## is-name

### Syntax

```
is-name sys-name
undo is-name
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

*symbolic-name*: Specifies a host name for the local IS, a string of 1 to 64 characters.

### Description

Use the **is-name** command to specify a host name for the IS to enable dynamic system ID to hostname mapping.

Use the **undo is-name** command to disable dynamic system ID to hostname mapping.

Dynamic system ID to hostname mapping is not enabled by default.

## Examples

```
# Configure a host name for the local IS.
```

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] is-name RUTA
```

## is-name map

### Syntax

```
is-name map sys-id map-sys-name
undo is-name map sys-id
```

## View

IS-IS view

## Default Level

2: System level

## Parameters

*sys-id*: System ID or pseudonode ID of a remote IS.

*map-sys-name*: Specifies a host name for the remote IS, a string of 1 to 64 characters.

## Description

Use the **is-name map** command to configure a system ID to host name mapping for a remote IS.

Use the **undo is-name map** command to remove the mapping.

Each remote IS system ID corresponds to only one name.

## Examples

```
# Map the host name RUTB to the system ID 0000.0000.0041 of the remote IS.
```

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] is-name map 0000.0000.0041 RUTB
```

## is-snmp-traps enable

### Syntax

```
is-snmp-traps enable
```

```
undo is-snmp-traps
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

None

### Description

Use the **is-snmp-traps enable** command to enable the SNMP Trap function of IS-IS.

Use the **undo is-snmp-traps** command to disable this function.

SNMP Trap is enabled by default.

### Examples

```
# Enable SNMP Trap.
```

```
<Sysname> system-view
[Sysname] isis
```

```
[Sysname-isis-1] is-snmp-traps enable
```

## log-peer-change (IS-IS view)

### Syntax

```
log-peer-change  
undo log-peer-change
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

None

### Description

Use the **log-peer-change** command to enable the logging of IS-IS neighbor state changes.

Use the **undo log-peer-change** command to disable the logging.

The logging is enabled by default.

After the logging is enabled, information about IS-IS adjacency state changes is sent to the configuration terminal.

### Examples

```
# Enable logging on the IS-IS adjacency state changes.
```

```
<Sysname> system-view  
[Sysname] isis  
[Sysname-isis-1] log-peer-change
```

## lsp-fragments-extend

### Syntax

```
lsp-fragments-extend [ [ level-1 | level-2 | level-1-2 ] [ mode-1 | mode-2 ] ] *  
undo lsp-fragments-extend
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

**mode-1**: Fragment extension mode 1, used on a network where some routers do not support LSP fragment extension.

**mode-2:** Fragment extension mode 2, used on a network where all routers support LSP fragment extension.

**level-1:** Applies the fragment extension mode to Level-1 LSPs.

**level-2:** Applies the fragment extension mode to Level-2 LSPs.

**level-1-2:** Applies the fragment extension mode to both Level-1 and Level-2 LSPs.

## Description

Use the **lsp-fragments-extend** command to enable an LSP fragment extension mode for a level.

Use the **undo lsp-fragments-extend** command to disable LSP fragment extension for a level.

LSP fragment extension is disabled by default.

Note that:

- If no mode is specified, LSP fragment extension mode 1 is enabled.
- If no level is specified, the LSP fragment extension mode is enabled for both Level-1 and Level-2.

## Examples

```
# Enable LSP fragment extension mode 1 for Level-2.
```

```
<Sysname> system-view
```

```
[Sysname] isis
```

```
[Sysname-isis-1] lsp-fragments-extend mode-1 level-2
```

## lsp-length originate

### Syntax

```
lsp-length originate size [ level-1 | level-2 ]
```

```
undo lsp-length originate [ level-1 | level-2 ]
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

**size:** Specifies the maximum size in bytes of LSP packets, ranging from 512 to 16384.

**level-1:** Applies the size to Level-1 LSP packets.

**level-2:** Applies the size to Level-2 LSP packets.

## Description

Use the **lsp-length originate** command to configure the maximum size of generated Level-1 or Level-2 LSPs.

Use the **undo lsp-length originate** command to restore the default.

By default, the maximum size of generated Level-1 and Level-2 LSPs is 1497 bytes.



## Note

If neither Level-1 nor Level-2 is specified in the command, the configured maximum size applies to the current IS-IS level.

---

## Examples

# Configure the maximum size of the generated Level-2 LSPs as 1024 bytes.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] lsp-length originate 1024 level-2
```

## Isp-length receive

### Syntax

```
Isp-length receive size
undo Isp-length receive
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

*size*: Maximum size of received LSPs, in the range of 512 to 16384 bytes.

### Description

Use the **Isp-length receive** command to configure the maximum size of received LSPs.

Use the **undo Isp-length receive** command to restore the default.

By default, the maximum size of received LSPs is 1497 bytes.

## Examples

# Configure the maximum size of received LSPs.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] lsp-length receive 1024
```

## maximum load-balancing (IS-IS view)

### Syntax

```
maximum load-balancing number
undo maximum load-balancing
```

## View

IS-IS view

## Default Level

2: System level

## Parameters

*number*: Maximum number of equal-cost routes for load balancing., in the range 1 to 4.

## Description

Use the **maximum load-balancing** command to configure the maximum number of equal-cost routes for load balancing.

Use the **undo maximum load-balancing** command to restore the default.

By default, the maximum number of equal-cost load balanced routes is 4.

## Examples

# Configure the maximum number of equal-cost load-balanced routes as 2.

```
<Sysname> system-view
[Sysname] isis 100
[Sysname-isis-100] maximum load-balancing 2
```

# Restore the default.

```
[Sysname-isis-100] undo maximum load-balancing
```

## network-entity

### Syntax

**network-entity** *net*

**undo network-entity** *net*

### View

IS-IS view

### Default Level

2: System level

### Parameters

*net*: Network Entity Title (NET) in the format of X...X.XXXX...XXXX.00, with the first part X...X being the area address, the middle part XXXX...XXXX (a total of 12 "X") being the router's system ID and the last part 00 being SEL.

### Description

Use the **network-entity** command to configure the Network Entity Title for an IS-IS routing process.

Use the **undo network-entity** command to delete a NET.

No NET is configured by default.

Related commands: **isis**, **isis enable**.

## Examples

```
# Specify the NET as 10.0001.1010.1020.1030.00, of which 10.0001 is the area ID and
1010.1020.1030 is the system ID.
```

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
```

## preference (IS-IS view)

### Syntax

```
preference { preference | route-policy route-policy-name } *
undo preference
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

*preference*: Specifies the preference for IS-IS protocol, ranging from 1 to 255.

**route-policy** *route-policy-name*: Routing policy name, a string of 1 to 19 characters. The preference applies to routes passing the routing policy.

### Description

Use the **preference** command to configure the preference for IS-IS.

Use the **undo preference** command to restore the default.

By default, IS-IS preference is 15.

If a routing policy is specified in this command, the preference (if any) set by the routing policy applies to those matched routes. Other routes use the preference set by the **preference** command.

When a router runs multiple routing protocols at the same time, the system will configure a preference to each routing protocol. If several protocols find routes to the same destination, the route of the routing protocol with the highest preference is selected.

### Examples

```
# Configure the preference of IS-IS protocol as 25.
```

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] preference 25
```

## reset isis all

### Syntax

```
reset isis all [ process-id | vpn-instance vpn-instance-name ]
```

## View

User view

## Default Level

3: Manage level

## Parameters

*process-id*: Clears the data structure information of an IS-IS process numbered from 1 to 65535.

**vpn-instance** *vpn-instance-name*: Clears the data structure information of a VPN instance named with a string of 1 to 31 characters.

## Description

Use the **reset isis all** command to clear all IS-IS data structure information.

No data structure information is cleared by default.

This command is used when the LSP needs to be updated immediately. For example, after performing the **area-authentication-mode** and **domain-authentication-mode** commands, you can use this command to clear old LSPs.

Related commands: **area-authentication-mode**, **domain authentication-mode**.

## Examples

```
# Clear all IS-IS data structure information.
```

```
<Sysname> reset isis all
```

## reset isis peer

### Syntax

```
reset isis peer system-id [ process-id | vpn-instance vpn-instance-name ]
```

## View

User view

## Default Level

3: Manage level

## Parameters

*system-id*: Specifies the system ID of an IS-IS neighbor.

*process-id*: Clears the data structure information of an IS-IS process with an ID from 1 to 65535.

*vpn-instance-name*: Clears the data structure information of a VPN instance named with a string of 1 to 31 characters.

## Description

Use the **reset isis peer** command to clear the data structure information of a specified IS-IS neighbor.

This command is used when you need to re-establish an IS-IS neighbor relationship.

## Examples

```
# Clear the data structure information of the neighbor with the system ID 0000.0c11.1111.  
<Sysname> reset isis peer 0000.0c11.1111
```

## set-overload

### Syntax

```
set-overload [ on-startup [ [ start-from-nbr system-id [ timeout1 [ nbr-timeout ] ] ] | timeout2 ] [ allow  
{ external | interlevel } * ]  
undo set-overload
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

**on-startup**: Sets the overload bit upon system startup.

**start-from-nbr** *system-id*: Starts the *nbr-timeout* timer when the router begins to establish the neighbor relationship with the neighbor. If the neighbor relationship is formed within the *nbr-timeout* interval, IS-IS keeps the overload bit set; if not, the bit is cleared. *system-id* specifies the neighbor.

*timeout1*: IS-IS keeps the overload bit set within the *timeout1* interval after the neighbor relationship is formed within the *nbr-timeout* interval. The *timeout1* interval is in the range 5 to 86400 seconds and defaults to 600 seconds.

*nbr-timeout*: The timer is started when the router begins to establish the neighbor relationship with the neighbor after system startup. The timer has an interval from 5 to 86400 seconds. The default is 1200 seconds.

*timeout2*: Sets the overload bit within the *timeout2* interval after system startup. The interval is in the range 5 to 86400 seconds and defaults to 600 seconds.

**allow**: Allows advertising address prefixes. By default, no address prefixes are allowed to be advertised when the overload bit is set.

**external**: Allows advertising IP address prefixes redistributed from other routing protocols with the **allow** keyword specified.

**interlevel**: Allows advertising IP address prefixes learnt from different IS-IS levels with the **allow** keyword specified.

### Description

Use the **set-overload** command to set the overload bit.

Use the **undo set-overload** command to clear the overload bit.

The overload bit is not set by default.

Note that:

- If the **on-startup** keyword is not specified, the command sets the overload bit immediately until the **undo set-overload** command is executed.

- If the **on-startup** keyword is specified, IS-IS sets the overload bit upon system startup and keeps it set within the *timeout2* interval.
- If both **on-startup** and **start-from-nbr** *system-id* are specified, IS-IS sets the overload bit from system startup to when the neighbor relationship with the specified neighbor is formed within the *nbr-timeout* interval, and from then on, IS-IS keeps the overload bit set within the *timeout1* interval. If the neighbor relationship with the specified neighbor is not formed within the *nbr-timeout* interval, the overload bit is cleared.

## Examples

```
# Set overload flag on the current router.
```

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] set-overload
```

## summary (IS-IS view)

### Syntax

```
summary ip-address { mask | mask-length } [ avoid-feedback | generate_null0_route | [ level-1 | level-1-2 | level-2 ] | tag tag ] *
```

```
undo summary ip-address { mask | mask-length } [ level-1 | level-1-2 | level-2 ]
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

*ip-address*: Destination IP address of the summary route.

*mask*: Mask of the destination IP address, in dotted decimal format.

*mask-length*: Mask length, in the range of 0 to 32.

**avoid-feedback**: Avoids learning summary routes by route calculation.

**generate\_null0\_route**: Generate the Null 0 route to avoid routing loops.

**level-1**: Summarize only the routes redistributed to Level-1.

**level-1-2**: Summarizes the routes redistributed to both Level-1 and Level-2.

**level-2**: Summarizes only the routes redistributed to Level-2.

**tag** *tag*: Specifies a management tag, in the range of 1 to 4294967295.

### Description

Use the **summary** command to configure a summary route.

Use the **undo summary** command to remove a summary route.

No summarization is configured by default.

If no level is specified, only the **level-2** routes will be summarized by default.

You can summarize multiple contiguous networks into a single network to reduce the size of the routing table, as well as that of LSP and LSDB generated by the router. It is allowed to summarize native IS-IS routes and redistributed routes. After summarization, the cost of the summary route is the smallest cost of those summarized routes.

Note that the router summarizes only routes in local LSPs.

## Examples

```
# Configure a summary route of 202.0.0.0/8.
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] summary 202.0.0.0 255.0.0.0
```

## timer lsp-generation

### Syntax

```
timer lsp-generation maximum-interval [ initial-interval [ second-wait-interval ] ] [ level-1 | level-2 ]
undo timer lsp-generation [ level-1 | level-2 ]
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

*maximum-interval*: Maximum wait interval in seconds for generating IS-IS LSPs, in the range 1 to 120.

*initial-interval*: Initial wait interval in milliseconds before generating the first IS-IS LSP, in the range 10 to 60000. The default is 0.

*second-wait-interval*: Wait interval in milliseconds before generating the second LSP, in the range 10 to 60000. The default is 0.

**level-1**: Applies the intervals to Level-1.

**level-2**: Applies the intervals to Level-2. If no level is specified, the specified intervals apply to both Level-1 and Level-2.

### Description

Use the **timer lsp-generation** command to specify the wait interval before generating IS-IS LSPs.

Use the **undo timer lsp-generation** command to restore the default.

By default, the wait interval before LSP generation is 2 seconds.

Note that:

- 1) If only the maximum interval is specified, IS-IS waits the maximum interval before generating an LSP.
- 2) If both the maximum and initial intervals are specified:
  - IS-IS waits the initial interval before generating the first LSP.

- If the network topology is unstable, that is, triggers occur at intervals shorter than the maximum interval, IS-IS waits the maximum interval before generating the first LSP until the network topology is stable.
- 3) If the maximum, initial, and second wait intervals are specified:
- IS-IS waits the initial interval before generating the first LSP.
  - If the network topology is unstable, that is, triggers occur at intervals shorter than the maximum interval,, IS-IS waits the *second-wait-interval* before generating the second LSP and penalty is applied on the wait interval before generating the next LSP. That is, for each subsequent trigger, the wait interval before generating the LSP will be two times the previous wait interval until the maximum interval is reached.
  - After the network topology is stable; that is, triggers occur at intervals greater than the maximum interval, the wait interval before generating LSPs is restored to the initial interval.

## Examples

# Set the maximum, initial, and second wait intervals to 10 seconds, 100 milliseconds and 200 milliseconds respectively.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1]timer lsp-generation 10 100 200
```

# Set the LSP generation interval to 15 seconds.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1]timer lsp-generation 15
```

## timer lsp-max-age

### Syntax

**timer lsp-max-age** *seconds*

**undo timer lsp-max-age**

### View

IS-IS view

### Default Level

2: System level

### Parameters

*seconds*: Specifies the LSP maximum aging time in seconds, ranging from 1 to 65535.

### Description

Use the **timer lsp-max-age** command to set the LSP maximum age in the LSDB.

Use the **undo timer lsp-max-age** command to restore the default.

The default LSP maximum age is 1200 seconds.

Related commands: **timer lsp-refresh**.

## Examples

```
# Set the maximum LSP age to 1500 seconds.
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] timer lsp-max-age 1500
```

## timer lsp-refresh

### Syntax

```
timer lsp-refresh seconds
undo timer lsp-refresh
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

*seconds*: LSP refresh interval in seconds, ranging from 1 to 65534.

### Description

Use the **timer lsp-refresh** command to configure the LSP refresh interval.

Use the **undo timer lsp-refresh** to restore the default.

The default LSP refresh interval is 900 seconds.

Related commands: **timer lsp-max-age**.



### Note

To refresh LSPs before they are aged out, the interval configured by the **timer lsp-refresh** command must be smaller than that configured by the **timer lsp-max-age** command.

---

## Examples

```
# Configure the LSP refresh interval as 1500 seconds.
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] timer lsp-refresh 1500
```

## timer spf

### Syntax

```
timer spf maximum-interval [initial-interval [second-interval ] ]
```

## undo timer spf

### View

IS-IS view

### Default Level

2: System level

### Parameters

*maximum-interval*: Maximum SPF calculation interval in seconds, ranging from 1 to 120.

*initial-interval*: Wait interval before the first SPF calculation, in milliseconds, ranging from 10 to 60000.

*second-interval*: Wait interval before the second SPF calculation, in milliseconds, ranging from 10 to 60000.

### Description

Use the **timer spf** command to set the SPF calculation interval.

Use the **undo timer spf** command to restore the default.

The default IS-IS SPF calculation interval is 10 seconds.

Note that:

- 1) If only the maximum interval is specified, IS-IS waits the maximum interval before performing the SPF calculation.
- 2) If both the maximum and initial intervals are specified:
  - IS-IS waits the initial interval before performing the first SPF calculation.
  - When SPF calculation triggers occur at intervals shorter than the maximum interval, the topology is considered unstable and IS-IS waits the maximum interval before performing the SPF calculation until the topology is stable.
- 3) If *maximum-interval*, *initial-interval*, and *second-interval* are specified:
  - IS-IS waits the initial interval before performing the first SPF calculation.
  - When SPF calculation triggers occur at intervals shorter than the maximum interval, the topology is considered unstable, IS-IS will wait the *second-interval* before performing the second SPF calculation and penalty is applied on the wait interval for the next SPF calculation. That is, for each subsequent trigger, the wait interval before SPF calculation will be two times the previous wait interval until the maximum interval is reached.
  - After the network topology becomes stable; that is, triggers occur at intervals greater than the maximum interval, the wait interval before SPF calculation is restored to the initial interval.

### Examples

# Configure the maximum SPF calculation interval as 10 seconds, the wait interval before the first SPF calculation as 100 milliseconds, and the wait interval before the second SPF calculation as 200 milliseconds.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1]timer spf 10 100 200
```

# Configure the maximum SPF calculation interval as 15 seconds.

```
<Sysname> system-view
[Sysname] isis
```

```
[Sysname-isis-1] timer spf 15
```

## virtual-system

### Syntax

```
virtual-system virtual-system-id  
undo virtual-system virtual-system-id
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

*virtual-system-id*: Virtual system ID of the IS-IS process.

### Description

Use the **virtual-system** command to configure a virtual system ID for the IS-IS process. Use the **undo virtual-system** command to remove a virtual system ID.

Up to 50 virtual system IDs can be configured for the IS-IS process.

### Examples

# Set a virtual system ID of 2222.2222.2222 for IS-IS process 1.

```
<Sysname> system-view  
[Sysname] isis  
[Sysname-isis-1] virtual-system 2222.2222.2222
```

# Table of Contents

<b>1 BGP Configuration Commands</b> .....	<b>1-1</b>
BGP Configuration Commands.....	1-1
aggregate .....	1-1
balance (BGP/BGP-VPN instance view) .....	1-2
bestroute as-path-neglect (BGP/BGP-VPN instance view).....	1-3
bestroute compare-med (BGP/BGP-VPN instance view) .....	1-4
bestroute med-confederation (BGP/BGP-VPN instance view) .....	1-5
bgp.....	1-5
compare-different-as-med (BGP/BGP-VPN instance view).....	1-6
confederation id .....	1-7
confederation nonstandard.....	1-8
confederation peer-as.....	1-8
dampening (BGP/BGP-VPN instance view).....	1-9
default ipv4-unicast.....	1-10
default local-preference (BGP/BGP-VPN instance view).....	1-11
default med (BGP/BGP-VPN instance view).....	1-12
default-route imported (BGP/BGP-VPN instance view) .....	1-13
display bgp group .....	1-13
display bgp network.....	1-15
display bgp paths.....	1-16
display bgp peer .....	1-17
display bgp routing-table .....	1-19
display bgp routing-table as-path-acl .....	1-20
display bgp routing-table cidr .....	1-21
display bgp routing-table community.....	1-22
display bgp routing-table community-list .....	1-23
display bgp routing-table dampened .....	1-23
display bgp routing-table dampening parameter.....	1-24
display bgp routing-table different-origin-as .....	1-25
display bgp routing-table flap-info .....	1-26
display bgp routing-table label.....	1-27
display bgp routing-table peer .....	1-28
display bgp routing-table regular-expression .....	1-29
display bgp routing-table statistic .....	1-29
ebgp-interface-sensitive .....	1-30
filter-policy export (BGP/BGP-VPN instance view) .....	1-31
filter-policy import (BGP/BGP-VPN instance view) .....	1-32
graceful-restart (BGP view).....	1-32
graceful-restart timer restart .....	1-33
graceful-restart timer wait-for-rib .....	1-34
group (BGP/BGP-VPN instance view) .....	1-34
import-route (BGP/BGP-VPN instance view) .....	1-35
log-peer-change .....	1-36

network (BGP/BGP-VPN instance view) .....	1-37
network short-cut (BGP/BGP-VPN instance view) .....	1-38
peer advertise-community (BGP/BGP-VPN instance view) .....	1-39
peer advertise-ext-community (BGP/BGP-VPN instance view) .....	1-39
peer allow-as-loop (BGP/BGP-VPN instance view) .....	1-40
peer as-number (BGP/BGP-VPN instance view) .....	1-41
peer as-path-acl (BGP/BGP-VPN instance view) .....	1-42
peer capability-advertise conventional .....	1-43
peer capability-advertise route-refresh .....	1-44
peer connect-interface (BGP/BGP-VPN instance view) .....	1-44
peer default-route-advertise (BGP/BGP-VPN instance view) .....	1-45
peer description (BGP/BGP-VPN instance view) .....	1-46
peer ebgp-max-hop (BGP/BGP-VPN instance view) .....	1-47
peer enable (BGP view) .....	1-48
peer fake-as (BGP/BGP-VPN instance view) .....	1-48
peer filter-policy (BGP/BGP-VPN instance view) .....	1-49
peer group (BGP/BGP-VPN instance view) .....	1-50
peer ignore (BGP/BGP-VPN instance view) .....	1-51
peer ip-prefix .....	1-52
peer keep-all-routes (BGP/BGP-VPN instance view) .....	1-53
peer log-change (BGP/BGP-VPN instance view) .....	1-53
peer next-hop-local (BGP/BGP-VPN instance view) .....	1-54
peer password .....	1-55
peer preferred-value (BGP/BGP-VPN instance view) .....	1-56
peer public-as-only (BGP/BGP-VPN instance view) .....	1-57
peer reflect-client (BGP/BGP-VPN instance view) .....	1-58
peer route-limit (BGP/BGP-VPN instance view) .....	1-59
peer route-policy (BGP/BGP-VPN instance view) .....	1-60
peer route-update-interval (BGP/BGP-VPN instance view) .....	1-61
peer substitute-as (BGP/BGP-VPN instance view) .....	1-61
peer timer (BGP/BGP-VPN instance view) .....	1-62
preference (BGP/BGP-VPN instance view) .....	1-63
reflect between-clients (BGP view) .....	1-64
reflector cluster-id (BGP view) .....	1-65
refresh bgp .....	1-65
reset bgp .....	1-66
reset bgp dampening .....	1-67
reset bgp flap-info .....	1-67
reset bgp ipv4 all .....	1-68
router-id .....	1-68
summary automatic .....	1-69
synchronization (BGP view) .....	1-70
timer (BGP/BGP-VPN instance view) .....	1-71

# 1 BGP Configuration Commands

---



## Note

The term “router” in this document refers to a generic router or an Ethernet switch running routing protocols.

---

## BGP Configuration Commands

---



## Note

For more information about routing policy configuration commands in this document, refer to *Routing Policy Commands* in the *IP Routing Volume*.

---

## aggregate

### Syntax

```
aggregate ip-address { mask | mask-length } [ as-set | attribute-policy route-policy-name |  
detail-suppressed | origin-policy route-policy-name | suppress-policy route-policy-name ] *  
undo aggregate ip-address { mask | mask-length }
```

### View

BGP view, BGP-VPN instance view

### Default Level

2: System level

### Parameters

*ip-address*: Summary address.

*mask*: Summary route mask, in dotted decimal notation.

*mask-length*: Length of summary route mask, in the range 0 to 32.

**as-set**: Creates a summary with AS set.

**attribute-policy** *route-policy-name*: Sets the attributes of the summary route according to the routing policy. The routing policy name is a string of 1 to 19 characters.

**detail-suppressed:** Only advertises the summary route.

**suppress-policy** *route-policy-name*: Suppresses specific routes defined in the routing policy. The routing policy name is a string of 1 to 19 characters.

**origin-policy** *route-policy-name*: References the routing policy to specify routes for summarization. The routing policy name is a string of 1 to 19 characters.

The keywords of the command are described as follows:

**Table 1-1** Functions of the keywords

Keywords	Function
<b>as-set</b>	Used to create a summary route, whose AS path contains the AS path information of summarized routes. Use this keyword carefully when many AS paths need to be summarized, because the frequent changes of these specific routes may lead to route oscillation.
<b>detail-suppressed</b>	This keyword does not suppress the summary route, but it suppresses the advertisement of all the more specific routes. To summarize only some specific routes, use the <b>peer filter-policy</b> command.
<b>suppress-policy</b>	Used to create a summary route and suppress the advertisement of some summarized routes. If you want to suppress some routes selectively and leave other routes still advertised, use the <b>if-match</b> clause of the <b>route-policy</b> command.
<b>origin-policy</b>	Selects only routes satisfying the routing policy for route summarization.
<b>attribute-policy</b>	Sets attributes except the AS-PATH attribute for the summary route. The same work can be done by using the <b>peer route-policy</b> command.

## Description

Use the **aggregate** command to create a summary route in the BGP routing table.

Use the **undo aggregate** command to remove a summary route.

By default, no summary route is configured.

## Examples

# In BGP view, create a summary of 192.213.0.0/16 in the BGP routing table.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] aggregate 192.213.0.0 255.255.0.0
```

# In BGP-VPN instance view, create a summary of 192.213.0.0/16 in BGP routing table (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] aggregate 192.213.0.0 255.255.0.0
```

## balance (BGP/BGP-VPN instance view)

### Syntax

**balance** *number*

**undo balance**

## View

BGP view/VPN instance view

## Default Level

2: System level

## Parameters

*number*: Number of BGP routes for load balancing. in the range 1 to 4.. When it is set to 1, load balancing is disabled.

## Description

Use the **balance** command to configure the number of BGP routes for load balancing.

Use the **undo balance** command to disable load balancing.

By default, no load balancing is configured.

Unlike IGP, BGP has no explicit metric for making load balancing decision. Instead, it implements load balancing using route selection rules.

Related commands: **display bgp routing-table**.

## Examples

# In BGP view, set the number of routes participating in BGP load balancing to 2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] balance 2
```

# In BGP-VPN instance view, set the number of routes participating in BGP load balancing to 2 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] balance 2
```

## **bestroute as-path-neglect (BGP/BGP-VPN instance view)**

### Syntax

**bestroute as-path-neglect**

**undo bestroute as-path-neglect**

### View

BGP view, BGP-VPN instance view

### Default Level

2: System level

### Parameters

None

## Description

Use the **bestroute as-path-neglect** command to configure BGP not to consider the AS\_PATH during best route selection.

Use the **undo bestroute as-path-neglect** command to configure BGP to consider the AS\_PATH during best route selection.

By default, BGP considers the AS\_PATH during best route selection.

## Examples

# In BGP view, ignore AS\_PATH in route selection.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] bestroute as-path-neglect
```

# In BGP-VPN instance view, ignore AS\_PATH in route selection (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] bestroute as-path-neglect
```

## bestroute compare-med (BGP/BGP-VPN instance view)

### Syntax

```
bestroute compare-med
undo bestroute compare-med
```

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

None

### Description

Use the **bestroute compare-med** command to enable the comparison of the MED for paths from each AS.

Use the **undo bestroute compare-med** command to disable this comparison.

This comparison is not enabled by default.

## Examples

# In BGP view, enable the comparison of MEDs for paths from each AS when selecting the best route.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] bestroute compare-med
```

# In BGP-VPN instance view, enable the comparison of MED for paths from each AS when selecting the best route. (The VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] bestroute compare-med
```

## bestroute med-confederation (BGP/BGP-VPN instance view)

### Syntax

```
bestroute med-confederation
undo bestroute med-confederation
```

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

None

### Description

Use the **bestroute med-confederation** command to enable the comparison of the MED for paths from confederation peers during best route selection.

Use the **undo bestroute med-confederation** command to disable the comparison.

The comparison is not enabled by default.

The system only compares MED values for paths from peers within the confederation. Paths from external ASs are advertised throughout the confederation without MED comparison.

### Examples

# In BGP view, enable the comparison of the MED for paths from peers within the confederation.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] bestroute med-confederation
```

# In BGP-VPN instance view, enable the comparison of the MED for paths from peers within the confederation. (The VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] bestroute med-confederation
```

## bgp

### Syntax

```
bgp as-number
```

**undo bgp** [ *as-number* ]

### View

System view

### Default Level

2: System level

### Parameters

*as-number*: Specifies the local AS number from 1 to 65535.

### Description

Use the **bgp** command to enable BGP and enter the BGP view.

Use the **undo bgp** command to disable BGP.

By default, BGP is not enabled.

### Examples

```
# Enable BGP and set local AS number to 100.
```

```
<Sysname> system-view
```

```
[Sysname] bgp 100
```

```
[Sysname-bgp]
```

## compare-different-as-med (BGP/BGP-VPN instance view)

### Syntax

**compare-different-as-med**

**undo compare-different-as-med**

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

None

### Description

Use the **compare-different-as-med** command to enable the comparison of the MED for paths from peers in different ASs.

Use the **undo compare-different-as-med** command to disable the comparison.

The comparison is disabled by default.

If several paths to one destination are available, the path with the smallest MED is selected.

Do not use this command unless associated ASs adopt the same IGP protocol and routing selection method.

## Examples

# In BGP view, enable the comparison of the MED for paths from peers in different ASs.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] compare-different-as-med
```

# In BGP-VPN instance view, enable the comparison of the MED for paths from peers in different ASs (The VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] compare-different-as-med
```

## confederation id

### Syntax

**confederation id** *as-number*

**undo confederation id**

### View

BGP view

### Default Level

2: System level

### Parameters

*as-number*: Number of the AS that contains multiple sub-ASs, in the range 1 to 65535.

### Description

Use the **confederation id** command to configure a confederation ID.

Use the **undo confederation id** command to remove a specified confederation.

By default, no confederation ID is configured.

Configuring a confederation can reduce IBGP connections in a large AS. You can split the AS into several sub-ASs, and each sub-AS remains fully meshed. These sub-ASs form a confederation. Key IGP attributes of a route, such as the next hop, MED, local preference, are not discarded when crossing each sub-AS. The sub-ASs still look like a whole from the perspective of other ASs. This can ensure the integrity of the former AS, and solve the problem of too many IBGP connections in the AS.

Related commands: **confederation nonstandard** and **confederation peer-as**.

## Examples

# Confederation 9 consists of four sub-ASs, namely, 38, 39, 40 and 41. The peer 10.1.1.1 is a member of the confederation while the peer 200.1.1.1 is outside of the confederation. Take sub AS 41 as an example.

```
<Sysname> system-view
[Sysname] bgp 41
[Sysname-bgp] confederation id 9
```

```
[Sysname-bgp] confederation peer-as 38 39 40
[Sysname-bgp] group Confed38 external
[Sysname-bgp] peer Confed38 as-number 38
[Sysname-bgp] peer 10.1.1.1 group Confed38
[Sysname-bgp] group Remote98 external
[Sysname-bgp] peer Remote98 as-number 98
[Sysname-bgp] peer 200.1.1.1 group Remote98
```

## confederation nonstandard

### Syntax

**confederation nonstandard**

**undo confederation nonstandard**

### View

BGP view

### Default Level

2: System level

### Parameters

None

### Description

Use the **confederation nonstandard** command to make the router compatible with routers not compliant with RFC3065 in the confederation.

Use the **undo confederation nonstandard** command to restore the default.

By default, all routers in the confederation comply with RFC3065.

All devices should be configured with this command to interact with those nonstandard devices in the confederation.

Related commands: **confederation id** and **confederation peer-as**.

### Examples

# AS100 contains routers not compliant with RFC3065 and comprises two sub-ASs, 64000 and 65000.

```
<Sysname> system-view
[Sysname] bgp 64000
[Sysname-bgp] confederation id 100
[Sysname-bgp] confederation peer-as 65000
[Sysname-bgp] confederation nonstandard
```

## confederation peer-as

### Syntax

**confederation peer-as** *as-number-list*

**undo confederation peer-as** [*as-number-list*]

## View

BGP view

## Default Level

2: System level

## Parameters

*as-number-list*: Sub-AS number list. Up to 32 sub-ASs can be configured in one command line. The expression is *as-number-list* = *as-number* &<1-32>, in which *as-number* specifies a sub-AS number, and &<1-32> indicates up to 32 numbers can be specified.

## Description

Use the **confederation peer-as** command to specify confederation peer sub-ASs.

Use the **undo confederation peer-as** command to remove specified confederation peer sub-ASs.

By default, no confederation peer sub-ASs are configured.

Before this configuration, the **confederation id** command must be used to specify the confederation for the sub-ASs.

If the **undo confederation peer-as** command without the *as-number-list* argument is used, all confederation peer sub-ASs are removed.

Related commands: **confederation nonstandard** and **confederation id**.

## Examples

```
# Specify confederation peer sub ASs 2000 and 2001.  
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] confederation id 10  
[Sysname-bgp] confederation peer-as 2000 2001
```

## dampening (BGP/BGP-VPN instance view)

### Syntax

**dampening** [ *half-life-reachable* *half-life-unreachable* *reuse* *suppress* *ceiling* | **route-policy** *route-policy-name* ] \*

**undo dampening**

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

*half-life-reachable*: Specifies a half-life for active routes from 1 to 45 minutes. By default, the value is 15 minutes.

*half-life-unreachable*: Specifies a half-life for suppressed routes from 1 to 45 minutes. By default, the value is 15 minutes.

*reuse*: Specifies a reuse threshold value for suppressed routes from 1 to 20000. A suppressed route whose penalty value decreases under the value is reused. By default, the reuse value is 750.

*suppress*: Specifies a suppression threshold from 1 to 20000. The route with a penalty value higher than the threshold is suppressed. The default value is 2000.

*ceiling*: Specifies a ceiling penalty value from 1001 to 20000. The value must be bigger than the *suppress* value. By default, the value is 16000.

*route-policy-name*: Routing policy name, a string of 1 to 19 characters.

*half-life-reachable*, *half-life-unreachable*, *reuse*, *suppress* and *ceiling* are mutually dependent. Once any one is configured, all the others should also be specified accordingly.

## Description

Use the **dampening** command to enable BGP route dampening and/or configure dampening parameters.

Use the **undo dampening** command to disable route dampening.

By default, no route dampening is configured.

The command dampens only EBGP routes rather than IBGP routes.

Related commands: **reset bgp dampening**, **reset bgp flap-info**, **display bgp routing-table dampened**, **display bgp routing-table dampening parameter** and **display bgp routing-table flap-info**.

## Examples

# In BGP view, configure BGP route dampening.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] dampening 15 15 1000 2000 10000
```

# In BGP-VPN instance view, configure BGP route dampening (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] dampening 15 15 1000 2000 10000
```

## default ipv4-unicast

### Syntax

**default ipv4-unicast**

**undo default ipv4-unicast**

### View

BGP view

### Default Level

2: System level

## Parameters

None

## Description

Use the **default ipv4-unicast** command to enable the default use of IPv4 unicast address family for the peers that are established using the **peer as-number** command.

Use the **undo default ipv4-unicast** command to disable the default use of IPv4 unicast address family for the peers that are established using the **peer as-number** command.

The use of IPv4 unicast address family is enabled by default.

Note that:

- The **default ipv4-unicast** or **undo default ipv4-unicast** command applies to only BGP peers that are established after it is executed.
- The **default ipv4-unicast** or **undo default ipv4-unicast** command applies to only BGP peers that are established using the **peer as-number** command.
- After executing the **undo default ipv4-unicast** command, you can use the **peer enable** command to enable the use of IPv4 address family for a peer.

## Examples

# Enable the default use of IPv4 unicast address family for the peers that are established using the **peer as-number** command.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] default ipv4-unicast
```

## default local-preference (BGP/BGP-VPN instance view)

### Syntax

**default local-preference** *value*

**undo default local-preference**

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

*value*: Default local preference, in the range 0 to 4294967295. The larger the value is, the higher the preference is.

### Description

Use the **default local-preference** command to configure the default local preference.

Use the **undo default local-preference** command to restore the default value.

By default, the default local preference is 100.

Using this command can affect BGP route selection.

## Examples

# In BGP view, set the default local preference to 180.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] default local-preference 180
```

# In BGP-VPN instance view, set the default local preference to 180 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] default local-preference 180
```

## default med (BGP/BGP-VPN instance view)

### Syntax

```
default med med-value
undo default med
```

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

*med-value*: Default MED value, in the range 0 to 4294967295.

### Description

Use the **default med** command to specify a default MED value.

Use the **undo default med** command to restore the default.

By default, the default *med-value* is 0.

Multi-exit discriminator (MED) is an external metric for routes. Different from local preference, MED is exchanged between ASs and will stay in the AS once it enters the AS. The route with a lower MED is preferred. When a router running BGP obtains several routes with an identical destination but different next-hops from various external peers, it will select the best route depending on the MED value. In the case that all other conditions are the same, the system first selects the route with the smallest MED as the best external route.

## Examples

# In BGP view, configure the default MED as 25.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] default med 25
```

# In BGP-VPN instance view, configure the default MED as 25 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
```

```
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] default med 25
```

## default-route imported (BGP/BGP-VPN instance view)

### Syntax

```
default-route imported
undo default-route imported
```

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

None

### Description

Use the **default-route imported** command to allow default route redistribution into the BGP routing table.

Use the **undo default-route imported** command to disallow the redistribution.

By default, default route redistribution is not allowed.

Using the **default-route imported** command cannot redistribute default routes. To do so, use the **import-route** command.

Related commands: **import-route**.

### Examples

# In BGP view, allow default route redistribution from OSPF into BGP.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] default-route imported
[Sysname-bgp] import-route ospf 1
```

# In BGP-VPN instance view, enable redistributing default route from OSPF into BGP (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] default-route imported
[Sysname-bgp-vpn1] import-route ospf 1
```

## display bgp group

### Syntax

```
display bgp group [ group-name ]
```

## View

Any view

## Default Level

1: Monitor level

## Parameters

*group-name*: Peer group name, a string of 1 to 47 characters.

## Description

Use the **display bgp group** command to display peer group information.

## Examples

# Display the information of the peer group **aaa**.

```
<Sysname> display bgp group aaa
BGP peer-group is aaa
Remote AS 200
Type : external
Maximum allowed prefix number: 4294967295
Threshold: 75%
Configured hold timer value: 180
Keepalive timer value: 60
Minimum time between advertisement runs is 30 seconds
Peer Preferred Value: 0
No routing policy is configured
Members:
Peer           V    AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down  State
-----
2.2.2.1       4    200      0        0      0      0 00:00:35 Active
```

**Table 1-2** display bgp group command output description

Field	Description
BGP peer-group	Name of the BGP peer group
Remote AS	AS number of peer group
type	Type of the BGP peer group: IBGP or EBGP
Maximum allowed prefix number	Maximum prefixes allowed to receive from the peer group
Threshold	Percentage of received prefixes from the peer group to maximum prefixes allowed to receive from the peer group; If the percentage is reached, the system generates alarm messages.
Configured hold timer value	Holdtime interval
Keepalive timer value	Keepalive interval
Minimum time between advertisement runs	Minimum interval for route advertisements
Peer Preferred Value	Preferred value specified for the routes from the peer

Field	Description
No routing policy is configured	No routing policy is configured.
Members	Detailed information of the members in the peer group
Peer	IPv4 address of the peer
V	BGP version running on the peer
AS	AS number of the peer
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages to be sent
PrefRcv	Number of prefixes received
Up/Down	The lasting time of the session/the lasting time of the current state (when no session is established)
State	State machine state of the peer

## display bgp network

### Syntax

**display bgp network**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display bgp network** command to display routing information advertised with the **network** command.

### Examples

# Display routing information advertised with the **network** command.

```
<Sysname> display bgp network
```

```
BGP Local Router ID is 10.1.4.2.
```

```
Local AS Number is 400.
```

```
Network          Mask          Route-policy    Short-cut
```

```
100.1.2.0        255.255.255.0
```

```
100.1.1.0        255.255.255.0
```

```
Short-cut
```

**Table 1-3 display bgp network** command output description

Field	Description
BGP Local Router ID	BGP Local Router ID
Local AS Number	Local AS Number
Network	Network address
Mask	Mask
Route-policy	Routing policy
Short-cut	Short-cut route

## display bgp paths

### Syntax

```
display bgp paths [ as-regular-expression ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*as-regular-expression*: AS path regular expression, a string of 1 to 80 characters.

### Description

Use the **display bgp paths** command to display information about BGP AS paths.

### Examples

# Display information about BGP paths matching the AS path regular expression.

```
<Sysname> display bgp paths ^200
```

```

Address      Hash      Refcount  MED      Path/Origin
0x5917100    11        1         0        200 300i
```

**Table 1-4 display bgp paths** command output description

Field	Description
Address	Route address in the local database, in dotted hexadecimal notation
Hash	Hash index
Refcount	Count of routes that reference the path
MED	MED of the path
Path	AS_PATH attribute of the path, recording the ASs it has passed to avoid routing loops

Field	Description	
Origin	Origin attribute of the path:	
	i	Indicates the route is interior to the AS. Summary routes and routes defined using the <b>network</b> command are considered IGP routes.
	e	Indicates that a route is learned from the exterior gateway protocol (EGP).
	?	Short for INCOMPLETE. It indicates that the origin of a route is unknown and the route is learned by other means.

## display bgp peer

### Syntax

```
display bgp peer [ ip-address { log-info | verbose } | group-name log-info | verbose ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ip-address*: IP address of an peer to be displayed, in dotted decimal notation.

*group-name*: Name of a peer group to be displayed, a string of 1 to 47 characters.

**log-info**: Displays the log information of the specified peer.

**verbose**: Displays the detailed information of the peer/peer group.

### Description

Use the **display bgp peer** command to display peer/peer group information.

### Examples

```
# Display the detailed information of the peer 10.110.25.20.
```

```
<Sysname> display bgp peer 10.110.25.20 verbose
```

```
Peer: 10.110.25.20 Local: 2.2.2.2
Type: EBGP link
BGP version 4, remote router ID 1.1.1.1
BGP current state: Established, Up for 00h01m51s
BGP current event: RecvKeepalive
BGP last state: OpenConfirm
Port: Local - 1029 Remote - 179
Configured: Active Hold Time: 180 sec Keepalive Time: 60 sec
Received : Active Hold Time: 180 sec
Negotiated: Active Hold Time: 180 sec
Peer optional capabilities:
Peer support bgp multi-protocol extended
```

Peer support bgp route refresh capability  
Address family IPv4 Unicast: advertised and received

Received: Total 5 messages, Update messages 1  
Sent: Total 4 messages, Update messages 0  
Maximum allowed prefix number: 4294967295  
Threshold: 75%  
Minimum time between advertisement runs is 30 seconds  
Optional capabilities:  
Route refresh capability has been enabled  
Peer Preferred Value: 0  
BFD: Enabled

Routing policy configured:  
No routing policy is configured

**Table 1-5 display bgp peer verbose** command output description

Field	Description
Peer	IP address of the peer
Local	Local router ID
Type	Peer type
BGP version	BGP version
remote router ID	Router ID of the peer
BGP current state	Current state of the peer
BGP current event	Current event of the peer
BGP last state	Previous state of the peer
Port	TCP port numbers of the local router and its peer
Configured: Active Hold Time	Local holdtime interval
Keepalive Time	Local keepalive interval
Received: Active Hold Time	Remote holdtime interval
Negotiated: Active Hold Time	Negotiated holdtime interval
Peer optional capabilities	Optional capabilities supported by the peer, including BGP multiprotocol extensions and route refresh
Address family IPv4 Unicast	Routes are advertised and received in IPv4 unicasts.
Received	Total numbers of received packets and updates
Sent	Total numbers of sent packets and updates
Maximum allowed prefix number	Maximum allowed prefix number
Threshold	Percentage of received prefixes from the peer group to maximum prefixes allowed to receive from the peer group; If the percentage is reached, the system generates alarm messages.
Minimum time between advertisement runs	Minimum route advertisement interval

Field	Description
Optional capabilities	Optional capabilities enabled by the peer
Peer Preferred Value	Preferred value specified for the routes from the peer
BFD	BFD is enabled or disabled.
Routing policy configured	Local routing policy

## display bgp routing-table

### Syntax

```
display bgp routing-table [ ip-address [ { mask | mask-length } [ longer-prefixes ] ] ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ip-address*: Destination IP address.

*mask*: Network mask, in dotted decimal notation.

*mask-length*: Mask length, in the range 0 to 32.

**longer-prefixes**: Matches the longest prefix.

### Description

Use the **display bgp routing-table** command to display specified BGP routing information in the BGP routing table.

### Examples

```
# Display BGP routing table information.
```

```
<Sysname> display bgp routing-table
```

```
Total Number of Routes: 1
```

```
BGP Local router ID is 10.10.10.1
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

```
Origin : i - IGP, e - EGP, ? - incomplete
```

```

Network          NextHop      MED          LocPrf      PrefVal Path/Ogn
* > 40.40.40.0/24  20.20.20.1   0            0           200 300i

```

**Table 1-6 display bgp routing** command output description

Field	Description	
Total Number of Routes	Total Number of Routes	
BGP Local router ID	BGP local router ID	
Status codes	Status codes: * – valid > – best d – damped h – history i – internal (IGP) s – summary suppressed (suppressed) S – Stale	
Origin	i – IGP (originated in the AS) e – EGP (learned through EGP) ? – incomplete (learned by some other means)	
Network	Destination network address	
Next Hop	Next hop IP address	
MED	MULTI_EXIT_DISC attribute	
LocPrf	Local preference value	
PrefVal	Preferred value of the route	
Path	AS_PATH attribute, recording the ASs the packet has passed to avoid routing loops	
PrefVal	Preferred value	
Ogn	Origin attribute of the route, which can be one of the following values:	
	i	Indicates that the route is interior to the AS. Summary routes and the routes injected with the <b>network</b> command are considered IGP routes.
	e	Indicates that the route is learned from the Exterior Gateway Protocol (EGP).
	?	Short for INCOMPLETE. It indicates that the origin of the route is unknown and the route is learned by other means.

## display bgp routing-table as-path-acl

### Syntax

**display bgp routing-table as-path-acl** *as-path-acl-number*

### View

Any view

## Default Level

1: Monitor level

## Parameters

*as-path-acl-number*: Displays routing information permitted by the AS path ACL, which is specified with a number from 1 to 256.

## Description

Use the **display bgp routing as-path-acl** command to display BGP routes permitted by an as-path ACL.

## Examples

# Display BGP routes permitted by AS path ACL 1.

```
<Sysname> display bgp routing-table as-path-acl 1
```

```
BGP Local router ID is 20.20.20.1
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

```
Origin : i - IGP, e - EGP, ? - incomplete
```

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*> 40.40.40.0/24	30.30.30.1	0		0	300i

Refer to [Table 1-6](#) for description on the fields above.

## display bgp routing-table cidr

### Syntax

```
display bgp routing-table cidr
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display bgp routing-table cidr** command to display BGP CIDR (Classless Inter-Domain Routing) routing information.

### Examples

# Display BGP CIDR routing information.

```
<Sysname> display bgp routing-table cidr
```

Total Number of Routes: 1

BGP Local router ID is 20.20.20.1

Status codes: \* - valid, > - best, d - damped,

h - history, i - internal, s - suppressed, S - Stale

Origin : i - IGP, e - EGP, ? - incomplete

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*> 40.40.40.0/24	30.30.30.1	0		0	300i

Refer to [Table 1-6](#) for description on the above fields.

## display bgp routing-table community

### Syntax

```
display bgp routing-table community [ aa:nn<1-13> ] [ no-advertise | no-export | no-export-subconfed ] * [ whole-match ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**aa:nn**: Community number. Both aa and nn are in the range 0 to 65535.

**<1-13>**: Argument before it can be entered up to 13 times.

**no-advertise**: Displays BGP routes that cannot be advertised to any peer.

**no-export**: Displays BGP routes that cannot be advertised out the AS. If a confederation is configured, it displays routes that cannot be advertised out the confederation, but can be advertised to other sub ASs in the confederation.

**no-export-subconfed**: Displays BGP routes that cannot be advertised out the AS or to other sub ASs in the configured confederation.

**whole-match**: Displays the BGP routes exactly matching the specified community attribute.

### Description

Use the **display bgp routing community** command to display BGP routing information with the specified BGP community attribute.

### Examples

```
# Display BGP routing information with the specified BGP community.
```

```
<Sysname> display bgp routing-table community 11:22
```

BGP Local router ID is 10.10.10.1

Status codes: \* - valid, > - best, d - damped,

h - history, i - internal, s - suppressed, S - Stale

Origin : i - IGP, e - EGP, ? - incomplete

	Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*>	10.10.10.0/24	0.0.0.0	0		0	i
*>	40.40.40.0/24	20.20.20.1			0	200 300i

Refer to [Table 1-6](#) for description on the fields above.

## display bgp routing-table community-list

### Syntax

```
display bgp routing-table community-list { basic-community-list-number [ whole-match ] | adv-community-list-number }&<1-16>
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*basic-community-list-number*: Specifies a basic community-list number from 1 to 99.

*adv-community-list-number*: Specifies an advanced community-list number from 100 to 199.

**whole-match**: Displays routes exactly matching the specified *basic-community-list*.

&<1-16>: Specifies the argument before it can be entered up to 16 times.

### Description

Use the **display bgp routing-table community-list** command to display BGP routing information matching the specified BGP community list.

### Examples

# Display BGP routing information matching BGP community list 100.

```
<Sysname> display bgp routing-table community-list 100
BGP Local router ID is 1.2.3.4
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network          NextHop      Metric      LocPrf      PrefVal Path
*>    3.3.3.0/30        1.2.3.4          0           0           ?
*>    4.4.0.0/20        1.2.3.4          0           0           ?
*>    4.5.6.0/26        1.2.3.4          0           0           ?
```

Refer to [Table 1-6](#) for description on the fields above.

## display bgp routing-table dampened

### Syntax

```
display bgp routing-table dampened
```

## View

Any view

## Default Level

1: Monitor level

## Parameters

None

## Description

Use the **display bgp routing-table dampened** command to display dampened BGP routes.

## Examples

# Display dampened BGP routes.

```
<Sysname> display bgp routing-table dampened
BGP Local router ID is 2.2.2.2
Status codes: * - valid, > - best, d - damped,
               h - history, i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
   Network          From          Reuse    Path/Origin
*d  77.0.0.0        12.1.1.1    00:29:20  100?
```

**Table 1-7** display bgp routing-table dampened command output description

Field	Description
From	IP address from which the route was received
Reuse	Reuse time of the route

Refer to [Table 1-6](#) for description on the other fields above.

## display bgp routing-table dampening parameter

### Syntax

**display bgp routing-table dampening parameter**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display bgp routing-table dampening parameter** command to display BGP route dampening parameters.

Related commands: **dampening**.

## Examples

# Display BGP route dampening parameters.

```
<Sysname> display bgp routing-table dampening parameter
Maximum Suppress Time(in second) : 3069
Ceiling Value                      : 16000
Reuse Value                        : 750
Reach HalfLife Time(in second)    : 900
Unreach HalfLife Time(in second): 900
Suppress-Limit                    : 2000
```

**Table 1-8** display bgp routing-table dampening parameter command output description

Field	Description
Maximum Suppress Time	Maximum Suppress Time
Ceiling Value	Ceiling penalty value
Reuse Value	Reuse value
Reach HalfLife Time(in second)	Half-life time of active routes
Unreach HalfLife Time(in second)	Half-life time of inactive routes
Suppress-Limit	Limit for a route to be suppressed

## display bgp routing-table different-origin-as

### Syntax

```
display bgp routing-table different-origin-as
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display bgp routing-table different-origin-as** command to display BGP routes originating from different autonomous systems.

## Examples

# Display BGP routes originating from different ASs.

```
<Sysname> display bgp routing-table different-origin-as
BGP Local router ID is 2.2.2.2
Status codes: * - valid, > - best, d - damped,
```

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*> 55.0.0.0	12.1.1.1	0		0	100?
*	14.1.1.2	0		0	300?

Refer to [Table 1-6](#) for description on the fields above.

## display bgp routing-table flap-info

### Syntax

```
display bgp routing-table flap-info [ regular-expression as-regular-expression | as-path-acl
as-path-acl-number | ip-address [ { mask | mask-length } [ longer-match ] ] ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*as-regular-expression*: Displays route flap information that matches the AS path regular expression, which is a string of 1 to 80 characters.

*as-path-acl-number*: Displays route flap information matching the AS path ACL. The number is in the range 1 to 256.

*ip-address*: Destination IP address.

*mask*: Mask, in dotted decimal notation.

*mask-length*: Mask length, in the range 0 to 32.

**longer-match**: Matches the longest prefix.

### Description

Use the **display bgp routing-table flap-info** command to display BGP route flap statistics.

### Examples

```
# Display BGP route flap statistics.
```

```
<Sysname> display bgp routing-table flap-info
```

```
BGP Local router ID is 2.2.2.2
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete
```

Network	From	Flaps	Duration	Reuse	Path/Origin
*> 55.0.0.0	12.1.1.1	2	00:00:16		100?
*d 77.0.0.0	12.1.1.1	5	00:34:02	00:27:08	100?

**Table 1-9** display bgp routing flap-info command output description

Field	Description
From	Source IP address of the route
Flaps	Number of routing flaps
Duration	Duration time of the flap route
Reuse	Reuse time of the route

Refer to [Table 1-6](#) for description on the other fields above.

## display bgp routing-table label

### Syntax

```
display bgp routing-table label
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display bgp routing-table label** command to display labeled BGP routing information.

### Examples

```
# Display labeled BGP routing information.
```

```
<Sysname> display bgp routing-table label
```

```
BGP Local router ID is 6.6.6.7
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

```
Origin : i - IGP, e - EGP, ? - incomplete
```

```
Total Number of Routes: 2
```

```
      Network          NextHop          In/Out Label
* >    4.4.4.4/32        127.0.0.1        3/NULL
* >    5.5.5.5/32        1.1.1.1          NULL/1024
```

The In/Out Label field refers to the inbound/outbound label. Refer to [Table 1-6](#) for the description of other fields.

## display bgp routing-table peer

### Syntax

```
display bgp routing-table peer ip-address { advertised-routes | received-routes }  
[ network-address [ mask | mask-length ] | statistic ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ip-address*: IP address of a peer.

**advertised-routes**: Displays routing information advertised to the specified peer.

**received-routes**: Displays routing information received from the specified peer.

*network-address*: IP address of the destination network.

*mask*: Mask of the destination network, in dotted decimal notation.

*mask-length*: Mask length, in the range 0 to 32.

**statistic**: Displays route statistics.

### Description

Use the **display bgp routing-table peer** command to display BGP routing information advertised to or received from the specified BGP peer.

Related commands: **display bgp peer**.

### Examples

```
# Display BGP routing information advertised to BGP peer 20.20.20.1.
```

```
<Sysname> display bgp routing-table peer 20.20.20.1 advertised-routes
```

```
Total Number of Routes: 2
```

```
BGP Local router ID is 30.30.30.1
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

```
Origin : i - IGP, e - EGP, ? - incomplete
```

	Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*>	30.30.30.0/24	0.0.0.0	0		0	i
*>	40.40.40.0/24	0.0.0.0	0		0	i

Refer to [Table 1-6](#) for description on the fields above.

## display bgp routing-table regular-expression

### Syntax

```
display bgp routing-table regular-expression as-regular-expression
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*as-regular-expression*: AS path regular expression, a string of 1 to 80 characters.

### Description

Use the **display bgp routing-table regular-expression** command to display BGP routing information matching the specified AS path regular expression.

### Examples

```
# Display BGP routing information matching AS path regular expression 300$.
```

```
<Sysname> display bgp routing-table regular-expression 300$
```

```
BGP Local router ID is 20.20.20.1
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

```
Origin : i - IGP, e - EGP, ? - incomplete
```

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*> 40.40.40.0/24	30.30.30.1	0		0	300i

Refer to [Table 1-6](#) for description on the fields above.

## display bgp routing-table statistic

### Syntax

```
display bgp routing-table statistic
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display bgp routing-table statistic** command to display BGP routing statistics.

## Examples

# Display BGP routing statistics.

```
<Sysname> display bgp routing-table statistic
```

```
Total Number of Routes: 4
```

**Table 1-10** display bgp routing-table statistic command output description

Field	Description
Total number of routes	Total number of routes

## ebgp-interface-sensitive

### Syntax

```
ebgp-interface-sensitive
```

```
undo ebgp-interface-sensitive
```

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

None

### Description

Use the **ebgp-interface-sensitive** command to enable the clearing of EBGp session on any interface that becomes down.

Use the undo **ebgp-interface-sensitive** command to disable the function.

This function is enabled by default.

## Examples

# In BGP view, enable the clearing of EBGp session on any interface that becomes down.

```
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] ebgp-interface-sensitive
```

# In BGP-VPN instance view, enable the clearing of EBGp session on any interface that becomes down (the VPN has been created).

```
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] ipv4-family vpn-instance vpn1  
[Sysname-bgp-vpn1] ebgp-interface-sensitive
```

## filter-policy export (BGP/BGP-VPN instance view)

### Syntax

```
filter-policy { acl-number | ip-prefix ip-prefix-name } export [ direct | isis process-id | ospf process-id | rip process-id | static ]
```

```
undo filter-policy export [ direct | isis process-id | ospf process-id | rip process-id | static ]
```

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

*acl-number*: Number of an ACL used to filter outgoing routing information, ranging from 2000 to 3999.

*ip-prefix-name*: Name of an IP prefix list used to filter outgoing routing information, a string of 1 to 19 characters.

**direct**: Filters direct routes.

**isis *process-id***: Filters outgoing routes redistributed from an ISIS process. The ID is in the range 1 to 65535.

**ospf *process-id***: Filters outgoing routes redistributed from the OSPF process with an ID from 1 to 65535.

**rip *process-id***: Filters outgoing routes redistributed from a RIP process. The ID is in the range 1 to 65535.

**static**: Filters static routes.

If no routing protocol is specified, all outgoing routes are filtered.

### Description

Use the **filter-policy export** command to configure the filtering of outgoing routes.

Use the **undo filter-policy export** command to remove the filtering.

If no routing protocol is specified, all redistributed routes are filtered when advertised.

By default, the filtering is not configured.

### Examples

# In BGP view, reference ACL 2000 to filter all outgoing routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] filter-policy 2000 export
```

# In BGP-VPN instance view, reference ACL 2000 to filter all outgoing routes (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] filter-policy 2000 export
```

## filter-policy import (BGP/BGP-VPN instance view)

### Syntax

```
filter-policy { acl-number | ip-prefix ip-prefix-name } import  
undo filter-policy import
```

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

*acl-number*: Number of an ACL used to filter incoming routing information, ranging from 2000 to 3999.

*ip-prefix-name*: Name of an IP prefix list used to filter incoming routing information, a string of 1 to 19 characters.

### Description

Use the **filter-policy import** command to configure the filtering of incoming routing information.

Use the **undo filter-policy import** command to disable the filtering.

By default, incoming routing information is not filtered.

### Examples

# In BGP view, reference ACL 2000 to filter incoming routing information.

```
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] filter-policy 2000 import
```

# In BGP-VPN instance view, reference ACL 2000 to filter incoming routing information (the VPN has been created).

```
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] ipv4-family vpn-instance vpn1  
[Sysname-bgp-vpn1] filter-policy 2000 import
```

## graceful-restart (BGP view)

### Syntax

```
graceful-restart  
undo graceful-restart
```

### View

BGP view

### Default Level

2: System level

## Parameters

None

## Description

Use the **graceful-restart** command to enable BGP Graceful Restart capability.

Use the **undo graceful-restart** command to disable BGP Graceful Restart capability.

By default, BGP Graceful Restart capability is disabled.



### Note

During main and backup boards switchover, a GR-capable BGP speaker can maintain the packet forwarding table. During restart, it may not maintain the forwarding table.

---

## Examples

```
# Enable the Graceful Restart capability for BGP process 100.
```

```
<Sysname> system-view
```

```
[Sysname] bgp 100
```

```
[Sysname-bgp] graceful-restart
```

## graceful-restart timer restart

### Syntax

```
graceful-restart timer restart timer
```

```
undo graceful-restart timer restart
```

### View

BGP view

### Default Level

2: System level

### Parameters

*timer*: Maximum time for a peer to reestablish a BGP session, in the range 3 to 600 seconds.

### Description

Use the **graceful-restart timer restart** command to configure the maximum time for a peer to reestablish a BGP session.

Use the **undo graceful-restart timer restart** command to restore the default.

By default, the maximum time for a peer to reestablish a BGP session is 150 seconds.

### Examples

```
# Configure the maximum time for a peer to reestablish a BGP session as 300 seconds.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] graceful-restart timer restart 300
```

## graceful-restart timer wait-for-rib

### Syntax

```
graceful-restart timer wait-for-rib timer
undo graceful-restart timer wait-for-rib
```

### View

BGP view

### Default Level

2: System level

### Parameters

*timer*: Time to wait for the End-of-RIB marker, in the range 3 to 300 seconds.

### Description

Use the **graceful-restart timer wait-for-rib** command to configure the time to wait for the End-of-RIB marker.

Use the **undo graceful-restart timer wait-for-rib** command to restore the default.

By default, the time to wait for the End-of-RIB marker is 180 seconds.



### Note

- After a BGP session has been successfully (re)established, the End-of-RIB marker must be received within the time specified with this command.
  - Using this command can speed up route convergence.
- 

### Examples

```
# Set the time to wait for the End-of-RIB marker to 100 seconds.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] graceful-restart timer wait-for-rib 100
```

## group (BGP/BGP-VPN instance view)

### Syntax

```
group group-name [ external | internal ]
undo group group-name
```

## View

BGP view/BGP-VPN instance view

## Default Level

2: System level

## Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

**external**: Creates an EBGP peer group, which can be the group of another sub AS in a confederation.

**internal**: Creates an IBGP peer group; not supported in BGP-VPN instance view.

## Description

Use the **group** command to create a peer group.

Use the **undo group** command to delete a peer group.

An IBGP peer group is created if neither **internal** nor **external** is specified.

## Examples

# In BGP view, create an EBGP peer group **test** with AS number 200, and add EBGP peers 10.1.1.1 and 10.1.2.1 into the group.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
[Sysname-bgp] peer test as-number 200
[Sysname-bgp] peer 10.1.1.1 group test
[Sysname-bgp] peer 10.1.2.1 group test
```

# In BGP-VPN instance view, create an EBGP peer group **test** with AS number 200, and add EBGP peers 10.1.1.1 and 10.1.2.1 into the group (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] group test external
[Sysname-bgp-vpn1] peer test as-number 200
[Sysname-bgp-vpn1] peer 10.1.1.1 group test
[Sysname-bgp-vpn1] peer 10.1.2.1 group test
```

## import-route (BGP/BGP-VPN instance view)

### Syntax

```
import-route protocol [ process-id | all-processes ] [ med med-value | route-policy route-policy-name ] *
```

```
undo import-route protocol [ process-id | all-processes ]
```

## View

BGP view/BGP-VPN instance view

## Default Level

2: System level

## Parameters

*protocol*: Redistributes routes from the specified routing protocol, which can be **direct**, **isis**, **ospf**, **rip** or **static** at present.

*process-id*: Process ID, in the range 1 to 65535. The default is 1. It is available only when the protocol is **isis**, **ospf**, or **rip**.

**all-processes**: Redistributes routes from all the processes of the specified protocol. This keyword takes effect only when the protocol is **rip**, **ospf**, or **isis**.

*med-value*: Specifies a MED value for redistributed routes, ranging from 0 to 4294967295. If the argument is not specified, the cost of the redistributed route is used as its MED in the BGP routing domain.

*route-policy-name*: Name of a routing policy used to filter redistributed routes, a string of 1 to 19 characters.

## Description

Use the **import-route** command to configure BGP to redistribute routes from a specified routing protocol and advertise redistributed routes.

Use the **undo import-route** command to disable route redistribution from a routing protocol.

By default, BGP does not redistribute routes from other protocols.

The ORIGIN attribute of routes redistributed with the **import-route** command is incomplete.

## Examples

# In BGP view, redistribute routes from RIP.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] import-route rip
```

# In BGP-VPN instance view, redistribute routes from RIP (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] import-route rip
```

## log-peer-change

### Syntax

**log-peer-change**

**undo log-peer-change**

### View

BGP view

## Default Level

2: System level

## Parameters

None

## Description

Use the **log-peer-change** command to enable the global BGP logging on peers going up and down.

Use the **undo log-peer-change** command to disable the function.

By default, the function is enabled.

## Examples

```
# Enable BGP logging on peers going up and down.
```

```
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] log-peer-change
```

## network (BGP/BGP-VPN instance view)

### Syntax

```
network ip-address [ mask | mask-length ] route-policy route-policy-name  
undo network ip-address [ mask | mask-length ]
```

### View

BGP view/BGP-VPN instance view

## Default Level

2: System level

## Parameters

*ip-address*: Destination IP address.

*mask*: Mask of the network address, in dotted decimal notation.

*mask-length*: Mask length, in the range 0 to 32.

*route-policy-name*: Routing policy applied to the route. The name is a string of 1 to 19 characters.

## Description

Use the **network** command to inject a network to the local BGP routing table.

Use the **undo network** command to remove a network from the BGP routing table.

By default, no network route is injected.

Note that:

- The network route to be injected must exist in the local IP routing table, and using a routing policy makes route management more flexible.
- The ORIGIN attribute of the network route injected with the **network** command is IGP.

## Examples

# In BGP view, inject the network segment 10.0.0.0/16.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] network 10.0.0.0 255.255.0.0
```

# In BGP-VPN instance view, advertise the network segment 10.0.0.0/16 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] network 10.0.0.0 255.255.0.0
```

## network short-cut (BGP/BGP-VPN instance view)

### Syntax

**network** *ip-address* [ *mask* | *mask-length* ] **short-cut**

**undo network** *ip-address* [ *mask* | *mask-length* ] **short-cut**

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

*ip-address*: Destination IP address.

*mask*: Mask of the network address, in dotted decimal notation.

*mask-length*: Mask length, in the range 0 to 32.

### Description

Use the **network short-cut** command to configure an eBGP route as a shortcut route.

Use the **undo network short-cut** command to restore the default.

By default, a received eBGP route has a priority of 255.

The **network short-cut** command allows you configure an eBGP route as a shortcut route that has the same priority as a local route and thus has greater likelihood to become the optimal route.

## Examples

# In BGP view, configure route 10.0.0.0/16 as a shortcut route.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] network 10.0.0.0 255.255.0.0 short-cut
```

# In BGP-VPN instance view, configure route 10.0.0.0/16 as a shortcut route. (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
```

```
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] network 10.0.0.0 255.255.0.0 short-cut
```

## peer advertise-community (BGP/BGP-VPN instance view)

### Syntax

```
peer { group-name | ip-address } advertise-community
undo peer { group-name | ip-address } advertise-community
```

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

### Description

Use the **peer advertise-community** command to advertise the community attribute to a peer/peer group.

Use the **undo peer advertise-community** command to disable the community attribute advertisement to a peer/peer group.

By default, no community attribute is advertised to any peer group/peer.

Related commands: **ip community-list**, **if-match community**, **apply community** (refer to *Routing Policy Commands* in the *IP Routing Volume*).

### Examples

# In BGP view, advertise the community attribute to peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test advertise-community
```

# In BGP-VPN instance view, advertise the community attribute to peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test advertise-community
```

## peer advertise-ext-community (BGP/BGP-VPN instance view)

### Syntax

```
peer { group-name | ip-address } advertise-ext-community
undo peer { group-name | ip-address } advertise-ext-community
```

## View

BGP view/BGP-VPN instance view

## Default Level

2: System level

## Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

## Description

Use the **peer advertise-ext-community** command to advertise the extended community attribute to a peer/peer group.

Use the **undo peer advertise-ext-community** command to disable the extended community attribute advertisement to a peer/peer group.

By default, no extended community attribute is advertised to a peer/peer group.

For related information, refer to the **ip extcommunity-list**, **if-match extcommunity** and **apply extcommunity** commands in *Routing Policy Commands* of the *IP Routing Volume*.

## Examples

# In BGP view, advertise the extended community attribute to the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test advertise-ext-community
```

# In BGP-VPN view, advertise the extended community attribute to the peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test advertise-community
```

## peer allow-as-loop (BGP/BGP-VPN instance view)

### Syntax

```
peer { group-name | ip-address } allow-as-loop [ number ]
undo peer { group-name | ip-address } allow-as-loop
```

## View

BGP view/BGP-VPN instance view

## Default Level

2: System level

## Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

*number*: Specifies the number of times for which the local AS number can appear in routes from the peer/peer group, in the range 1 to 10. The default number is 1.

## Description

Use the **peer allow-as-loop** command to allow the local AS number to exist in the AS\_PATH attribute of routes from a peer/peer group, and to configure the number of times the local AS number can appear.

Use the **undo peer allow-as-loop** command to remove the configuration.

By default, the local AS number is not allowed in routes from a peer/peer group.

Related commands: **display bgp routing-table peer**.

## Examples

# In BGP view, configure the number of times the local AS number can appear in AS-path attribute of routes from peer 1.1.1.1 as 2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 1.1.1.1 allow-as-loop 2
```

# In BGP-VPN instance view, configure the number of times for which the local AS number can appear in AS-path attribute of routes from peer 1.1.1.1 as 2 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 1.1.1.1 allow-as-loop 2
```

## peer as-number (BGP/BGP-VPN instance view)

### Syntax

```
peer { group-name | ip-address } as-number as-number
undo peer group-name as-number
undo peer ip-address
```

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

*as-number*: AS number of the peer or peer group, in the range 1 to 65535.

### Description

Use the **peer as-number** command to specify a peer/peer group with an AS number.

Use the **undo peer as-number** command to delete a peer group.

Use the **undo peer** command to delete a peer.

By default, no peer or peer group is specified.

You can specify the AS number of a peer in either of the following two ways:

- Use the **peer ip-address as-number as-number** command. After that, the system creates the specified peer by default.
- Specify the AS number of the peer when adding it to the specified peer group by using the **peer ip-address group group-name as-number as-number** command; or use the **peer as-number** command to specify the AS number of a peer group, and then a newly added peer will belong to the AS.

The AS number of a peer/peer group cannot be modified directly. To do so, you have to delete the peer/peer group and configure it again.

## Examples

# In BGP view, specify peer group **test** in AS 100.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test as-number 100
```

# In BGP-VPN instance view, specify peer group **test2** in AS 200 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test2 as-number 200
```

## peer as-path-acl (BGP/BGP-VPN instance view)

### Syntax

```
peer { group-name | ip-address } as-path-acl as-path-acl-number { export | import }
undo peer { group-name | ip-address } as-path-acl as-path-acl-number { export | import }
```

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

*as-path-acl-number*: AS path ACL number, in the range 1 to 256.

**export**: Filters outgoing routes.

**import**: Filters incoming routes.

### Description

Use the **peer as-path-acl** command to configure the filtering of routes incoming from or outgoing to a peer/peer group based on a specified AS path ACL.

Use the **undo peer as-path-acl** command to remove the configuration.

By default, no AS path ACL filtering is configured.

Related commands: **ip as-path**, **if-match as-path** and **apply as-path** (refer to *IP Routing Policy Commands* in the *IP Routing Volume*).

## Examples

# In BGP view, reference the AS path ACL 1 to filter routes outgoing to the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test as-path-acl 1 export
```

# In BGP-VPN instance view, reference the AS path ACL 1 to filter routes outgoing to the peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test as-path-acl 1 export
```

## peer capability-advertise conventional

### Syntax

```
peer { group-name | ip-address } capability-advertise conventional
undo peer { group-name | ip-address } capability-advertise conventional
```

### View

BGP view

### Default Level

2: System level

### Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

### Description

Use the **peer capability-advertise conventional** command to disable BGP multi-protocol extension and route refresh for a peer/peer group.

Use the **undo peer capability-advertise** command to enable BGP multi-protocol extension and route refresh for a peer/peer group.

By default, BGP multi-protocol extension and route refresh are enabled.

## Examples

# In BGP view, disable multi-protocol extension and route refresh for peer 160.89.2.33.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 160.89.2.33 as-number 100
```

```
[Sysname-bgp] peer 160.89.2.33 capability-advertise conventional
```

## peer capability-advertise route-refresh

### Syntax

```
peer { group-name | ip-address } capability-advertise route-refresh  
undo peer { group-name | ip-address } capability-advertise route-refresh
```

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

### Description

Use the **peer capability-advertise route-refresh** command to enable the BGP route refresh capability.

Use the **undo peer capability-advertise route-refresh** command to disable the capability.

The capability is enabled by default.

### Examples

# In BGP view, enable BGP route refresh for peer 160.89.2.33.

```
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] peer 160.89.2.33 as-number 100  
[Sysname-bgp] peer 160.89.2.33 capability-advertise route-refresh
```

# In BGP-VPN instance view, enable BGP route refresh for peer 160.89.2.33 (The VPN has been created).

```
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] ipv4-family vpn-instance vpn1  
[Sysname-bgp-vpn1] peer 160.89.2.33 as-number 200  
[Sysname-bgp-vpn1] peer 160.89.2.33 capability-advertise route-refresh
```

## peer connect-interface (BGP/BGP-VPN instance view)

### Syntax

```
peer { group-name | ip-address } connect-interface interface-type interface-number  
undo peer { group-name | ip-address } connect-interface
```

### View

BGP view/BGP-VPN instance view

## Default Level

2: System level

## Parameters

*group-name*: Name of a peer group, a string 1 to 47 characters.

*ip-address*: IP address of a peer.

*interface-type interface-number*: Specifies the type and number of the interface.

## Description

Use the **peer connect-interface** command to specify the source interface for establishing TCP connections to a peer/peer group.

Use the **undo peer connect-interface** command to restore the default.

By default, BGP uses the outbound interface of the best route to the BGP peer/peer group as the source interface for establishing a TCP connection to the peer/peer group.

Note that:

To establish multiple BGP connections to another BGP router, you need to specify on the local router the respective source interfaces for establishing TCP connections to the peers on the peering BGP router; otherwise, the local BGP router may fail to establish TCP connections to the peers when using the outbound interfaces of the best routes as the source interfaces.

## Examples

# In BGP view, specify loopback 0 as the source interface for routing updates to the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test connect-interface loopback 0
```

# In BGP-VPN instance view, specify loopback 0 as the source interface for routing updates to the peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test connect-interface loopback 0
```

## peer default-route-advertise (BGP/BGP-VPN instance view)

### Syntax

```
peer { group-name | ip-address } default-route-advertise [ route-policy route-policy-name ]
undo peer { group-name | ip-address } default-route-advertise
```

### View

BGP view/BGP-VPN instance view

## Default Level

2: System level

## Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

*route-policy-name*: Routing policy name, a string of 1 to 19 characters.

## Description

Use the **peer default-route-advertise** command to advertise a default route to a peer/peer group.

Use the **undo peer default-route-advertise** command to disable default route advertisement to a peer/peer group.

By default, no default route is advertised to a peer/peer group.

With this command used, the router unconditionally sends a default route with the next hop being itself to the peer/peer group regardless of whether the default route is available in the routing table.

## Examples

# In BGP view, advertise a default route to peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test default-route-advertise
```

# In BGP-VPN instance view, advertise a default route to peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test default-route-advertise
```

## peer description (BGP/BGP-VPN instance view)

### Syntax

**peer** { *group-name* | *ip-address* } **description** *description-text*

**undo peer** { *group-name* | *ip-address* } **description**

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

## Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

*description-text*: Description information for the peer/peer group, a string of 1 to 79 characters.

## Description

Use the **peer description** command to configure the description information for a peer/peer group.

Use the **undo peer description** command to remove the description information of a peer/peer group.

By default, no description information is configured for a peer/peer group.

Create a peer/peer group before configuring a description for it.

Related commands: **display bgp peer**.

## Examples

# In BGP view, configure the description information of the peer group test as ISP1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test description ISP1
```

# In BGP-VPN instance view, configure the description information of the peer group test as ISP1(the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test description ISP1
```

## peer ebgp-max-hop (BGP/BGP-VPN instance view)

### Syntax

```
peer { group-name | ip-address } ebgp-max-hop [ hop-count ]
undo peer { group-name | ip-address } ebgp-max-hop
```

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

*hop-count*: Maximum hop count, in the range 1 to 255. The default is 64.

### Description

Use the **peer ebgp-max-hop** command to allow establishing an EBGP connection with a peer/peer group that is on an indirectly connected network.

Use the **undo peer ebgp-max-hop** command to restore the default.

By default, this feature is disabled.

You can use the argument *hop-count* to specify the maximum route hop count of the EBGP connection.

## Examples

# In BGP view, allow establishing the EBGP connection with the peer group **test** that is on an indirectly connected network.

```
<Sysname> system-view
[Sysname] bgp 100
```

```
[Sysname-bgp] peer test ebgp-max-hop
```

# In BGP-VPN instance view, allow establishing the EBGP connection with the peer group **test** that is on an indirectly connected network (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test ebgp-max-hop
```

## peer enable (BGP view)

### Syntax

```
peer ip-address enable
undo peer ip-address enable
```

### View

BGP view

### Default Level

2: System level

### Parameters

*ip-address*: IP address of a peer.

### Description

Use the **peer enable** command to enable the specified peer.

Use the **undo peer enable** command to disable the specified peer.

By default, the BGP peer is enabled.

If a peer is disabled, the router will not exchange routing information with the peer.

### Examples

```
# Disable peer 18.10.0.9.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 18.10.0.9 group group1
[Sysname-bgp] undo peer 18.10.0.9 enable
```

## peer fake-as (BGP/BGP-VPN instance view)

### Syntax

```
peer { group-name | ip-address } fake-as as-number
undo peer { group-name | ip-address } fake-as
```

### View

BGP view/BGP-VPN instance view

## Default Level

2: System level

## Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

*as-number*: Local autonomous system number, in the range 1 to 65535.

## Description

Use the **peer fake-as** command to configure a fake local AS number for a peer or peer group.

Use the **undo peer fake-as** command to remove the configuration.

By default, no fake local AS number is configured for a peer or peer group.



### Note

The **peer fake-as** command is only applicable to an EBGP peer or peer group.

---

## Examples

# In BGP view, configure a fake AS number of 200 for the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test fake-as 200
```

# In BGP-VPN instance view, configure a fake AS number of 200 for the peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test fake-as 200
```

## peer filter-policy (BGP/BGP-VPN instance view)

### Syntax

```
peer { group-name | ip-address } filter-policy acl-number { export | import }
undo peer { group-name | ip-address } filter-policy [ acl-number ] { export | import }
```

### View

BGP view/BGP-VPN instance view

## Default Level

2: System level

## Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

*acl-number*: ACL number, in the range 2000 to 3999.

**export**: Applies the filter-policy to routes advertised to the peer/peer group.

**import**: Applies the filter-policy to routes received from the peer/peer group.

## Description

Use the **peer filter-policy** command to configure an ACL-based filter policy for a peer or peer group.

Use the **undo peer filter-policy** command to remove the configuration.

By default, no ACL-based filter policy is configured for a peer or peer group.

Related commands: **peer as-path-acl**.

## Examples

# In BGP view, apply the ACL 2000 to filter routes advertised to the peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test filter-policy 2000 export
```

# In BGP-VPN instance view, apply the ACL 2000 to filter routes advertised to the peer group test (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test filter-policy 2000 export
```

## peer group (BGP/BGP-VPN instance view)

### Syntax

```
peer ip-address group group-name [ as-number as-number ]
```

```
undo peer ip-address group group-name
```

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

## Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

*as-number*: AS number of the peer, in the range 1 to 65535.

## Description

Use the **peer group** command to add a peer to a peer group.

Use the **undo peer group** command to delete a specified peer from a peer group.

By default, no peer is added into a peer group.

If you have specified an AS number for the peer to be added, make sure that the *as-number* argument is consistent with the specified peer AS number.

If you have not created the peer to be added, the system automatically creates the peer when you execute the command.

## Examples

# In BGP view, add the peer 10.1.1.1 to the EBGP peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
[Sysname-bgp] peer test as-number 2004
[Sysname-bgp] peer 10.1.1.1 group test
```

# In BGP-VPN view, add the peer 10.1.1.1 to the EBGP peer group test (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] group test external
[Sysname-bgp-vpn1] peer test as-number 2004
[Sysname-bgp-vpn1] peer 10.1.1.1 group test
```

## peer ignore (BGP/BGP-VPN instance view)

### Syntax

```
peer { group-name | ip-address } ignore
undo peer { group-name | ip-address } ignore
```

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

### Description

Use the **peer ignore** command to disable session establishment with a peer or peer group.

Use the **undo peer ignore** command to remove the configuration.

By default, session establishment with a peer or peer group is allowed.

After the **peer ignore** command is executed, the system disables the session with the specified peer or peer group and clears all the related routing information. For a peer group, this means all sessions with the peer group will be tore down.

## Examples

# In BGP view, disable session establishment with peer 10.10.10.10.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 10.10.10.10 ignore
```

# In BGP-VPN instance view, disable session establishment with peer 10.10.10.10 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 10.10.10.10 ignore
```

## peer ip-prefix

### Syntax

```
peer { group-name | ip-address } ip-prefix ip-prefix-name { export | import }
undo peer { group-name | ip-address } ip-prefix { export | import }
```

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

*ip-prefix-name*: IP prefix list name, a string of 1 to 19 characters.

**export**: Applies the filter to routes advertised to the specified peer/peer group.

**import**: Applies the filter to routes received from the specified peer/peer group.

### Description

Use the **peer ip-prefix** command to reference an IP prefix list to filter routes received from or advertised to a peer or peer group.

Use the **undo peer ip-prefix** command to remove the configuration.

By default, no IP prefix list based filtering is configured.

## Examples

# In BGP view, use the IP prefix list **list 1** to filter routes advertised to the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test ip-prefix list1 export
```

# In BGP-VPN view, use the IP prefix list **list 1** to filter routes advertised to the peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test ip-prefix list1 export
```

## peer keep-all-routes (BGP/BGP-VPN instance view)

### Syntax

```
peer { group-name | ip-address } keep-all-routes
undo peer { group-name | ip-address } keep-all-routes
```

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

### Description

Use the **peer keep-all-routes** command to save original routing information from a peer or peer group, including routes that fail to pass the inbound policy (if configured).

Use the **undo peer keep-all-routes** command to disable this function.

By default, the function is not enabled.

### Examples

# In BGP view, save routing information from peer 131.100.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 131.100.1.1 as-number 200
[Sysname-bgp] peer 131.100.1.1 keep-all-routes
```

# In BGP-VPN instance view, save routing information from peer 131.100.1.1(the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 131.100.1.1 as-number 200
[Sysname-bgp-vpn1] peer 131.100.1.1 keep-all-routes
```

## peer log-change (BGP/BGP-VPN instance view)

### Syntax

```
peer { group-name | ip-address } log-change
undo peer { group-name | ip-address } log-change
```

## View

BGP view/BGP-VPN instance view

## Default Level

2: System level

## Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

## Description

Use the **peer log-change** command to enable the logging of session state and event information for a specified peer or peer group.

Use the **undo peer log-change** command to remove the configuration.

The logging is enabled by default.

## Examples

# In BGP view, enable the logging of session state and event information for peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test log-change
```

# In BGP-VPN instance view, enable the logging of session state and event information for peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test log-change
```

## peer next-hop-local (BGP/BGP-VPN instance view)

### Syntax

**peer** { *group-name* | *ip-address* } **next-hop-local**

**undo peer** { *group-name* | *ip-address* } **next-hop-local**

### View

BGP view /BGP-VPN instance view

### Default Level

2: System level

### Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

## Description

Use the **peer next-hop-local** command to specify the router as the next hop for routes sent to a peer/peer group.

Use the **undo peer next-hop-local** command to remove the configuration.

By default, routes advertised to an EBGP peer/peer group take the local router as the next hop, while routes sent to an IBGP peer/peer group do not take the local router as the next hop.

## Examples

# In BGP view, set the next hop of routes advertised to peer group **test** to the router itself.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test next-hop-local
```

# In BGP-VPN instance view, set the next hop of routes advertised to peer group **test** to the router itself (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test next-hop-local
```

## peer password

### Syntax

```
peer { group-name | ip-address } password { cipher | simple } password
undo peer { group-name | ip-address } password
```

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

**cipher**: Displays the configured password in cipher text format.

**simple**: Displays the configured password in plain text format.

*password*: Password, a string of 1 to 80 characters when the **simple** keyword is used, or when the **cipher** keyword and plain text password are used; a string of 24 or 108 characters when the cipher text password and the **cipher** keyword are used.

## Description

Use the **peer password** command to configure BGP to perform MD5 authentication when a TCP connection is being established with a peer/peer group.

Use the **undo peer password** command to disable the function.

By default, no MD5 authentication is performed for TCP connection establishment.

Once MD5 authentication is enabled, both parties must be configured with the same authentication mode and password. Otherwise, the TCP connection will not be set up.

## Examples

# In BGP view, perform MD5 authentication on the TCP connection set up between the local router 10.1.100.1 and the peer router 10.1.100.2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 10.1.100.2 password simple aabbcc
```

# Perform the similar configuration on the peer.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 10.1.100.1 password simple aabbcc
```

# In BGP-VPN instance view, perform MD5 authentication on the TCP connection set up between the local router 10.1.100.1 and the peer router 10.1.100.2(the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 10.1.100.2 password simple aabbcc
```

# Perform the similar configuration on the peer.

```
<Sysname> system-view
[Sysname] bgp 200
[Sysname-bgp-vpn1] peer 10.1.100.1 password simple aabbcc
```

## peer preferred-value (BGP/BGP-VPN instance view)

### Syntax

```
peer { group-name | ip-address } preferred-value value
undo peer { group-name | ip-address } preferred-value
```

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

*value*: Preferred value, in the range 0 to 65535.

### Description

Use the **peer preferred-value** command to assign a preferred value to routes received from a peer or peer group.

Use the **undo peer preferred-value** command to restore the default value.

The default preferred value is 0.

Routes learned from a peer have an initial preferred value. Among multiple routes that have the same destination/mask and are learned from different peers, the one with the greatest preferred value is selected as the route to the destination.

Note that:

If you both reference a routing policy and use the **peer { group-name | ip-address } preferred-value value** command to set a preferred value for routes from a peer, the routing policy sets a specified non-zero preferred value for routes matching it. Other routes not matching the routing policy uses the value set with the command. If the preferred value specified in the routing policy is zero, the routes matching it will also use the value set with the command. For information about using a routing policy to set a preferred value, refer to the command **peer { group-name | ip-address } route-policy route-policy-name { export | import }** in this document, and the command **apply preferred-value preferred-value** in *Routing Policy Commands of the IP Routing Volume*.

## Examples

# In BGP view, configure the preferred value as 50 for routes from peer 131.108.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 131.108.1.1 preferred-value 50
```

# In BGP-VPN instance view, configure the preferred value as 50 for routes from peer 131.108.1.1 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 131.108.1.1 preferred-value 50
```

## peer public-as-only (BGP/BGP-VPN instance view)

### Syntax

```
peer { group-name | ip-address } public-as-only
undo peer { group-name | ip-address } public-as-only
```

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

### Description

Use the **peer public-as-only** command to not keep private AS numbers in BGP updates sent to a

peer/peer group.

Use the **undo peer public-as-only** command to keep private AS numbers in BGP updates sent to a peer/peer group.

By default, BGP updates carry private AS numbers.

The command does not take effect if the BGP update has both public and private AS numbers. The range of private AS number is from 64512 to 65535.

## Examples

# In BGP view, carry no private AS number in BGP updates sent to the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test public-as-only
```

# In BGP-VPN instance view, carry no private AS number in BGP updates sent to the peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test public-as-only
```

## peer reflect-client (BGP/BGP-VPN instance view)

### Syntax

```
peer { group-name | ip-address } reflect-client
undo peer { group-name | ip-address } reflect-client
```

### View

BGP view

### Default Level

2: System level

### Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

### Description

Use the **peer reflect-client** command to configure the router as a route reflector and specify a peer/peer group as a client.

Use the **undo peer reflect-client** command to remove the configuration.

By default, neither the route reflector nor the client is configured.

Related commands: **reflect between-clients** and **reflect cluster-id**.

## Examples

# In BGP view, configure the local device as a route reflector and specify the IBGP peer group **test** as a client.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test reflect-client
```

## peer route-limit (BGP/BGP-VPN instance view)

### Syntax

```
peer { group-name | ip-address } route-limit prefix-number [ { alert-only | reconnect reconnect-time }
| percentage-value ] *
```

```
undo peer { group-name | ip-address } route-limit
```

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

*prefix-number*: Number of prefixes that can be received from the peer or peer group. in the range 1 to 12288. If the number of prefixes received from the peer/peer group reaches the *prefix-number*, the router will tear down the connection to the peer/peer group.

**alert-only**: If the number of prefixes received from the peer/peer group reaches the *prefix-number*, the router will not tear down the connection to the peer/peer group but display an alarm message.

**reconnect** *reconnect-time*: Specifies a reconnect time, after which, the router will re-establish a connection to the peer/peer group. It has no default value and is in the range 1 to 65535 seconds.

*percentage-value*: Threshold value for the router to display an alarm message (that is, the router displays an alarm message when the ratio of the number of received prefixes to the *prefix-number* reaches the *percentage*). It is in the range 1 to 100 and defaults to 75.

### Description

Use the **peer route-limit** command to set the number of route prefixes that can be received from a peer/peer group.

Use the **undo peer route-limit** command to restore the default.

The number is not limited by default.

### Examples

# In BGP view, set the number of route prefixes that can be received from peer 129.140.6.6 to 10000.

```
<Sysname> system-view
[Sysname] bgp 109
[Sysname-bgp] peer 129.140.6.6 as-number 110
[Sysname-bgp] peer 129.140.6.6 route-limit 10000
```

# In BGP-VPN instance view, set the number of route prefixes that can be received from peer 129.140.6.6 to 10000 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 109
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 129.140.6.6 as-number 110
[Sysname-bgp-vpn1] peer 129.140.6.6 route-limit 10000
```

## peer route-policy (BGP/BGP-VPN instance view)

### Syntax

```
peer { group-name | ip-address } route-policy route-policy-name { export | import }
undo peer { group-name | ip-address } route-policy route-policy-name { export | import }
```

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

*route-policy-name*: Routing policy name, a string of 1 to 19 characters.

**export**: Applies the routing policy to routes outgoing to the peer (or peer group).

**import**: Applies the routing policy to routes incoming from the peer (or peer group).

### Description

Use the **peer route-policy** command to apply a routing policy to routes incoming from or outgoing to a peer or peer group.

Use the **undo peer route-policy** command to remove the configuration.

By default, no routing policy is applied to routes from/to the peer/peer group.

The **peer route-policy** command does not apply the **if-match interface** clause in the referenced routing policy. Refer to *Routing Policy Commands* in the *IP Routing Volume* for related commands.

### Examples

# In BGP view, apply routing policy **test-policy** to routes outgoing to the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test route-policy test-policy export
```

# In BGP-VPN instance view, apply the routing policy **test-policy** to routes outgoing to the peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test route-policy test-policy export
```

## peer route-update-interval (BGP/BGP-VPN instance view)

### Syntax

```
peer { group-name | ip-address } route-update-interval interval
undo peer { group-name | ip-address } route-update-interval
```

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

*interval*: Minimum interval for sending the same update message. The range is 5 to 600 seconds.

### Description

Use the **peer route-update-interval** command to specify the interval for sending the same update to a peer/peer group.

Use the **undo peer route-update-interval** command to restore the default value.

By default, the interval is 5 seconds for IBGP peers, and 30 seconds for EBGP peers.

### Examples

# In BGP view, specify the interval for sending the same update to peer group **test** as 10 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test as-number 100
[Sysname-bgp] peer test route-update-interval 10
```

# In BGP-VPN instance view, specify the interval for sending the same update to peer group **test** as 10 seconds (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test as-number 100
[Sysname-bgp-vpn1] peer test route-update-interval 10
```

## peer substitute-as (BGP/BGP-VPN instance view)

### Syntax

```
peer { group-name | ip-address } substitute-as
undo peer { group-name | ip-address } substitute-as
```

### View

BGP view/BGP-VPN instance view

## Default Level

2: System level

## Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

## Description

Use the **peer substitute-as** command to replace the AS number of a peer/peer group in the AS\_PATH attribute with the local AS number.

Use the **undo peer substitute-as** command to remove the configuration.

No AS number is replaced by default.

## Examples

# In BGP view, substitute local AS number for AS number of peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 1.1.1.1 substitute-as
```

# In BGP-VPN instance view, substitute local AS number for AS number of peer 1.1.1.1 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 1.1.1.1 substitute-as
```

## peer timer (BGP/BGP-VPN instance view)

### Syntax

**peer** { *group-name* | *ip-address* } **timer** **keepalive** *keepalive* **hold** *holdtime*

**undo peer** { *group-name* | *ip-address* } **timer**

### View

BGP view/BGP-VPN instance view

## Default Level

2: System level

## Parameters

*group-name*: Name of a peer group, a string of 1 to 47 characters.

*ip-address*: IP address of a peer.

*keepalive*: Keepalive interval in seconds, ranging from 1 to 21845.

*holdtime*: Holdtime interval in seconds, ranging from 3 to 65535.

## Description

Use the **peer timer** command to configure the keepalive interval and holdtime interval for a peer or peer group.

Use the **undo peer timer** command to restore the default.

By default, the *keepalive* and *holdtime* are 60s and 180s respectively.

Note that:

- The timer configured with this command is preferred to the timer configured with the **timer** command.
- The holdtime interval must be at least three times the keepalive interval.

Related commands: **timer**.

## Examples

# In BGP view, configure the keepalive interval and holdtime interval for peer group **test** as 60s and 180s.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test timer keepalive 60 hold 180
```

# In BGP-VPN instance view, configure the keepalive interval and holdtime interval for peer group **test** as 60s and 180s (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test timer keepalive 60 hold 180
```

## preference (BGP/BGP-VPN instance view)

### Syntax

```
preference { external-preference internal-preference local-preference | route-policy
route-policy-name }
```

```
undo preference
```

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

*external-preference*: Preference of EBGP routes, in the range 1 to 255.

*internal-preference*: Preference of IBGP routes, in the range 1 to 255.

*local-preference*: Preference of local routes, in the range 1 to 255.

*route-policy-name*: Routing policy name, a string of 1 to 19 characters. Using the routing policy can set a preference for routes matching it. The default value applies to routes not matching the routing policy.

## Description

Use the **preference** command to configure preferences for external, internal, and local routes.

Use the **undo preference** command to restore the default.

For *external-preference*, *internal-preference* and *local-preference*, the greater the preference value is, the lower the preference is, and the default values are 255, 255, 130 respectively.

## Examples

# In BGP view, configure preferences for EBGP, IBGP and local routes as 20, 20 and 200.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] preference 20 20 200
```

# In BGP-VPN instance view, configure preferences for EBGP, IBGP and local routes as 20, 20 and 200 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] preference 20 20 200
```

## reflect between-clients (BGP view)

### Syntax

```
reflect between-clients
undo reflect between-clients
```

### View

BGP view

### Default Level

2: System level

### Parameters

None

## Description

Use the **reflect between-clients** command to enable route reflection between clients.

Use the **undo reflect between-clients** command to disable this function.

By default, route reflection between clients is enabled.

After a route reflector is configured, it reflects the routes of a client to other clients. If the clients of a route reflector are fully meshed, you need disable route reflection between clients to reduce routing costs.

Related commands: **reflector cluster-id** and **peer reflect-client**.

## Examples

# Disable route reflection between clients.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] undo reflect between-clients
```

## reflector cluster-id (BGP view)

### Syntax

```
reflector cluster-id { cluster-id | ip-address }
undo reflector cluster-id
```

### View

BGP view

### Default Level

2: System level

### Parameters

*cluster-id*: Cluster ID in the format of an integer from 1 to 4294967295.

*ip-address*: Cluster ID in the format of an IPv4 address in dotted decimal notation.

### Description

Use the **reflector cluster-id** command to configure the cluster ID of the route reflector.

Use the **undo reflector cluster-id** command to remove the configured cluster ID.

By default, each route reflector uses its router ID as the cluster ID.

Usually, there is only one route reflector in a cluster. The router ID of the route reflector is the ID of the cluster. You can configure multiple route reflectors to improve network stability. In this case, using this command can configure the identical cluster ID for all the route reflectors to avoid routing loops.

Related commands: **reflect between-clients** and **peer reflect-client**.

### Examples

```
# Set the cluster ID to 80.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] reflector cluster-id 80
```

## refresh bgp

### Syntax

```
refresh bgp { all | ip-address | group group-name | external | internal } { export | import }
```

### View

User view

### Default Level

1: Monitor level

## Parameters

**all**: Soft-resets all BGP connections.

*ip-address*: Soft-resets the BGP connection to a peer.

*group-name*: Soft-resets connections to a peer group, name of which is a string of 1 to 47 characters.

**external**: EBGP connection.

**internal**: IBGP connection.

**export**: Outbound soft reset.

**import**: Inbound soft reset.

## Description

Use the **refresh bgp** command to perform soft reset on specified BGP connections. Using this function can refresh the BGP routing table without tearing down BGP connections and apply a newly configured routing policy.

To perform BGP soft reset, all routers in the network must support route-refresh. If a router not supporting route-refresh exists in the network, you need to configure the **peer keep-all-routes** command to save all routing updates before performing soft reset.

## Examples

```
# Perform inbound BGP soft reset.
```

```
<Sysname> refresh bgp all import
```

## reset bgp

### Syntax

```
reset bgp { as-number | ip-address [ flap-info ] | all | external | group group-name | internal }
```

### View

User view

### Default Level

1: Monitor level

## Parameters

*as-number*: Resets BGP connections to peers in the AS.

*ip-address*: Specifies the IP address of a peer with which to reset the connection.

**flap-info**: Clears route flap information.

**all**: Resets all BGP connections.

**external**: Resets all the EBGP connections.

**group** *group-name*: Resets connections with the specified BGP peer group.

**internal**: Resets all the iBGP connections.

## Description

Use the **reset bgp** command to reset specified BGP connections.

## Examples

```
# Reset all the BGP connections.  
<Sysname> reset bgp all
```

## reset bgp dampening

### Syntax

```
reset bgp dampening [ ip-address [ mask | mask-length ] ]
```

### View

User view

### Default Level

1: Monitor level

### Parameters

*ip-address*: Destination IP address of a route.

*mask*: Mask, in dotted decimal notation.

*mask-length*: Mask length, in the range 0 to 32.

### Description

Use the **reset bgp dampening** command to clear route dampening information and release suppressed routes.

Related commands: **dampening**, **display bgp routing-table dampened**.

## Examples

```
# Clear damping information of route 20.1.0.0/16 and release the suppressed route.  
<Sysname> reset bgp dampening 20.1.0.0 255.255.0.0
```

## reset bgp flap-info

### Syntax

```
reset bgp flap-info [ ip-address [ mask-length | mask ] | as-path-acl as-path-acl-number | regexp  
as-path-regular-expression ]
```

### View

User view

### Default Level

1: Monitor level

### Parameters

*ip-address*: Clears the flap statistics of a route.

*mask-length*: Mask length, in the range 0 to 32.

*mask*: Network mask, in dotted decimal notation.

*as-path-acl-number*: Clears the flap statistics of routes matching an AS path ACL, number of which is in the range 1 to 256.

*as-path-regular-expression*: Clears the flap statistics of routes matching the AS path regular expression, which is a string of 1 to 80 characters.

### Description

Use the **reset bgp flap-info** command to clear the flap statistics of routes matching the specified filter.

### Examples

```
# Clear the flap statistics of all routes matching AS path ACL 10.
```

```
<Sysname> reset bgp flap-info as-path-acl 10
```

## reset bgp ipv4 all

### Syntax

```
reset bgp ipv4 all
```

### View

User view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **reset bgp ipv4 all** command to reset all the BGP connections of IPv4 unicast address family.

### Examples

```
# Reset all the BGP connections of IPv4 unicast address family.
```

```
<Sysname> reset bgp ipv4 all
```

## router-id

### Syntax

```
router-id router-id
```

```
undo router-id
```

### View

BGP view

### Default Level

2: System level

## Parameters

*router-id*: Router ID in IP address format.

## Description

Use the **router-id** command to specify a router ID.

Use the **undo router-id** command to remove the router ID.

To run BGP protocol, a router must have a router ID, which is an unsigned 32-bit integer, the unique ID of the router in the AS.

You can specify a router ID manually. If not, the system selects an IP address as the router ID. The selection sequence is the highest IP address among loopback interface addresses; if not available, then the highest IP address of interfaces. It is recommended to specify a loopback interface address as the router ID to enhance network reliability.

Only when the interface with the selected Router ID or the manual Router ID is deleted will the system select another ID for the router.

## Examples

```
# Specifies the Router ID as 10.18.4.221.  
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] router-id 10.18.4.221
```

## summary automatic

### Syntax

**summary automatic**

**undo summary automatic**

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

None

### Description

Use the **summary automatic** command to enable automatic summarization for redistributed subnets.

Use the **undo summary automatic** command to disable automatic summarization.

By default, automatic summarization is disabled.

Note that:

- Neither the default route nor the routes imported using the **network** command can be summarized automatically.
- The **summary automatic** command helps BGP limit the number of routes redistributed from IGP to reduce the size of the routing table.

## Examples

# In BGP view, enable automatic route summarization.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] summary automatic
```

# In BGP-VPN instance view, enable automatic summarization (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] summary automatic
```

## synchronization (BGP view)

### Syntax

**synchronization**

**undo synchronization**

### View

BGP view

### Default Level

2: System level

### Parameters

None

### Description

Use the **synchronization** command to enable the synchronization between the BGP and IGP routes.

Use the **undo synchronization** command to disable the synchronization.

The feature is disabled by default.

With this feature enabled and when a non-BGP router is responsible for forwarding packets in an AS, BGP speakers in the AS cannot advertise routing information to other ASs unless all routers in the AS know the latest routing information.

When a BGP router receives an IBGP route, it checks only whether the next hop is reachable by default. If the synchronization is enabled, the IBGP route is synchronized and advertised to EBGP peers only when the route is also advertised by IGP. Otherwise, the IBGP route cannot be advertised to EBGP peers.

## Examples

# Enable the synchronization between BGP and IGP routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] synchronization
```

## timer (BGP/BGP-VPN instance view)

### Syntax

```
timer keepalive keepalive hold holdtime  
undo timer
```

### View

BGP view/BGP-VPN instance view

### Default Level

2: System level

### Parameters

*keepalive*: Keepalive interval in seconds, ranging from 1 to 21845.

*holdtime*: Holdtime interval in seconds, ranging from 3 to 65535.

### Description

Use the **timer** command to configure BGP keepalive interval and holdtime interval.

Use the **undo timer** command to restore the default.

By default, BGP keepalive and holdtime intervals are 60s and 180s.

Note that:

- Timer configured using the **peer timer** command is preferred to the timer configured using this command.
- The holdtime interval must be at least three times the keepalive interval.
- The configured timer applies to all the BGP peers, while it becomes valid only after the corresponding BGP connections are reset.

Related commands: **peer timer**.

### Examples

# Configure keepalive interval and holdtime interval as 60s and 180s.

```
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] timer keepalive 60 hold 180
```

# In BGP-VPN instance view, configure keepalive interval and holdtime interval as 60s and 180s (the VPN has been created).

```
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] ipv4-family vpn-instance vpn1  
[Sysname-bgp-vpn1] timer keepalive 60 hold 180
```

# Table of Contents

<b>1 IPv6 Static Routing Configuration Commands .....</b>	<b>1-1</b>
IPv6 Static Routing Configuration Commands .....	1-1
delete ipv6 static-routes all .....	1-1
ipv6 route-static .....	1-2

# 1 IPv6 Static Routing Configuration Commands

---



## Note

Throughout this chapter, the term “router” refers to a router in a generic sense or a Layer 3 switch running routing protocols.

---

## IPv6 Static Routing Configuration Commands

### delete ipv6 static-routes all

#### Syntax

```
delete ipv6 static-routes all
```

#### View

System view

#### Default Level

2: System level

#### Parameters

None

#### Description

Use the **delete ipv6 static-routes all** command to delete all static routes including the default route.

When using this command, you will be prompted whether to continue the deletion and only after you confirm the deletion will the static routes be deleted.

Related commands: **display ipv6 routing-table**, **ipv6 route-static**.

#### Examples

```
# Delete all IPv6 static routes.
```

```
<Sysname> system-view
```

```
[Sysname] delete ipv6 static-routes all
```

```
This will erase all ipv6 static routes and their configurations, you must reconfigure all static routes
```

```
Are you sure?[Y/N]Y
```

## ipv6 route-static

### Syntax

```
ipv6 route-static ipv6-address prefix-length [ interface-type interface-number ] nexthop-address  
[ preference preference-value ]
```

```
undo ipv6 route-static ipv6-address prefix-length [ interface-type interface-number ]  
[ nexthop-address ] [ preference preference-value ]
```

### View

System view

### Default Level

2: System level

### Parameters

*ipv6-address prefix-length*: IPv6 address and prefix length.

*interface-type interface-number*: Interface type and interface number of the output interface.

*nexthop-address*: Next hop IPv6 address.

*preference-value*: Route preference value, in the range of 1 to 255. The default is 60.

### Description

Use the **ipv6 route-static** command to configure an IPv6 static route.

Use the **undo ipv6 route-static** command to remove an IPv6 static route.

An IPv6 static route that has the destination address configured as **::/0** (a prefix length of 0) is the default IPv6 route. If the destination address of an IPv6 packet does not match any entry in the routing table, this default route will be used to forward the packet.

Related commands: **display ipv6 routing-table**, **delete ipv6 static-routes all**.

### Examples

```
# Configure a static IPv6 route, with the destination address being 1:1:2::/24 and next hop being  
1:1:3::1.
```

```
<Sysname> system-view
```

```
[Sysname] ipv6 route-static 1:1:2:: 24 1:1:3::1
```

# Table of Contents

<b>1 RIPng Configuration Commands</b> .....	<b>1-1</b>
RIPng Configuration Commands .....	1-1
checkzero .....	1-1
default cost (RIPng view).....	1-2
display ripng .....	1-2
display ripng database.....	1-3
display ripng interface.....	1-4
display ripng route .....	1-6
filter-policy export .....	1-7
filter-policy import (RIPng view).....	1-7
import-route .....	1-8
maximum load-balancing (RIPng view).....	1-9
preference .....	1-10
ripng.....	1-10
ripng default-route .....	1-11
ripng enable.....	1-12
ripng metricin .....	1-12
ripng metricout.....	1-13
ripng poison-reverse.....	1-14
ripng split-horizon .....	1-14
ripng summary-address.....	1-15
timers .....	1-16

# 1 RIPng Configuration Commands

---



## Note

The term “router” in this document refers to a router in a generic sense or a Layer 3 switch.

---

## RIPng Configuration Commands

### checkzero

#### Syntax

```
checkzero
undo checkzero
```

#### View

RIPng view

#### Default Level

2: System level

#### Parameters

None

#### Description

Use the **checkzero** command to enable the zero field check on RIPng packets.

Use the **undo checkzero** command to disable the zero field check.

The zero field check is enabled by default.

Some fields in RIPng packet headers must be zero. These fields are called zero fields. You can enable the zero field check on RIPng packet headers. If any such field contains a non-zero value, the RIPng packet will be discarded.

#### Examples

```
# Disable the zero field check on RIPng packet headers of RIPng 100.
```

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] undo checkzero
```

## default cost (RIPng view)

### Syntax

**default cost** *cost*

**undo default cost**

### View

RIPng view

### Default Level

2: System level

### Parameters

*cost*: Default metric of redistributed routes, in the range of 0 to 16.

### Description

Use the **default cost** command to specify the default metric of redistributed routes.

Use the **undo default cost** command to restore the default.

The default metric of redistributed routes is 0.

The specified default metric applies to the routes redistributed by the **import-route** command with no metric specified.

Related commands: **import-route**.

### Examples

# Set the default metric of redistributed routes to 2.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] default cost 2
```

## display ripng

### Syntax

**display ripng** [ *process-id* ]

### View

Any view

### Default Level

1: Monitor level

### Parameters

*process-id*: RIPng process ID, in the range of 1 to 65535.

### Description

Use the **display ripng** command to display the running status and configuration information of a RIPng process. If *process-id* is not specified, information of all RIPng processes will be displayed.

## Examples

# Display the running status and configuration information of all configured RIPng processes.

```
<Sysname> display ripng
  RIPng process : 1
    Preference : 100
    Checkzero : Enabled
    Default Cost : 0
    Maximum number of balanced paths : 8
    Update time : 30 sec(s) Timeout time : 180 sec(s)
    Suppress time : 120 sec(s) Garbage-Collect time : 120 sec(s)
    Number of periodic updates sent : 0
    Number of trigger updates sent : 0
```

**Table 1-1 display ripng command output description**

Field	Description
RIPng process	RIPng process ID
Preference	RIPng route priority
Checkzero	Indicates whether zero field check for RIPng packet headers is enabled
Default Cost	Default metric of redistributed routes
Maximum number of balanced paths	Maximum number of load balanced routes
Update time	RIPng update interval, in seconds
Timeout time	RIPng timeout interval, in seconds
Suppress time	RIPng suppress interval, in seconds
Garbage-Collect time	RIPng garbage collection interval, in seconds
Number of periodic updates sent	Number of periodic updates sent
Number of trigger updates sent	Number of triggered updates sent

## display ripng database

### Syntax

```
display ripng process-id database
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*process-id*: RIPng process ID, in the range of 1 to 65535.

## Description

Use the **display ripng database** command to display all active routes in the advertising database of the specified RIPng process, which are sent in normal RIPng update messages.

## Examples

# Display the active routes in the database of RIPng process 100.

```
<Sysname> display ripng 100 database
 2001:7B::2:2A1:5DE/64,
     cost 4, Imported
 1:13::/120,
     cost 4, Imported
 1:32::/120,
     cost 4, Imported
 1:33::/120,
     cost 4, Imported
 100::/32,
     via FE80::200:5EFF:FE04:3302, cost 2
 3FFE:C00:C18:1::/64,
     via FE80::200:5EFF:FE04:B602, cost 2
 3FFE:C00:C18:1::/64,
     via FE80::200:5EFF:FE04:B601, cost 2
 3FFE:C00:C18:2::/64,
     via FE80::200:5EFF:FE04:B602, cost 2
 3FFE:C00:C18:3::/64,
     via FE80::200:5EFF:FE04:B601, cost 2
 4000:1::/64,
     via FE80::200:5EFF:FE04:3302, cost 2
 4000:2::/64,
     via FE80::200:5EFF:FE04:3302, cost 2
 1111::/64,
     cost 0, RIPng-interface
```

**Table 1-2 display ripng database** command output description

Field	Description
2001:7B::2:2A1:5DE/64	IPv6 destination address/prefix length
via	Next hop IPv6 address
cost	Route metric value
Imported	Route redistributed from another routing protocol
RIPng-interface	Route learned from the interface

## display ripng interface

### Syntax

```
display ripng process-id interface [ interface-type interface-number ]
```

## View

Any view

## Default Level

1: Monitor level

## Parameters

*process-id*: RIPng process ID, in the range of 1 to 65535.

*interface-type interface-number*: Specifies an interface.

## Description

Use the **display ripng interface** command to display the interface information of the RIPng process.

If no interface is specified, information about all interfaces of the RIPng process will be displayed.

## Examples

# Display the interface information of RIPng process 1.

```
<Sysname> display ripng 1 interface
Interface-name: Vlan-interface100
    Link Local Address: FE80::20F:E2FF:FE30:C16C
    Split-horizon: on                Poison-reverse: off
    MetricIn: 0                      MetricOut: 1
    Default route: off
    Summary address:
        3:: 64
        3:: 16
```

**Table 1-3 display ripng interface** command output description

Field	Description
Interface-name	Name of an interface running RIPng
Link Local Address	Link-local address of an interface running RIPng
Split-horizon	Indicates whether the split horizon function is enabled (on: Enabled; off: Disabled)
Poison-reverse	Indicates whether the poison reverse function is enabled (on: Enabled; off: Disabled)
MetricIn/MetricOut	Additional metric to incoming and outgoing routes
Default route	<ul style="list-style-type: none"><li>• Only/Originate: <b>Only</b> means that the interface advertises only the default route. <b>Originate</b> means that the default route and other RIPng routes are advertised.</li><li>• <b>Off</b> indicates that no default route is advertised or the garbage-collect time expires after the default route advertisement was disabled.</li><li>• In garbage-collect status: With default route advertisement disabled, the interface advertises the default route with metric 16 during the garbage-collect time.</li></ul>
Summary address	The summarized IPv6 prefix and the summary IPv6 prefix on the interface

## display ripng route

### Syntax

```
display ripng process-id route
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*process-id*: RIPng process ID, in the range of 1 to 65535.

### Description

Use the **display ripng route** command to display all RIPng routes and timers associated with each route of a RIPng process.

### Examples

# Display the routing information of RIPng process 100.

```
<Sysname> display ripng 100 route
  Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
  -----

Peer FE80::200:5EFF:FE04:B602 on Vlan-interface100
Dest 3FFE:C00:C18:1::/64,
  via FE80::200:5EFF:FE04:B602, cost 2, tag 0, A, 34 Sec

Dest 3FFE:C00:C18:2::/64,
  via FE80::200:5EFF:FE04:B602, cost 2, tag 0, A, 34 Sec
```

**Table 1-4 display ripng route** command output description

Field	Description
Peer	Neighbor connected to the interface
Dest	IPv6 destination address
via	Next hop IPv6 address
cost	Routing metric value
tag	Route tag
Sec	Time that a route entry stays in a particular state
"A"	The route is in the aging state.
"S"	The route is in the suppressed state.
"G"	The route is in the Garbage-collect state.

## filter-policy export

### Syntax

```
filter-policy { acl6-number | ipv6-prefix ipv6-prefix-name } export [ protocol [ process-id ] ]  
undo filter-policy export [ protocol [ process-id ] ]
```

### View

RIPng view

### Default Level

2: System level

### Parameters

*acl6-number*: Specifies the number of an ACL to filter advertised routing information, in the range of 2000 to 3999.

**ipv6-prefix** *ipv6-prefix-name*: Specifies the name of an IPv6 prefix list used to filter routing information, a string of 1 to 19 characters.

*protocol*: Filters routes redistributed from a routing protocol, currently including **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng**, and **static**.

*process-id*: Process number of the specified routing protocol, in the range of 1 to 65535. This argument is available only when the routing protocol is **rip**, **ospf**, or **isis**.

### Description

Use the **filter-policy export** command to define an outbound route filtering policy. Only routes passing the filter can be advertised in the update messages.

Use the **undo filter-policy export** command to restore the default.

By default, RIPng does not filter any outbound routing information.

With the *protocol* argument specified, only routing information redistributed from the specified routing protocol will be filtered. Otherwise, all outgoing routing information will be filtered.

### Examples

```
# Use IPv6 prefix list Filter 2 to filter advertised RIPng updates.  
<Sysname> system-view  
[Sysname] ripng 100  
[Sysname-ripng-100] filter-policy ipv6-prefix Filter2 export
```

## filter-policy import (RIPng view)

### Syntax

```
filter-policy { acl6-number | ipv6-prefix ipv6-prefix-name } import  
undo filter-policy import
```

### View

RIPng view

## Default Level

2: System level

## Parameters

*acl6-number*: Specifies the number of an ACL to filter incoming routing information, in the range of 2000 to 3999.

**ipv6-prefix** *ipv6-prefix-name*: Specifies the name of an IPv6 prefix list to filter incoming routes, in the range 1 to 19 characters.

## Description

Use the **filter-policy import** command to define an inbound route filtering policy. Only routes which match the filtering policy can be received.

Use the **undo filter-policy import** command to disable inbound route filtering.

By default, RIPng does not filter incoming routing information.

## Examples

# Reference IPv6 prefix list **Filter1** to filter incoming RIPng updates.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy ipv6-prefix Filter1 import
```

## import-route

### Syntax

```
import-route protocol [ process-id ] [ allow-ibgp ] [ cost cost | route-policy route-policy-name ] *
undo import-route protocol [ process-id ]
```

### View

RIPng view

## Default Level

2: System level

## Parameters

*protocol*: Specifies a routing protocol from which to redistribute routes. Currently, it can be **bgp4+**, **direct**, **isisv6**, **ospfv3**, or **static**.

*process-id*: Process ID, in the range of 1 to 65535. The default is 1. This argument is available only when the protocol is **isisv6**, or **ospfv3**.

*cost*: Routing metric of redistributed routes, in the range of 0 to 16. If *cost value* is not specified, the metric is the default metric specified by the **default cost** command.

**route-policy** *route-policy-name*: Specifies a routing policy by its name with 1 to 19 characters.

**allow-ibgp**: Optional keyword when the specified *protocol* is **bgp4+**. The **import-route bgp4+** command redistributes only EBGP routes. The **import-route bgp4+ allow-ibgp** command redistributes additionally IBGP routes, thus be cautious when using it.

## Description

Use the **import-route** command to redistribute routes from another routing protocol.

Use the **undo import-route** command to disable redistributing routes from another routing protocol.

By default, RIPng does not redistribute routes from other routing protocols.

- You can configure a routing policy to redistribute only needed routes.
- You can specify a cost for redistributed routes using the **cost** keyword.

Related commands: **default cost**.

## Examples

```
# Redistribute IPv6-IS-IS routes (process 7) and specify the metric as 7.
```

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] import-route isisv6 7 cost 7
```

## maximum load-balancing (RIPng view)

### Syntax

```
maximum load-balancing number
```

```
undo maximum load-balancing
```

### View

RIPng view

### Default Level

2: System level

### Parameters

*number*: Maximum number of equal-cost load-balanced routes. Its value is in the range 1 to 4..

## Description

Use the **maximum load-balancing** command to specify the maximum number of equal-cost routes for load balancing.

Use the **undo maximum load-balancing** command to restore the default.

By default, the maximum number of equal cost routes for load balancing is 4.



### Note

Configure the maximum number according to the memory size.

---

## Examples

```
# Set the maximum number of load balanced routes with equal cost to 2.
```

```
<Sysname> system-view
```

```
[Sysname] ripng 100
[Sysname-ripng-100] maximum load-balancing 2

# Restore the default.

[Sysname-ripng-100] undo maximum load-balancing
```

## preference

### Syntax

```
preference [ route-policy route-policy-name ] preference
undo preference [ route-policy ]
```

### View

RIPng view

### Default Level

2: System level

### Parameters

*route-policy-name*: Name of a routing policy, in the range of 1 to 19 characters.

*preference*: RIPng route priority, in the range of 1 to 255.

### Description

Use the **preference** command to specify the RIPng route priority.

Use the **undo preference route-policy** command to restore the default.

By default, the priority of a RIPng route is 100.

Using the **route-policy** keyword can set a priority for routes filtered in by the routing policy:

- If a priority is set in the routing policy, the priority applies to matched routes, and the priority set by the **preference** command applies to routes not matched.
- If no priority is set in the routing policy, the one set by the **preference** command applies to all routes.

### Examples

```
# Set the RIPng route priority to 120.
```

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] preference 120
```

```
# Restore the default RIPng route priority.
```

```
[Sysname-ripng-100] undo preference
```

## ripng

### Syntax

```
ripng [ process-id ]
undo ripng [ process-id ]
```

## View

System view

## Default Level

2: System level

## Parameters

*process-id*: RIPng process ID, in the range of 1 to 65535. The default value is 1.

## Description

Use the **ripng** command to create a RIPng process and enter RIPng view.

Use the **undo ripng** command to disable a RIPng process.

By default, no RIPng process is enabled.

## Examples

# Create RIPng process 100 and enter its view.

```
<Sysname> system-view  
[Sysname] ripng 100  
[Sysname-ripng-100]
```

# Disable RIPng process 100.

```
[Sysname] undo ripng 100
```

## ripng default-route

### Syntax

```
ripng default-route { only | originate } [ cost cost ]
```

```
undo ripng default-route
```

### View

Interface view

### Default Level

2: System level

### Parameters

**only**: Indicates that only the IPv6 default route (::/0) is advertised through the interface.

**originate**: Indicates that the IPv6 default route (::/0) is advertised without suppressing other routes.

*cost*: Metric of the advertised default route, in the range of 1 to 15, with a default value of 1.

### Description

Use the **ripng default-route** command to advertise a default route with the specified routing metric to a RIPng neighbor.

Use the **undo ripng default-route** command to stop advertising or forwarding the default route.

By default, a RIP process does not advertise any default route.

After you execute this command, the generated RIPng default route is advertised in a route update over the specified interface. This IPv6 default route is advertised without considering whether it already exists in the local IPv6 routing table.

## Examples

# Advertise only the default route through VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng default-route only
```

# Advertise the default route together with other routes through VLAN-interface 101.

```
<Sysname> system-view
[Sysname] interface vlan-interface 101
[Sysname-Vlan-interface101] ripng default-route originate
```

## ripng enable

### Syntax

```
ripng process-id enable
undo ripng enable
```

### View

Interface view

### Default Level

2: System level

### Parameters

*process-id*: RIPng process ID, in the range of 1 to 65535.

### Description

Use the **ripng enable** command to enable RIPng on the specified interface.

Use the **undo ripng enable** command to disable RIPng on the specified interface.

By default, RIPng is disabled on an interface.

## Examples

# Enable RIPng100 on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng 100 enable
```

## ripng metricin

### Syntax

```
ripng metricin value
undo ripng metricin
```

## View

Interface view

## Default Level

2: System level

## Parameters

*value*: Additional metric for received routes, in the range of 0 to 16.

## Description

Use the **ripng metricin** command to specify an additional metric for received RIPng routes.

Use the **undo ripng metricin** command to restore the default.

By default, the additional metric to received routes is 0.

Related commands: **ripng metricout**.

## Examples

# Specify the additional routing metric as 12 for RIPng routes received by VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng metricin 12
```

## ripng metricout

### Syntax

**ripng metricout** *value*

**undo ripng metricout**

### View

Interface view

### Default Level

2: System level

### Parameters

*value*: Additional metric to advertised routes, in the range of 1 to 16.

### Description

Use the **ripng metricout** command to configure an additional metric for RIPng routes advertised by an interface.

Use the **undo rip metricout** command to restore the default.

The default additional routing metric is 1.

Related commands: **ripng metricin**.

### Examples

# Set the additional metric to 12 for routes advertised by VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng metricout 12
```

## ripng poison-reverse

### Syntax

```
ripng poison-reverse
undo ripng poison-reverse
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **rip poison-reverse** command to enable the poison reverse function.

Use the **undo rip poison-reverse** command to disable the poison reverse function.

By default, the poison reverse function is disabled.

### Examples

Enable the poison reverse function for RIPng update messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng poison-reverse
```

## ripng split-horizon

### Syntax

```
ripng split-horizon
undo ripng split-horizon
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

## Description

Use the **rip split-horizon** command to enable the split horizon function.

Use the **undo rip split-horizon** command to disable the split horizon function.

By default, the split horizon function is enabled.

Note that:

- The split horizon function is necessary for preventing routing loops. Therefore, you are not recommended to disable it.
- In special cases, make sure that it is necessary to disable the split horizon function before doing so.



### Note

If both the poison reverse and split horizon functions are enabled, only the poison reverse function takes effect.

---

## Examples

Enable the split horizon function on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng split-horizon
```

## ripng summary-address

### Syntax

```
ripng summary-address ipv6-address prefix-length
undo ripng summary-address ipv6-address prefix-length
```

### View

Interface view

### Default Level

2: System level

### Parameters

*ipv6-address*: Destination IPv6 address of the summary route.

*prefix-length*: Prefix length of the destination IPv6 address of the summary route, in the range of 0 to 128. It indicates the number of consecutive 1s of the prefix, which defines the network ID.

## Description

Use the **ripng summary-address** command to configure a summary network to be advertised through the interface.

Use the **undo ripng summary-address** command to remove the summary.

Networks falling into the summary network will not be advertised. The cost of the summary route is the lowest cost among summarized routes.

## Examples

# Assign an IPv6 address with the 64-bit prefix to VLAN-interface 100 and configure a summary with the 35-bit prefix length.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001:200::3EFF:FE11:6770/64
[Sysname-Vlan-interface100] ripng summary-address 2001:200:: 35
```

## timers

### Syntax

**timers** { **garbage-collect** *garbage-collect-value* | **suppress** *suppress-value* | **timeout** *timeout-value* | **update** *update-value* } \*

**undo timers** { **garbage-collect** | **suppress** | **timeout** | **update** } \*

### View

RIPng view

### Default Level

2: System level

### Parameters

*garbage-collect-value*: Interval of the garbage-collect timer in seconds, in the range of 1 to 86400.

*suppress-value*: Interval of the suppress timer in seconds, in the range of 0 to 86400.

*timeout-value*: Interval of the timeout timer in seconds, in the range of 1 to 86400.

*update-value*: Interval of the update timer in seconds, in the range of 1 to 86400.

### Description

Use the **timers** command to configure RIPng timers.

Use the **undo timers** command to restore the default.

By default, the garbage-collect timer is 120 seconds, the suppress timer 120 seconds, the timeout timer 180 seconds, and the update timer 30 seconds.

RIPng is controlled by the above four timers.

- The update timer defines the interval between update messages.
- The timeout timer defines the route aging time. If no update message related to a route is received within the aging time, the metric of the route is set to 16 in the routing table.
- The suppress timer defines for how long a RIPng route stays in the suppressed state. When the metric of a route is 16, the route enters the suppressed state. In the suppressed state, only routes which come from the same neighbor and whose metric is less than 16 will be received by the router to replace unreachable routes.
- The garbage-collect timer defines the interval from when the metric of a route becomes 16 to when it is deleted from the routing table. During the garbage-collect timer length, RIPng advertises the

route with the routing metric set to 16. If no update message is announced for that route before the garbage-collect timer expires, the route will be completely deleted from the routing table.

Note that:

- You are not recommended to change the default values of these timers under normal circumstances.
- The lengths of these timers must be kept consistent on all routers and access servers in the network

## Examples

# Configure the update, timeout, suppress, and garbage-collect timers as 5s, 15s, 15s and 30s.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] timers update 5
[Sysname-ripng-100] timers timeout 15
[Sysname-ripng-100] timers suppress 15
[Sysname-ripng-100] timers garbage-collect 30
```

# Table of Contents

<b>1 OSPFv3 Configuration Commands</b> .....	<b>1-1</b>
OSPFv3 Configuration Commands.....	1-1
abr-summary (OSPFv3 area view).....	1-1
area (OSPFv3 view) .....	1-2
bandwidth-reference.....	1-2
default cost .....	1-3
default-cost (OSPFv3 area view) .....	1-4
default-route-advertise.....	1-4
display ospfv3.....	1-5
display ospfv3 graceful-restart status.....	1-7
display ospfv3 interface .....	1-8
display ospfv3 lsdb .....	1-9
display ospfv3 lsdb statistic.....	1-12
display ospfv3 next-hop.....	1-13
display ospfv3 peer.....	1-13
display ospfv3 peer statistic .....	1-15
display ospfv3 request-list.....	1-16
display ospfv3 retrans-list.....	1-18
display ospfv3 routing.....	1-19
display ospfv3 statistics.....	1-21
display ospfv3 topology .....	1-22
display ospfv3 vlink.....	1-23
filter-policy export (OSPFv3 view) .....	1-24
filter-policy import (OSPFv3 view).....	1-25
graceful-restart enable.....	1-26
graceful-restart helper enable .....	1-27
graceful-restart helper strict-lsa-checking .....	1-27
graceful-restart interval.....	1-28
import-route (OSPFv3 view).....	1-28
log-peer-change .....	1-29
maximum load-balancing (OSPFv3 view) .....	1-30
ospfv3 .....	1-31
ospfv3 area.....	1-31
ospfv3 cost .....	1-32
ospfv3 dr-priority.....	1-33
ospfv3 mtu-ignore.....	1-33
ospfv3 network-type .....	1-34
ospfv3 peer.....	1-35
ospfv3 timer dead.....	1-35
ospfv3 timer hello .....	1-36
ospfv3 timer retransmit.....	1-37
ospfv3 timer poll .....	1-38
ospfv3 trans-delay .....	1-38

preference .....	1-39
router-id .....	1-40
silent-interface(OSPFv3 view).....	1-40
spf timers .....	1-41
stub (OSPFv3 area view) .....	1-42
vlink-peer (OSPFv3 area view) .....	1-42

# 1 OSPFv3 Configuration Commands

---

## OSPFv3 Configuration Commands

### abr-summary (OSPFv3 area view)

#### Syntax

```
abr-summary ipv6-address prefix-length [ not-advertise ]  
undo abr-summary ipv6-address prefix-length
```

#### View

OSPFv3 area view

#### Default Level

2: System level

#### Parameters

*ipv6-address*: Destination IPv6 address of the summary route.

*prefix-length*: Prefix length of the destination IPv6 address, in the range 0 to 128. This argument specifies the number of consecutive 1s of the prefix, which defines the network ID.

**not-advertise**: Specifies not to advertise the summary IPv6 route.

#### Description

Use the **abr-summary** command to configure an IPv6 summary route on an area border router.

Use the **undo abr-summary** command to remove an IPv6 summary route. Then the summarized routes are advertised.

By default, no route summarization is available on an ABR.

You can use this command only on an ABR to configure a summary route for the area. The ABR advertises only the summary route to other areas. Multiple contiguous networks may be available in an area, where you can summarize them with one route for advertisement.

#### Examples

```
# Summarize networks 2000:1:1:1::/64 and 2000:1:1:2::/64 in Area 1 with 2000:1:1::/48.
```

```
<Sysname> system-view  
[Sysname] ospfv3 1  
[Sysname-ospfv3-1] area 1  
[Sysname-ospfv3-1-area-0.0.0.1] abr-summary 2000:1:1:: 48
```

## area (OSPFv3 view)

### Syntax

```
area area-id
```

### View

OSPFv3 view

### Default Level

2: System level

### Parameters

*area-id*: ID of an area, a decimal integer (in the range of 0 to 4294967295 and changed to IPv4 address format by the system) or an IPv4 address.

### Description

Use the **area** command to enter OSPFv3 area view.



#### Note

The undo form of the command is not available. An area is removed automatically if there is no configuration and no interface is up in the area.

---

### Examples

```
# Enter OSPFv3 Area 0 view.  
<Sysname> system-view  
[Sysname] ospfv3 1  
[Sysname-ospfv3-1] area 0  
[Sysname-ospfv3-1-area-0.0.0.0]
```

## bandwidth-reference

### Syntax

```
bandwidth-reference value  
undo bandwidth-reference
```

### View

OSPFv3 view

### Default Level

2: System level

### Parameters

*value*: Bandwidth reference value for link cost calculation, in the range 1 to 2147483648 Mbps.

## Description

Use the **bandwidth-reference** command to specify a reference bandwidth value for link cost calculation.

Use the **undo bandwidth-reference** command to restore the default value.

The default value is 100 Mbps.

You can configure an OSPFv3 cost for an interface with one of the following two methods:

- Configure the cost value in interface view.
- Configure a bandwidth reference value, and OSPFv3 computes the cost automatically based on the bandwidth reference value: Interface OSPFv3 cost = Bandwidth reference value/Interface bandwidth. If the calculated cost is greater than 65535, the value of 65535 is used.

If no cost value is configured for an interface, OSPFv3 computes the interface cost value automatically:

## Examples

# Specify the reference bandwidth value as 1000 Mbps.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] bandwidth-reference 1000
```

## default cost

### Syntax

**default cost** *value*

**undo default cost**

### View

OSPFv3 view

### Default Level

2: System level

### Parameters

*value*: Specifies a default cost for redistributed routes, in the range of 1 to 16777214.

## Description

Use the **default cost** command to configure a default cost for redistributed routes.

Use the **undo default cost** command to restore the default.

By default, the default cost is 1.

You need to configure the default cost value for redistributed routes to advertise them throughout the whole AS.

## Examples

# Specify the default cost for redistributed routes as 10.

```
<Sysname> system-view
[Sysname] ospfv3 1
```

```
[Sysname-ospfv3-1] default cost 10
```

## default-cost (OSPFv3 area view)

### Syntax

```
default-cost value  
undo default-cost
```

### View

OSPFv3 area view

### Default Level

2: System level

### Parameters

*value*: Specifies a cost for the default route advertised to the stub area, in the range of 0 to 65535. The default is 1.

### Description

Use the **default-cost** command to specify the cost of the default route to be advertised to the stub area.

Use the **undo-default-cost** command to restore the default value.

Use of this command is only available on the ABR that is connected to a stub area.

You have two commands to configure a stub area: **stub**, **defaulted-cost**. You need to use the **stub** command on routers connected to a stub area to configure the area as stub.

Related commands: **stub**.

### Examples

```
# Configure Area1 as a stub area, and specify the cost of the default route advertised to the stub area as 60.
```

```
<Sysname> system-view  
[Sysname] ospfv3  
[Sysname-ospfv3-1] area 1  
[Sysname-ospfv3-1-area-0.0.0.1] stub  
[Sysname-ospfv3-1-area-0.0.0.1] default-cost 60
```

## default-route-advertise

### Syntax

```
default-route-advertise [ always | cost cost | route-policy  
route-policy-name | type type ] *  
undo default-route-advertise
```

### View

OSPFv3 view

## Default Level

2: System level

## Parameters

**always**: Generates a default route in an ASE LSA into the OSPF routing domain regardless of whether the default route exists in the routing table. Without this keyword, the command can distribute a default route in a Type-5 LSA into the OSPF routing domain only when the default route exists in the routing table.

**cost** *cost*: Specifies a cost for the default route, in the range 1 to 16777214. The default is 1.

**route-policy** *route-policy-name*: Specifies a route policy, the name of which is a string of 1 to 19 characters.

**type** *type*: Specifies a type for the ASE LSA: 1 or 2. The default is 2.

## Description

Use the **default-route-advertise** command to generate a default route into the OSPF routing domain.

Use the **undo default-route-advertise** command to disable OSPF from redistributing a default route.

By default, no default route is redistributed.

Using the **import-route** command cannot redistribute a default route. To do so, you need to use the **default-route-advertise** command. If no default route exists in the router's routing table, use the **default-route-advertise always** command to generate a default route in a Type-5 LSA.

You can reference a routing policy to set the cost and type of the default route:

- The router advertises the default route only when it passes the routing policy.
- The default route passing the routing policy uses the cost set by the **apply cost** clause, and the type set by the **apply cost-type** clause in the routing policy.
- The default route cost's priority from high to low is: the cost set by the **apply cost** clause in the routing policy, the one set by the **default-route-advertise** command and the one set by the **default cost** command.
- The default route type's priority from high to low is: the type set by the **apply cost-type** clause in the routing policy, and the one set by the **default-route-advertise** command.
- If the **always** keyword is included, the default route is advertised regardless of whether it passes the routing policy and uses the cost and type specified by the **apply cost**, **apply cost-type** clauses in the first node of the routing policy.

Related commands: **import-route**.

## Examples

```
# Generate a default route into the OSPFv3 routing domain.
```

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] default-route-advertise always
```

## display ospfv3

### Syntax

```
display ospfv3 [ process-id ]
```

## View

Any view

## Default Level

1: Monitor level

## Parameters

*process-id*: Specifies the ID of an OSPFv3 process, ranging from 1 to 65535.

## Description

Use the **display ospfv3** command to display the brief information of an OSPFv3 process. If no process ID is specified, OSPFv3 brief information about all processes will be displayed.

## Examples

# Display brief information about all OSPFv3 processes.

```
<Sysname> display ospfv3
Routing Process "OSPFv3 (1)" with ID 1.1.1.1
  Graceful restart restarter enabled
  Graceful restart helper enabled
  Graceful restart helper strict-lsa-checking enabled
  Graceful restart interval 150 secs
  SPF schedule delay 5 secs, Hold time between SPFs 10 secs
  Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
  Number of external LSA 0. These external LSAs' checksum Sum 0x0000
  Number of AS-Scoped Unknown LSA 0
  Number of LSA originated 3
  Number of LSA received 0
  Number of areas in this router is 1
    Area 0.0.0.1
      Number of interfaces in this area is 1
      SPF algorithm executed 1 times
      Number of LSA 2. These LSAs' checksum Sum 0x20C8
      Number of Unknown LSA 0
```

**Table 1-1** display ospfv3 command output description

Field	Description
Routing Process "OSPFv3 (1)" with ID 1.1.1.1	OSPFv3 process is 1, and router ID is 1.1.1.1.
Graceful restart restarter enabled	The current process supports GR.
Graceful restart helper enabled	The current process supports the GR Helper capability.
Graceful restart helper strict-lsa-checking enabled	The current process supports GR Helper strict LSA checking.
Graceful restart interval 150 secs	GR restart interval
SPF schedule delay	Delay interval of SPF calculation
Hold time between SPFs	Hold time between SPF calculations

Field	Description
Minimum LSA interval	Minimum interval for generating LSAs
Minimum LSA arrival	Minimum LSA repeat arrival interval
Number of external LSA	Number of ASE LSAs
These external LSAs' checksum Sum	Sum of all the ASE LSAs' checksum
Number of AS-Scoped Unknown LSA	Number of LSAs with unknown flooding scope
Number of LSA originated	Number of LSAs originated
Number of LSA received	Number of LSAs received
Number of areas in this router	Number of areas this router is attached to
Area	Area ID
Number of interfaces in this area	Number of interfaces attached to this area
SPF algorithm executed 1 times	SPF algorithm is executed 1 time
Number of LSA	Number of LSAs
These LSAs' checksum Sum	Sum of all LSAs' checksum
Number of Unknown LSA	Number of unknown LSAs

## display ospfv3 graceful-restart status

### Syntax

**display ospfv3** [*process-id*] **graceful-restart status**

### View

Any view

### Default Level

1: Monitor level

### Parameters

*process-id*: ID of an OSPFv3 process, ranging from 1 to 65535.

### Description

Use the **display ospfv3 graceful-restart status** command to display GR status of the specified OSPFv3 process.

If no process ID is specified, GR status of all processes will be displayed.

### Examples

# Display GR status of all OSPFv3 processes (GR Restarter).

```
<Sysname> display ospfv3 graceful-restart status
      OSPFv3 Router with ID (1.1.1.1) (Process 1)
      graceful restart information
```

```
GR status      : Normal
```

**Table 1-2** display ospfv3 graceful-restart status command output description

Field	Description
OSPFv3 Router with ID (1.1.1.1) (Process 1) graceful restart information	The GR status of OSPFv3 process 1 with router ID 1.1.1.1 is displayed.
GR status	GR status, which can be: <ul style="list-style-type: none"><li>• GR in progress: Indicates GR is in process.</li><li>• Calculating routes: Indicates route calculation is in process.</li><li>• Flushing LSAs: Indicates the device is flushing stale LSA.</li><li>• Normal: Indicates the device is not in GR or Helper status.</li><li>• Helper: Indicates the Helper status.</li></ul>

## display ospfv3 interface

### Syntax

```
display ospfv3 interface [ interface-type interface-number | statistic ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*interface-type interface-number*: Interface type and interface number.

**statistic**: Displays the interface statistics.

### Description

Use the **display ospfv3 interface** command to display OSPFv3 interface information.

### Examples

```
# Display OSPFv3 interface information.
```

```
<Sysname> display ospfv3 interface vlan-interface 10
Vlan-interface 10 is up, line protocol is up
  Interface ID 518
  IPv6 Prefixes
    FE80::1441:0:E213:1 (Link-Local Address)
    2000:1::1
  OSPFv3 Process (1), Area 0.0.0.1, Instance ID 0
  Router ID 2.2.2.2, Network Type POINTOPOINT, Cost: 1562
  Transmit Delay is 1 sec, State Point-To-Point, Priority 1
  No designated router on this link
  No backup designated router on this link
  Timer interval configured, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5
```

```

Hello due in 00:00:02
Neighbor Count is 1, Adjacent neighbor count is 1

```

**Table 1-3 display ospfv3 interface command output description**

Field	Description
Interface ID	Interface ID
IPv6 Prefixes	IPv6 Prefix
OSPFv3 Process	OSPFv3 Process
Area	Area ID
Instance ID	Instance ID
Router ID	Router ID
Network Type	Network type of the interface
Cost	Cost value of the interface
Transmit Delay	Transmission delay of the interface
State	Interface state
Priority	DR priority of the interface
No designated router on this link	No designated router on this link
No backup designated router on this link	No backup designated router on this link
Timer interval configured, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5	Time intervals in seconds configured on the interface, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5
Hello due in 00:00:02	Hello packet will be sent in 2 seconds
Neighbor Count	Number of Neighbors on the interface
Adjacent neighbor count	Number of Adjacencies on the interface

## display ospfv3 lsdb

### Syntax

```

display ospfv3 [ process-id ] lsdb [ [ external | inter-prefix | inter-router | intra-prefix | link |
network | router | grace ] [ link-state-id ] [ originate-router router-id ] | total ]

```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**process-id**: Specifies ID of an OSPFv3 process, ranging from 1 to 65535.

**external**: Displays information about AS-external LSAs.

**inter-prefix**: Displays information about Inter-area-prefix LSAs.

**inter-router:** Displays information about Inter-area-router LSAs.

**intra-prefix:** Displays information about Intra-area-prefix LSAs.

**link:** Displays information about Link-LSAs.

**network:** Displays information about Network-LSAs.

**router:** Displays information about Router-LSAs.

**grace:** Displays information about Grace-LSAs

*link-state-id:* Link state ID, an IPv4 address.

**originate-router** *router-id:* ID of the advertising router .

**total:** Displays the LSA statistics information in the LSDB.

## Description

Use the **display ospfv3 lsdb** command to display OSPFv3 LSDB information.

## Examples

```
# Display OSPFv3 LSDB information.
```

```
<Sysname> display ospfv3 lsdb
```

```
                OSPFv3 Router with ID (1.1.1.1) (Process 1)
                Link-LSA (Interface Vlan-interface100)
-----
Link State ID   Origin Router   Age   SeqNum   CkSum   Prefix
2.50.0.99      1.1.1.1        0212  0x80000002 0x1053   1

                Router-LSA (Area 0.0.0.0)
-----
Link State ID   Origin Router   Age   SeqNum   CkSum   Link
0.0.0.0        1.1.1.1        0167  0x80000004 0x0a21   0

                Intra-Area-Prefix-LSA (Area 0.0.0.0)
-----
Link State ID   Origin Router   Age   SeqNum   CkSum   Prefix   Reference
0.0.0.1        1.1.1.1        0162  0x80000004 0x0cac   1   Router-LSA
```

**Table 1-4 display ospfv3 lsdb** command output description

Field	Description
Link-LSA	Type 8 LSA
Link State ID	Link State ID
Origin Router	Originating Router
Age	Age of LSAs
Seq#	LSA sequence number
CkSum	LSA Checksum
Prefix	Number of Prefixes
Router-LSA	Router-LSA

Field	Description
Link	Number of links
Network-LSA	Network-LSA
Intra-Area-Prefix-LSA	Type 9 LSA
Reference	Type of referenced LSA

# Display Link-local LSA information in the LSDB.

```
<Sysname> display ospfv3 lsdb link
      OSPFv3 Router with ID (1.1.1.1) (Process 1)
          Link-LSA (Interface Vlan-interface100)
-----
LS age           : 634
LS Type          : Link-LSA
Link State ID    : 2.50.0.99
Originating Router: 1.1.1.1
LS Seq Number    : 0x80000002
Checksum         : 0x1053
Length          : 56
Priority         : 1
Options          : 0x000013 (-|R|-|-|E|V6)
Link-Local Address: FE80::200:FCFF:FE00:6505
Number of Prefixes: 1
  Prefix         : 1::/64
  Prefix Options: 0 (-|-|-|-)
```

**Table 1-5 display ospfv3 lsdb command output description**

Field	Description
LS age	Age of LSA
LS Type	Type of LSA
Originating Router	Originating Router
LS Seq Number	LSA Sequence Number
Checksum	LSA Checksum
Length	LSA Length
Priority	Router Priority
Options	Options
Link-Local Address	Link-Local Address
Number of Prefixes	Number of Prefixes
Prefix	Address prefix
Prefix Options	Prefix options

## display ospfv3 lsdb statistic

### Syntax

```
display ospfv3 lsdb statistic
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display ospfv3 lsdb statistic** command to display LSA statistics in the OSPFv3 LSDB.

### Examples

```
# Display OSPFv3 LSDB statistics.
```

```
<System> display ospfv3 lsdb statistic
```

```
                OSPFv3 Router with ID (1.1.1.1) (Process 1)
                LSA Statistics
-----
Area ID          Router   Network  InterPre  InterRou  IntraPre  Link   Grace  ASE
0.0.0.0          2       1        1         0         1
0.0.0.1          1       0        1         0         1
Total            3       1        2         0         2         3     0     0
```

**Table 1-6** Descriptions on the fields of the **display ospfv3 lsdb statistic** command output description

Field	Description
Area ID	Area ID
Router	Router-LSA number
Network	Network-LSA number
InterPre	Inter-Area-Prefix-LSA number
InterRou	Inter-Area-Router-LSA number
IntraPre	Intra-Area-Prefix-LSA number
Link	Link-LSA number
Grace	Grace-LSA number
ASE	AS-external-LSA number
Total	Total LSA number

## display ospfv3 next-hop

### Syntax

```
display ospfv3 [ process-id ] next-hop
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*process-id*: Specifies ID of an OSPFv3 process, ranging from 1 to 65535.

### Description

Use the **display ospfv3 next-hop** command to display OSPFv3 next hop information. If no process is specified, next hop information of all OSPFv3 processes is displayed.

### Examples

# Display OSPFv3 next hop information.

```
<Sysname> display ospfv3 next-hop
```

```
                OSPFv3 Router with ID (2.2.2.2) (Process 1)
Neighbor-Id      Next-Hop                Interface    RefCount
1.1.1.1          FE80::20F:E2FF:FE00:1   Vlan100     1
```

**Table 1-7 display ospfv3 next-hop** command output description

Field	Description
Neighbor-Id	Neighboring router ID
Next-hop	Next-hop address
Interface	Outbound interface
RefCount	Reference count

## display ospfv3 peer

### Syntax

```
display ospfv3 [ process-id ] [ area area-id ] peer [ [ interface-type interface-number ] [ verbose ] | peer-router-id ]
```

### View

Any view

### Default Level

1: Monitor level

## Parameters

*process-id*: Specifies the ID of an OSPFv3 process, ranging from 1 to 65535.

**area**: Specifies to display neighbor information of the specified area.

*area-id*: The ID of an area, a decimal integer that is translated into IPv4 address format by the system (in the range of 0 to 4294967295) or an IPv4 address.

*interface-type interface-number*: interface type and number.

**verbose**: Display detailed neighbor information.

*peer-router-id*: Router-ID of the specified neighbor.

## Description

Use the **display ospfv3 peer** command to display OSPFv3 neighbor information.

- If no *area-id* is specified, the neighbor information of all areas is displayed.
- If no *process-id* is specified, the information of all processes is displayed.
- If no interface or neighbor Router-ID is specified, the neighbor information of all interfaces is displayed.

## Examples

# Display the neighbor information of OSPFv3 process 1 on an interface.

```
<Sysname> display ospfv3 1 peer vlan-interface 10
                OSPFv3 Process (1)
Neighbor ID      Pri   State           Dead Time   Interface   Instance ID
1.1.1.1          1    Full/ -         00:00:30   vlan10      0
```

**Table 1-8** display ospfv3 peer command output description

Field	Description
Neighbor ID	Router ID of a neighbor
Pri	Priority of neighbor router
State	Neighbor state
Dead Time	Dead time remained
Interface	Interface connected to the neighbor
Instance ID	Instance ID

# Display detailed neighbor information of OSPFv3 process 100 of an interface.

```
<Sysname> display ospfv3 1 peer vlan-interface 33 verbose
                OSPFv3 Process (1)
Neighbor 1.1.1.1 is Full, interface address FE80::20F:E2FF:FE49:8050
  In the area 0.0.0.1 via interface Vlan-interface33
  DR is 1.1.1.1 BDR is 2.2.2.2
  Options is 0x000013 (-|R|-|-|E|V6)
  Dead timer due in 00:00:39
  Neighbor is up for 00:25:31
  Database Summary List 0
```

```

Link State Request List 0
Link State Retransmission List 0
Graceful restart state: Normal

```

**Table 1-9 display ospfv3 peer verbose command output description**

Field	Description
Neighbor	Neighbor ID
interface address	Interface address
In the area 0.0.0.1 via interface Vlan-interface33	Interface Vlan-interface33 belongs to area 1
DR is 0.0.0.0 BDR is 0.0.0.0	Neither DR nor BDR is elected
Options is 0x000013 (- R - - E V6)	The option is 0x000013 (- R - - E V6)
Dead timer due in 00:00:29	Dead timer due in 00:00:29
Neighbor is up for 00:25:31	Neighbor is up for 00:25:31
Database Summary List	Number of LSAs sent in DD packet
Link State Request List	Number of LSAs in the link state request list
Link State Retransmission List	Number of LSAs in the link state retransmission list
Graceful restart state	GR status, which can be: <ul style="list-style-type: none"> <li>• Doing GR: Indicates GR is in process.</li> <li>• Complete GR: Indicates the neighbor has completed GR.</li> <li>• Normal: Indicates normal status</li> <li>• Helper: Indicates the device is a GR Helper of the neighbor.</li> </ul>

## display ospfv3 peer statistic

### Syntax

```
display ospfv3 peer statistic
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display ospfv3 peer statistic** command to display information about all OSPFv3 neighbors on the router, that is, numbers of neighbors in different states.

### Examples

```
# Display information about all OSPFv3 neighbors.
```

```
<Sysname> display ospfv3 peer statistic
```

```

                OSPFv3 Router with ID (1.1.1.1) (Process 1)
                Neighbor Statistics
-----
Area ID          Down      Init      2-way      ExStar      Exchange  Loading  Full
0.0.0.0          0         0         0           0           0         0        1
Total            0         0         0           0           0         0        1

```

**Table 1-10** display ospfv3 peer statistic command output description

Field	Description
Area ID	Area ID
Down	In this state, neighbor initial state, the router has not received any information from a neighboring router for a period of time.
Init	In this state, the device received a Hello packet from the neighbor but the packet contains no Router ID of the neighbor. Mutual communication is not setup.
2-Way	Indicates mutual communication between the router and its neighbor is available. DR/BDR election is finished under this state (or higher).
ExStart	In this state, the router decides on the initial DD sequence number and master/slave relationship of the two parties.
Exchange	In this state, the router exchanges DD packets with the neighbor.
Loading	In this state, the router sends LSRs to request the neighbor for needed LSAs.
Full	Indicates LSDB synchronization has been accomplished between neighbors.
Total	Total number of neighbors under the same state

## display ospfv3 request-list

### Syntax

```
display ospfv3 [ process-id ] request-list [ { external | inter-prefix | inter-router | intra-prefix | link |
network | router | grace } [ link-state-id ] [ originate-router ip-address ] | statistics ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*process-id*: OSPFv3 process ID, in the range 1 to 65535.

**external**: Displays the AS-external LSA information of the OSPFv3 link state request list.

**inter-prefix**: Displays the Inter-area-prefix LSA information of the OSPFv3 link state request list.

**inter-router**: Displays the Inter-area-router LSA information of the OSPFv3 link state request list.

**intra-prefix**: Displays the Intra-area-prefix LSA information of the OSPFv3 link state request list.

**link**: Displays the Link LSA information of the OSPFv3 link state request list.

**network:** Displays the Network-LSA information of the OSPFv3 link state request list.

**router:** Displays the Router-LSA information of the OSPFv3 link state request list.

**grace:** Displays the Grace-LSA information of the OSPFv3 link state request list.

*link-state-id:* Link state ID, in the format of an IPv4 address.

**originate-router ip-address:** Specifies the router ID of an advertising router.

**statistics:** Displays the LSA statistics of the OSPFv3 link state request list.

## Description

Use the **display ospfv3 request-list** command to display OSPFv3 link state request list information. If no process is specified, the link state request list information of all OSPFv3 processes is displayed.

## Examples

# Display the information of OSPFv3 link state request list.

```
<Sysname> display ospfv3 request-list
      OSPFv3 Router with ID (11.1.1.1) (Process 1)
      Interface Vlan100   Area-ID 0.0.0.0
      -----
      Nbr-ID   12.1.1.1
LS-Type      LS-ID      AdvRouter   SeqNum      Age   CkSum
Router-LSA   0.0.0.0    12.1.1.1    0x80000014  774   0xe5b0
```

**Table 1-11** display ospfv3 request-list command output description

Field	Description
Interface	Interface name
Area-ID	Area ID
Nbr-ID	Neighbor router ID
LS-Type	Type of LSA
LS-ID	Link state ID
AdvRouter	Advertising router
SeqNum	LSA sequence number
Age	Age of LSA
CkSum	Checksum

# Display the statistics of OSPFv3 link state request list.

```
<Sysname> display ospfv3 request-list statistics
      OSPFv3 Router with ID (11.1.1.1) (Process 1)
Interface Neighbor   LSA-Count
Vlan100   10.1.1.1     0
```

**Table 1-12** display ospfv3 request-list statistics command output description

Field	Description
Interface	Interface name
Neighbor	Neighbor router ID
LSA-Count	Number of LSAs in the request list

## display ospfv3 retrans-list

### Syntax

```
display ospfv3 [ process-id ] retrans-list [ { external | inter-prefix | inter-router | intra-prefix | link | network | router | grace } [ link-state-id ] [ originate-router ip-address ] | statistics ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*process-id*: OSPFv3 process ID, in the range 1 to 65535.

**external**: Displays the AS-external LSA information of the OSPFv3 link state retransmission list.

**inter-prefix**: Displays the Inter-area-prefix LSA information of the OSPFv3 link state retransmission list.

**inter-router**: Displays the Inter-area-router LSA information of the OSPFv3 link state retransmission list.

**intra-prefix**: Displays the Intra-area-prefix LSA information of the OSPFv3 link state retransmission list.

**link**: Displays the Link LSA information of the OSPFv3 link state retransmission list.

**network**: Displays the Network-LSA information of the OSPFv3 link state retransmission list.

**router**: Displays the Router-LSA information of the OSPFv3 link state retransmission list.

**grace**: Displays the Grace-LSA information of the OSPFv3 link state request list.

*link-state-id*: Link state ID, in the format of an IPv4 address.

**originate-router ip-address**: Specifies the router ID of an advertising router.

**statistics**: Displays the LSA statistics of the OSPFv3 link state retransmission list.

### Description

Use the **display ospfv3 retrans-list** command to display the OSPFv3 link state retransmission list.

If no process is specified, the link state retransmission list information of all OSPFv3 processes is displayed.

### Examples

# Display the information of the OSPFv3 link state retransmission list.

```
<Sysname> display ospfv3 retrans-list
      OSPFv3 Router with ID (11.1.1.1) (Process 1)
```

```

                Interface Vlan100      Area-ID 0.0.0.0
-----
Nbr-ID      12.1.1.1
LS-Type          LS-ID          AdvRouter      SeqNum      Age  CkSum
Link-LSA        0.15.0.24      12.1.1.1      0x80000003  519  0x7823
Router-LSA      0.0.0.0          12.1.1.1      0x80000014  774  0xe5b0

```

**Table 1-13** display ospfv3 retrans-list command output description

Field	Description
Interface	Interface name
Area-ID	Area ID
Nbr-ID	Neighbor router ID
LS-Type	Type of LSA
LS-ID	Link state ID
AdvRouter	Advertising Router
SeqNum	LSA sequence Number
Age	Age of LSA
CkSum	Checksum

# Display the statistics of OSPFv3 link state retransmission list.

```

<Sysname>display ospfv3 retrans-list statistics
                OSPFv3 Router with ID (11.1.1.1) (Process 1)
Interface  Neighbor      LSA-Count
Vlan100    12.1.1.1      2

```

**Table 1-14** display ospfv3 retrans-list statistics command output description

Field	Description
Interface	Interface name
Neighbor	Neighbor ID
LSA-Count	Number of LSAs in the retransmission request list

## display ospfv3 routing

### Syntax

```

display ospfv3 [ process-id ] routing [ ipv6-address prefix-length | ipv6-address/prefix-length |
abr-routes | asbr-routes | all | statistics ]

```

### View

Any view

### Default Level

1: Monitor level

## Parameters

*process-id*: Specifies the ID of an OSPFv3 process, ranging from 1 to 65535.

*ipv6-address*: IPv6 address prefix.

*prefix-length*: Prefix length, in the range 0 to 128.

**abr-routes**: Displays routes to ABR.

**asbr-routes**: Displays routes to ASBR.

**all**: Displays all routes.

**statistics**: Displays the OSPFv3 routing table statistics .

## Description

Use the **display ospfv3 routing** command to display OSPFv3 routing table information.

If no process is specified, routing table information of all OSPFv3 processes is displayed.

## Examples

# Display OSPFv3 routing table information.

```
<Sysname> display ospfv3 routing
```

```
E1 - Type 1 external route,    IA - Inter area route,    I - Intra area route
E2 - Type 2 external route,    * - Selected route
```

```
OSPFv3 Router with ID (1.1.1.1) (Process 1)
```

```
-----
*Destination: 2001::/64
```

```
Type           : I                               Cost           : 1
NextHop        : directly-connected              Interface: Vlan100
```

**Table 1-15 display ospfv3 routing** command output description

Field	Description
Destination	Destination network segment
Type	Route type
Cost	Route cost value
Next-hop	Next hop address
Interface	Outbound interface

# Display the statistics of OSPFv3 routing table.

```
<Sysname> display ospfv3 routing statistics
```

```
OSPFv3 Router with ID (1.1.1.1) (Process 1)
```

```
OSPFv3 Routing Statistics
```

```
Intra-area-routes : 1
Inter-area-routes : 0
External-routes   : 0
```

**Table 1-16** display ospfv3 routing statistics command output description

Field	Description
Intra-area-routes	Number of Intra-area-routes
Inter-area-routes	Number of inter-area routes
External-routes	Number of external routes

## display ospfv3 statistics

### Syntax

**display ospfv3 statistics**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display ospfv3 statistics** command to display outbound/inbound OSPFv3 packet statistics on associated interface(s).

### Examples

# Display outbound/inbound OSPFv3 packet statistics on associated interfaces.

```
<Sysname> display ospfv3 statistics
                OSPFv3 Statistics
Interface Vlan-interface1 Instance 0
Type           Input      Output
Hello          2          2
DB Description 5          4
Ls Req         2          1
Ls Upd         5          4
Ls Ack         3          4
Discarded      0          0
```

**Table 1-17** display ospfv3 statistics command output description

Field	Description
Interface	Interface name
Instance	Instance number
Type	Type of packet
Input	Number of packets received by the interface

Field	Description
Output	Number of packets sent by the interface
Hello	Hello packet
DB Description	Database description packet
Ls Req	Link state request packet
Ls Upd	Link state update packet
Ls Ack	Link state acknowledgement packet
Discarded	Discarded packet

## display ospfv3 topology

### Syntax

```
display ospfv3 [ process-id ] topology [ area area-id ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*process-id*: Displays the topology information of an OSPFv3 process; The process ID ranges from 1 to 65535.

*area*: Displays the topology information of the specified area.

*area-id*: ID of an area, a decimal integer (in the range of 0 to 4294967295) that is translated into IPv4 address format by the system or an IPv4 address.

### Description

Use the **display ospfv3 topology** command to display OSPFv3 topology information. If no process is specified, topology information of all OSPFv3 processes is displayed.

### Examples

```
# Display OSPFv3 area 1 topology information.
<Sysname> display ospfv3 topology area 1
                OSPFv3 Process (1)
OSPFv3 Area (0.0.0.1) topology
Type  ID(If-Index)      Bits      Metric   Next-Hop      Interface
Rtr   1.1.1.1              --        --       --            --
Rtr   2.2.2.2              1         1        2.2.2.2      Vlan100
```

**Table 1-18 display ospfv3 topology command output description**

Field	Description
Type	Type of node
ID(If-Index)	Router ID
Bits	Flag bit
Metric	Cost value
Next-Hop	Next hop
Interface	Outbound interface

## display ospfv3 vlink

### Syntax

```
display ospfv3 [ process-id ] vlink
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*process-id*: Specifies the ID of an OSPFv3 process, ranging from 1 to 65535.

### Description

Use the **display ospfv3 vlink** command to display OSPFv3 virtual link information. If no process is specified, virtual link information of all OSPFv3 processes is displayed.

### Examples

```
# Display OSPFv3 virtual link information.
```

```
<Sysname> display ospfv3 vlink
Virtual Link VLINK1 to router 1.1.1.1 is up
Transit area :0.0.0.1 via interface Vlan-interface100, instance ID: 0
Local address: 2000:1::1
Remote address: 2001:1:1::1
Transmit Delay is 1 sec, State: P-To-P,
Timer intervals configured, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5
Hello due in 00:00:02
Adjacency state :Full
```

**Table 1-19 display ospfv3 vlink command output description**

Field	Description
Virtual Link VLINK1 to router 1.1.1.1 is up	The virtual link VLINK1 to router 1.1.1.1 is up
Transit area 0.0.0.1 via interface Vlan-interface100	Interface Vlan-interface100 in transit area 0.0.0.1.
instance ID	Instance ID
Local address	Local IPv6 address
Remote address	Remote IPv6 address
Transmit Delay	Transmit delay of sending LSAs
State	Interface state
Timer intervals configured, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5	Timer intervals in seconds, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5
Hello due in 00:00:02	Send hello packets in 2 seconds.
Adjacency state	Adjacency state

## filter-policy export (OSPFv3 view)

### Syntax

```
filter-policy { acl6-number | ipv6-prefix ipv6-prefix-name } export [ bgp4+ | direct | isisv6 process-id | ospfv3 process-id | ripng process-id | static ]
undo filter-policy export [ bgp4+ | direct | isisv6 process-id | ospfv3 process-id | ripng process-id | static ]
```

### View

OSPFv3 view

### Default Level

2: System level

### Parameters

**acl6-number**: Specifies the ACL6 number, ranging from 2000 to 3999.

**ipv6-prefix ipv6-prefix-name**: Specifies the name of an IPv6 prefix list, a string of up to 19 characters.

**bgp4+**: Filters BGP4+ routes.

**direct**: Filters direct routes.

**isisv6 process-id**: Specifies to filter the routes of an IPv6-IS-IS process, which is in the range of 1 to 65535.

**ospfv3 process-id**: Specifies to filter the routes of an OSPFv3 process, which is in the range of 1 to 65535.

**ripng process-id**: Specifies to filter the routes of a RIPng process, which in the range of 1 to 65535.

**static**: Specifies to filter static routes.

## Description

Use the **filter-policy export** command to filter redistributed routes.

Use the **undo filter-policy export** command to remove the configuration.

If no protocol is specified, all redistributed routes will be filtered.

By default, IPv6 OSPFv3 does not filter redistributed routes.



Using the **filter-policy export** command filters only routes redistributed by the **import-route** command. If the **import-route** command is not configured to redistribute routes from other protocols, use of the **filter-policy export** command does not take effect.

---

## Examples

# Filter all redistributed routes using IPv6 ACL 2001.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2001
[Sysname-acl6-basic-2001] rule permit source 2002:1:: 64
[Sysname-acl6-basic-2001] quit
[Sysname] ospfv3
[Sysname-ospfv3-1] filter-policy 2001 export
```

## filter-policy import (OSPFv3 view)

### Syntax

```
filter-policy { acl6-number | ipv6-prefix ipv6-prefix-name } import
undo filter-policy import
```

### View

OSPFv3 view

### Default Level

2: System level

### Parameters

*acl6-number*: Specifies an ACL number, ranging from 2000 to 3999.

**ipv6-prefix** *ipv6-prefix-name*: Specifies the name of an IPv6 prefix list, a string of up to 19 characters.

## Description

Use the **filter-policy import** command to configure OSPFv3 to filter routes computed from received LSAs.

Use the **undo filter-policy import** command to remove the configuration.

By default, OSPFv3 does not filter routes computed from received LSAs.

---



Using the **filter-policy import** command only filters routes computed by OSPFv3. The routes that fail to pass are not added to the routing table.

---

## Examples

```
# Filter received routes using the IPv6 prefix list abc.
```

```
<Sysname> system-view
[Sysname] ip ipv6-prefix abc permit 2002:1:: 64
[Sysname] ospfv3 1
[Sysname-ospfv3-1] filter-policy ipv6-prefix abc import
```

## graceful-restart enable

### Syntax

```
graceful-restart enable
undo graceful-restart enable
```

### View

```
OSPFv3 view
```

### Default Level

```
2: System level
```

### Parameters

```
None
```

### Description

Use the **graceful-restart enable** command to enable the GR capability for OSPFv3.

Use the **undo graceful-restart enable** command to disable the GR capability for OSPFv3.

By default, the GR capability for OSPFv3 is disabled.

You cannot enable the GR capability for an area of the current process already configured with the **vlink-peer** command.

## Examples

```
# Enable the GR capability for OSPFv3 process 1.
```

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] graceful-restart enable
```

## graceful-restart helper enable

### Syntax

```
graceful-restart helper enable
undo graceful-restart helper enable
```

### View

OSPFv3 view

### Default Level

2: System level

### Parameters

None

### Description

Use the **graceful-restart helper enable** command to enable the GR Helper capability for OSPFv3.

Use the **undo graceful-restart helper enable** command to disable the GR Helper capability for OSPFv3.

By default, the GR Helper capability for OSPFv3 is enabled.

### Examples

```
# Enable the GR Helper capability for OSPFv3 process 1.
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] graceful-restart helper enable
```

## graceful-restart helper strict-lsa-checking

### Syntax

```
graceful-restart helper strict-lsa-checking
undo graceful-restart helper strict-lsa-checking
```

### View

OSPFv3 view

### Default Level

2: System level

### Parameters

None

### Description

Use the **graceful-restart helper strict-lsa-checking** command to enable strict LSA checking for the GR Helper. When an LSA change on the GR Helper is detected, the GR Helper device exits the GR Helper mode.

Use the **undo graceful-restart helper strict-lsa-checking** command to disable strict LSA checking for the GR Helper.

By default, strict LSA checking for the GR Helper is disabled.

## Examples

```
# Enable strict LSA checking for the GR Helper in OSPFv3 process 1.
```

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] graceful-restart helper strict-lsa-checking
```

## graceful-restart interval

### Syntax

```
graceful-restart interval interval-value
undo graceful-restart interval
```

### View

OSPFv3 view

### Default Level

2: System level

### Parameters

*interval-value*: GR restart interval, in the range of 40 to 1800 seconds.

### Description

Use the **graceful-restart interval** command to configure the GR restart interval.

Use the **undo graceful-restart interval** command to restore the default.

By default, the GR restart interval is 120 seconds

The value of the GR restart interval cannot be smaller than the maximum OSPFv3 neighbor dead time of all the OSPFv3 interfaces; otherwise, GR restart may fail.

Related commands: **ospfv3 timer dead**

## Examples

```
# Configure the GR restart interval for OSPF process 1 as 100 seconds.
```

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] graceful-restart interval 100
```

## import-route (OSPFv3 view)

### Syntax

```
import-route { bgp4+ [ allow-ibgp ] | direct | isisv6 process-id | ospfv3 process-id | ripng process-id | static } [ cost value | route-policy route-policy-name | type type ] *
undo import-route { bgp4+ | direct | isisv6 process-id | ospfv3 process-id | ripng process-id | static }
```

**import-route** *protocol* [ *process-id* | **allow-ibgp** ] [ **cost** *cost* | **route-policy** *route-policy-name* | **type** *type* ] \*

**undo import-route** *protocol* [ *process-id* ]

## View

OSPFv3 view

## Default Level

2: System level

## Parameters

*protocol*: Redistributes routes from a specified routing protocol, which can be **bgp4+**, **direct**, **isisv6**, **ospf v3**, **ripng**, or **static**.

*process-id*: Process ID of the routing protocol, in the range 1 to 65536. It defaults to 1. This argument takes effect only when the protocol is **isisv6**, **ospfv3**, or **ripng**.

**allow-ibgp**: Allows redistributing iBGP routes. This keyword takes effect only the protocol is **bgp4+**.

**cost** *cost*: Specifies a cost for redistributed routes, ranging from 1 to 16777214. The default is 1.

**route-policy** *route-policy-name*: Redistributes only the routes that match the specified route policy. *route-policy-name* is a string of 1 to 19 characters.

**type** *type*: Specifies the type for redistributed routes, 1 or 2. It defaults to 2.



### Caution

Using the **import-route bgp4+** command redistributes only EBGP routes, while using the **import-route bgp4+ allow-ibgp** command redistributes both EBGP and IBGP routes.

---

## Description

Use the **import-route** command to redistribute routes.

Use the **undo import-route** command to disable routes redistribution.

IPv6 OSPFv3 does not redistribute routes from other protocols by default.

## Examples

# Configure to redistribute routes from RIPng and specify the type as type 2 and cost as 50.

```
<Sysname> system-view
```

```
[Sysname] ospfv3
```

```
[Sysname-ospfv3-1] import-route ripng 10 type 2 cost 50
```

## log-peer-change

### Syntax

**log-peer-change**

**undo log-peer-change**

## View

OSPFv3 view

## Default Level

2: System level

## Parameters

None

## Description

Use the **log-peer-change** command to enable the logging on neighbor state changes.

Use the **undo maximum load-balancing** command to disable the logging.

With this feature enabled, information about neighbor state changes of the current OSPFv3 process will display on the configuration terminal.

## Examples

```
# Disable the logging on neighbor state changes of OSPFv3 process 100.
```

```
<Sysname> system-view  
[Sysname] ospfv3 100  
[Sysname-ospfv3-100] undo log-peer-change
```

## maximum load-balancing (OSPFv3 view)

### Syntax

**maximum load-balancing** *maximum*

**undo maximum load-balancing**

### View

OSPFv3 view

### Default Level

2: System level

### Parameters

*maximum*: Maximum number of equal-cost routes for load-balancing. Its value is in the range 1 to 4. The argument being set to 1 means no load balancing is available.

### Description

Use the **maximum load-balancing** command to configure the maximum number of equal-cost routes for load-balancing.

Use the **undo maximum load-balancing** command to restore the default.

By default, the maximum number of equal-cost routes for load-balancing in OSPFv3 is 4.

### Examples

```
# Configure the maximum number of equal-cost routes for load-balancing as 2.
```

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] maximum load-balancing 2
```

## ospfv3

### Syntax

```
ospfv3 [ process-id ]
undo ospfv3 [ process-id ]
```

### View

System view

### Default Level

2: System level

### Parameters

*process-id*: OSPFv3 process ID, ranging from 1 to 65535. The process ID defaults to 1.

### Description

Use the **ospfv3** command to enable an OSPFv3 process and enter OSPFv3 view.

Use the **undo ospfv3** command to disable an OSPFv3 process.

The system runs no OSPFv3 process by default.

Related commands: **router-id**.



#### Note

An OSPFv3 process can run normally only when Router ID is configured in OSPFv3 view. Otherwise, you can find the process, but which cannot generate any LSA.

---

### Examples

```
# Enable the OSPFv3 process with process ID as 120 and configure the Router ID as 1.1.1.1.
```

```
<Sysname> system-view
[Sysname] ospfv3 120
[Sysname-ospfv3-120] router-id 1.1.1.1
```

## ospfv3 area

### Syntax

```
ospfv3 process-id area area-id [ instance instance-id ]
undo ospfv3 process-id area area-id [ instance instance-id ]
```

## View

Interface view

## Default Level

2: System level

## Parameters

*process-id*: OSPFv3 process ID, in the range 1 to 65535.

*area-id*: Area ID, a decimal integer (in the range of 0 to 4294967295) that is translated into IPv4 address format by the system or an IPv4 address.

*instance-id*: Instance ID of an interface, in the range 0 to 255. The default is 0.

## Description

Use the **ospfv3 area** command to enable an OSPFv3 process on the interface and specify the area for the interface.

Use the **undo ospfv3 area** command to disable an OSPFv3 process.

OSPFv3 is not enabled on an interface by default.

## Examples

# Enable OSPFv3 process 1 on an interface that belongs to instance 1 and specify area 1 for the interface.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 1 area 1 instance 1
```

## ospfv3 cost

### Syntax

**ospfv3 cost** *value* [ **instance** *instance-id* ]

**undo ospfv3 cost** [ **instance** *instance-id* ]

### View

Interface view

### Default Level

2: System level

### Parameters

*value*: OSPFv3 cost, in the range 0 to 65535 for a loopback interface and 1 to 65535 for other interfaces.

*instance-id*: Instance ID of an interface, in the range of 0 to 255, which defaults to 0.

### Description

Use the **ospfv3 cost** command to configure the OSPFv3 cost of the interface in an instance.

Use the **undo ospfv3 cost** command to restore the default OSPFv3 cost of the interface in an instance.

By default, a router's interface automatically calculates the OSPFv3 cost based on its bandwidth. For a VLAN interface of a switch, the cost value defaults to 1; for a loopback interface, the cost value defaults to 0.

## Examples

```
# Specifies the OSPFv3 cost of the interface in instance 1 as 33 .
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 cost 33 instance 1
```

## ospfv3 dr-priority

### Syntax

```
ospfv3 dr-priority priority [ instance instance-id ]
undo ospfv3 dr-priority [ instance instance-id ]
```

### View

Interface view

### Default Level

2: System level

### Parameters

*priority*: DR priority, in the range 0 to 255.

*instance-id*: ID of the instance an interface belongs to, in the range 0 to 255, which defaults to 0.

### Description

Use the **ospfv3 dr-priority** command to set the DR priority for an interface in an instance.

Use the **undo ospfv3 dr-priority** command to restore the default value.

The DR priority on an interface defaults to 1.

An interface's DR priority determines its privilege in DR/BDR selection, and the interface with the highest priority is preferred.

## Examples

```
# Set the DR priority for an interface in instance 1 to 8.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 dr-priority 8 instance 1
```

## ospfv3 mtu-ignore

### Syntax

```
ospfv3 mtu-ignore [ instance instance-id ]
undo ospfv3 mtu-ignore [ instance instance-id ]
```

## View

Interface view

## Default Level

2: System level

## Parameters

*instance-id*: Instance ID, in the range 0 to 255, which defaults to 0.

## Description

Use the **ospfv3 mtu-ignore** command to configure an interface to ignore MTU check during DD packet exchange.

Use the **undo ospfv3 mtu-ignore** command to restore the default.

By default, an interface performs MTU check during DD packet exchange. A neighbor relationship can be established only if the interface's MTU is the same as that of the peer.

## Examples

# Configure an interface that belongs to instance 1 to ignore MTU check during DD packet exchange.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 mtu-ignore instance 1
```

## ospfv3 network-type

### Syntax

```
ospfv3 network-type { broadcast | nbma | p2mp [ non-broadcast ] | p2p } [ instance instance-id ]
undo ospfv3 network-type [ instance instance-id ]
```

## View

Interface view

## Default Level

2: System level

## Parameters

**broadcast**: Specifies the network type as Broadcast.

**nbma**: Specifies the network type as NBMA.

**p2mp**: Specifies the network type as P2MP.

**p2p**: Specifies the network type as P2P.

**non-broadcast**: Specifies the interface to send packets in unicast mode. By default, an OSPFv3 interface whose network type is P2MP sends packets in multicast mode.

*instance-id*: The instance ID of an interface, in the range of 0 to 255, which defaults to 0.

## Description

Use the **ospfv3 network-type** command to set the network type for an OSPFv3 interface.

Use the **undo ospfv3 network-type** command to restore the default.

By default, network type is broadcast.

### Examples

```
# Configure the interface's network type as NBMA.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 network-type nbma
```

## ospfv3 peer

### Syntax

```
ospfv3 peer ipv6-address [ dr-priority dr-priority ] [ instance instance-id ]
undo ospfv3 peer ipv6-address [ instance instance-id ]
```

### View

Interface view

### Default Level

2: System level

### Parameters

*ipv6-address*: Neighbor link-local IP address.

*dr-priority*: Neighbor DR priority, in the range 0 to 255. The default is 1.

*instance-id*: Interface instance ID, in the range 0 to 255. The default is 0.

### Description

Use the **ospfv3 peer** command to specify a neighbor and the DR priority of the neighbor.

Use the **undo ospfv3 peer** command to remove the configuration.

A router uses the priority set with the **ospfv3 peer** command to determine whether to send a hello packet to the neighbor rather than use it for DR election.

### Examples

```
# Specify the neighbor fe80::1111.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 peer fe80::1111
```

## ospfv3 timer dead

### Syntax

```
ospfv3 timer dead seconds [ instance instance-id ]
undo ospfv3 timer dead [ instance instance-id ]
```

## View

Interface view

## Default Level

2: System level

## Parameters

*seconds*: Dead time in seconds, ranging from 1 to 2147483647.

*instance-id*: Instance ID of an interface, in the range of 0 to 255, which defaults to 0.

## Description

Use the **ospfv3 timer dead** command to configure the OSPFv3 neighbor dead time for an interface that belongs to a specified instance.

Use the **undo ospfv3 timer dead** command to restore the default.

By default, the OSPFv3 neighbor dead time is 40 seconds for P2P and Broadcast interfaces, and is not supported on P2MP and NBMA interfaces at present.

OSPFv3 neighbor dead time: if an interface receives no hello packet from a neighbor after dead time elapses, the interface will consider the neighbor dead.

The **dead seconds** value is at least four times the **Hello seconds** value and must be identical on interfaces attached to the same network segment.

Related commands: **ospfv3 timer hello**.

## Examples

# Configure the OSPFv3 neighbor dead time as 80 seconds for the interface in instance 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 timer dead 80 instance 1
```

## ospfv3 timer hello

### Syntax

**ospfv3 timer hello** *seconds* [ **instance** *instance-id* ]

**undo ospfv3 timer hello** [ **instance** *instance-id* ]

### View

Interface view

### Default Level

2: System level

### Parameters

*seconds*: Interval between hello packets, ranging from 1 to 65535.

*instance-id*: Instance ID of an interface, in the range of 0 to 255, which defaults to 0.

## Description

Use the **ospfv3 timer hello** command to configure the hello interval for an interface that belongs to an instance.

Use the **undo ospfv3 timer hello** command to restore the default .

By default, the hello interval is 10 seconds for P2P and Broadcast interfaces, and is not supported on the P2MP or NBMA interfaces at present.

Related commands: **ospfv3 timer dead**.

## Examples

# Configure the hello interval as 20 seconds for an interface in instance 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 timer hello 20 instance 1
```

## ospfv3 timer retransmit

### Syntax

**ospfv3 timer retransmit** *interval* [ **instance** *instance-id* ]

**undo ospfv3 timer retransmit** [ **instance** *instance-id* ]

### View

Interface view

### Default Level

2: System level

### Parameters

*interval*: LSA retransmission interval in seconds, ranging from 1 to 65535.

*instance-id*: Instance ID of an interface, in the range of 0 to 255, which defaults to 0.

## Description

Use the **ospfv3 timer retransmit** command to configure the LSA retransmission interval for an interface in an instance.

Use the **undo ospfv3 timer retransmit** command to restore the default.

The interval defaults to 5 seconds.

After sending a LSA to its neighbor, the device waits for an acknowledgement. If receiving no acknowledgement after the LSA retransmission interval elapses, it will retransmit the LSA.

The LSA retransmission interval should not be too small for avoidance of unnecessary retransmissions.

## Examples

# Configure the LSA retransmission interval on an interface in instance 1 as 12 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 timer retransmit 12 instance 1
```

## ospfv3 timer poll

### Syntax

```
ospfv3 timer poll seconds [ instance instance-id ]
undo ospfv3 timer poll [ instance instance-id ]
```

### View

Interface view

### Default Level

2: System level

### Parameters

*seconds*: Poll interval in seconds, in the range 1 to 65535.

*instance-id*: Interface instance ID, in the range 0 to 255. The default is 0.

### Description

Use the **ospfv3 timer poll** command to set the poll interval on an NBMA interface.

Use the **undo ospfv3 timer poll** command to restore the default value.

By default, the poll interval is 120 seconds.

### Examples

# Set the poll timer interval on the current interface to 130 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf timer poll 130
```

## ospfv3 trans-delay

### Syntax

```
ospfv3 trans-delay seconds [ instance instance-id ]
undo ospfv3 trans-delay [ instance instance-id ]
```

### View

Interface view

### Default Level

2: System level

### Parameters

*seconds*: Transmission delay in seconds, ranging from 1 to 3600.

*instance-id*: Instance ID of an interface, in the range of 0 to 255, with the default as 0.

### Description

Use the **ospfv3 trans-delay** command to configure the transmission delay for an interface with an instance ID.

Use the **undo ospfv3 trans-delay** command to restore the default.

The transmission delay defaults to 1s.

As LSAs are aged in the LSDB (incremented by 1 every second) but not aged on transmission, it is necessary to add a delay time to the age time before sending a LSA. This configuration is important for low-speed networks.

## Examples

```
# Configure the transmission delay as 3 seconds for an interface in instance 1.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 trans-delay 3 instance 1
```

## preference

### Syntax

```
preference [ ase ] [ route-policy route-policy-name ] preference
undo preference [ ase ]
```

### View

OSPFv3 view

### Default Level

2: System level

### Parameters

**ase**: Applies the preference to OSPFv3 external routes. If the keyword is not specified, the preference applies to OSPFv3 internal routes.

**route-policy** *route-policy-name*: References a routing policy to set preference for specific routes. The name is a string of 1 to 19 characters.

*Preference*: Preference of OSPFv3, in the range 1 to 255.

### Description

Use the **preference** command to specify a preference for OSPFv3 routes.

Use the **undo preference** command to restore the default.

By default, the preference for OSPFv3 internal routes is 10, and that for OSPFv3 external routes is 150.

The smaller the value is, the higher the preference is.

A router may run multiple routing protocols. Each protocol has a preference. When several routing protocols find multiple routes to the same destination, the route found by the protocol with the highest preference is selected.

## Examples

```
# Set a preference of 150 for OSPFv3 routes.
```

```
<Sysname> system-view
[Sysname] OSPFv3
[Sysname-OSPFv3-1] preference 150
```

## router-id

### Syntax

```
router-id router-id  
undo router-id
```

### View

OSPFv3 view

### Default Level

2: System level

### Parameters

*router-id*: 32-bit router ID, in IPv4 address format.

### Description

Use the **router-id** command to configure the OSPFv3 router ID.

Use the **undo router-id** command to remove a configured router ID.

Router ID is the unique identifier of a device running an OSPFv3 process in the autonomous system. The OSPFv3 process cannot run without a Router ID.

Make sure that different processes have different Router IDs.

Related commands: **ospfv3**.

### Examples

# Configure the Router ID as 10.1.1.3 for OSPFv3 process 1.

```
<Sysname> system-view  
[Sysname] ospfv3 1  
[Sysname-ospfv3-1] router-id 10.1.1.3
```

## silent-interface(OSPFv3 view)

### Syntax

```
silent-interface { interface-type interface-number | all }  
undo silent-interface { interface-type interface-number | all }
```

### View

OSPFv3 view

### Default Level

2: System level

### Parameters

*interface-type interface-number*: Interface type and number

**all**: Specifies all interfaces.

## Description

Use the **silent-interface** command to disable the specified interface from sending OSPFv3 packets.

Use the **undo silent-interface** command to restore the default.

An interface is able to send OSPFv3 packets by default.

## Examples

```
# Disable an interface from sending OSPFv3 packets in OSPFv3 processes 100.
```

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] router-id 10.110.1.9
[Sysname-ospfv3-100] silent-interface vlan-interface 10
```

## spf timers

### Syntax

```
spf timers delay-interval hold-interval
```

```
undo spf timers
```

### View

OSPFv3 view

### Default Level

2: System level

### Parameters

*delay-interval*: Interval in seconds between when OSPFv3 receives a topology change and when it starts SPF calculation. in the range 1 to 65535.

*hold-interval*: Hold interval in seconds between two consecutive SPF calculations, in the range 1 to 65535.

## Description

Use the **spf timers** command to configure the delay interval and hold interval for OSPFv3 SPF calculation.

Use the **undo spf timers** command to restore the default.

The delay interval and hold interval default to 5s and 10s.

An OSPFv3 router works out a shortest path tree with itself as root based on the LSDB, and decides on the next hop to a destination network according the tree. Adjusting the SPF calculation interval can restrain bandwidth and router resource from over consumption due to frequent network changes.

## Examples

```
# Configure the delay interval and hold interval as 6 seconds for SPF calculation.
```

```
<Sysname> system-view
[Sysname]ospfv3 1
[Sysname-ospfv3-1] spf timers 6 6
```

## stub (OSPFv3 area view)

### Syntax

```
stub [ no-summary ]  
undo stub
```

### View

OSPFv3 area view

### Default Level

2: System level

### Parameters

**no-summary**: This argument is only applicable to the ABR of a stub area. With it configured, the ABR advertises only a default route in a Summary-LSA to the stub area (such an area is called a totally stub area).

### Description

Use the **stub** command to configure an area as a stub area.

Use the **undo stub** command to remove the configuration.

By default, an area is not configured as a stub area.

When an area is configured as a stub area, all the routers attached to the area must be configured with the **stub** command.

Related commands: **default-cost**.

### Examples

```
# Configure OSPFv3 area 1 as a stub area.
```

```
<Sysname> system-view  
[Sysname] ospfv3 1  
[Sysname-ospfv3-1] area 1  
[Sysname-ospfv3-1-area-0.0.0.1] stub
```

## vlink-peer (OSPFv3 area view)

### Syntax

```
vlink-peer router-id [ hello seconds | retransmit seconds | trans-delay seconds | dead seconds |  
instance instance-id ] *  
undo vlink-peer router-id [ hello | retransmit | trans-delay | dead ] *
```

### View

OSPFv3 area view

### Default Level

2: System level

## Parameters

*router-id*: Router ID for a virtual link neighbor.

**hello seconds**: Specifies the interval in seconds for sending Hello packets, ranging from 1 to 8192, with the default as 10. This value must be equal to the **hello seconds** configured on the virtual link peer.

**retransmit seconds**: Specifies the interval in seconds for retransmitting LSA packets, ranging from 1 to 3600, with the default as 5.

**trans-delay seconds**: Specifies the delay interval in seconds for sending LSA packets, ranging from 1 to 3600, with the default as 1.

**dead seconds**: Specifies the neighbor dead time in seconds, ranging from 1 to 32768, with the default as 40. This value must be equal to the **dead seconds** configured on the virtual link peer, and at least four times the value of **hello seconds**.

**instance Instance-id**: Instance ID of an virtual link, in the range of 0 to 255, with the default as 0.

## Description

Use the **vlink-peer** command to create and configure a virtual link.

Use the **undo vlink-peer** command to remove a virtual link.

For a non-backbone area without a direct connection to the backbone area or for a backbone area that cannot maintain connectivity, you can use the **vlink-peer** command to create logical links. A virtual link can be considered as an interface with OSPFv3 enabled, because parameters such as **hello**, **dead**, **retransmit** and **trans-delay** are configured in the similar way.

Both ends of a virtual link are ABRs that are configured with the **vlink-peer** command.

Note that: If you have enabled the GR capability for the current process, you cannot execute the **vlink-peer** command for the process.

## Examples

# Create a virtual link to 10.110.0.3.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 10.0.0.0
[Sysname-ospfv3-1-area-10.0.0.0] vlink-peer 10.110.0.3
```

# Table of Contents

<b>1 IPv6 IS-IS Configuration Commands</b> .....	<b>1-1</b>
IPv6 IS-IS Configuration Commands.....	1-1
display isis route ipv6.....	1-1
ipv6 default-route-advertise.....	1-3
ipv6 enable.....	1-4
ipv6 filter-policy export.....	1-5
ipv6 filter-policy import.....	1-6
ipv6 import-route.....	1-6
ipv6 import-route isisv6 level-2 into level-1.....	1-8
ipv6 import-route limit.....	1-8
ipv6 maximum load-balancing.....	1-9
ipv6 preference.....	1-10
ipv6 summary.....	1-10
isis ipv6 enable.....	1-11

# 1 IPv6 IS-IS Configuration Commands

---

## IPv6 IS-IS Configuration Commands

---



### Note

IPv6 IS-IS supports all the features of IPv4 IS-IS except that it advertises IPv6 routing information instead. This document describes only IPv6 IS-IS exclusive commands. Refer to *IS-IS Commands* in the *IP Routing Volume* for other IS-IS configuration commands.

---

## display isis route ipv6

### Syntax

```
display isis route ipv6 [ [ level-1 | level-2 ] | verbose ] * [ process-id ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**verbose:** Displays detailed IPv6 IS-IS routing information.

*process-id:* IS-IS process ID, in the range 1 to 65535.

**level-1:** Display Level-1 IPv6 IS-IS routes only.

**level-2:** Displays Level-2 IPv6 IS-IS routes only.



### Note

If no level is specified, both Level-1 and Level-2 (namely Level-1-2) routing information will be displayed.

---

### Description

Use the **display isis route ipv6** command to display IPv6 IS-IS routing information.

## Examples

# Display IPv6 IS-IS routing information.

```
<Sysname> display isis route ipv6
          Route information for ISIS(1)
          -----
          ISIS(1) IPv6 Level-1 Forwarding Table
          -----
Destination: 2001:2::                               PrefixLen: 64
Flag       : D/L/-                                   Cost       : 10
Next Hop   : Direct                                  Interface:  Vlan200
          Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
```

**Table 1-1 display isis route ipv6 command output description**

Field	Description
Destination	IPv6 destination address prefix
PrefixLen	Length of the prefix
Flag/Flags	Flag of routing information status D: This is a direct route. R: The route has been added into the routing table. L: The route has been advertised in a LSP. U: Route leaking flag, indicating the Level-1 route is from Level-2. <b>U</b> means the route will not be returned to Level-2.
Cost	Value of cost
Next Hop	Next hop
Interface	Outbound interface

# Display detailed IPv6 IS-IS routing information.

```
<Sysname> display isis route ipv6 verbose
          Route information for ISIS(1)
          -----
          ISIS(1) IPv6 Level-1 Forwarding Table
          -----
IPv6 Dest  : 2001:1::/64                               Cost : 20           Flag : R/-/-
Admin Tag  : -                                         Src Count : 2
NextHop    :                                           Interface :           ExitIndex :
          FE80::200:FCFF:FE00:7507                   Vlan200           0x00000003
IPv6 Dest  : 2001:2::/64                               Cost : 10           Flag : D/L/-
Admin Tag  : -                                         Src Count : 2
NextHop    :                                           Interface :           ExitIndex :
          Direct                                       Vlan200           0x00000000
          Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
```

**Table 1-2** display isis route ipv6 verbose command output description

Field	Description
IPv6 Dest	IPv6 destination
Cost	Value of cost
Flag/Flags	Flag of routing information status D: This is a direct route. R: The route has been added into the routing table. L: The route has been advertised in a LSP. U: Route leaking flag, indicating the Level-1 route is from Level-2. <b>U</b> means the route will not be returned to Level-2.
Admin Tag	Administrative tag
Src Count	Number of advertisement sources
Next Hop	Next hop
Interface	Outbound interface
ExitIndex	Outbound interface index

## ipv6 default-route-advertise

### Syntax

```
ipv6 default-route-advertise [ [ level-1 | level-2 | level-1-2 ] | route-policy route-policy-name ] *  
undo ipv6 default-route-advertise [ route-policy route-policy-name ]
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

*route-policy-name*: Specifies the name of a routing policy with a string of 1 to 19 characters.

**level-1**: Specifies the default route as Level-1.

**level-2**: Specifies the default route as Level-2.

**level-1-2**: Specifies the default route as Level-1-2.



### Note

If no level is specified, the default route belongs to Level-2.

---

## Description

Use the **ipv6 default-route-advertise** command to generate a Level-1 or Level-2 IPv6 IS-IS default route.

Use the **undo ipv6 default-route-advertise** command to disable generating a default route.

No IPv6 IS-IS default route is generated by default.

With a routing policy, you can configure IPv6 IS-IS to generate the default route that must match the routing policy. You can use the **apply isis level-1** command in routing policy view to generate a default route in L1 LSPs, or use the **apply isis level-2** command in routing policy view to generate a default route in L2 LSPs, and use the **apply isis level-1-2** in routing policy view to generate a default route in L1 and L2 LSPs respectively.

Refer to *Routing Policy Commands* in the *IP Routing Volume* for information about the **apply isis** command.

## Examples

# Configure the router to generate a default route in Level-2 LSPs.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] ipv6 default-route-advertise
```

## ipv6 enable

### Syntax

```
ipv6 enable
undo ipv6 enable
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

None

## Description

Use the **ipv6 enable** command to enable IPv6 for the IPv6 IS-IS process.

Use the **undo ipv6 enable** command to disable IPv6.

IPv6 is disabled by default.

## Examples

# Create IS-IS routing process 1, and enable IPv6 for the process.

```
<Sysname> system-view
[Sysname] ipv6
[Sysname] isis 1
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
```

```
[Sysname-isis-1] ipv6 enable
```

## ipv6 filter-policy export

### Syntax

```
ipv6 filter-policy { acl6-number | ipv6-prefix ipv6-prefix-name | route-policy route-policy-name }  
export [ protocol [ process-id ] ]  
undo ipv6 filter-policy export [ protocol [ process-id ] ]
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

*acl6-number*: Number of a basic or advanced IPv6 ACL used to filter redistributed routes before advertisement, ranging from 2000 to 3999. Refer to *ACL Configuration* in the *Security Volume* for ACL information.

*ipv6-prefix-name*: Name of an IPv6 prefix list used to filter the redistributed routes before advertisement, a string of 1 to 19 characters. Refer to *Routing Policy Configuration* in the *IP Routing Volume* for IPv6 prefix list information.

*route-policy-name*: Name of a routing policy used to filter the redistributed routes before advertisement, a string of 1 to 19 characters. Refer to *Routing Policy Configuration* in the *IP Routing Volume* for routing policy information.

*protocol*: Filter routes redistributed from the specified routing protocol before advertisement. The routing protocol can be **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng** or **static** at present. If no protocol is specified, routes redistributed from all protocols are filtered before advertisement.

*process-id*: Process ID of the routing protocol, ranging from 1 to 65535. This argument is available when the protocol is **isisv6**, **ospfv3** or **ripng**.

### Description

Use the **ipv6 filter-policy export** command to configure IPv6 IS-IS to filter redistributed routes before advertisement.

Use the **undo ipv6 filter-policy export** command to disable the filtering.

The filtering is disabled by default.

In some cases, only routes satisfying certain conditions will be advertised. You can configure the filtering conditions using the **ipv6 filter-policy** command.

You can use the **ipv6 filter-policy export** command, which filters redistributed routes only when they are advertised to other routers, in combination with the **ipv6 import-route** command.

- If no protocol is specified, routes redistributed from all protocols are filtered before advertisement.
- If a protocol is specified, only routes redistributed from the protocol are filtered before advertisement.

Related commands: **ipv6 filter-policy import**.

## Examples

```
# Reference the ACL6 2006 to filter all the redistributed routes before advertisement.
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] ipv6 filter-policy 2006 export
```

## ipv6 filter-policy import

### Syntax

```
ipv6 filter-policy { acl6-number | ipv6-prefix ipv6-prefix-name | route-policy route-policy-name }
import
undo ipv6 filter-policy import
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

*acl6-number*: Number of a basic or advanced IPv6 ACL used to filter incoming routes, ranging from 2000 to 3999.

*ipv6-prefix-name*: Name of an IPv6 prefix list used to filter incoming routes, a string of 1 to 19 characters.

*route-policy-name*: Name of a routing policy used to filter incoming routes, a string of 1 to 19 characters.

### Description

Use the **ipv6 filter-policy import** command to configure IPv6 IS-IS to filter the received routes.

Use the **undo ipv6 filter-policy import** command to disable the filtering.

The filtering is disabled by default.

In some cases, only the routing information satisfying certain conditions will be received. You can configure the filtering conditions using the **ipv6 filter-policy** command.

Related commands: **ipv6 filter-policy export**.

## Examples

```
# Reference the IPv6 ACL 2003 to filter the received routes.
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] ipv6 filter-policy 2003 import
```

## ipv6 import-route

### Syntax

```
ipv6 import-route protocol [ process-id ] [ allow-ibgp ] [ cost cost ] [ level-1 | level-2 | level-1-2 ] |
route-policy route-policy-name | tag tag ] *
```

**undo ipv6 import-route** *protocol* [ *process-id* ]

## View

IS-IS view

## Default Level

2: System level

## Parameters

*protocol*: Redistributes routes from a specified routing protocol, which can be **direct**, **static**, **ripng**, **isisv6**, **bgp4+** or **ospfv3**.

*process-id*: Process ID of the routing protocol of **ripng**, **isisv6** or **ospfv3**, in the range of 1 to 65535. The default is 1.

*cost*: Cost for redistributed routes, ranging from 0 to 4261412864.

**level-1**: Redistributes routes into Level-1 routing table.

**level-2**: Redistributes routes into Level-2 routing table.

**level-1-2**: Redistributes routes into Level-1 and Level-2 routing tables.

*route-policy-name*: Name of a routing policy used to filter routes when they are being redistributed, a string of 1 to 19 characters.

*tag*: Specifies a administrative tag number for the redistributed routes, in the range of 1 to 4294967295.

**allow-ibgp**: Allows to redistribute IBGP routes. This keyword is optional when the *protocol* is **bgp4+**.

## Description

Use the **ipv6 import-route** command to enable IPv6 IS-IS to redistribute routes from another routing protocol.

Use the **undo ipv6 import-route** command to disable route redistribution.

Route redistribution is disabled by default.

If no level is specified, the routes are imported to Level-2 routing table by default.

IPv6 IS-IS considers redistributed routes as routes to destinations outside the local routing domain.

You can specify a cost and a level for redistributed routes.



### Caution

Using the **import-route bgp4+ allow-ibgp** command will redistribute both EBGP and IBGP routes. The redistributed IBGP routes may cause routing loops. Therefore, be cautious with this command.

---

## Examples

# Configure IPv6-IS-IS to redistribute static routes and set the cost 15 for them.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1]ipv6 import-route static cost 15
```

## ipv6 import-route isisv6 level-2 into level-1

### Syntax

```
ipv6 import-route isisv6 level-2 into level-1 [ filter-policy { acl6-number | ipv6-prefix  
ipv6-prefix-name | route-policy route-policy-name } | tag tag ] *
```

```
undo ipv6 import-route isisv6 level-2 into level-1
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

*acl6-number*: Number of a basic or advanced ACL6 used to filter routes when they are leaking from Level-2 to Level-1, ranging from 2000 to 3999.

*ipv6-prefix-name*: Name of an IPv6 prefix list used to filter routes when they are leaking from Level-2 to Level-1, a string of 1 to 19 characters.

*route-policy-name*: Name of a routing policy used to filter routes when they are leaking from Level-2 to Level-1, a string of 1 to 19 characters.

*tag*: Specifies a administrative tag number for the leaked routes, in the range of 1 to 4294967295.

### Description

Use the **ipv6 import-route isisv6 level-2 into level-1** to enable IPv6 IS-IS route leaking from Level-2 to Level-1.

Use the **undo ipv6 import-route isisv6 level-2 into level-1** command to disable the leaking.

The leaking is disabled by default.

The route leaking feature enables a Level-1-2 router to advertise routes destined to the Level-2 area and other Level-1 areas to the Level-1 and Level-1-2 routers in the local area.

### Examples

```
# Enable IPv6 IS-IS route leaking from Level-2 to Level-1.
```

```
<Sysname> system-view
```

```
[Sysname] isis 1
```

```
[Sysname-isis-1] ipv6 import-route isisv6 level-2 into level-1
```

## ipv6 import-route limit

### Syntax

```
ipv6 import-route limit number
```

```
undo ipv6 import-route limit
```

### View

IS-IS view

## Default Level

2: System level

## Parameters

*number*: Maximum number of redistributed Level 1/Level 2 IPv6 routes. Its value is in the range 1 to 6144 and defaults to 6144.

## Description

Use the **ipv6 import-route limit** command to configure the maximum number of redistributed Level 1/Level 2 IPv6 routes.

Use the **undo ipv6 import-route limit** command to restore the default.

## Examples

# Configure IS-IS process 1 to redistribute up to 1000 Level 1/Level 2 IPv6 routes.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1]ipv6 import-route limit 1000
```

## ipv6 maximum load-balancing

### Syntax

**ipv6 maximum load-balancing** *number*

**undo ipv6 maximum load-balancing**

### View

IS-IS view

### Default Level

2: System level

### Parameters

*number*: Maximum number of equal-cost routes for load balancing. Its value is in the range 1 to 4 and defaults to 4.

### Description

Use the **ipv6 maximum load-balancing** command to configure the maximum number of equal-cost routes for load balancing.

Use the **undo ipv6 maximum load-balancing** command to restore the default.



#### Note

Configure the maximum number of equivalent load-balanced routes according to the memory capacity.

---

## Examples

```
# Configure the maximum number of equivalent load-balanced routing as 2.
<Sysname> system-view
[Sysname] isis 100
[Sysname-isis-100] ipv6 maximum load-balancing 2
```

## ipv6 preference

### Syntax

```
ipv6 preference { preference | route-policy route-policy-name } *
undo ipv6 preference
```

### View

IS-IS view

### Default Level

2: System level

### Parameters

*preference*: Preference for IPv6 IS-IS, ranging from 1 to 255.  
*route-policy-name*: Name of a routing policy, a string of 1 to 19 characters.

### Description

Use the **ipv6 preference** command to configure the preference for IPv6 IS-IS protocol.  
Use the **undo ipv6 preference** command to configure the default preference for IPv6 IS-IS protocol.  
The default preference is 15.

When a router runs multiple dynamic routing protocols at the same time, the system will assign a preference to each routing protocol. If several protocols find routes to the same destination, the route found by the protocol with the highest preference is selected.

## Examples

```
# Configure the preference of IPv6 IS-IS protocol as 20.
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] ipv6 preference 20
```

## ipv6 summary

### Syntax

```
ipv6 summary ipv6-prefix prefix-length [ avoid-feedback | generate_null0_route | [ level-1 | level-1-2 | level-2 ] ] tag tag ] *
undo ipv6 summary ipv6-prefix prefix-length [ level-1 | level-1-2 | level-2 ]
```

### View

IS-IS view

## Default Level

2: System level

## Parameters

*ipv6-prefix*: IPv6 prefix of the summary route.

*prefix-length*: Length of the IPv6 prefix, in the range of 0 to 128.

**avoid-feedback**: Specifies to avoid learning summary routes via routing calculation.

**generate\_null0\_route**: Generates the NULL 0 route to avoid routing loops.

**level-1**: Specifies to summarize only the routes redistributed to Level-1 area.

**level-1-2**: Specifies to summarize all the routes redistributed to Level-1 and Level-2 areas.

**level-2**: Specifies to summarize only the routes redistributed to Level-2 area.

*tag*: Value of a administrative tag, in the range of 1 to 4294967295.



### Note

If no level is specified in the command, the default is **level-2**.

---

## Description

Use the **ipv6 summary** command to configure an IPv6 IS-IS summary route.

Use the **undo ipv6 summary** command to remove the summary route.

Route summarization is disabled by default.

Configuring summary routes can reduce the size of the route table, LSPs and LSDB. Routes to be summarized can be IS-IS routes or redistributed routes. The cost of a summary route is the smallest cost among all summarized routes.

## Examples

```
# Configure a summary route of 2002::/32.  
<Sysname> system-view  
[Sysname] isis  
[Sysname-isis-1] ipv6 summary 2002:: 32
```

## isis ipv6 enable

### Syntax

**isis ipv6 enable** [ *process-id* ]

**undo isis ipv6 enable**

### View

Interface view

## Default Level

2: System level

## Parameters

*process-id*: IS-IS process ID, ranging from 1 to 65535. The default is 1.

## Description

Use the **isis ipv6 enable** command to enable IPv6 for the specified IS-IS process on the interface.

Use the **undo isis ipv6 enable** command to disable the configuration.

IPv6 is disabled on the interface by default.

## Examples

# Enable global IPv6, create IS-IS routing process 1, enable IPv6 for the process, and enable IPv6 for the process on VLAN-interface100.

```
<Sysname> system-view
[Sysname] ipv6
[Sysname] isis 1
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
[Sysname-isis-1] ipv6 enable
[Sysname-isis-1] quit
[Sysname] interface Vlan-interface 100
[Sysname--Vlan-interface100] ipv6 address 2002::1/64
[Sysname--Vlan-interface100] isis ipv6 enable 1
```

# Table of Contents

<b>1 IPv6 BGP Configuration Commands</b> .....	<b>1-1</b>
IPv6 BGP Configuration Commands .....	1-1
aggregate (IPv6 address family view) .....	1-1
balance (IPv6 address family view) .....	1-2
bestroute as-path-neglect (IPv6 address family view) .....	1-3
bestroute compare-med (IPv6 address family view) .....	1-3
bestroute med-confederation (IPv6 address family view) .....	1-4
compare-different-as-med (IPv6 address family view) .....	1-5
dampening (IPv6 address family view) .....	1-6
default local-preference (IPv6 address family view) .....	1-7
default med (IPv6 address family view) .....	1-7
default-route imported (IPv6 address family view) .....	1-8
display bgp ipv6 group .....	1-9
display bgp ipv6 network .....	1-10
display bgp ipv6 paths .....	1-11
display bgp ipv6 peer .....	1-12
display bgp ipv6 routing-table .....	1-13
display bgp ipv6 routing-table as-path-acl .....	1-15
display bgp ipv6 routing-table community .....	1-16
display bgp ipv6 routing-table community-list .....	1-17
display bgp ipv6 routing-table dampened .....	1-17
display bgp ipv6 routing-table dampening parameter .....	1-18
display bgp ipv6 routing-table different-origin-as .....	1-19
display bgp ipv6 routing-table flap-info .....	1-20
display bgp ipv6 routing-table peer .....	1-21
display bgp ipv6 routing-table regular-expression .....	1-22
display bgp ipv6 routing-table statistic .....	1-23
filter-policy export (IPv6 address family view) .....	1-23
filter-policy import (IPv6 address family view) .....	1-24
group (IPv6 address family view) .....	1-25
import-route (IPv6 address family view) .....	1-25
ipv6-family .....	1-26
network (IPv6 address family view) .....	1-27
peer advertise-community (IPv6 address family view) .....	1-27
peer advertise-ext-community (IPv6 address family view) .....	1-28
peer allow-as-loop (IPv6 address family view) .....	1-29
peer as-number (IPv6 address family view) .....	1-30
peer as-path-acl (IPv6 address family view) .....	1-30
peer capability-advertise route-refresh .....	1-31
peer connect-interface (IPv6 address family view) .....	1-32
peer default-route-advertise .....	1-33
peer description (IPv6 address family view) .....	1-33
peer ebgp-max-hop (IPv6 address family view) .....	1-34

peer fake-as (IPv6 address family view) .....	1-35
peer filter-policy (IPv6 address family view) .....	1-35
peer group (IPv6 address family view) .....	1-36
peer ignore (IPv6 address family view) .....	1-37
peer ipv6-prefix .....	1-38
peer keep-all-routes (IPv6 address family view) .....	1-38
peer log-change (IPv6 address family view) .....	1-39
peer next-hop-local (IPv6 address family view) .....	1-40
peer preferred-value (IPv6 address family view) .....	1-40
peer public-as-only (IPv6 address family view) .....	1-41
peer reflect-client (IPv6 address family view) .....	1-42
peer route-limit (IPv6 address family view) .....	1-43
peer route-policy (IPv6 address family view) .....	1-44
peer route-update-interval (IPv6 address family view) .....	1-45
peer substitute-as (IPv6 address family view) .....	1-45
peer timer (IPv6 address family view) .....	1-46
preference (IPv6 address family view) .....	1-47
reflect between-clients (IPv6 address family view) .....	1-48
reflector cluster-id (IPv6 address family view) .....	1-48
refresh bgp ipv6 .....	1-49
reset bgp ipv6 .....	1-50
reset bgp ipv6 dampening .....	1-50
reset bgp ipv6 flap-info .....	1-51
router-id .....	1-52
synchronization (IPv6 address family view) .....	1-52
timer (IPv6 address family view) .....	1-53

# 1 IPv6 BGP Configuration Commands

---

## IPv6 BGP Configuration Commands

### aggregate (IPv6 address family view)

#### Syntax

```
aggregate ipv6-address prefix-length [ as-set | attribute-policy route-policy-name | detail-suppressed | origin-policy route-policy-name | suppress-policy route-policy-name ] *  
undo aggregate ipv6-address prefix-length
```

#### View

IPv6 address family view

#### Default Level

2 System level

#### Parameters

*ipv6-address*: Summary address.

*prefix-length*: Length of summary route mask, in the range 0 to 128.

**as-set**: Creates a summary with AS set.

**attribute-policy** *route-policy-name*: Sets the attributes of the summary route according to the routing policy. The routing policy name is a string of 1 to 19 characters.

**detail-suppressed**: Only advertises the summary route.

**suppress-policy** *route-policy-name*: Suppresses specific routes defined in the routing policy. The routing policy name is a string of 1 to 19 characters.

**origin-policy** *route-policy-name*: References the routing policy to specify routes for summarization. The routing policy name is a string of 1 to 19 characters.

The keywords of the command are described as follows:

**Table 1-1** Functions of the keywords

Keywords	Function
<b>as-set</b>	Used to create a summary route, whose AS path contains the AS path information of summarized routes. Use this keyword carefully when many AS paths need to be summarized, because the frequent changes of these specific routes may lead to route oscillation.
<b>detail-suppressed</b>	This keyword does not suppress the summary route, but it suppresses the advertisement of all the more specific routes. To summarize only some specific routes, use the <b>peer filter-policy</b> command.

Keywords	Function
<b>suppress-policy</b>	Used to create a summary route and suppress the advertisement of some summarized routes. If you want to suppress some routes selectively and leave other routes still advertised, use the <b>if-match</b> clause of the <b>route-policy</b> command.
<b>origin-policy</b>	Selects only routes satisfying the routing policy for route summarization.
<b>attribute-policy</b>	Sets attributes except the AS-PATH attribute for the summary route. The same work can be done by using the <b>peer route-policy</b> command.

### Description

Use the **aggregate** command to create an IPv6 summary route in the IPv6 BGP routing table.

Use the **undo aggregate** command to remove an IPv6 summary route.

By default, no summary route is configured.

### Examples

# In IPv6 address family view, create a summary of 12::/64 in the IPv6 routing table.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] aggregate 12:: 64
```

### balance (IPv6 address family view)

#### Syntax

**balance** *number*

**undo balance**

#### View

IPv6 address family view

#### Default Level

2: System level

#### Parameters

*number*: Number of BGP routes participating in load balancing. Its value is in the range 1 to 4. When it is set to 1, load balancing is disabled.

#### Description

Use the **balance** command to configure the number of routes participating in IPv6 BGP load balancing.

Use the **undo balance** command to restore the default.

The feature is not available by default.

Unlike IGP, BGP has no explicit metric for making load balancing decision. Instead, it implements load balancing by defining its routing rule.

Related commands: **display bgp ipv6 routing-table**.

## Examples

```
# Set the number of routes participating in IPv6 BGP load balancing to 2.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] balance 2
```

## bestroute as-path-neglect (IPv6 address family view)

### Syntax

```
bestroute as-path-neglect
undo bestroute as-path-neglect
```

### View

IPv6 address family view

### Default Level

2: System level

### Parameters

None

### Description

Use the **bestroute as-path-neglect** command to configure the IPv6 BGP router to not evaluate the AS\_PATH during best route selection.

Use the **undo bestroute as-path-neglect** command to configure the IPv6 BGP router to use the AS\_PATH during best route selection.

By default, the router takes AS\_PATH as a factor when selecting the best route.

## Examples

```
# Ignore AS_PATH in route selection.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] bestroute as-path-neglect
```

## bestroute compare-med (IPv6 address family view)

### Syntax

```
bestroute compare-med
undo bestroute compare-med
```

### View

IPv6 address family view

## Default Level

2: System level

## Parameters

None

## Description

Use the **bestroute compare-med** command to enable the comparison of the MED for paths from each AS.

Use the **undo bestroute compare-med** command to disable this comparison.

This comparison is not enabled by default.



### Caution

After the **bestroute compare-med** command is executed, the **balance** command does not take effect.

---

## Examples

```
# Compare the MED for paths from an AS for selecting the best route.
```

```
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] ipv6-family  
[Sysname-bgp-af-ipv6] bestroute compare-med
```

## bestroute med-confederation (IPv6 address family view)

### Syntax

**bestroute med-confederation**

**undo bestroute med-confederation**

### View

IPv6 address family view

## Default Level

2: System level

## Parameters

None

## Description

Use the **bestroute med-confederation** command to enable the comparison of the MED for paths from confederation peers for best route selection.

Use the **undo bestroute med-confederation** command to disable the configuration.

By default, this comparison is not enabled.

With this feature enabled, the system can only compare the MED for paths from peers within the confederation. Paths from external ASs are advertised throughout the confederation without MED comparison.

## Examples

```
# Compare the MED for paths from peers within the confederation.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] bestroute med-confederation
```

## compare-different-as-med (IPv6 address family view)

### Syntax

```
compare-different-as-med
undo compare-different-as-med
```

### View

IPv6 address family view

### Default Level

2: System level

### Parameters

None

### Description

Use the **compare-different-as-med** command to enable the comparison of the MED for paths from peers in different ASs.

Use the **undo compare-different-as-med** command to disable the comparison.

The comparison is disabled by default.

If there are several paths available for one destination, the path with the smallest MED value is selected.

Do not use this command unless associated ASs adopt the same IGP protocol and routing selection method.

## Examples

```
# Enable to compare the MED for paths from peers in different ASs.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] compare-different-as-med
```

## dampening (IPv6 address family view)

### Syntax

```
dampening [ half-life-reachable half-life-unreachable reuse suppress ceiling | route-policy  
route-policy-name ] *
```

```
undo dampening
```

### View

IPv6 address family view

### Default Level

2: System level

### Parameters

*half-life-reachable*: Half-life for reachable routes, in the range 1 to 45 minutes. By default, the value is 15 minutes.

*half-life-unreachable*: Half-life for unreachable routes, in the range 1 to 45 minutes. By default, the value is 15 minutes.

*reuse*: Reuse threshold value for suppressed routes, in the range 1 to 20000. Penalty value of a suppressed route decreasing under the value is reused. By default, its value is 750.

*suppress*: Suppression threshold from 1 to 20000, which should be bigger than the *reuse* value. Routes with a penalty value bigger than the threshold are suppressed. By default, it is 2000.

*ceiling*: Ceiling penalty value from 1001 to 20000. The value must be bigger than the *suppress* value. By default, the value is 16000.

*route-policy-name*: Routing policy name, a string of 1 to 19 characters.

*half-life-reachable*, *half-life-unreachable*, *reuse*, *suppress* and *ceiling* are mutually dependent. Once any one is configured, all the others should also be specified accordingly.

### Description

Use the **dampening** command to enable IPv6 BGP route dampening or/and configure dampening parameters.

Use the **undo dampening** command to disable route dampening.

By default, no route dampening is configured.

Related commands: **reset bgp ipv6 dampening**, **reset bgp ipv6 flap-info**, **display bgp ipv6 routing-table dampened**, **display bgp ipv6 routing-table dampening parameter**, **display bgp ipv6 routing-table flap-info**.

### Examples

```
# Enable IPv6 BGP route dampening and configure route dampening parameters.
```

```
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] ipv6-family  
[Sysname-bgp-af-ipv6] dampening 10 10 1000 2000 3000
```

## default local-preference (IPv6 address family view)

### Syntax

```
default local-preference value  
undo default local-preference
```

### View

IPv6 address family view

### Default Level

2: System level

### Parameters

*value*: Default local preference, in the range 0 to 4294967295. The larger the value is, the higher the preference is.

### Description

Use the **default local-preference** command to configure the default local preference.

Use the **undo default local-preference** command to restore the default value.

By default, the default local preference is 100.

Use this command to affect IPv6 BGP route selection.

### Examples

# Two devices A and B in the same AS are connected to another AS. Change the local preference of B from default value 100 to 180, making the route passing B preferred.

```
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] ipv6-family  
[Sysname-bgp-af-ipv6] default local-preference 180
```

## default med (IPv6 address family view)

### Syntax

```
default med med-value  
undo default med
```

### View

IPv6 address family view

### Default Level

2: System level

### Parameters

*med-value*: MED value, in the range 0 to 4294967295.

## Description

Use the **default med** command to specify the default MED value.

Use the **undo default med** command to restore the default.

By default, the default *med-value* is 0.

The multi-exit discriminator (MED) is an external metric of a route. Different from local preference, MED is exchanged between ASs and will stay in the AS once it enters the AS. The route with a lower MED is preferred. When a router running BGP obtains several routes with the identical destination and different next-hops from various external peers, it will select the best route depending on the MED value. In the case that all other conditions are the same, the system first selects the route with the smaller MED value as the best route for the autonomous system.

## Examples

# Devices A and B belong to AS100 and device C belongs to AS200. C is the peer of A and B. Configure the MED of A as 25 to make C select the path from B.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] default med 25
```

## default-route imported (IPv6 address family view)

### Syntax

```
default-route imported
undo default-route imported
```

### View

IPv6 address family view

### Default Level

2: System level

### Parameters

None

## Description

Use the **default-route imported** command to enable the redistribution of default route into the IPv6 BGP routing table.

Use the **undo default-route imported** command to disable the redistribution.

By default, the redistribution is not enabled.

## Examples

# Enable the redistribution of default route from OSPFv3 into IPv6 BGP.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
```

```
[Sysname-bgp-af-ipv6] default-route imported
[Sysname-bgp-af-ipv6] import-route ospfv3 1
```

## display bgp ipv6 group

### Syntax

```
display bgp ipv6 group [ ipv6-group-name ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ipv6-group-name*: Peer group name, a string of 1 to 47 characters.

### Description

Use the **display bgp ipv6 group** command to display IPv6 peer group information.

If no *ipv6-group-name* is specified, information about all peer groups is displayed.

### Examples

# Display the information of the IPv6 peer group **aaa**.

```
<Sysname> display bgp ipv6 group aaa
```

```
BGP peer-group is aaa
remote AS number not specified
Type : external
Maximum allowed prefix number: 4294967295
Threshold: 75%
Configured hold timer value: 180
Keepalive timer value: 60
Minimum time between advertisement runs is 30 seconds
Peer Preferred Value: 0
No routing policy is configured
Members:
Peer          V    AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down  State
20:20::20:1  4    200      170      141      0        2 02:13:35 Established
```

**Table 1-2 display bgp ipv6 group** command output description

Field	Description
BGP peer-group	Name of the peer group
remote AS	AS number of the peer group
Type	Type of the peer group
Maximum allowed prefix number	Maximum allowed prefix number

Field	Description
Threshold	Threshold value
hold timer value	Holdtime
Keepalive timer value	Keepalive interval
Minimum time between advertisement runs	Minimum interval between advertisements
Peer Preferred Value	Preferred value of the routes from the peer
No routing policy is configured	No routing policy is configured for the peer
Members	Group members
Peer	IPv6 address of the peer
V	Peer BGP version
AS	AS number
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages to be sent
PrefRcv	Number of prefixes received
Up/Down	The lasting time of a session/the lasting time of present state (when no session is established)
State	State machine state of peer

## display bgp ipv6 network

### Syntax

```
display bgp ipv6 network
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display bgp ipv6 network** command to display IPv6 routes advertised with the **network** command.

### Examples

```
# Display IPv6 routes advertised with the network command.
```

```
<Sysname> display bgp ipv6 network
  BGP Local Router ID is 1.1.1.2.
  Local AS Number is 200.
```

Network	Mask	Route-policy	Short-cut
2002::	64		
2001::	64		Short-cut

**Table 1-3 display bgp ipv6 network command output description**

Field	Description
BGP Local Router ID	BGP Local Router ID
Local AS Number	Local AS Number
Network	Network address
Prefix	Prefix length
Route-policy	Routing policy
Short-cut	Shortcut route

## display bgp ipv6 paths

### Syntax

```
display bgp ipv6 paths [ as-regular-expression ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*as-regular-expression*: AS path regular expression, a string of 1 to 80 characters.

### Description

Use the **display bgp ipv6 paths** command to display IPv6 BGP path information.

If no parameter is specified, all path information will be displayed.

### Examples

# Display IPv6 BGP path information.

```
<Sysname> display bgp ipv6 paths
```

Address	Hash	Refcount	MED	Path/Origin
0x5917098	1	1	0	i
0x59171D0	9	2	0	100i

**Table 1-4 display bgp ipv6 paths** command output description

Field	Description	
Address	Route destination address in local database, in dotted hexadecimal notation	
Hash	Hash index	
Refcount	Count of routes that used the path	
MED	MED of the path	
Path	AS_PATH attribute of the path, recording the ASs it has passed, for avoiding routing loops	
Origin	Origin attribute of the route, which can take on one of the following values:	
	i	Indicates the route is interior to the AS. Summary routes and routes defined using the <b>network</b> command are considered IGP routes.
	e	Indicates that a route is learned from the exterior gateway protocol (EGP).
	?	Short for INCOMPLETE. It indicates that the origin of a route is unknown and the route is learned by other means. BGP sets Origin attribute of routes learned from other IGP protocols to INCOMPLETE.

## display bgp ipv6 peer

### Syntax

```
display bgp ipv6 peer [ group-name log-info | ipv4-address verbose | ipv6-address { log-info | verbose } | verbose ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

*ipv4-address*: IPv4 address of a peer.

*ipv6-address*: Specifies the IPv6 address of a peer to be displayed.

**log-info**: Displays log information of the specified peer.

**verbose**: Displays the detailed information of the peer.

### Description

Use the **display bgp ipv6 peer** command to display peer/peer group information.

If no parameter specified, information about all peers and peer groups is displayed.

### Examples

```
# Display all IPv6 peer information.
```

```
<Sysname> display bgp ipv6 peer
```

```
BGP Local router ID : 20.0.0.1  
local AS number : 100  
Total number of peers : 1                Peers in established state : 1
```

```
Peer      V    AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down    State  
20::21   4    200  17       19       0       3  00:09:59  Established
```

**Table 1-5 display bgp ipv6 peer command output description**

Field	Description
Peer	IPv6 address of the peer
V	Peer BGP version
AS	AS number
MsgRcvd	Messages received
MsgSent	Messages sent
OutQ	Messages to be sent
PrefRcv	Number of prefixes received
Up/Down	The lasting time of a session/the lasting time of present state (when no session is established)
State	Peer state

## display bgp ipv6 routing-table

### Syntax

```
display bgp ipv6 routing-table [ ipv6-address prefix-length ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ipv6-address*: Destination IPv6 address.

*prefix-length*: Prefix length of the IPv6 address, in the range 0 to 128.

### Description

Use the **display bgp ipv6 routing-table** command to display IPv6 BGP routing table information.

### Examples

```
# Display the IPv6 BGP routing table.
```

```
<Sysname> display bgp ipv6 routing-table
```

```
Total Number of Routes: 2
```

```
BGP Local router ID is 30.30.30.1
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

```
Origin : i - IGP, e - EGP, ? - incomplete
```

```
*> Network : 30:30::                               PrefixLen : 64
    NextHop  : 30:30::30:1                           LocPrf    :
    PrefVal  : 0                                       Label     : NULL
    MED      : 0
    Path/Ogn: i
```

```
*> Network : 40:40::                               PrefixLen : 64
    NextHop  : 40:40::40:1                           LocPrf    :
    PrefVal  : 0                                       Label     : NULL
    MED      : 0
    Path/Ogn: i
```

**Table 1-6** display bgp ipv6 routing-table command output description

Field	Description
Local router ID	Local router ID
Status codes	Status codes: * – valid > – best d – damped h – history i – internal (IGP) s – summary suppressed (suppressed) S – Stale
Origin	i – IGP (originated in the AS) e – EGP (learned through EGP) ? – incomplete (learned by other means)
Network	Destination network address
PrefixLen	Prefix length
NextHop	Next Hop
MED	MULTI_EXIT_DISC attribute
LocPrf	Local preference value
Path	AS_PATH attribute, recording the ASs the packet has passed to avoid routing loops
PrefVal	Preferred value
Label	Label

Field	Description	
Ogn	Origin attribute of the route, which can take on one of the following values:	
	i	Indicates that a route is interior to the AS. Summary routes and the routes configured using the <b>network</b> command are considered IGP routes.
	e	Indicates that a route is learned from the exterior gateway protocol (EGP).
	?	Short for INCOMPLETE. It indicates that the origin of a route is unknown and the route is learned by other means. BGP sets Origin attribute of routes learned from other IGP protocols to INCOMPLETE.

## display bgp ipv6 routing-table as-path-acl

### Syntax

```
display bgp ipv6 routing-table as-path-acl as-path-acl-number
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*as-path-acl-number*. Number of an AS path ACL permitted by which to display routing information, ranging from 1 to 256.

### Description

Use the **display bgp ipv6 routing-table as-path-acl** command to display routes filtered through the specified AS path ACL.

### Examples

# Display routes filtered through the AS path ACL 20.

```
<Sysname> display bgp ipv6 routing-table as-path-acl 20
BGP Local router ID is 30.30.30.1
Status codes: * - valid, > - best, d - damped,
               h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete

*> Network : 30:30::                               PrefixLen : 64
    NextHop : 30:30::30:1                            LocPrf    :
    PrefVal : 0                                       Label     : NULL
    MED     : 0
    Path/Ogn: i
```

Refer to [Table 1-6](#) for description on the fields above.

## display bgp ipv6 routing-table community

### Syntax

```
display bgp ipv6 routing-table community [ aa:nn&<1-13> ] [ no-advertise | no-export | no-export-subconfed ] * [ whole-match ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*aa:nn*: Community number; both *aa* and *nn* are in the range 0 to 65535.

*&<1-13>*: Indicates the argument before it can be entered up to 13 times.

**no-advertise**: Displays IPv6 BGP routes that cannot be advertised to any peer.

**no-export**: Displays IPv6 BGP routes that cannot be advertised out the AS; if there is a confederation, it displays IPv6 BGP routes that cannot be advertised out the confederation, but can be advertised to other sub ASs in the confederation.

**no-export-subconfed**: Displays IPv6 BGP routes that cannot be advertised out the AS or to other sub ASs if a confederation is configured.

**whole-match**: Displays the IPv6 BGP routes exactly matching the specified community attribute.

### Description

Use the **display bgp ipv6 routing-table community** command to display the routing information with the specified community attribute.

### Examples

```
# Display the routing information with community attribute no-export.
```

```
<Sysname> display bgp ipv6 routing-table community no-export
```

```
BGP Local router ID is 30.30.30.1
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

```
Origin : i - IGP, e - EGP, ? - incomplete
```

```
*> Network : 30:30::                               PrefixLen : 64
NextHop   : 30:30::30:1                             LocPrf    :
PrefVal   : 0                                         Label     : NULL
MED       : 0
Path/Ogn  : i
```

Refer to [Table 1-6](#) for description on the fields above.

## display bgp ipv6 routing-table community-list

### Syntax

```
display bgp ipv6 routing-table community-list { basic-community-list-number [ whole-match ] | adv-community-list-number }&<1-16>
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*basic-community-list-number*: Specifies a basic community-list number, in the range 1 to 99.

*adv-community-list-number*: Specifies an advanced community-list number, in the range 100 to 199.

**whole-match**: Displays routes exactly matching the specified *basic-community-list-number*.

&<1-16>: Specifies to allow entering the argument before it up to 16 times.

### Description

Use the **display bgp ipv6 routing-table community-list** command to view the routing information matching the specified IPv6 BGP community list.

### Examples

# Display the routing information matching the specified IPv6 BGP community list.

```
<Sysname> display bgp ipv6 routing-table community-list 99
BGP Local router ID is 30.30.30.1
Status codes: * - valid, > - best, d - damped,
               h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete

*> Network : 30:30::                               PrefixLen : 64
    NextHop : 30:30::30:1                           LocPrf    :
    PrefVal : 0                                       Label     : NULL
    MED     : 0
    Path/Ogn: i
```

Refer to [Table 1-6](#) for description on the fields above.

## display bgp ipv6 routing-table dampened

### Syntax

```
display bgp ipv6 routing-table dampened
```

### View

Any view

## Default Level

1: Monitor level

## Parameters

None

## Description

Use the **display bgp ipv6 routing-table dampened** command to display the IPv6 BGP dampened routes.

## Examples

```
# Display IPv6 BGP dampened routes.
```

```
<Sysname> display bgp ipv6 routing-table dampened
```

```
BGP Local router ID is 1.1.1.1
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

```
Origin : i - IGP, e - EGP, ? - incomplete
```

```
*d Network : 111::                               PrefixLen : 64
   From      : 122::1                             Reuse      : 00:29:34
   Path/Ogn: 200?
```

**Table 1-7** display bgp ipv6 routing-table dampened command output description

Field	Description
From	Source IP address of a route
Reuse	Time for reuse

Refer to [Table 1-6](#) for description on the fields above.

## display bgp ipv6 routing-table dampening parameter

### Syntax

```
display bgp ipv6 routing-table dampening parameter
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

## Description

Use the **display bgp ipv6 routing-table dampening parameter** command to display IPv6 BGP routing dampening parameters.

Related commands: **dampening**.

## Examples

# Display IPv6 BGP routing dampening parameters.

```
<Sysname> display bgp ipv6 routing-table dampening parameter
Maximum Suppress Time(in second)      : 3069
Ceiling Value                          : 16000
Reuse Value                            : 750
Reach HalfLife Time(in second)        : 900
Unreach HalfLife Time(in second)      : 900
Suppress-Limit                        : 2000
```

**Table 1-8** Description on the above fields

Field	Description
Maximum Suppress Time	Maximum Suppress Time
Ceiling Value	Upper limit of penalty value
Reuse Value	Reuse Value
Reach HalfLife Time(in second)	Half-life time of active routes
Unreach HalfLife Time(in second)	Half-life time of inactive routes
Suppress-Limit	Suppress value

## display bgp ipv6 routing-table different-origin-as

### Syntax

```
display bgp ipv6 routing-table different-origin-as
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display bgp ipv6 routing-table different-origin-as** command to display IPv6 BGP routes originating from different autonomous systems.

### Examples

# Display routes from different ASs.

```
<Sysname> display bgp ipv6 routing-table different-origin-as
```

```
BGP Local router ID is 2.2.2.2
```

```
Status codes: * - valid, > - best, d - damped,  
              h - history, i - internal, s - suppressed, S - Stale  
Origin : i - IGP, e - EGP, ? - incomplete
```

```
*> Network : 222::                PrefixLen : 64  
NextHop   : 122::2                LocPrf    :  
PrefVal   : 0                     Label     : NULL  
MED       : 0  
Path/Ogn  : 100 ?
```

Refer to [Table 1-6](#) for description on the fields above.

## display bgp ipv6 routing-table flap-info

### Syntax

```
display bgp ipv6 routing-table flap-info [ regular-expression as-regular-expression | as-path-acl  
as-path-acl-number | ipv6-address [ prefix-length [ longer-match ] ] ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*as-regular-expression*: AS path regular expression to be matched, a string of 1 to 80 characters.

*as-path-acl-number*: Number of the specified AS path ACL to be matched, ranging from 1 to 256.

*ipv6-address*: IPv6 address of a route to be displayed.

*prefix-length*: Prefix length of the IPv6 address, in the range 0 to 128.

**longer-match**: Matches the longest prefix.

### Description

Use the **display bgp ipv6 routing-table flap-info** command to display IPv6 BGP route flap statistics.

### Examples

```
# Display IPv6 BGP route flap statistics.
```

```
<Sysname> display bgp ipv6 routing-table flap-info
```

```
BGP Local router ID is 1.1.1.1
```

```
Status codes: * - valid, > - best, d - damped,  
              h - history, i - internal, s - suppressed, S - Stale  
Origin : i - IGP, e - EGP, ? - incomplete
```

```
*d Network : 111::                PrefixLen : 64
```

```

From      : 122::1                Flaps      : 3
Duration  : 00:13:47             Reuse      : 00:16:36
Path/Ogn  : 200?

```

**Table 1-9** display bgp ipv6 routing-table flap-info command output description

Field	Description
Flaps	Number of flaps
Duration	Flap duration
Reuse	Reuse time of the route

Refer to [Table 1-6](#) for description on the fields above.

## display bgp ipv6 routing-table peer

### Syntax

```

display bgp ipv6 routing-table peer { ipv4-address | ipv6-address } { advertised-routes |
received-routes } [ network-address prefix-length | statistic ]

```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ipv4-address*: Specifies the IPv4 peer to be displayed.

*ipv6-address*: Specifies the IPv6 peer to be displayed.

**advertised-routes**: Routing information advertised to the specified peer.

**received-routes**: Routing information received from the specified peer.

*network-address prefix-length*: IPv6 address and prefix length. The prefix length ranges from 0 to 128.

**statistic**: Displays route statistics.

### Description

Use the **display bgp ipv6 routing-table peer** command to display the routing information advertised to or received from the specified IPv4 or IPv6 BGP peer.

### Examples

# Display the routing information advertised to the specified BGP peer.

```

<Sysname> display bgp ipv6 routing-table peer 10:10::10:1 advertised-routes
Total Number of Routes: 2

```

```
BGP Local router ID is 20.20.20.1
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

```
Origin : i - IGP, e - EGP, ? - incomplete
```

```
*> Network : 20:20:: PrefixLen : 64
NextHop : 20:20::20:1 LocPrf :
PrefVal : 0 Label : NULL
MED : 0
Path/Ogn: i
```

```
*> Network : 40:40:: PrefixLen : 64
NextHop : 30:30::30:1 LocPrf :
PrefVal : 0 Label : NULL
MED : 0
Path/Ogn: 300 i
```

Refer to [Table 1-6](#) for description on the fields above.

## display bgp ipv6 routing-table regular-expression

### Syntax

```
display bgp ipv6 routing-table regular-expression as-regular-expression
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*as-regular-expression*: AS regular expression, a string of 1 to 80 characters.

### Description

Use the **display bgp ipv6 routing-table regular-expression** command to display the routes permitted by the specified AS regular expression.

### Examples

```
# Display routing information matching the specified AS regular expression.
```

```
<Sysname> display bgp ipv6 routing-table regular-expression ^100
```

```
BGP Local router ID is 20.20.20.1
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

```
Origin : i - IGP, e - EGP, ? - incomplete
```

```
*> Network : 50:50:: PrefixLen : 64
NextHop : 10:10::10:1 LocPrf :
PrefVal : 0 Label : NULL
MED : 0
Path/Ogn: 100 i
```

Refer to [Table 1-6](#) for description on the fields above.

## display bgp ipv6 routing-table statistic

### Syntax

```
display bgp ipv6 routing-table statistic
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display bgp ipv6 routing-table statistic** command to display IPv6 BGP routing statistics.

### Examples

```
# Display IPv6 BGP routing statistics.
```

```
<Sysname> display bgp ipv6 routing-table statistic
```

```
Total Number of Routes: 1
```

## filter-policy export (IPv6 address family view)

### Syntax

```
filter-policy { acl6-number | ipv6-prefix ipv6-prefix-name } export [ protocol process-id ]
```

```
undo filter-policy export [ protocol process-id ]
```

### View

IPv6 address family view

### Default Level

2: System level

### Parameters

*acl6-number*: Specifies the number of an ACL6 used to match against the destination of routing information. The number is in the range 2000 to 3999.

*ipv6-prefix-name*: Specifies the name of an IPv6 prefix list used to match against the destination of routing information. The name is a string of 1 to 19 characters.

*protocol*: Filters routes redistributed from the routing protocol. It can be **direct**, **isisv6**, **ospfv3**, **ripng**, or **static** at present. If no protocol is specified, all routes will be filtered when advertised.

*process-id*: Process ID of the routing protocol, in the range 1 to 65535. It is available only when the protocol is **isisv6**, **ospfv3** or **ripng**.

## Description

Use the **filter-policy export** command to filter outbound routes using a specified filter.

Use the **undo filter-policy export** command to cancel filtering outbound routes.

By default, no outbound routing information is filtered.

If a protocol is specified, only routes redistributed from the specified protocol are filtered. If no protocol is specified, all redistributed routes will be filtered.

## Examples

```
# Reference ACL6 2001 to filter all outbound IPv6 BGP routes.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] filter-policy 2001 export
```

## filter-policy import (IPv6 address family view)

### Syntax

```
filter-policy { acl6-number | ipv6-prefix ipv6-prefix-name } import
undo filter-policy import
```

### View

IPv6 address family view

### Default Level

2: System level

### Parameters

*acl6-number*: Number of an IPv6 ACL used to match against the destination address field of routing information, ranging from 2000 to 3999.

*ipv6-prefix-name*: Name of an IPv6 prefix list used to match against the destination address field of routing information, a string of 1 to 19 characters.

## Description

Use the **filter-policy import** command to filter inbound routing information using a specified filter.

Use the **undo filter-policy import** command to cancel filtering inbound routing information.

By default, no inbound routing information is filtered.

## Examples

```
# Reference ACL6 2001 to filter all inbound routes.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] filter-policy 2001 import
```

## group (IPv6 address family view)

### Syntax

```
group ipv6-group-name [ internal | external ]  
undo group ipv6-group-name
```

### View

IPv6 address family view

### Default Level

2: System level

### Parameters

*ipv6-group-name*: Name of an IPv6 peer group, a string of 1 to 47 characters.

**internal**: Creates an iBGP peer group.

**external**: Creates an eBGP peer group, which can be a group of another sub AS in the confederation.

### Description

Use the **group** command to create a peer group.

Use the **undo group** command to delete a peer group.

An iBGP peer group will be created if neither **internal** nor **external** is selected.

### Examples

```
# Create an iBGP peer group named test.
```

```
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname] ipv6-family  
[Sysname-bgp-af-ipv6] group test
```

## import-route (IPv6 address family view)

### Syntax

```
import-route protocol [ process-id [ med med-value | route-policy route-policy-name ] * ]  
undo import-route protocol [ process-id ]
```

### View

IPv6 address family view

### Default Level

2: System level

### Parameters

*protocol*: Redistributes routes from the specified protocol, which can be **direct**, **isisv6**, **ospfv3**, **ripng** and **static** at present.

*process-id*: Process ID, in the range 1 to 65535. The default is 1. It is available only when the protocol is **isisv6**, **ospfv3** or **ripng**.

*med-value*: Applies the MED value to redistributed routes. The value is in the range 0 to 4294967295. If not specified, the cost of the redistributed route is used as its MED in the IPv6 BGP routing domain.

*route-policy-name*: Name of a routing policy used to filter redistributed routes, a string of 1 to 19 characters.

## Description

Use the **import-route** command to redistribute routes from another routing protocol.

Use the **undo import-route** command to remove the configuration.

By default, IPv6 BGP does not redistribute routes from any routing protocol.

The routes redistributed using the **import-route** command has the incomplete origin attribute.

## Examples

```
# Redistribute routes from RIPng 1.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] import-route ripng 1
```

## ipv6-family

### Syntax

```
ipv6-family
undo ipv6-family
```

### View

BGP view

### Default Level

2: System level

### Parameters

None

### Description

Use the **ipv6-family** command to enter IPv6 address family view.

Use the **undo ipv6-family** command to remove all configurations from the view.

IPv4 BGP unicast view is the default.

## Examples

```
# Enter IPv6 address family view.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
```

[ Sysname-bgp-af-ipv6 ]

## network (IPv6 address family view)

### Syntax

```
network ipv6-address prefix-length [ short-cut | route-policy route-policy-name ]
undo network ipv6-address prefix-length [ short-cut ]
```

### View

IPv6 address family view

### Default Level

2: System level

### Parameters

*ipv6-address*: IPv6 address.

*prefix-length*: Prefix length of the address, in the range 0 to 128.

**short-cut**: If the keyword is specified for an eBGP route, the route will use the local routing management value rather than that of eBGP routes, so the preference of the route is reduced.

*route-policy-name*: Name of a routing policy, a string of 1 to 19 characters.

### Description

Use the **network** command to advertise a network to the IPv6 BGP routing table.

Use the **undo network** command to remove an entry from the IPv6 BGP routing table.

By default, no route is advertised.

Note that:

- The route to be advertised must exist in the local IP routing table, and using a routing policy makes route management more flexible.
- The route advertised to the BGP routing table using the **network** command has the IGP origin attribute.

### Examples

# Advertise the network 2002::/16 into the IPv6 BGP routing table.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] network 2002:: 16
```

## peer advertise-community (IPv6 address family view)

### Syntax

```
peer { group-name | ipv4-address | ipv6-address } advertise-community
undo peer { group-name | ipv4-address | ipv6-address } advertise-community
```

## View

IPv6 address family view

## Default Level

2: System level

## Parameters

*group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

*ipv4-address*: IPv4 address of a peer.

*ipv6-address*: IPv6 address of a peer.

## Description

Use the **peer advertise-community** command to advertise the community attribute to a peer/peer group.

Use the **undo peer advertise-community** command to remove the configuration.

By default, no community attribute is advertised to any peer group/peer.

## Examples

```
# Advertise the community attribute to the peer 1:2::3:4.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 advertise-community
```

## peer advertise-ext-community (IPv6 address family view)

### Syntax

```
peer { group-name | ipv4-address | ipv6-address } advertise-ext-community
undo peer { group-name | ipv4-address | ipv6-address } advertise-ext-community
```

## View

IPv6 address family view

## Default Level

2: System level

## Parameters

*group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

*ipv4-address*: IPv4 address of a peer.

*ipv6-address*: IPv6 address of a peer.

## Description

Use the **peer advertise-ext-community** command to advertise the extended community attribute to a peer/peer group.

Use the **undo peer advertise-ext-community** command to remove the configuration.

By default, no extended community attribute is advertised to a peer/peer group.

## Examples

```
# Advertise the extended community attribute to the peer 1:2::3:4.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 advertise-ext-community
```

## peer allow-as-loop (IPv6 address family view)

### Syntax

```
peer { group-name | ipv4-address | ipv6-address } allow-as-loop [ number ]
undo peer { group-name | ipv4-address | ipv6-address } allow-as-loop
```

### View

IPv6 address family view

### Default Level

2: System level

### Parameters

*group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

*ipv4-address*: IPv4 address of a peer.

*ipv6-address*: IPv6 address of a peer.

*number*: Specifies the number of times for which the local AS number can appear in routes from the peer/peer group, in the range 1 to 10. The default number is 1.

### Description

Use the **peer allow-as-loop** command to configure IPv6 BGP to allow the local AS number to exist in the AS\_PATH attribute of routes from a peer/peer group, and to configure the times for which it can appear.

Use the **undo peer allow-as-loop** command to disable the function.

The local AS number is not allowed to exist in the AS\_PATH attribute of routes by default.

## Examples

```
# Configure the number of times for which the local AS number can appear in the AS_PATH of routes
from peer 1::1 as 2.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1::1 allow-as-loop 2
```

## peer as-number (IPv6 address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } as-number as-number
undo peer ipv6-group-name as-number
undo peer ipv6-address
```

### View

IPv6 address family view

### Default Level

2: System level

### Parameters

*ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of a peer.

*as-number*: AS number of the peer/peer group, in the range 1 to 65535.

### Description

Use the **peer as-number** command to specify a peer/peer group with an AS number.

Use the **undo peer as-number** command to delete a peer group.

Use the **undo peer** command to delete a peer.

By default, no peer/peer group is specified.

### Examples

# Specify peer group **test** in AS 200.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test as-number 200
```

## peer as-path-acl (IPv6 address family view)

### Syntax

```
peer { group-name | ipv4-address | ipv6-address } as-path-acl as-path-acl-number { import | export }
undo peer { group-name | ipv4-address | ipv6-address } as-path-acl as-path-acl-number { import | export }
```

### View

IPv6 address family view

### Default Level

2: System level

## Parameters

*group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

*ipv4-address*: IPv4 address of a peer.

*ipv6-address*: IPv6 address of a peer.

*as-path-acl-number*: Number of an AS path ACL, in the range 1 to 256.

**import**: Filters incoming routes.

**export**: Filters outgoing routes.

## Description

Use the **peer as-path-acl** command to specify an AS path ACL to filter routes incoming from or outgoing to a peer/peer group.

Use the **undo peer as-path-acl** command to remove the configuration.

By default, no AS path list is specified for filtering.

## Examples

```
# Specify the AS path ACL 3 to filter routes outgoing to the peer 1:2::3:4.
```

```
<Sysname> system-view
[Sysname] ip as-path 3 permit ^200
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-path-acl 3 export
```

## peer capability-advertise route-refresh

### Syntax

```
peer { ipv6-group-name | ipv6-address } capability-advertise route-refresh
undo peer { ipv6-group-name | ipv6-address } capability-advertise route-refresh
```

### View

IPv6 address family view

### Default Level

2: System level

## Parameters

*ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of a peer.

## Description

Use the **peer capability-advertise route-refresh** command to enable IPv6 BGP route-refresh.

Use the **undo peer capability-advertise route-refresh** command to disable the function.

By default, route-refresh is enabled.

## Examples

```
# Disable route-refresh of peer 1:2::3:4.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] undo peer 1:2::3:4 capability-advertise route-refresh
```

## peer connect-interface (IPv6 address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } connect-interface interface-type interface-number
undo peer { ipv6-group-name | ipv6-address } connect-interface
```

### View

IPv6 address family view

### Default Level

2: System level

### Parameters

*ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of a peer.

*interface-type interface-number*: Specifies the type and name of the interface.

### Description

Use the **peer connect-interface** command to specify the source interface for establishing TCP connections to an IPv6 BGP peer or peer group.

Use the **undo peer connect-interface** command to restore the default.

By default, BGP uses the outbound interface of the best route to the IPv6 BGP peer/peer group as the source interface for establishing a TCP connection.

Note that:

To establish multiple BGP connections to a BGP router, you need to specify on the local router the respective source interfaces for establishing TCP connections to the peers on the peering BGP router; otherwise, the local BGP router may fail to establish TCP connections to the peers when using the outbound interfaces of the best routes as the source interfaces.

## Examples

```
# Specify loopback 0 as the source interface for routing updates to peer 1:2::3:4.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 connect-interface loopback 0
```

## peer default-route-advertise

### Syntax

```
peer { group-name | ipv4-address | ipv6-address } default-route-advertise [ route-policy  
route-policy-name ]
```

```
undo peer { group-name | ipv4-address | ipv6-address } default-route-advertise
```

### View

IPv6 address family view

### Default Level

2: System level

### Parameters

*group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

*ipv4-address*: IPv4 address of a peer.

*ipv6-address*: IPv6 address of a peer.

*route-policy-name*: Route-policy name, a string of 1 to 19 characters.

### Description

Use the **peer default-route-advertise** command to advertise a default route to a peer/peer group.

Use the **undo peer default-route-advertise** command to disable advertising a default route.

By default, no default route is advertised to a peer/peer group.

Using this command does not require the default route available in the routing table. With this command used, the router sends the default route unconditionally to the peer/peer group with the next hop being itself.

### Examples

```
# Advertise a default route to peer 1:2::3:4.
```

```
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] ipv6-family  
[Sysname-bgp-af-ipv6] peer 1:2::3:4 default-route-advertise
```

## peer description (IPv6 address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } description description-text
```

```
undo peer { ipv6-group-name | ipv6-address } description
```

### View

IPv6 address family view

### Default Level

2: System level

## Parameters

*ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of a peer.

*description-text*: Description information for the peer/peer group, a string of 1 to 79 characters.

## Description

Use the **peer description** command to configure the description information for a peer/peer group.

Use the **undo peer description** command to remove the description information of a peer/peer group.

By default, no description information is configured for a peer (group).

You need create a peer/peer group before configuring a description for it.

## Examples

```
# Configure the description for the peer group test as ISP1.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test description ISP1
```

## peer ebgp-max-hop (IPv6 address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } ebgp-max-hop [ hop-count ]
```

```
undo peer { ipv6-group-name | ipv6-address } ebgp-max-hop
```

### View

IPv6 address family view

### Default Level

2: System level

## Parameters

*ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of a peer.

*hop-count*: Maximum hop count, in the range 1 to 255. By default, the value is 64.

## Description

Use the **peer ebgp-max-hop** command to allow establishing the eBGP connection to a peer/peer group indirectly connected.

Use the **undo peer ebgp-max-hop** command to remove the configuration.

By default, this feature is disabled.

You can use the argument *hop-count* to specify the maximum router hops of the eBGP connection.

## Examples

```
# Allow establishing the eBGP connection with the peer group test on an indirectly connected network.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test ebgp-max-hop
```

## peer fake-as (IPv6 address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } fake-as as-number
undo peer { ipv6-group-name | ipv6-address } fake-as
```

### View

IPv6 address family view

### Default Level

2: System level

### Parameters

*ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of a peer.

*as-number*: Local autonomous system number, in the range 1 to 65535.

### Description

Use the **peer fake-as** command to configure a fake local AS number for a peer or peer group.

Use the **undo peer fake-as** command to remove the configuration.

By default, no fake local AS number is configured for a peer or peer group.

## Examples

```
# Configure a fake AS number of 200 for the peer group test.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test fake-as 200
```

## peer filter-policy (IPv6 address family view)

### Syntax

```
peer { group-name | ipv4-address | ipv6-address } filter-policy acl6-number { import | export }
undo peer { group-name | ipv4-address | ipv6-address } filter-policy [ acl6-number ] { import | export }
```

## View

IPv6 address family view

## Default Level

2: System level

## Parameters

*group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

*ipv4-address*: IPv4 address of a peer.

*ipv6-address*: IPv6 address of a peer.

*acl6-number*: IPv6 ACL number, in the range 2000 to 3999.

**import**: Applies the filter-policy to routes received from the peer/peer group.

**export**: Applies the filter-policy to routes advertised to the peer/peer group.

## Description

Use the **peer filter-policy** command to configure an ACL-based filter policy for a peer or peer group.

Use the **undo peer filter-policy** command to remove the configuration.

By default, no ACL-based filter policy is configured for a peer or peer group.

## Examples

```
# Apply the ACL6 2000 to filter routes advertised to the peer 1:2::3:4.  
<Sysname> system-view  
[Sysname] acl ipv6 number 2000  
[Sysname-acl6-basic-2000] rule permit source 2001:1:: 64  
[Sysname-acl6-basic-2000] quit  
[Sysname] bgp 100  
[Sysname-bgp] ipv6-family  
[Sysname-bgp-af-ipv6] peer 1:2::3:4 filter-policy 2000 export
```

## peer group (IPv6 address family view)

### Syntax

```
peer { ipv4-address | ipv6-address } group group-name [ as-number as-number ]  
undo peer ipv6-address group group-name
```

### View

IPv6 address family view

### Default Level

2: System level

### Parameters

*group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

*ipv4-address*: IPv4 address of a peer.

*ipv6-address*: IPv6 address of a peer.

*as-number*: Specifies the AS number of the peer/peer group, in the range 1 to 65535.

## Description

Use the **peer group** command to add a peer to a configured peer group.

Use the **undo peer group** command to delete a specified peer from a peer group.

By default, the peer does not belong to any peer group.

## Examples

```
# Create a peer group named test and add the peer 1:2::3:4 to the peer group.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 200
[Sysname-bgp-af-ipv6] peer 1:2::3:4 group test
```

## peer ignore (IPv6 address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } ignore
```

```
undo peer { ipv6-group-name | ipv6-address } ignore
```

### View

IPv6 address family view

### Default Level

2: System level

### Parameters

*ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of a peer.

## Description

Use the **peer ignore** command to terminate the session to a peer or peer group.

Use the **undo peer ignore** command to remove the configuration.

By default, a router can establish sessions with a peer or peer group.

After the **peer ignore** command is executed, the system terminates the active session(s) with the specified peer or peer group and clears all the related routing information. For a peer group, this means all the sessions with the peer group will be tore down.

## Examples

```
# Terminate the session with peer 1:2::3:4.
```

```
<Sysname> system-view
[Sysname] bgp 100
```

```
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 ignore
```

## peer ipv6-prefix

### Syntax

```
peer { group-name | ipv4-address | ipv6-address } ipv6-prefix ipv6-prefix-name { import | export }
undo peer { group-name | ipv4-address | ipv6-address } ipv6-prefix { import | export }
```

### View

IPv6 address family view

### Default Level

2: System level

### Parameters

*group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

*ipv4-address*: IPv4 address of a peer.

*ipv6-address*: IPv6 address of a peer.

*ipv6-prefix-name*: IPv6 prefix list name, a string of 1 to 19 characters.

**import**: Applies the filtering policy to routes received from the specified peer/peer group.

**export**: Applies the filtering policy to routes advertised to the specified peer/peer group.

### Description

Use the **peer ipv6-prefix** command to specify an IPv6 prefix list to filter routes incoming from or outgoing to a peer or peer group.

Use the **undo peer ipv6-prefix** command to remove the configuration.

By default, no IPv6 prefix list is specified for filtering.

### Examples

```
# Reference the IPv6 prefix list list 1 to filter routes outgoing to peer 1:2::3:4.
```

```
<Sysname> system-view
[Sysname] ip ipv6-prefix list1 permit 2002:: 64
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 ipv6-prefix list1 export
```

## peer keep-all-routes (IPv6 address family view)

### Syntax

```
peer { group-name | ipv4-address | ipv6-address } keep-all-routes
undo peer { group-name | ipv4-address | ipv6-address } keep-all-routes
```

### View

IPv6 address family view

## Default Level

2: System level

## Parameters

*group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

*ipv4-address*: IPv4 address of a peer.

*ipv6-address*: IPv6 address of a peer.

## Description

Use the **peer keep-all-routes** command to save the original routing information from a peer or peer group, including even routes that failed to pass the inbound policy.

Use the **undo peer keep-all-routes** command to disable this function.

By default, the function is not enabled.

## Examples

```
# Save routing information from peer 1:2::3:4.  
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] ipv6-family  
[Sysname-bgp-af-ipv6] peer 1:2::3:4 keep-all-routes
```

## peer log-change (IPv6 address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } log-change  
undo peer { ipv6-group-name | ipv6-address } log-change
```

### View

IPv6 address family view

## Default Level

2: System level

## Parameters

*ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of a peer.

## Description

Use the **peer log-change** command to enable the logging of session state and event information of a specified peer or peer group.

Use the **undo peer log-change** command to remove the configuration.

The logging is enabled by default.

## Examples

```
# Enable the logging of session state and event information of peer 1:2::3:4.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 log-change
```

## peer next-hop-local (IPv6 address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } next-hop-local
undo peer { ipv6-group-name | ipv6-address } next-hop-local
```

### View

IPv6 address family view

### Default Level

2: System level

### Parameters

*ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of a peer.

### Description

Use the **peer next-hop-local** command to configure the next hop of routes advertised to a peer/peer group as the local router.

Use the **undo peer next-hop-local** command to restore the default.

By default, the system sets the next hop of routes advertised to an eBGP peer/peer group to the local router, but does not set for routes outgoing to an iBGP peer/peer group.

### Examples

# Set the next hop of routes advertised to eBGP peer group **test** to the router itself.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test internal
[Sysname-bgp-af-ipv6] peer test next-hop-local
```

## peer preferred-value (IPv6 address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } preferred-value value
undo peer { ipv6-group-name | ipv6-address } preferred-value
```

### View

IPv6 address family view

## Default Level

2: System level

## Parameters

*ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of a peer.

*value*: Preferred value, in the range 0 to 65535.

## Description

Use the **peer preferred-value** command to assign a preferred value to routes received from a peer or peer group.

Use the **undo peer preferred-value** command to restore the default.

By default, routes received from a peer or peer group have a preferred value of 0.

Routes learned from peers each have an initial preferred value. Among multiple routes to the same destination, the route with the biggest value is selected.

Note that:

If you both reference a routing policy and use the command **peer { ipv6-group-name | ipv6-address } preferred-value value** to set a preferred value for routes from a peer, the routing policy sets a non-zero preferred value for routes matching it. Other routes not matching the routing policy uses the value set with the command. If the preferred value in the routing policy is zero, the routes matching it will also use the value set with the command. For information about using a routing policy to set a preferred value, refer to the command **peer { group-name | ipv4-address | ipv6-address } route-policy route-policy-name { import | export }** in this document, and the command **apply preferred-value preferred-value** in *Routing Policy Commands of the IP Routing Volume*.

## Examples

```
# Configure the preferred value as 50 for routes from peer 1:2::3:4.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 preferred-value 50
```

## peer public-as-only (IPv6 address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } public-as-only
undo peer { ipv6-group-name | ipv6-address } public-as-only
```

### View

IPv6 address family view

## Default Level

2: System level

## Parameters

*ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of a peer.

## Description

Use the **peer public-as-only** command to configure IPv6 BGP updates to a peer/peer group to not carry private AS numbers.

Use the **undo peer public-as-only** command to allow IPv6 BGP updates to a peer/peer group to carry private AS numbers.

By default, BGP updates carry the private AS number.

The command does not take effect if the BGP update has both the public AS number and private AS number. The range of private AS number is from 64512 to 65535.

## Examples

# Configure BGP updates sent to the peer 1:2::3:4 to not carry private AS numbers.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 public-as-only
```

## peer reflect-client (IPv6 address family view)

### Syntax

**peer** { *group-name* | *ipv4-address* | *ipv6-address* } **reflect-client**

**undo peer** { *group-name* | *ipv4-address* | *ipv6-address* } **reflect-client**

### View

IPv6 address family view

### Default Level

2: System level

## Parameters

*group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

*ipv4-address*: IPv4 address of a peer.

*ipv6-address*: IPv6 address of a peer.

## Description

Use the **peer reflect-client** command to configure the router as a route reflector and specify a peer/peer group as a client.

Use the **undo peer reflect-client** command to remove the configuration.

By default, neither route reflector nor client is configured.

Related commands: **reflect between-clients**, **reflector cluster-id**.

## Examples

```
# Configure the local device as a route reflector and specify the peer group test as a client.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test
[Sysname-bgp-af-ipv6] peer test reflect-client
```

## peer route-limit (IPv6 address family view)

### Syntax

```
peer { group-name | ipv4-address | ipv6-address } route-limit prefix-number [ { alert-only | reconnect reconnect-time } | percentage ] *
```

```
undo peer { group-name | ipv4-address | ipv6-address } route-limit
```

### View

IPv6 address family view

### Default Level

2: System level

### Parameters

*group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

*ipv4-address*: IPv4 address of a peer.

*ipv6-address*: IPv6 address of a peer.

*prefix number*: Specifies the upper limit of prefixes that can be received from the peer or peer group. The value is in the range 1 to 6144.. When the received prefixes from the peer/peer group reach the specified upper limit, the router will disconnect from the peer/peer group.

**alert-only**: When the received prefixes from the peer/peer group reach the specified upper limit, the router will display alarm messages rather than disconnect from the peer/peer group.

*reconnect-time*: Interval for the router to reconnect to the peer/peer group. The argument has no default. It ranges from 1 to 65535 seconds.

*percentage*: Specifies a percentage value. If the percentage of received routes to the upper limit reaches the value, the router will generate alarm messages. The default is 75. The value is in the range 1 to 100.

### Description

Use the **peer route-limit** command to set the maximum number of prefixes that can be received from a peer/peer group.

Use the **undo peer route-limit** command to restore the default.

By default, the router has no limit on prefixes from a peer/peer group.

The router will end the peer relation when the number of address prefixes received for the peer exceeds the limit.

## Examples

```
# Set the number of prefixes allowed to receive from the peer 1:2::3:4 to 100.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 route-limit 100
```

## peer route-policy (IPv6 address family view)

### Syntax

```
peer { group-name | ipv4-address | ipv6-address } route-policy route-policy-name { import | export }
undo peer { group-name | ipv4-address | ipv6-address } route-policy route-policy-name { import | export }
```

### View

IPv6 address family view

### Default Level

2: System level

### Parameters

*group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

*ipv4-address*: IPv4 address of a peer.

*ipv6-address*: IPv6 address of a peer.

*route-policy-name*: Specifies route-policy name, a string of 1 to 19 characters.

**import**: Applies the routing policy to routes from the peer (group).

**export**: Applies the routing policy to routes sent to the peer (group).

### Description

Use the **peer route-policy** command to apply a routing policy to routes incoming from or outgoing to a peer or peer group.

Use the **undo peer route-policy** command to remove the configuration.

By default, no routing policy is specified for the peer (group).

Use of the **peer route-policy** command does not apply the **if-match interface** clause defined in the routing policy. Refer to *Routing Policy Commands* in the *IP Routing Volume* for related information.

## Examples

```
# Apply the routing policy test-policy to routes received from the peer group test.
<Sysname> system-view
[Sysname] route-policy test-policy permit node 10
[Sysname-route-policy] if-match cost 10
[Sysname-route-policy] apply cost 65535
[Sysname-route-policy] quit
[Sysname] bgp 100
```

```
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test route-policy test-policy import
```

## peer route-update-interval (IPv6 address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } route-update-interval interval
undo peer { ipv6-group-name | ipv6-address } route-update-interval
```

### View

IPv6 address family view

### Default Level

2: System level

### Parameters

*ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of a peer.

*interval*: Specifies the minimum interval for sending the same update to a peer (group) from 5 to 600 seconds.

### Description

Use the **peer route-update-interval** command to specify the interval for sending the same update to a peer/peer group.

Use the **undo peer route-update-interval** command to restore the default.

By default, the interval is 15 seconds for the iBGP peer, and 30 seconds for the eBGP peer.

### Examples

# Specify the interval for sending the same update to the peer 1:2::3:4 as 10 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] peer 1:2::3:4 route-update-interval 10
```

## peer substitute-as (IPv6 address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } substitute-as
undo peer { ipv6-group-name | ipv6-address } substitute-as
```

### View

IPv6 address family view

## Default Level

2: System level

## Parameters

*ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of a peer.

## Description

Use the **peer substitute-as** command to substitute the local AS number for the AS number of a peer/peer group in the AS\_PATH attribute.

Use the **undo peer substitute-as** command to remove the configuration.

The substitution is not configured by default.

## Examples

```
# Substitute the local AS number for the AS number of peer 1:2::3:4.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 substitute-as
```

## peer timer (IPv6 address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } timer keepalive keepalive hold holdtime
undo peer { ipv6-group-name | ipv6-address } timer
```

### View

IPv6 address family view

## Default Level

2: System level

## Parameters

*ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of a peer.

*keepalive*: Specifies the keepalive interval in seconds, ranging from 1 to 21845.

*holdtime*: Specifies the holdtime in seconds, ranging from 3 to 65535.

## Description

Use the **peer timer** command to configure keepalive interval and holdtime interval for a peer or peer group.

Use the **undo peer timer** command to restore the default.

*keepalive* interval defaults to 60 seconds, and *holdtime* interval defaults to 180 seconds

Note that:

- The timer configured with this command is preferred to the timer configured with the **timer** command.
- The holdtime interval must be at least three times the keepalive interval.

Related commands: **timer**.

## Examples

# Configure the keepalive interval and holdtime interval for the peer group test as 60 seconds and 180 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test timer keepalive 60 hold 180
```

## preference (IPv6 address family view)

### Syntax

```
preference { external-preference internal-preference local-preference | route-policy
route-policy-name }
undo preference
```

### View

IPv6 address family view

### Default Level

2: System level

### Parameters

*external-preference*: Preference of eBGP route learned from an eBGP peer, in the range 1 to 255.

*internal-preference*: Preference of iBGP route learned from an iBGP peer, in the range 1 to 255.

*local-preference*: Preference of IPv6 BGP local route, in the range 1 to 255.

*route-policy-name*: Routing policy name, a string of 1 to 19 characters. The routing policy can set a preference for routes passing it. The default value applies to the routes filtered out.

### Description

Use the **preference** command to configure preferences for eBGP, iBGP, and local routes.

Use the **undo preference** command to restore the default.

The bigger the preference value is, the lower the preference is. The default values of *external-preference*, *internal-preference* and *local-preference* are 255, 255 and 130 respectively.

## Examples

# Configure preferences for eBGP, iBGP, and local routes as 20, 20 and 200.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
```

```
[Sysname-bgp-af-ipv6] preference 20 20 200
```

## reflect between-clients (IPv6 address family view)

### Syntax

```
reflect between-clients  
undo reflect between-clients
```

### View

IPv6 address family view

### Default Level

2: System level

### Parameters

None

### Description

Use the **reflect between-clients** command to enable route reflection between clients.

Use the **undo reflect between-clients** command to disable this function.

By default, route reflection between clients is enabled.

After a route reflector is configured, it reflects routes between clients. If the clients are fully meshed, it is recommended to disable route reflection on the route reflector to reduce costs.

Related commands: **reflector cluster-id**, **peer reflect-client**.

### Examples

```
# Enable route reflection between clients.  
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] ipv6-family  
[Sysname-bgp-af-ipv6] reflect between-clients
```

## reflector cluster-id (IPv6 address family view)

### Syntax

```
reflector cluster-id cluster-id  
undo reflector cluster-id
```

### View

IPv6 address family view

### Default Level

2: System level

## Parameters

*cluster-id*: Specifies the cluster ID of the route reflector, an integer from 1 to 4294967295 (the system translates it into an IPv4 address) or an IPv4 address.

## Description

Use the **reflector cluster-id** command to configure the cluster ID of the route reflector.

Use the **undo reflector cluster-id** command to remove the configured cluster ID.

By default, a route reflector uses its router ID as the cluster ID.

Usually, there is only one route reflector in a cluster, so the router ID of the route reflector identifies the cluster. If multiple route reflectors are configured to improve the stability of the network, you should use this command to configure the identical cluster ID for all the reflectors to avoid routing loops.

Related commands: **reflect between-clients**, **peer reflect-client**.

## Examples

# Set 50 as the cluster ID for the route reflector, which is one of multiple route reflectors in the cluster.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] reflector cluster-id 50
```

## refresh bgp ipv6

### Syntax

```
refresh bgp ipv6 { ipv4-address | ipv6-address | all | external | group group-name | internal } { export | import }
```

### View

User view

### Default Level

1: Monitor level

## Parameters

*ipv4-address*: Soft-resets the connection with an IPv4 BGP peer.

*ipv6-address*: Soft-resets the connection with an IPv6 BGP peer.

**all**: Soft-resets all IPv6 BGP connections.

**external**: Soft-resets eBGP connections.

**group** *ipv6-group-name*: Soft-resets connections with a peer group. The name of the peer group is a string of 1 to 47 characters.

**internal**: Soft-resets iBGP connections.

**export**: Performs soft reset in outbound direction.

**import**: Performs soft reset in inbound direction.

## Description

Use the **refresh bgp ipv6** command to soft reset specified IPv4/IPv6 BGP connections. With this feature, you can refresh the IPv4/IPv6 BGP routing table and apply a new available policy without tearing down BGP connections.

To perform IPv4/IPv6 BGP soft reset, all routers in the network should support route-refresh. If a router not supporting route refresh exists in the network, you need to use the **peer keep-all-routes** command on the local router to save all route updates before performing soft reset.

## Examples

```
# Soft reset inbound IPv6 BGP connections.
```

```
<Sysname> refresh bgp ipv6 all import
```

## reset bgp ipv6

### Syntax

```
reset bgp ipv6 { as-number | ipv4-address | ipv6-address [ flap-info ] | all | external | group group-name | internal }
```

### View

User view

### Default Level

1: Monitor level

### Parameters

*as-number*: Resets the IPv6 BGP connections to peers in the specified AS.

*ipv4-address*: Resets the connection to the specified IPv4 BGP peer.

*ipv6-address*: Resets the connection to the specified IPv6 BGP peer.

**flap-info**: Clears route flap information.

**all**: Resets all IPv6 BGP connections.

**external**: Resets all the eBGP connections.

**group** *group-name*: Resets the connections to the specified IPv6 BGP peer group.

**internal**: Resets all the iBGP connections.

## Description

Use the **reset bgp ipv6** command to reset specified IPv4/IPv6 BGP connections.

## Examples

```
# Reset all the IPv6 BGP connections.
```

```
<Sysname> reset bgp ipv6 all
```

## reset bgp ipv6 dampening

### Syntax

```
reset bgp ipv6 dampening [ ipv6-address prefix-length ]
```

## View

User view

## Default Level

1: Monitor level

## Parameters

*ipv6-address*: IPv6 address

*prefix-length*: Prefix length of the address, in the range 0 to 128.

## Description

Use the **reset bgp ipv6 dampening** command to clear dampened IPv6 BGP route information and release suppressed routes.

If no *ipv6-address prefix-length* is specified, all dampened IPv6 BGP route information will be cleared.

## Examples

# Clear the dampened information of routes to 2345::/64 and release suppressed routes.

```
<Sysname> reset bgp ipv6 dampening 2345:: 64
```

## reset bgp ipv6 flap-info

### Syntax

```
reset bgp ipv6 flap-info [ ipv6-address/prefix-length | as-path-acl as-path-acl-number | regex  
as-path-regexp ]
```

## View

User view

## Default Level

1: Monitor level

## Parameters

*ipv6-address*: Clears the flap statistics for the specified IPv6 address.

*prefix-length*: Prefix length of the address, in the range 1 to 128.

*as-path-acl-number*: Clears the flap statistics for routes matching the AS path ACL. The number is in the range 1 to 256.

*as-path-regexp*: Clears the flap statistics for routes matching the AS path regular expression.

## Description

Use the **reset bgp ipv6 flap-info** command to clear IPv6 routing flap statistics.

If no parameters are specified, the flap statistics of all the routes will be cleared

## Examples

# Clear the flap statistics of the routes matching AS path ACL 10.

```
<Sysname> system-view
```

```
[Sysname] ip as-path 10 permit ^100.*200$
[Sysname] quit
<Sysname> reset bgp ipv6 flap-info as-path-acl 10
```

## router-id

### Syntax

```
router-id router-id
undo router-id
```

### View

BGP view

### Default Level

2: System level

### Parameters

*router-id*: Router ID in IP address format.

### Description

Use the **router-id** command to specify a router ID for the router.

Use the **undo router-id** command to remove a router ID.

To run IPv6 BGP protocol, a router must have a router ID, an unsigned 32-bit integer and the unique ID of the router in the AS.

A router ID can be configured manually. If not, the system will select a router ID automatically from the current interfaces' IPv4 addresses. The selection sequence is the highest IPv4 address of Loopback interfaces' addresses, then the highest IPv4 address of physical interfaces' addresses if no Loopback interfaces are configured.

Only when the interface with the router ID is removed or the manually configured router ID is removed, will the system select another Router ID. To improve network reliability, it is recommended to configure the IPv4 address of a loopback interface as the router ID.

### Examples

```
# Specify the router ID of the router as 10.18.4.221.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] router-id 10.18.4.221
```

## synchronization (IPv6 address family view)

### Syntax

```
synchronization
undo synchronization
```

### View

IPv6 address family view

## Default Level

2: System level

## Parameters

None

## Description

Use the **synchronization** command to enable the synchronization between IPv6 BGP and IGP.

Use the **undo synchronization** command to disable the synchronization.

The feature is disabled by default.

With this feature enabled and when a non-BGP router is responsible for forwarding packets in an AS, IPv6 BGP speakers in the AS cannot advertise routing information to other ASs unless all routers in the AS know the latest routing information.

By default, upon receiving an IPv6 iBGP route, the BGP router only checks whether the next hop is reachable before advertisement. If synchronization is enabled, the iBGP route can be advertised to eBGP peers only when the route is also advertised by the IGP.

## Examples

```
# Enable the route synchronization between IPv6 BGP and IGP.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] synchronization
```

## timer (IPv6 address family view)

### Syntax

```
timer keepalive keepalive hold holdtime
```

```
undo timer
```

### View

IPv6 address family view

## Default Level

2: System level

## Parameters

*keepalive*: Keepalive interval in seconds, ranging from 1 to 21845.

*holdtime*: Holdtime interval in seconds, ranging from 3 to 65535.

## Description

Use the **timer** command to specify IPv6 BGP keepalive interval and holdtime interval.

Use the **undo timer** command to restore the default.

By default, the keepalive and holdtime intervals are 60s and 180s respectively.

Note that:

- Timer configured using the **peer timer** command is preferred to the timer configured using the **timer** command.
- The holdtime interval must be at least three times the keepalive interval.
- The configured timer applies to all the IPv6 BGP peers. It becomes valid only after the corresponding IPv6 BGP connections are reset.

Related commands: **peer timer**.

## Examples

# Configure keepalive interval and holdtime interval as 60 and 180 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] timer keepalive 60 hold 180
```

# Table of Contents

<b>1 Route Policy Configuration Commands</b>	<b>1-1</b>
Common Route Policy Configuration Commands	1-1
apply as-path	1-1
apply comm-list delete	1-2
apply community	1-2
apply cost	1-3
apply cost-type	1-4
apply extcommunity	1-5
apply isis	1-5
apply local-preference	1-6
apply origin	1-7
apply preference	1-8
apply preferred-value	1-8
apply tag	1-9
display ip as-path	1-10
display ip community-list	1-10
display ip extcommunity-list	1-11
display route-policy	1-11
if-match as-path	1-12
if-match community	1-13
if-match cost	1-14
if-match extcommunity	1-14
if-match interface	1-15
if-match route-type	1-16
if-match tag	1-17
ip as-path	1-17
ip community-list	1-18
ip extcommunity-list	1-19
route-policy	1-20
IPv4 Route Policy Configuration Commands	1-21
apply ip-address next-hop	1-21
display ip ip-prefix	1-22
if-match acl	1-22
if-match ip	1-23
if-match ip-prefix	1-24
ip ip-prefix	1-24
reset ip ip-prefix	1-26
IPv6 Route Policy Configuration Commands	1-26
apply ipv6 next-hop	1-26
display ip ipv6-prefix	1-27
if-match ipv6	1-28
ip ipv6-prefix	1-28
reset ip ipv6-prefix	1-30



# 1 Route Policy Configuration Commands

---



The common configuration commands of route policy are applicable to both IPv4 and IPv6.

---

## Common Route Policy Configuration Commands

### apply as-path

#### Syntax

```
apply as-path as-number&<1-10> [ replace ]  
undo apply as-path
```

#### View

Route policy view

#### Default Level

2: System level

#### Parameters

*as-number*: Autonomous system number, in the range of 1 to 65535.

&<1-10>: Indicates you can enter up to 10 AS numbers.

**replace**: Replaces the original AS numbers.

#### Description

Use the **apply as-path** command to apply the specified AS numbers to BGP routes.

Use the **undo apply as-path** command to remove the clause configuration.

No AS\_PATH attribute is set by default.

With the **replace** keyword included, the **apply as-path** command replaces the original AS\_PATH attribute with the specified AS numbers. Without the **replace** keyword, this command adds the specified AS numbers before the original AS\_PATH attribute.

#### Examples

```
# Configure node 10 in permit mode of route policy policy1: add AS number 200 before the original  
AS_PATH attribute of BGP routing information matching AS-PATH list 1.
```

```
<Sysname> system-view  
[Sysname] route-policy policy1 permit node 10
```

```
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply as-path 200
```

## apply comm-list delete

### Syntax

```
apply comm-list comm-list-number delete
undo apply comm-list
```

### View

Route policy view

### Default Level

2: System level

### Parameters

*comm-list-number*: Community list number. A basic community list number ranges from 1 to 99. An advanced community list number ranges from 100 to 199.

### Description

Use the **apply comm-list delete** command to remove the community attributes specified by the community list from BGP routing information.

Use the **undo apply comm-list** command to remove the clause configuration.

No community attributes are removed from BGP routing information by default.

### Examples

# Configure node 10 in permit mode of route policy **policy1**: remove the community attributes specified in community list 1 from the BGP routing information matching AS-PATH list 1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply comm-list 1 delete
```

## apply community

### Syntax

```
apply community { none | additive | { community-number<1-16> | aa:nn<1-16> | internet | no-export-subconfed | no-export | no-advertise } * [ additive ] }
undo apply community
```

### View

Route policy view

### Default Level

2: System level

## Parameters

**none:** Removes the community attributes of BGP routes.

*community-number:* Community sequence number, in the range 1 to 4294967295.

*aa:nn:* Community number; both aa and nn are in the range 0 to 65535.

*&<1-16>:* Indicates the argument before it can be entered up to 16 times.

**internet:** Sets the **internet** community attribute for BGP routes. Routes with this attribute can be advertised to all BGP peers.

**no-export-subconfed:** Sets the **no-export-subconfed** community attribute for BGP routes. Routes with this attribute cannot be advertised out the sub autonomous system.

**no-advertise:** Sets the **no-advertise** community attribute for BGP routes. Routes with this attribute cannot be advertised to any peers.

**no-export:** Sets the **no-export** community attribute for BGP routes. Routes with this attribute cannot be advertised out the autonomous system or confederation, but can be advertised to other sub ASs in the confederation.

**additive:** Adds the specified community attribute to the original community attribute of BGP routes.

## Description

Use the **apply community** command to set the specified community attribute for BGP routes.

Use the **undo apply community** command to remove the apply clause.

No community attribute is set for BGP routes by default.

Related commands: **ip community-list**, **if-match community**, **route-policy**.

## Examples

# Configure node 16 in permit mode of route policy **setcommunity**: Set the no-export community attribute for BGP routes matching AS-PATH list 8.

```
<Sysname> system-view
[Sysname] route-policy setcommunity permit node 16
[Sysname-route-policy] if-match as-path 8
[Sysname-route-policy] apply community no-export
```

## apply cost

### Syntax

**apply cost** [ + | - ] *value*

**undo apply cost**

### View

Route policy view

### Default Level

2: System level

### Parameters

**+**: Increases a cost value.

**+**: Decreases a cost value.

**cost**: Cost in the range 0 to 4294967295.

## Description

Use the **apply cost** command to set a cost for routing information.

Use the **undo apply cost** command to remove the clause configuration.

No cost is set for routing information by default.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply local-preference**, **apply origin**, **apply tag**.

## Examples

# Configure node 10 in permit mode of route policy **policy1**: set a cost of 120 for routing information whose outbound interface is Vlan-interface 10.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match interface Vlan-interface 10
[Sysname-route-policy] apply cost 120
```

## apply cost-type

### Syntax

```
apply cost-type { external | internal | type-1 | type-2 }
undo apply cost-type
```

### View

Route policy view

### Default Level

2: System level

### Parameters

**external**: IS-IS external route.

**internal**: IS-IS internal route.

**type-1**: Type-1 external route of OSPF.

**type-2**: Type-2 external route of OSPF.

## Description

Use the **apply cost-type** command to set a cost type for routing information.

Use the **undo apply cost-type** command to remove the clause configuration.

No cost type is set for routing information by default.

## Examples

# Create node 10 in permit mode of route policy **policy1**: If a route has a tag of 8, set the cost type for the route to IS-IS internal route.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match tag 8
[Sysname-route-policy] apply cost-type internal
```

## apply extcommunity

### Syntax

```
apply extcommunity { rt route-target }&<1-16> [ additive ]
undo apply extcommunity
```

### View

Route policy view

### Default Level

2: System level

### Parameters

**rt route-target**: Sets the route target extended community attribute, which is a string of 3 to 21 characters. A *route-target* has two forms:

16-bit AS number: 32-bit self-defined number, for example, 101:3;

32-bit IP address: 16-bit self-defined number, for example, 192.168.122.15:1.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

**additive**: Adds the specified attribute to the original RT community attribute.

### Description

Use the **apply extcommunity** command to apply the specified RT extended community attribute to BGP routes.

Use the **undo apply extcommunity** command to remove the clause configuration.

No RT extended community attribute is set for BGP routing information by default.

### Examples

# Configure node 10 in permit mode of route policy **policy1**: If a BGP route matches AS-PATH list 1, add the RT extended community attribute 100:2 to the route.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply extcommunity rt 100:2 additive
```

## apply isis

### Syntax

```
apply isis { level-1 | level-1-2 | level-2 }
undo apply isis
```

## View

Route policy view

## Default Level

2: System level

## Parameters

**level-1:** Redistributes routes into IS-IS level-1.

**level-2:** Redistributes routes into IS-IS level-2.

**level-1-2:** Redistributes routes into both IS-IS level-1 and level-2.

## Description

Use the **apply isis** command to redistribute routes into a specified ISIS level.

Use the **undo apply isis** command to remove the clause configuration.

No IS-IS level is set by default.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply cost**, **apply origin**, **apply tag**.

## Examples

# Configure node 10 in permit mode of route policy **policy1**: If a route has a tag of 8, redistribute the route to IS-IS level-2.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match tag 8
[Sysname-route-policy] apply isis level-2
```

## apply local-preference

### Syntax

**apply local-preference** *preference*

**undo apply local-preference**

### View

Route policy view

### Default Level

2: System level

### Parameters

*preference*: BGP local preference, in the range 0 to 4294967295.

### Description

Use the **apply local-preference** command to set the specified local preference for BGP routes.

Use the **undo apply local-preference** command to remove the clause configuration.

No local preference is set for BGP routing information by default.

Related commands: **route-policy**.

## Examples

# Configure node 10 in permit mode of route policy **policy1**: If a route matches AS-PATH list 1, set a local preference of 130 for the route.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply local-preference 130
```

## apply origin

### Syntax

```
apply origin { igp | egp as-number | incomplete }
undo apply origin
```

### View

Route policy view

### Default Level

2: System level

### Parameters

**igp**: Sets the origin attribute of BGP routing information to IGP.

**egp**: Sets the origin attribute of BGP routing information to EGP.

*as-number*: Autonomous system number for EGP routes, in the range of 1 to 65535.

**incomplete**: Sets the origin attribute of BGP routing information to unknown.

### Description

Use the **apply origin** command to set the specified origin attribute for BGP routes.

Use the **undo apply origin** command to remove the clause configuration.

No origin attribute is set for BGP routing information by default.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply local-preference**, **apply cost**, **apply tag**.

## Examples

# Configure node 10 in permit mode of route policy **policy1**: If BGP routing information matches AS-PATH list 1, set the origin attribute of the routing information to IGP.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply origin igp
```

## apply preference

### Syntax

```
apply preference preference  
undo apply preference
```

### View

Route policy view

### Default Level

2: System level

### Parameters

*preference*: Routing protocol preference, in the range of 1 to 255.

### Description

Use the **apply preference** command to set a preference for a routing protocol.

Use the **undo apply preference** command to remove the clause configuration.

No preference is set for a routing protocol by default.

If you have set preferences for routing protocols with the **preference** command, using the **apply preference** command will set a new preference for the matching routing protocol. Non-matching routing protocols still use the preferences set by the **preference** command.

### Examples

```
# Configure node 10 in permit mode of route policy policy1: Set the preference for OSPF external routes to 90.
```

```
<Sysname> system-view  
[Sysname] route-policy policy1 permit node 10  
[Sysname-route-policy] if-match route-type external-type1or2  
[Sysname-route-policy] apply preference 90
```

## apply preferred-value

### Syntax

```
apply preferred-value preferred-value  
undo apply preferred-value
```

### View

Route policy view

### Default Level

2: System level

### Parameters

*preferred-value*: Preferred value, in the range of 0 to 65535.

## Description

Use the **apply preferred-value** command to set a preferred value for BGP routes.

Use the **undo apply preferred-value** command to remove the clause configuration.

No preferred value is set for BGP routes by default.

## Examples

# Configure node 10 in permit mode of route policy **policy1**: Set a preferred value of 66 for BGP routing information matching AS-PATH list 1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply preferred-value 66
```

## apply tag

### Syntax

**apply tag** *value*

**undo apply tag**

### View

Route policy view

### Default Level

2: System level

### Parameters

*value*: Tag value, in the range 0 to 4294967295.

## Description

Use the **apply tag** command to set a specified tag value for RIP, OSPF or IS-IS routing information.

Use the **undo apply tag** command to remove the clause configuration.

No routing tag is set for RIP, OSPF or IS-IS routing information by default.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply local-preference**, **apply cost**, **apply origin**.

## Examples

# Configure node 10 in permit mode of route policy **policy1**: set a tag of 100 for OSPF external routes.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match route-type external-type1
[Sysname-route-policy] apply tag 100
```

## display ip as-path

### Syntax

```
display ip as-path [ as-path-number ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*as-path-number*: AS-PATH list number, in the range of 1 to 256.

### Description

Use the **display ip as-path** command to display BGP AS-PATH list information.

Information about all BGP AS-PATH lists will be displayed if no *as-path-number* is specified.

Related commands: **ip as-path**, **if-match as-path**, **apply as-path**.

### Examples

# Display the information of BGP AS-PATH list 1.

```
<Sysname> display ip as-path 1
ListID   Mode      Expression
1        permit    2
```

**Table 1-1** display ip as-path command output description

Field	Description
ListID	AS-PATH list ID
Mode	Matching mode: permit, deny
Expression	Regular expression for matching

## display ip community-list

### Syntax

```
display ip community-list [ basic-community-list-number | adv-community-list-number ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*basic-community-list-number*: Basic community list number, in the range of 1 to 99.

*adv-community-list-number*: Advanced community list number, in the range of 100 to 199.

## Description

Use the **display ip community-list** command to display BGP community list information.

All BGP community list information will be displayed if no *basic-community-list-number* or *adv-community-list-number* is specified.

Related commands: **ip community-list**, **if-match community**, **apply community**.

## Examples

# Display the information of the BGP community list 1.

```
<Sysname> display ip community-list 1
Community List Number 1
    permit 1:1 1:2 2:2
```

## display ip extcommunity-list

### Syntax

```
display ip extcommunity-list [ ext-comm-list-number ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ext-comm-list-number*: Extended community list number, in the range of 1 to 199.

## Description

Use the **display ip extcommunity-list** command to display BGP extended community list information.

All BGP extended community list information will be displayed if no *ext-comm-list-number* is specified.

Related commands: **ip extcommunity-list**, **if-match extcommunity**, **apply extcommunity**.

## Examples

# Display the information of BGP extended community list 1.

```
<Sysname> display ip extcommunity-list 1
Extended Community List Number 1
    permit rt : 9:6
```

## display route-policy

### Syntax

```
display route-policy [ route-policy-name ]
```

### View

Any view

## Default Level

1: Monitor level

## Parameters

*route-policy-name*: Route policy name, a string of 1 to 19 characters.

## Description

Use the **display route-policy** command to display route policy information.

All route policy information will be displayed if no *route-policy-name* is specified.

Related commands: **route-policy**.

## Examples

```
# Display the information of route policy 1.
<Sysname> display route-policy policy1
Route-policy : policy1
  permit : 10
    if-match ip-prefix abc
    apply cost 120
```

**Table 1-2 display route-policy** command output description.

Field	Description
Route-policy	Route policy name
Permit	Match mode of route policy node 10
if-match ip-prefix abc	Match criterion
apply cost 120	If the match criterion is satisfied, set a cost of 120 for routing information.

## if-match as-path

### Syntax

```
if-match as-path as-path-number&<1-16>
undo if-match as-path [ as-path-number&<1-16> ]
```

### View

Route policy view

## Default Level

2: System level

## Parameters

*as-path-number*: AS path list number, in the range of 1 to 256.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

## Description

Use the **if-match as-path** command to specify AS-PATH list(s) for matching against the AS path attribute of BGP routing information.

Use the **undo if-match as-path** command to remove the match criterion.

The match criterion is not configured by default.

Related commands: **route-policy**, **ip as-path-acl**.

## Examples

# Define AS-PATH list 2, allowing BGP routing information containing AS number 200 or 300 to pass. Configure node 10 in permit mode of route policy **test**: specify AS-PATH list 2 for matching.

```
<Sysname> system-view
[Sysname] ip as-path 2 permit *_200.*300
[Sysname] route-policy test permit node 10
[Sysname-route-policy] if-match as-path 2
```

## if-match community

### Syntax

```
if-match community { basic-community-list-number [ whole-match ] | adv-community-list-number }&<1-16>
```

```
undo if-match community [ basic-community-list-number | adv-community-list-number ]&<1-16>
```

### View

Route policy view

### Default Level

2: System level

### Parameters

*basic-community-list-number*: Basic community list number, in the range of 1 to 99.

*adv-community-list-number*: Advanced community list number, in the range of 100 to 199.

**whole-match**: Exactly matches the specified community list(s).

&<1-16>: Indicates the argument before it can be entered up to 16 times.

## Description

Use the **if-match community** command to specify community list(s) for matching against the community attribute of BGP routing information.

Use the **undo if-match community** command to remove the match criterion.

The match criterion is not configured by default.

Related commands: **route-policy**, **ip community-list**.

## Examples

# Define community list 1, allowing BGP routing information with community number 100 or 200 to pass. Then configure node 10 in permit mode of route policy **test**: specify community-list 1 for matching.

```
<Sysname> system-view
[Sysname] ip community-list 1 permit 100 200
[Sysname] route-policy test permit node 10
[Sysname-route-policy] if-match community 1
```

## if-match cost

### Syntax

```
if-match cost value
undo if-match cost
```

### View

Route policy view

### Default Level

2: System level

### Parameters

*cost*: Cost in the range 0 to 4294967295.

### Description

Use the **if-match cost** command to match routing information having the specified cost.

Use the **undo if-match cost** command to remove the match criterion.

The match criterion is not configured by default.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply cost**, **apply local-preference**, **apply origin**, **apply tag**.

### Examples

# Configure node 10 in permit mode of route policy **policy1**: define an if-match clause to permit routing information with a cost of 8.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match cost 8
```

## if-match extcommunity

### Syntax

```
if-match extcommunity ext-comm-list-number&<1-16>
undo if-match extcommunity [ ext-comm-list-number&<1-16> ]
```

### View

Route policy view

### Default Level

2: System level

## Parameters

*ext-comm-list-number*: Extended community list number, in the range of 1 to 199.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

## Description

Use the **if-match extcommunity** command to specify extended community list(s) for matching against the extended community attribute of BGP routing information.

Use the **undo if-match extcommunity** command to remove the match criterion.

The match criterion is not configured by default.

## Examples

# Configure node 10 in permit mode of route policy **policy1** to match BGP routing information to extended community lists 100 and 150.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match extcommunity 100 150
```

## if-match interface

### Syntax

**if-match interface** { *interface-type interface-number* }&<1-16>

**undo if-match interface** [ *interface-type interface-number* ]&<1-16>

### View

Route policy view

### Default Level

2: System level

## Parameters

*interface-type*: Interface type

*interface-number*: Interface number

&<1-16>: Indicates the argument before it can be entered up to 16 times.

## Description

Use the **if-match interface** command to specify interface(s) for matching against the outbound interface of routing information.

Use the **undo if-match interface** command to remove the match criterion.

The match criterion is not configured by default.

Related commands: **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply cost**, **apply local-preference**, **apply origin**, **apply tag**.

## Examples

# Configure node 10 in permit mode of route policy **policy1** to permit routing information with the outbound interface as VLAN-interface 1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match interface vlan-interface 1
```

## if-match route-type

### Syntax

**if-match route-type** { **internal** | **external-type1** | **external-type2** | **external-type1or2** | **is-is-level-1** | **is-is-level-2** | **nssa-external-type1** | **nssa-external-type2** | **nssa-external-type1or2** } \*

**undo if-match route-type** [ **internal** | **external-type1** | **external-type2** | **external-type1or2** | **is-is-level-1** | **is-is-level-2** | **nssa-external-type1** | **nssa-external-type2** | **nssa-external-type1or2** ] \*

### View

Route policy view

### Default Level

2: System level

### Parameters

**internal**: Internal routes (OSPF intra-area and inter-area routes).

**external-type1**: OSPF Type 1 external routes.

**external-type2**: OSPF Type 2 external routes.

**external-type1or2**: OSPF Type 1 or 2 external routes.

**is-is-level-1**: IS-IS Level-1 routes.

**is-is-level-2**: IS-IS Level-2 routes.

**nssa-external-type1**: OSPF NSSA Type 1 external routes.

**nssa-external-type2**: OSPF NSSA Type 2 external routes.

**nssa-external-type1or2**: OSPF NSSA Type 1 or 2 external routes.

### Description

Use the **if-match route-type** command to configure a route type match criterion.

Use the **undo if-match route-type** command to remove the match criterion.

The match criterion is not configured by default.

## Examples

# Configure node 10 in permit mode of route policy **policy1** to match OSPF internal routes.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match route-type internal
```

## if-match tag

### Syntax

```
if-match tag value  
undo if-match tag
```

### View

Route policy view

### Default Level

2: System level

### Parameters

*value*: Specifies a tag from 0 to 4294967295.

### Description

Use the **if-match tag** command to match routing information having the specified tag.

Use the **undo if-match tag** command to remove the match criterion.

The match criterion is not configured by default.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **route-policy**, **apply ip-address next-hop**, **apply cost**, **apply local-preference**, **apply origin**, **apply tag**.

### Examples

# Configure node 10 in permit mode of route policy **policy1** to permit RIP, OSPF and IS-IS routing information with a tag of 8.

```
<Sysname> system-view  
[Sysname] route-policy policy1 permit node 10  
[Sysname-route-policy] if-match tag 8
```

## ip as-path

### Syntax

```
ip as-path as-path-number { deny | permit } regular-expression  
undo ip as-path as-path-number
```

### View

System view

### Default Level

2: System level

### Parameters

*as-path-number*: AS-PATH list number, in the range of 1 to 256.

**deny**: Specifies the matching mode for the AS-PATH list as deny.

**permit:** Specifies the matching mode for the AS-PATH list as permit.

*regular-expression:* AS-PATH regular expression, a string of 1 to 50 characters.

BGP routing updates contain the AS path attribute field that identifies the autonomous systems through which the routing information has passed. An AS-PATH regular expression, for example, `^200.*100$`, matches the AS path attribute that starts with AS200 and ends with AS100. For the meanings of special characters used in regular expressions, refer to "CLI Display" in *Basic System Configuration* in the *System Volume*.

## Description

Use the **ip as-path** command to create an AS-PATH list.

Use the **undo ip as-path** command to remove an AS-PATH list.

No AS-PATH list is created by default.

## Examples

# Create AS-PATH list 1, permitting routing information whose AS\_PATH attribute starts with 10.

```
<Sysname> system-view
[Sysname] ip as-path 1 permit ^10
```

## ip community-list

### Syntax

```
ip community-list basic-comm-list-num { deny | permit } [ community-number-list ] [ internet | no-advertise | no-export | no-export-subconfed ] *
```

```
undo ip community-list basic-comm-list-num [ community-number-list ] [ internet | no-advertise | no-export | no-export-subconfed ] *
```

```
ip community-list adv-comm-list-num { deny | permit } regular-expression
```

```
undo ip community-list adv-comm-list-num [ regular-expression ]
```

### View

System view

### Default Level

2: System level

### Parameters

*basic-comm-list-num:* Basic community list number, in the range 1 to 99.

*adv-comm-list-num:* Advanced community list number, in the range 100 to 199.

*regular-expression:* Regular expression of advanced community attribute, a string of 1 to 50 characters.

**deny:** Specifies the matching mode of the community list as deny.

**permit:** Specifies the matching mode of the community list as permit.

*community-number-list:* Community number list, which is in the *community number* or *aa:nn* format; a *community number* is in the range 1 to 4294967295; *aa* and *nn* are in the range 0 to 65535. Up to 16 community numbers can be entered.

**internet:** Routes with this attribute can be advertised to all BGP peers. By default, all routes have this attribute.

**no-advertise:** Routes with this attribute cannot be advertised to other BGP peers.

**no-export:** Routes with this attribute cannot be advertised out the local AS, or the confederation but can be advertised to other ASs in the confederation.

**no-export-subconfed:** Routes with this attribute cannot be advertised out the local AS, or to other sub ASs in the confederation.

## Description

Use the **ip community-list** to define a community list entry.

Use the **undo ip community-list** command to remove a community list or entry.

No community list is defined by default.

## Examples

# Define basic community list 1 to permit routing information with the **internet** community attribute.

```
<Sysname> system-view
[Sysname] ip community-list 1 permit internet
```

# Define advanced community list 100 to permit routing information with the community attribute starting with 10.

```
<Sysname> system-view
[Sysname] ip community-list 100 permit ^10
```

## ip extcommunity-list

### Syntax

```
ip extcommunity-list ext-comm-list-number { deny | permit } { rt route-target } &<1-16>
undo ip extcommunity-list ext-comm-list-number
```

### View

System view

### Default Level

2: System level

### Parameters

*ext-comm-list-number*: Extended community list number, in the range 1 to 199.

**permit**: Specifies the matching mode for the extended community list as permit.

**deny**: Specifies the matching mode for the extended community list as deny.

**rt** *route-target*: Specifies the route target extended community attribute, which is a string of 3 to 21 characters. A *route-target* has two forms:

A 16-bit AS number: a 32-bit self-defined number, for example, 101:3;

A 32-bit IP address: a 16-bit self-defined number, for example, 192.168.122.15:1.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

## Description

Use the **ip extcommunity-list** to define an extended community list entry.

Use the **undo ip extcommunity-list** command to remove an extended community list.

No extended community list is defined by default.

## Examples

# Define extended community list 1 to permit routing information with RT 200:200.

```
<Sysname> system-view
[Sysname] ip extcommunity-list 1 permit rt 200:200
```

## route-policy

### Syntax

**route-policy** *route-policy-name* { **permit** | **deny** } **node** *node-number*

**undo route-policy** *route-policy-name* [ **node** *node-number* ]

### View

System view

### Default Level

2: System level

### Parameters

*route-policy-name*: Route policy name, a string of 1 to 19 characters.

**permit**: Specifies the matching mode of the route policy node as permit. If a route satisfies all the if-match clauses of the node, it passes the node and then is executed with the apply clauses of the node. If not, it goes to the next node of the route policy.

**deny**: Specifies the matching mode of the route policy node as deny. If a route satisfies all the if-match clauses of the node, it cannot pass the node and will not go to the next node.

**node** *node-number*: Node number, in the range 0 to 65535. A node with a smaller number is matched first.

## Description

Use the **route-policy** command to create a route policy and a node of it and enter route policy view.

Use the **undo route-policy** command to remove a route policy or a node of it.

No route policy is created by default.

A route policy is used for routing information filtering or policy based routing. It contains several nodes and each node comprises a set of if-match and apply clauses. The if-match clauses define the matching criteria of the node and the apply clauses define the actions to be taken on packets passing the node. The relation between the if-match clauses of a node is logic AND, namely, all the if-match clauses must be satisfied. The relation between different route policy nodes is logic OR, namely, a packet passing a node passes the route policy.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **apply ip-address next-hop**, **apply local-preference**, **apply cost**, **apply origin**, **apply tag**.

## Examples

```
# Configure node 10 in permit mode of route policy policy1 and enter route policy view.
```

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy]
```

# IPv4 Route Policy Configuration Commands

## apply ip-address next-hop

### Syntax

```
apply ip-address next-hop ip-address
undo apply ip-address next-hop
```

### View

Route policy view

### Default Level

2: System level

### Parameters

*ip-address*: IP address of the next hop.

### Description

Use the **apply ip-address next-hop** command to set a next hop for IPv4 routing information.

Use the **undo apply ip-address next-hop** command to remove the clause configuration.

No next hop is set for IPv4 routing information by default.

This command cannot set a next hop for redistributed routes.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply local-preference**, **apply cost**, **apply origin**, **apply tag**.

## Examples

```
# Configure node 10 in permit mode of route policy policy1 to set next hop 193.1.1.8 for routes matching AS-PATH list 1.
```

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply ip-address next-hop 193.1.1.8
```

## display ip ip-prefix

### Syntax

```
display ip ip-prefix [ ip-prefix-name ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ip-prefix-name*: IP prefix list name, a string of 1 to 19 characters.

### Description

Use the **display ip ip-prefix** command to display the statistics of an IPv4 prefix list. If no *ip-prefix-name* is specified, statistics for all IPv4 prefix lists will be displayed.

Related commands: **ip ip-prefix**.

### Examples

# Display the statistics of IPv4 prefix list **abc**.

```
<Sysname> display ip ip-prefix abc
Prefix-list abc
Permitted 0
Denied 0
      index: 10          permit 1.0.0.0/11          ge 22 le 32
```

**Table 1-3** display ip ip-prefix command output description.

Field	Description
Prefix-list	Name of the IPv4 prefix list
Permitted	Number of routes satisfying the match criterion
Denied	Number of routes not satisfying the match criterion
index	Index of the IPv4 prefix list
permit	Matching mode: permit or deny
1.0.0.0/11	IP address and mask
ge	greater-equal, the lower limit
le	less-equal, the higher limit

## if-match acl

### Syntax

```
if-match acl acl-number
```

```
undo if-match acl
```

## View

Route policy view

## Default Level

2: System level

## Parameters

*acl-number*: ACL number from 2000 to 3999.

## Description

Use the **if-match acl** command to configure an ACL match criterion.

Use the **undo if-match acl** command to remove the match criterion.

No ACL match criterion is configured by default.

Related commands: **if-match interface**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply cost**, **apply local-preference**, **apply origin**, **apply tag**.

## Examples

```
# Configure node 10 of route policy policy1 to permit routes matching ACL 2000.
```

```
<Sysname> system-view  
[Sysname] route-policy policy1 permit node 10  
[Sysname-route-policy] if-match acl 2000
```

## if-match ip

### Syntax

```
if-match ip { next-hop | route-source } { acl acl-number | ip-prefix ip-prefix-name }
```

```
undo if-match ip { next-hop | route-source } [ acl | ip-prefix ]
```

### View

Route policy view

### Default Level

2: System level

### Parameters

**next-hop**: Matches the next hop of routing information to the filter.

**route-source**: Matches the source address of routing information to the filter.

**acl** *acl-number*: Matches an ACL with a number from 2000 to 2999.

**ip-prefix** *ip-prefix-name*: Matches an IP prefix list with a name being a string of 1 to 19 characters.

### Description

Use the **if-match ip** command to configure a next hop or source address match criterion for IPv4 routes.

Use the **undo if-match ip** command to remove the match criterion.

The match criterion is not configured by default.

Related commands: **route-policy**.

## Examples

# Configure node 10 of route policy **policy1** to permit routing information whose next hop address matches IP prefix list **p1**.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match ip next-hop ip-prefix p1
```

## if-match ip-prefix

### Syntax

```
if-match ip-prefix ip-prefix-name
undo if-match ip-prefix
```

### View

Route policy view

### Default Level

2: System level

### Parameters

*ip-prefix-name*: Matches an IP prefix list with a name being a string of 1 to 19 characters.

### Description

Use the **if-match ip-prefix** command to configure an IP prefix list based match criterion.

Use the **undo if-match ip-prefix** command to remove the match criterion.

No IP prefix list based match criterion is configured by default.

Related commands: **if-match interface**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply cost**, **apply local-preference**, **apply origin**, **apply tag**.

## Examples

# Configure node 10 of route policy **policy2** to permit routes whose destination address matches IP prefix list **p1**.

```
<Sysname> system-view
[Sysname] route-policy policy2 permit node 10
[Sysname-route-policy] if-match ip-prefix p1
```

## ip ip-prefix

### Syntax

```
ip ip-prefix ip-prefix-name [ index index-number ] { permit | deny } ip-address mask-length
[ greater-equal min-mask-length ] [ less-equal max-mask-length ]
undo ip ip-prefix ip-prefix-name [ index index-number ]
```

## View

System view

## Default Level

2: System level

## Parameters

*ip-prefix-name*: IPv4 prefix list name, a string of 1 to 19 characters.

*index-number*: Index number, in the range 1 to 65535, for uniquely specifying an item of the IPv4 prefix list. An index with a smaller number is matched first.

**permit**: Specifies the matching mode for the IPv4 prefix list item as permit, that is, if a route matches the item, the route passes the IPv4 prefix list without needing to match against the next item; if not, it will match against the next item (suppose the IPv4 prefix list has multiple items configured).

**deny**: Specifies the matching mode for the IPv4 prefix list item as deny, that is, if a route matches the item, the route neither passes the filter nor matches against the next item; if not, the route will match against the next item (suppose the IPv4 prefix list has multiple items configured).

*ip-address mask-length*: Specifies an IPv4 prefix and mask length. The *mask-length* is in the range 0 to 32.

*min-mask-length*, *max-mask-length*: Specifies the prefix range. **greater-equal** means “greater than or equal to” and **less-equal** means “less than or equal to”. The range relation is  $mask-length \leq min-mask-length \leq max-mask-length \leq 32$ . If only the *min-mask-length* is specified, the prefix length range is [ *min-mask-length*, 32 ]. If only the *max-mask-length* is specified, the prefix length range is [ *mask-length*, *max-mask-length* ]. If both *min-mask-length* and *max-mask-length* are specified, the prefix length range is [ *min-mask-length*, *max-mask-length* ].

## Description

Use the **ip ip-prefix** command to configure an IPv4 prefix list or an item of it.

Use the **undo ip ip-prefix** command to remove an IPv4 prefix list or an item of it.

No IPv4 prefix list is configured by default.

An IPv4 prefix list is used to filter IPv4 addresses. It may have multiple items, each of which specifies a range of IPv4 prefixes. The relation between the items is logic OR, namely, if an item is passed, the IPv4 prefix list is passed. If no item is passed, the IP prefix list cannot be passed.

The IP prefix range is determined by *mask-length* and [ *min-mask-length*, *max-mask-length* ]. If both *mask-length* and [ *min-mask-length*, *max-mask-length* ] are specified, the IP address must satisfy both of them.

If both *ip-address* and *mask-length* are specified as 0.0.0.0 0, only the default route will be matched.

To match all routes, use 0.0.0.0 0 **less-equal** 32.

## Examples

```
# Define IP prefix list p1 to permit routes matching network 10.0.192.0/8 and with mask length 17 or 18.
```

```
<Sysname> system-view
```

```
[Sysname] ip ip-prefix p1 permit 10.0.192.0 8 greater-equal 17 less-equal 18
```

## reset ip ip-prefix

### Syntax

```
reset ip ip-prefix [ ip-prefix-name ]
```

### View

User view

### Default Level

2: System level

### Parameters

*ip-prefix-name*: IP prefix list name, a string of 1 to 19 characters.

### Description

Use the **reset ip ip-prefix** command to clear the statistics of a specified IPv4 prefix list. If no *ip-prefix-name* is specified, the statistics of all IPv4 prefix lists will be cleared.

### Examples

```
# Clear the statistics of IPv4 prefix list abc.
```

```
<Sysname> reset ip ip-prefix abc
```

## IPv6 Route Policy Configuration Commands

### apply ipv6 next-hop

#### Syntax

```
apply ipv6 next-hop ipv6-address
```

```
undo apply ipv6 next-hop
```

#### View

Route policy view

#### Default Level

2: System level

#### Parameters

*ipv6-address*: Next hop IPv6 address.

#### Description

Use the **apply ipv6 next-hop** command to set a next hop for IPv6 routes.

Use the **undo apply ipv6 next-hop** command to remove the clause configuration.

No next hop address is set for IPv6 routing information by default.

This command cannot set a next hop for redistributed routes.

## Examples

# Configure node 10 of route policy **policy1** to set next hop 3ff3:506::1 for IPv6 routing information matching AS-PATH list 1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply ipv6 next-hop 3ffe:506::1
```

## display ip ipv6-prefix

### Syntax

```
display ip ipv6-prefix [ ipv6-prefix-name ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ipv6-prefix-name*: IPv6 prefix list name, a string of 1 to 19 characters.

### Description

Use the **display ip ipv6-prefix** command to display the statistics of the specified IPv6 prefix list. If no IPv6 prefix list is specified, the statistics of all IPv6 prefix lists will be displayed.

## Examples

# Display the statistics of all IPv6 prefix lists.

```
<Sysname> display ip ipv6-prefix
Prefix-list6 abc
Permitted 0
Denied 0
      index:   10           permit  ::/0
      index:   20           permit  ::/1           ge 1   le 128
```

**Table 1-4** display ip ipv6-prefix command output description

Field	Description
Prefix-list6	Name of the IPv6 prefix list
Permitted	Number of routes satisfying the match criterion
Denied	Number of routes not satisfying the match criterion
Index	Index number of the prefix list
Permit	Matching mode of the item: permit, or deny
::/1	IPv6 address and prefix length for matching

Field	Description
ge	greater-equal, the lower prefix length
Le	less-equal, the upper prefix length

## if-match ipv6

### Syntax

```
if-match ipv6 { address | next-hop | route-source } { acl acl6-number | prefix-list ipv6-prefix-name }
undo if-match ipv6 { address | next-hop | route-source } [ acl / prefix-list ]
```

### View

Route policy view

### Default Level

2: System level

### Parameters

**address**: Matches the destination address of IPv6 routing information.

**next-hop**: Matches the next hop of IPv6 routing information.

**route-source**: Matches the source address of IPv6 routing information.

**acl** *acl6-number*: Specifies the number of an IPv6 ACL for filtering, in the range 2000 to 3999 for **address**, and 2000 to 2999 for **next-hop** and **route-source**.

**prefix-list** *ipv6-prefix-name*: Specifies the name of a IPv6 prefix list for filtering, a string of 1 to 19 characters.

### Description

Use the **if-match ipv6** command to configure a destination, next hop or source address based match criterion for IPv6 routes.

Use the **undo if-match ipv6** command to remove the match criterion.

The match criterion is not configured by default.

### Examples

```
# Configure node 10 of route policy policy1 to permit routing information whose next hop address matches IPv6 prefix list p1.
```

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match ipv6 next-hop prefix-list p1
```

## ip ipv6-prefix

### Syntax

```
ip ipv6-prefix ipv6-prefix-name [ index index-number ] { deny | permit } ipv6-address prefix-length
[ greater-equal min-prefix-length ] [ less-equal max-prefix-length ]
```

**undo ip ipv6-prefix** *ipv6-prefix-name* [ **index** *index-number* ]

## View

System view

## Default Level

2: System level

## Parameters

*ipv6-prefix-name*: IPv6 prefix list name, a string of 1 to 19 characters, for uniquely specifying an IPv6 prefix list.

*index-number*: Index number, in the range 1 to 65535, for uniquely specifying an IPv6 prefix list item. An item with a smaller *index-number* will be matched first.

**permit**: Specifies the matching mode for the IPv6 prefix list item as permit, that is, if a route matches the item, it passes the IPv6 prefix list without needing to match against the next item; if not, it will match against the next item (suppose the IPv6 prefix list has multiple items configured).

**deny**: Specifies the matching mode for the IPv6 prefix list item as deny, that is, if a route matches the item, the route neither passes the filter nor matches against the next item; if not, the route will match against the next item (suppose the IPv6 prefix list has multiple items configured).

*ipv6-address prefix-length*: Specifies an IPv6 prefix and prefix length. A *prefix-length* is in the range 0 to 128. When specified as :: 0, the arguments match the default route.

**greater-equal** *min-prefix-length*: Greater than or equal to the minimum prefix length.

**less-equal** *max-prefix-length*: Less than or equal to the maximum prefix length.

The length relation is  $mask-length \leq min-mask-length \leq max-mask-length \leq 128$ . If only the *min-prefix-length* is specified, the prefix length range is [ *min-prefix-length*, 128 ]. If only the *max-prefix-length* is specified, the prefix length range is [ *prefix-length*, *max-prefix-length* ]. If both the *min-prefix-length* and *max-prefix-length* are specified, the prefix length range is [ *min-prefix-length*, *max-prefix-length* ].

## Description

Use the **ip ipv6-prefix** command to configure an IPv6 prefix list or an item of it.

Use the **undo ip ipv6-prefix** command to remove an IPv6 prefix list or an item.

No IPv6 prefix list is configured by default.

An IPv6 prefix list may have multiple items, and each of them specifies a range of IPv6 prefixes. The relation between items is logic OR, namely, if a route passes an item of it, the route will pass the IPv6 prefix list.

The IPv6 prefix range is determined by *prefix-length* and [ *min-prefix-length*, *max-prefix-length* ]. If both *mask-length* and [ *min-mask-length*, *max-mask-length* ] are specified, then the IPv6 addresses must satisfy both of them.

If *ipv6-address prefix-length* is specified as :: 0, only the default route matches.

To match all routes, configure :: 0 **less-equal** 128.

## Examples

```
# Permit IPv6 addresses with a mask length between 32 bits and 64 bits.
```

```
<Sysname> system-view
```

```
[Sysname] ip ipv6-prefix abc permit :: 0 greater-equal 32 less-equal 64
```

# Deny IPv6 addresses with the prefix being 3FEE:D00::/32, and prefix length being greater than or equal to 32 bits.

```
<Sysname> system-view
```

```
[Sysname] ip ipv6-prefix abc deny 3FEE:D00:: 32 less-equal 128
```

## reset ip ipv6-prefix

### Syntax

```
reset ip ipv6-prefix [ ipv6-prefix-name ]
```

### View

User view

### Default Level

2: System level

### Parameters

*ipv6-prefix-name*: IPv6 prefix list name, a string of 1 to 19 characters.

### Description

Use the **reset ip ipv6-prefix** command to clear the statistics of the specified IPv6 prefix list. If no name is specified, the statistics of all IPv6 prefix lists will be cleared.

### Examples

```
# Clear the statistics of IPv6 prefix list abc.
```

```
<Sysname> reset ip ipv6-prefix abc
```

# Table of Contents

<b>1 BFD Configuration Commands</b> .....	<b>1-1</b>
BFD Configuration Commands .....	1-1
bfd authentication-mode .....	1-1
bfd detect-multiplier .....	1-2
bfd echo-source-ip .....	1-3
bfd min-echo-receive-interval .....	1-3
bfd min-receive-interval .....	1-4
bfd min-transmit-interval .....	1-5
bfd session init-mode .....	1-5
display bfd debugging-switches .....	1-6
display bfd interface .....	1-7
display bfd paf .....	1-8
display bfd session .....	1-9
isis bfd enable .....	1-11
ospf bfd enable .....	1-12
peer <i>ip-address</i> bfd .....	1-12
reset bfd session statistics .....	1-13
rip bfd enable .....	1-14
snmp-agent trap enable bfd .....	1-15

# 1 BFD Configuration Commands

---



## Note

Switch 4800G is centralized devices that support IRF. Multiple 4800G switches can form a distributed chassis switch in a logical sense, in which the master and slave switches are like the master and slave boards of a distributed switch. The centralized 4800G series switches are implemented in a distributed way after they form an IRF stack.

---

## BFD Configuration Commands

### bfd authentication-mode

#### Syntax

```
bfd authentication-mode { md5 key-id key | sha1 key-id key | simple key-id password }  
undo bfd authentication-mode
```

#### View

Interface view

#### Default Level

2: System level

#### Parameters

**md5**: Uses message digest 5 (MD5) authentications.

**sha1**: Uses secure hash algorithm (SHA-1) authentication.

**simple**: Uses plaint text authentication.

*key-id*: Authentication key ID, in the range 1 to 255.

*key*: A string of 1 to 16 characters. It is displayed as a 24-byte cipher text string when the **display current-configuration** command is executed.

*password*: Password, a string of 1 to 16 characters when the **simple** keyword is used. It is displayed when the **display current-configuration** command is executed.

#### Description

Use the **bfd authentication-mode** command to configure the BFD authentication mode and key on the interface.

Use the **undo bfd authentication-mode** command to remove the authentication mode on the interface (only one authentication mode can be configured on an interface).

By default, no authentication is configured on an interface.

---



The authentication mode, key-id, key (or password) used by both ends trying to establish a BFD session must be the same. If one end changes its authentication mode, it sends the authentication packets in both the new and the old mode at the same time until the other end also changes to the same authentication mode.

---

## Examples

# Configure VLAN-interface 1 to support MD5 authentication, setting the authentication key-id to 15 and authentication key to **BfdKey**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] bfd authentication-mode md5 15 BfdKey
```

## bfd detect-multiplier

### Syntax

```
bfd detect-multiplier value
undo bfd detect-multiplier
```

### View

Interface view

### Default Level

2: System level

### Parameters

*value*: Maximum number of consecutive BFD packets that the remote device fails to receive from the local device interface before considering the BFD session down, in the range of 3 to 50.

### Description

Use the **bfd detect-multiplier** command to configure the maximum number of consecutive BFD packets that the remote device fails to receive from the local device before considering the BFD session down.

Use the **undo bfd detect-multiplier** command to restore the default.

The default is 5.

## Examples

# Configure the detect multiplier as 6 on VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
```

```
[Sysname-Vlan-interface1] bfd detect-multiplier 6
```

## bfd echo-source-ip

### Syntax

```
bfd echo-source-ip ip-address  
undo bfd echo-source-ip
```

### View

System view

### Default Level

2: System level

### Parameters

*ip-address*: Source IP address of BFD echo packets.

### Description

Use the **bfd echo-source-ip** command to configure the source IP address of BFD echo packets.

Use the **undo bfd echo-source-ip** command to remove the configured source IP address of BFD echo packets.

Note that, since a large amount of ICMP redirect packets may be sent by the remote device, causing network congestion, do not configure the source IP address of the BFD echo packets to belong to the same network segment as any interface address of the device.

### Examples

```
# Configure the source IP address of BFD echo packets as 10.1.1.1.
```

```
<Sysname> system-view  
[Sysname] bfd echo-source-ip 10.1.1.1
```

## bfd min-echo-receive-interval

### Syntax

```
bfd min-echo-receive-interval value  
undo bfd min-echo-receive-interval
```

### View

Interface view

### Default Level

2: System level

### Parameters

*value*: Minimum BFD echo receiving interval, in milliseconds. in the range of 200 to 1000.

## Description

Use the **bfd min-echo-receive-interval** command to configure the minimum BFD echo packet receiving interval on the interface.

Use the **undo bfd min-echo-receive-interval** command to restore the default minimum BFD echo packet receiving interval on the interface.

## Examples

```
# Configure the minimum BFD echo receiving interval on VLAN-interface 1 as 300 milliseconds.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] bfd min-echo-receive-interval 300
```

## bfd min-receive-interval

### Syntax

```
bfd min-receive-interval value
undo bfd min-receive-interval
```

### View

Interface view

### Default Level

2: System level

### Parameters

*value*: Minimum interval for receiving BFD control packets, in milliseconds. in the range of 200 to 1000.

## Description

Use the **bfd min-receive-interval** command to configure the minimum interval for receiving BFD control packets.

Use the **undo bfd min-receive-interval** command to restore the default minimum interval for receiving BFD control packets.

Note that, if the remote device sends BFD control packets at an interval shorter than the minimum receiving interval of the local device, the remote device changes its sending interval to the minimum receiving interval of the local device.

## Examples

```
# Configure the minimum interval for receiving BFD control packets on VLAN-interface 1 as 300 milliseconds.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] bfd min-receive-interval 300
```

## bfd min-transmit-interval

### Syntax

```
bfd min-transmit-interval value  
undo bfd min-transmit-interval
```

### View

Interface view

### Default Level

2: System level

### Parameters

*value*: Minimum interval for transmitting BFD control packets, in milliseconds. in the range of 200 to 1000.

### Description

Use the **bfd min-transmit-interval** command to configure the minimum interval for transmitting BFD control packets.

Use the **undo bfd min-transmit-interval** command to restore the default minimum interval for transmitting BFD control packets.

Note that, the minimum interval for transmitting BFD control packets through an interface ensures BFD control packets are not transmitted faster than the device can deal with. The actual interval for transmitting BFD control packets at the local device should be the greater between the minimum interval for sending BFD control packets configured on the local interface and the minimum interval for receiving BFD control packets on the remote device.

### Examples

```
# Configure the minimum interval for transmitting BFD control packets on VLAN-interface 1 as 300 milliseconds.
```

```
<Sysname> system-view  
[Sysname] interface vlan-interface 1  
[Sysname-Vlan-interface1] bfd min-transmit-interval 300
```

## bfd session init-mode

### Syntax

```
bfd session init-mode { active / passive }  
undo bfd session init-mode
```

### View

System view

### Default Level

2: System level

## Parameters

**active:** Uses the active mode. In the active mode, upon being enabled with BFD, an interface actively transmits a BFD control packet to the remote device.

**passive:** Uses the passive mode. In the passive mode, an interface does not actively transmit a BFD control packet to the remote end; it transmits a BFD control packet only after receiving a BFD control packet from the remote end.

## Description

Use the **bfd session init-mode** command to configure the mode for establishing a BFD session.

Use the **undo bfd session init-mode** command to restore the default. By default, BFD sessions are established in the **active** mode.

## Examples

# Configure the session establishment mode as **passive**.

```
<Sysname> system-view  
[Sysname] bfd session init-mode passive
```

## display bfd debugging-switches

### Syntax

```
display bfd debugging-switches
```

### View

Any view

### Default Level

2: System level

### Parameters

None

### Description

Use the **display bfd debugging-switches** command to display enabled BFD debugging switches.

### Examples

# Display enabled BFD debugging switches.

```
<Sysname> display bfd debugging-switches  
BFD Error debugging is on  
BFD Event debugging is on  
BFD FSM debugging is on  
BFD Packet Receive debugging is on  
BFD Packet Send debugging is on  
BFD SCM debugging is on  
BFD Timer debugging is on
```

## display bfd interface

### Syntax

```
display bfd interface [ verbose ]
```

### View

Any view

### Default Level

2: System level

### Parameters

**verbose**: Displays detailed interface information.

### Description

Use the **display bfd interface** command to display information about BFD-enabled interfaces.

Besides the information displayed by the **display bfd interface** command, the **display bfd interface verbose** command displays brief session information of the interfaces.

### Examples

# Display information about BFD-enabled interfaces.

```
<Sysname> display bfd interface
```

```
Total Interface Num: 1
```

```
      Interface: Vlan-interface1          Session Num: 1
Min Trans Inter: 200ms                   Min Recv Inter: 200ms
      DetectMult: 3                       Min Echo Recv Inter: 400ms
      Auth mode: Simple
```

# Display detailed information about BFD-enabled interfaces.

```
<Sysname> display bfd interface verbose
```

```
Total Interface Num: 1
```

```
      Interface: Vlan-interface1          Session Num: 0
Min Trans Inter: 300ms                   Min Recv Inter: 300ms
      DetectMult: 5                       Min Echo Recv Inter: 400ms
      Auth mode: Simple
```

```
LD/RD      SourceAddr      DestAddr      ConnType      State      Mode
2/2        192.168.11.11      192.168.11.10  Direct      Up        Ctrl
```

**Table 1-1** display bfd interface command output description

Field	Description
Interface	Interface name
Session Num	Number of sessions established on the local interface

Field	Description
Min Trans Inter	Expected minimum transmit interval configured on the interface
Min Recv Inter	Expected minimum receive interval configured on the interface
DetectMult	Session detection multiplier
Auth mode	Session authentication mode: simple, MD5, or SHA-1
LD	Local ID of the session
RD	Remote ID of the session
SourceAddr	Source IP address of the session
DestAddr	Destination IP address of the session
ConnType	Connection type of the interface
State	Session state
Mode	Working mode of the session: control packet (Ctrl) mode or echo packet (Echo) mode.

## display bfd paf

### Syntax

**display bfd paf**

### View

Any view

### Default Level

2: System level

### Parameters

None

### Description

Use the **display bfd paf** command to display PAF configuration information.

### Examples

# Display BFD PAF configuration information.

```
<Sysname> display bfd paf
```

```

          BFD PAF Information:
Control Packet Min-Transmit-Interval(ms): 200
Control Packet Min-Receive-Interval(ms) : 200
Echo Packet Min-Receive-Interval(ms)    : 200
Max Session Number                       : 10

```

**Table 1-2 display bfd paf command output description**

Field	Description
Min-Transmit-Interval	Minimum transmit interval
Min-Receive-Interval	Minimum receive interval
Max Session Number	Supported maximum number of sessions

## display bfd session

### Syntax

- On a centralized device:

**display bfd session [ verbose ]**

- On a distributed device:

**display bfd session [ verbose ] [ slot *slot-number* [ all | verbose ] ]**

### View

Any view

### Default Level

2: System level

### Parameters

**verbose:** Displays detailed session information.

**slot *slot-number*:** Displays the session information of the specified board/slot. The *slot-number* argument specifies a member device by its ID in an IRF stack. The range of a slot number depends on the total number of member devices and the member ID configuration of the IRF stack.

**all:** Displays detailed information about all the BFD sessions on the board, including those not maintained by the board, on a distributed device.

### Description

Use the **display bfd session [ slot *slot-number* ]** command to display BFD session information. If no slot number is specified, all the BFD session information of the device will be displayed. On a distributed device, if a slot number is specified, the information about the BFD sessions maintained by the specified board will be displayed. This command displays the following interface-related information: session local ID, session remote ID, source address, destination address, session state, length of time before session detection timer expires, and the name of the interface of the session.

Besides the information displayed by the **display bfd session** command (except the length of time before session detection timer expires), the **display bfd session verbose** command displays:

On a centralized device: minimum transmit interval, minimum receive interval, actual transmit interval, actual session detection timer, packets sent and received by the session, time when the session was established, last time when the session was down, last time when the session was up, authentication mode, connection type, registered protocol and diagnostic information;

On a distributed device: minimum transmit interval, minimum receive interval, actual transmit interval, actual session detection timer, time when the session was established, last time when the session was

down, last time when the session was up, authentication mode, connection type, board maintaining the session, registered protocol, and diagnostic information.

Use the **display bfd session [ slot slot-number all ]** command to display the detailed information of the BFD sessions on the board (or the main control board) in the specified slot, including those sessions not maintained by the board.

## Examples

# Display detailed information about all the BFD sessions.

```
<Sysname> display bfd session
```

```
Total Session Num: 2          Init mode: Active
```

```
Session Working Under Ctrl Mode:
```

LD/RD	SourceAddr	DestAddr	State	Holdtime	Interface
1/1	192.168.11.11	192.168.11.10	Up	550ms	vlan1
2/2	192.168.12.11	192.168.12.10	Up	/	vlan2

# Display detailed information about the sessions maintained by the device.

```
<Sysname> display bfd session verbose
```

```
Total Session Num: 3          Init Mode: Active
```

```
Session Working Under Echo Mode:
```

```
Local Discr: 1
  Source IP: 19.82.3.2          Destination IP: 19.82.3.61
  Session State: Up            Interface: Vlan-interface999
  Min Recv Inter: 400ms        Act Trans Inter: 400ms
  Act Detect Inter: 2000ms      Establish Time: 00:02:27
  Last Down Time: 00:02:27      Last Up Time: 00:04:33
  Connect Type: Direct          Board Num: 8
  Protocol: Track
  Diag Info: No Diagnostic
```

```
Local Discr: 2
  Source IP: 19.82.3.2          Destination IP: 19.82.3.62
  Session State: Up            Interface: Vlan-interface999
  Min Recv Inter: 400ms        Act Trans Inter: 400ms
  Act Detect Inter: 2000ms      Establish Time: 00:02:27
  Last Down Time: 00:04:45      Last Up Time: 00:04:46
  Connect Type: Direct          Board Num: 8
  Protocol: Track
  Diag Info: No Diagnostic
```

```
Session Working Under Ctrl Mode:
```

```
Local Discr: 3                Remote Discr: 3
```

```

Source IP: 19.82.3.2      Destination IP: 19.82.3.3
Session State: Up        Interface: Vlan-interface999
Min Trans Inter: 400ms   Act Trans Inter: 400ms
Min Recv Inter: 400ms   Act Detect Inter: 2000ms
Establish Time: 04:09:28 Last Down Time: 04:09:28
Last Up Time: 04:09:28  Auth mode: None
Connect Type: Direct     Board Num: 8
Protocol: OSPF
Diag Info: No Diagnostic

```

**Table 1-3 display bfd session command output description**

Field	Description
Local Discr	Local ID of the session
Remote Discr	Remote ID of the session
Source IP	Source IP address of the session
Destination IP	Destination IP address of the session
Session State	Session state
Holdtime	Length of time before session detection timer expires
Interface	Name of the interface of the session
Min Recv Inter	Expected minimum receive interval configured on the interface
Act Trans Inter	Actual transmit interval
Act Detect Inter	Actual session detection timer
Connect Type	Connection type of the interface
Board Num	Board maintaining the session
Protocol	Registered protocol
Diag Info	Diagnostic information about the session

## **isis bfd enable**

### **Syntax**

**isis bfd enable**

**undo isis bfd enable**

### **View**

Interface view

### **Default Level**

2: System level

### **Parameters**

None

## Description

Use the **isis bfd enable** command to enable BFD on an IS-IS interface for link failure detection.

Use the **undo isis bfd enable** command to disable BFD on an IS-IS interface.

By default, an IS-IS interface is not enabled with BFD.

## Examples

# Enable IS-IS and BFD on VLAN-interface 11 of the switch.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] isis enable
[Sysname-Vlan-interface11] isis bfd enable
```

## ospf bfd enable

### Syntax

**ospf bfd enable**

**undo ospf bfd enable**

### View

Interface view

### Default Level

2: System level

### Parameters

None

## Description

Use the **ospf bfd enable** command to enable BFD for link failure detection on an OSPF interface.

Use the **undo ospf bfd enable** command to disable BFD on an OSPF interface.

By default, an OSPF interface is not enabled with BFD.

## Examples

# Enable OSPF and BFD on VLAN-interface 11 of the router.

```
<Sysname> system-view
[Sysname] ospf
[Sysname-ospf-1] area 0
[Sysname-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.255.255
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] ospf bfd enable
```

## peer ip-address bfd

### Syntax

**peer ip-address bfd**

**undo peer *ip-address* bfd**

## View

BGP view, BGP-VPN instance view

## Default Level

2: System level

## Parameters

*ip-address*: IP address of a peer.

## Description

Use the **peer bfd** command to enable BFD on the interface to a BGP peer.

Use the **undo peer bfd** command to disable BFD on the interface to a BGP peer.

By default, a BGP interface is not enabled with BFD for link failure detection.

Note that if GR capability is enabled for BGP, use BFD with caution.

## Examples

# Enable BFD on the interface to a BGP peer.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 1.1.1.1 bfd
```

## reset bfd session statistics

### Syntax

- On a centralized device:  
**reset bfd session statistics**
- On a distributed device:  
**reset bfd session statistics [slot *slot-number* ]**

### View

User view

### Default Level

2: System level

### Parameters

**slot *slot-number***: Clears session statistics about the board in the specified slot. The *slot-number* argument specifies a member device by its ID in an IRF stack. The range of a slot number depends on the total number of member devices and the member ID configuration of the IRF stack.

### Description

Use the **reset bfd session statistics** command to clear the BFD session statistics of the current protocol. On a distributed device, if a slot number is specified, statistics about the BFD sessions maintained by the specified board will be cleared.

## Examples

- On a distributed device

# Clear statistics about the BFD sessions on the board in Slot 2.

```
<Sysname> reset bfd session statistics slot 2
```

- On a centralized device

# Clear statistics about all the BFD sessions of the current protocol.

```
<Sysname> reset bfd session statistics
```

## rip bfd enable

### Syntax

```
rip bfd enable
```

```
undo rip bfd enable
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **rip bfd enable** command to enable BFD on the RIP interface.

Use the **undo rip bfd enable** command to restore the default.

Disabling BFD on a RIP interface will notify BFD to delete the corresponding session.

By default, a RIP interface is not enabled with BFD.



#### Note

- BFD echo-mode detection only works for a RIP neighbor one hop away.
  - Using the **undo peer** command does not delete the neighbor relationship at once and therefore cannot bring down the BFD session at once.
  - For RIP configuration, refer to *RIP Configuration* in the *IP Routing Volume*
- 

## Examples

# Enable BFD on RIP interface VLAN-interface 11.

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 11
```

```
[Sysname-Vlan-interface11] rip bfd enable
```

## snmp-agent trap enable bfd

### Syntax

```
snmp-agent trap enable bfd
undo snmp-agent trap enable bfd
```

### View

System view

### Default Level

3: Manage level

### Parameters

None

### Description

Use the **snmp-agent trap enable bfd** command to enable sending BFD traps.

Use the **undo snmp-agent trap enable bfd** command to disable sending BFD traps.

By default, sending BFD traps is enabled.

### Examples

```
# Disable sending BFD traps.
```

```
<Sysname> system-view
```

```
[Sysname] undo snmp-agent trap enable bfd
```

# Table of Contents

<b>1 MCE Configuration Commands</b> .....	<b>1-1</b>
MCE Configuration Commands .....	1-1
description .....	1-1
display bgp vpnv4 vpn-instance group .....	1-1
display bgp vpnv4 vpn-instance network .....	1-3
display bgp vpnv4 vpn-instance paths .....	1-4
display bgp vpnv4 vpn-instance peer .....	1-5
display bgp vpnv4 vpn-instance routing-table .....	1-7
display ip routing-table vpn-instance .....	1-10
display ip vpn-instance .....	1-11
domain-id .....	1-12
export route-policy .....	1-13
ext-community-type .....	1-13
filter-policy export .....	1-14
filter-policy import .....	1-15
import route-policy .....	1-16
ip binding vpn-instance .....	1-16
ip vpn-instance .....	1-17
ipv4-family vpn-instance .....	1-18
peer allow-as-loop .....	1-18
peer group .....	1-19
refresh bgp vpn-instance .....	1-20
reset bgp vpn-instance .....	1-20
reset bgp vpn-instance dampening .....	1-21
reset bgp vpn-instance flap-info .....	1-22
route-distinguisher .....	1-22
routing-table limit .....	1-23
vpn-instance-capability simple .....	1-24
vpn-target .....	1-24

# 1 MCE Configuration Commands

---



## Note

This chapter only describes the commands related to the multi-CE (MCE) feature. For information about the routing protocol configuration commands in the configuration examples, refer to the *IPv4 Routing* module of this manual.

---

## MCE Configuration Commands

### description

#### Syntax

```
description text  
undo description
```

#### View

VPN instance view

#### Default Level

2: System level

#### Parameters

*text*: Description for the VPN instance, a string of 1 to 80 characters.

#### Description

Use the **description** command to configure a description for the current VPN instance.

Use the **undo description** command to delete the description.

#### Examples

```
# Configure the description of VPN instance vpn1.  
<Sysname> system-view  
[Sysname] ip vpn-instance vpn1  
[Sysname-vpn-instance-vpn1] description vpn1
```

### display bgp vpnv4 vpn-instance group

#### Syntax

```
display bgp vpnv4 vpn-instance vpn-instance-name group [ group-name ]
```

## View

Any view

## Default Level

1: Monitor level

## Parameters

*vpn-instance-name*: Name of the VPN instance, a string of 1 to 31 characters.

*group-name*: Name of the BGP peer group, a string of 1 to 47 characters.

## Description

Use the **display bgp vpnv4 group** command display information about a specified or all BGP VPNv4 peer group.

## Examples

# Display information about BGP VPNv4 peer group a for VPN instance vpn1.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 group a
```

```
BGP peer-group is a
remote AS number not specified
Type : external
Maximum allowed prefix number: 4294967295
Threshold: 75%
Configured hold timer value: 180
Keepalive timer value: 60
Minimum time between advertisement runs is 30 seconds
Peer Preferred Value: 0
No routing policy is configured
Members:
Peer      V   AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down  State
-----
10.1.1.1  4   200    18       21       0       1       00:12:58  Established
```

**Table 1-1** Description on the fields of the **display bgp vpnv4 group** command

Field	Description
BGP peer-group	Name of the BGP peer group
remote AS number	Number of the remote AS
Type	Peer group type
Maximum allowed prefix number	Maximum number of routes that the VPN instance supports
Threshold	Threshold value
Configured hold timer value	Setting of the hold timer
Keepalive timer value	Keepalive interval
Minimum time between advertisement runs	Minimum route advertisement interval

Field	Description
Peer Preferred Value	Weight for the routes from the peer
No routing policy is configured	Whether the VPN instance is configured with a routing policy
Peer	IP address of the peer
V	Version of BGP that the peer runs
AS	AS number of the peer group
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages waiting to be sent to the peer
PrefRcv	Number of prefixes received
Up/Down	Duration of the BGP session in the current state
State	Status of the peer

## display bgp vpnv4 vpn-instance network

### Syntax

**display bgp vpnv4 vpn-instance *vpn-instance-name* network**

### View

Any view

### Default Level

1: Monitor level

### Parameters

*vpn-instance-name*: Name of a VPN instance, a string of 1 to 31 characters.

### Description

Use the **display bgp vpnv4 network** command to display information about BGP VPNv4 routes injected into a specified or all VPN instances.

### Examples

# Display information about BGP VPNv4 routes injected into VPN instance vpn1.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 network
  BGP Local Router ID is 104.1.1.1.
  Local AS Number is 400.
  Route Distinguisher: 100:1 (1)
  Network           Mask           Route-policy     Short-cut
  104.1.101.1       255.255.255.255
```

**Table 1-2** Description on the fields of the **display bgp vpnv4 network** command

Field	Description
BGP Local Router ID	Router ID of the local BGP router
Local AS Number	Local AS number
Network	Advertised network route
Mask	Mask of the advertised network route
Route-policy	Routing policy configured
Short-cut	Indicates whether the route is a short-cut route

## display bgp vpnv4 vpn-instance paths

### Syntax

```
display bgp vpnv4 vpn-instance vpn-instance-name paths [as-regular-expression ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*vpn-instance-name*: Name of the VPN instance, a string of 1 to 31 characters.

*as-regular-expression*: Regular expression for filtering the AS path information to be displayed.

### Description

Use the **display bgp vpnv4 paths** command to display the BGP VPNv4 AS path information.

### Examples

# Display the BGP VPNv4 AS path information of VPN instance vpn1.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 paths
```

Address	Hash	Refcount	MED	Path/Origin
0x6E72D18	0	1	0	200?
0x6E72E50	0	1	0	i
0x6E72B78	1	1	0	?
0x6E72BE0	1	2	0	?

**Table 1-3** Description on the fields of the **display bgp vpnv4 paths** command

Field	Description
Address	Routing address in the local database
Hash	Hash bucket for storing routes
Refcount	Number of times that the path is referenced

Field	Description
MED	Metric for routes
Path/Origin	AS_PATH attribute/Route origin code

## display bgp vpnv4 vpn-instance peer

### Syntax

```
display bgp vpnv4 vpn-instance vpn-instance-name peer [ group-name log-info | ip-address
{ log-info | verbose } | verbose ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*vpn-instance-name*: Name of the VPN instance, a string of 1 to 31 characters.

*group-name*: Name of a peer group, a string of 1 to 47 characters.

**log-info**: Displays the log information about the peer group.

*ip-address*: IP address of the peer.

**verbose**: Displays detailed information.

### Description

Use the **display bgp vpnv4 peer** command to display information about BGP VPNv4 peers.

### Examples

# Display information about BGP VPNv4 peers of VPN instance vpn1.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 peer
```

```
BGP local router ID : 2.2.2.2
Local AS number : 100
Total number of peers : 1                Peers in established state : 1
Peer      V   AS  MsgRcvd  MsgSent  OutQ   PrefRcv  Up/Down      State
10.1.1.1  4   200      24       29      0         1  00:18:47  Established
```

**Table 1-4** Description on the fields of display bgp vpnv4 vpn-instance peer

Field	Description
BGP Local router ID	Router ID of the local BGP router
local AS number	Local AS number
Total number of peers	Total number of peers
Peers in established state	Number of peers in the state of established

Field	Description
Peer	IP address of the peer
V	Version of BGP that the peer runs
AS	AS number of the peer group
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages waiting to be sent to the peer
PrefRcv	Number of received prefixes
Up/Down	Duration of the BGP session in the current state
State	Status of the peer

# Display detailed information about BGP VPNv4 peers of VPN instance vpn1.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 peer verbose
```

```
Peer: 10.1.1.1 Local: 2.2.2.2
Type: EBGP link
BGP version 4, remote router ID 10.1.1.1
BGP current state: Established, Up for 00h19m26s
BGP current event: KATimerExpired
BGP last state: OpenConfirm
Port: Local - 179 Remote - 1025
Configured: Active Hold Time: 180 sec Keepalive Time:60 sec
Received : Active Hold Time: 180 sec
Negotiated: Active Hold Time: 180 sec Keepalive Time:60 sec
Peer optional capabilities:
Peer support bgp multi-protocol extended
Peer support bgp route refresh capability
Address family IPv4 Unicast: advertised and received
```

```
Received: Total 25 messages, Update messages 1
Sent: Total 30 messages, Update messages 4
Maximum allowed prefix number: 4294967295
Threshold: 75%
Minimum time between advertisement runs is 30 seconds
Optional capabilities:
Route refresh capability has been enabled
Peer Preferred Value: 0
```

```
Routing policy configured:
No routing policy is configured
```

**Table 1-5** Description on the fields of the **display bgp vpnv4 peer verbose** command

Field	Description
Peer	IP address of the peer
Local	IP address of the local router
Type	BGP type
BGP version	Version of BGP that the peer runs
remote router ID	Router ID of the remote router
BGP current state	Current status of the BGP session
Up for	Duration since the peer is established
BGP current event	Current event of the BGP session
BGP last state	State that the BGP session was in before transitioning to the current status
Port	Local and remote ports of the BGP session
Configured	Settings of the local timers, including the active hold interval and keepalive interval
Received	Received active hold interval
Negotiated	Negotiated active hold interval and keepalive time
Peer optional capabilities	Optional capabilities of the peer
Peer support bgp multi-protocol extended	The peer supports multiprotocol extension.
Peer support bgp route refresh capability	The peer supports route refresh capability.
Address family IPv4 Unicast	IPv4 unicast family capability
Received	Total number of received messages and the number of received update messages
Sent	Total number of sent messages and the number of sent update messages
Maximum allowed prefix number	Maximum number of routes that the VPN instance supports
Threshold	Threshold value
Minimum time between advertisement runs	Minimum route advertisement interval
Optional capabilities	Local optional capabilities
Route refresh capability has been enabled	Whether the route refresh capability is supported
Peer Preferred Value	Weight for the routes from the peer
Routing policy configured	Routing policy configured

## display bgp vpnv4 vpn-instance routing-table

### Syntax

```
display bgp vpnv4 vpn-instance vpn-instance-name routing-table [ network-address [ { mask-length | mask-address } ] [ longer-prefixes ] ] | as-path-acl as-path-acl-number | cidr | community
```

```
[ aa:nn ]&<1-13>[ no-export-subconfed | no-advertise | no-export ]* [ whole-match ] |
community-list { basic-community-list-number [ whole-match ] |
adv-community-list-number }&<1-16> | dampened | dampening parameter | different-origin-as |
flap-info [ as-path-acl as-path-acl-number | network-address [ mask [ longer-match ] | mask-length
[ longer-match ] ] | regular-expression as-regular-expression ] | peer ip-address { advertised-routes
| received-routes } | regular-expression as-regular-expression | statistic ]
```

## View

Any view

## Default Level

1: Monitor level

## Parameters

*vpn-instance-name*: Name of the VPN instance, a string of 1 to 31 characters.

*network-address*: IP address of the destination segment.

*mask-length*: Length of the network mask, in the range 0 to 32.

*mask-address*: Network mask, in the format of X.X.X.X.

**longer-prefixes**: Specifies to match the longest prefix.

**as-path-acl** *as-path-acl-number*: Filters routing information using the specified AS\_PATH list. The *as-path-acl-number* argument ranges from 1 to 256.

**cidr**: Displays classless interdomain routing (CIDR) information.

**community**: Displays routing information of the specified BGP community in the routing table.

*aa:nn*&<1-13>: Community number. Both the *aa* and *nn* parameters range from 0 to 65535. &<1-13> means that you can enter the parameter combination up to 13 times.

**no-export-subconfed**: A route with this attribute is neither advertised out of the local AS, nor advertised to the other sub-ASs in the confederation.

**no-advertise**: A route with this attribute is not advertised to any other BGP peer.

**no-export**: A route with this attribute is not advertised out of the local AS or, if existing, confederation. However, it is advertised to the other sub-ASs in the confederation.

**whole-match**: Performs exact match.

**community-list**: Displays routing information of the specified BGP community list.

*basic-community-list-number*: Basic community list number, in the range 1 to 99.

*adv-community-list-number*: Advanced community list number, in the range 100 to 199.

&<1-16>: Specifies that the argument before it can be entered up to 16 times.

**dampened**: Displays information about dampened BGP VPNv4 routes.

**dampening parameter**: Configured BGP VPNv4 route dampening parameters.

**different-origin-as**: Displays information about routes with different AS origins.

**flap-info**: Displays BGP VPNv4 route flap statistics.

**longer-match**: Displays flap statistics for routes with greater mask lengths than that specified by the *network-address* { *mask* | *mask-length* } combination.

**peer** *ip-address*: Specifies a peer by its IP address.

**advertised-routes:** Displays routing information sent to the specified peer.

**received-routes:** Displays routing information received from the specified peer.

**regular-expression** *as-regular-expression:* Displays routing information matching the specified AS regular expression.

**statistic:** Displays BGP VPNv4 route statistics.

## Description

Use the **display bgp vpnv4 vpn-instance routing-table** command to display the BGP VPNv4 routing information of a specified VPN instance.

## Examples

# Display the BGP VPNv4 routing information of VPN instance vpn1.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 routing-table
Total Number of Routes: 5

BGP Local router ID is 2.2.2.2
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete
Network      NextHop      MED      LocPrf    PrefVal  Path/Ogn
* > i 10.0.0.0  1.1.1.1     0        100       0        i
* > 10.1.1.0/24 0.0.0.0     0         0         0        ?
* > 20.0.0.0    10.1.1.1    0         0         99       200?
* > i 123.1.1.1/32 1.1.1.1     0        100       0        ?
* > 124.1.1.1/32 0.0.0.0     0         0         0        ?
```

**Table 1-6** Description on the fields of display bgp vpnv4 vpn-instance routing-table

Field	Description
Total Number of Routes	Total number of routes
BGP Local router ID	Router ID of the local BGP router
Status codes	Route status code. For valid values.
Origin	Route origin code. For valid values.
Network	Network address in the BGP routing table
NextHop	Address of the next hop
MED	Metric associated with the destination network
LocPrf	Local preference
PrefVal	Preferred value of the protocol
Path/Ogn	AS_PATH attribute/Route origin code.

## display ip routing-table vpn-instance

### Syntax

```
display ip routing-table vpn-instance vpn-instance-name [ verbose ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*vpn-instance-name*: Name of the VPN instance, a string of 1 to 31 characters.

**verbose**: Displays detailed information.

### Description

Use the **display ip routing-table vpn-instance** command to display the routing information of a VPN instance.

### Examples

```
# Display the routing information of VPN instance vpn2.
```

```
<Sysname> display ip routing-table vpn-instance vpn2
```

```
Routing Tables: vpn2
```

```
Destinations : 5          Routes : 5
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
10.214.20.0/24	Direct	0	0	10.214.20.3	Vlan20
10.214.20.3/32	Direct	0	0	127.0.0.1	InLoop0
192.168.10.0/24	RIP	100	1	10.214.20.2	Vlan20

**Table 1-7** Description on the fields of display ip routing-table vpn-instance

Field	Description
Destinations	Number of destination addresses
Routes	Number of routes
Destination/Mask	Destination address/mask length
Proto	Protocol discovering the route
Pre	Preference of the route
Cost	Cost of the route
NextHop	Address of the next hop along the route
Interface	Outbound interface for forwarding packets to the destination segment

## display ip vpn-instance

### Syntax

```
display ip vpn-instance [ instance-name vpn-instance-name ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*vpn-instance-name*: Name of the VPN instance, a string of 1 to 31 characters.

### Description

Use the **display ip vpn-instance** command to display information about a VPN instance or all VPN instances.

If you do not specify any parameter, the command displays brief information about all VPN instances.

### Examples

# Display information about all VPN instances.

```
<Sysname> display ip vpn-instance
Total VPN-Instances configured : 2

VPN-Instance Name      RD          Create Time
vpn1                    22:1       2003/10/13 09:32:45
vpn2                    33:3       2003/10/13 09:42:59
```

**Table 1-8** Description on the fields of the **display ip vpn-instance** command

Field	Description
VPN-Instance Name	Name of the VPN instance
RD	RD of the VPN instance
Create Time	Time when the VPN instance was created

# Display detailed information about a specified VPN instance.

```
<Sysname> display ip vpn-instance instance-name vpn1
VPN-Instance Name and ID : vpn1, 1
Create time : 2008/08/27 16:34:08
Up time : 0 days, 00 hours, 24 minutes and 37 seconds
Route Distinguisher : 10:1
Export VPN Targets : 10:1
Import VPN Targets : 10:1
Description : this is vpn1
Maximum Routes Limit : 1000
Threshold Value(%): 100
```

Interfaces : Vlan-interface2, LoopBack0

**Table 1-9** Description on the fields of display ip vpn-instance instance-name

Field	Description
VPN-Instance Name and ID	Name and ID of the VPN instance
CreateTime	Time when the VPN instance was created
Up time	Duration of the VPN instance
Route Distinguisher	RD of the VPN instance
Export VPN Targets	Export target attribute of the VPN instance
Import VPN Targets	Import target attribute of the VPN instance
Import Route Policy	Import routing policy of the VPN instance
Description	Description of the VPN instance
Maximum number of Routes	Maximum number of routes of the VPN instance
Threshold Value(%)	Threshold (in percentage) for the maximum number of routes supported by the VPN instance. If this value is reached, the VPN instance rejects new routes.
Interfaces	Interface to which the VPN instance is bound

## domain-id

### Syntax

```
domain-id domain-id [ secondary ]  
undo domain-id [ domain-id ]
```

### View

OSPF view

### Default Level

2: System level

### Parameters

*domain-id*: OSPF domain ID, in integer or dotted decimal notation. If it is in integer, it ranges from 0 to 4,294,967,295.

**secondary**: Uses the domain ID as secondary. With this keyword not specified, the domain ID configured is primary.

### Description

Use the **domain-id** command to configure an OSPF domain ID.

Use the **undo domain-id** command to restore the default.

By default, the OSPF domain ID is 0.

With no parameter specified, the **undo domain-id** command deletes the primary domain ID.

Usually, routes injected from PEs are advertised as External-LSAs. However, routes to different destinations in the same OSPF domain must be advertised as Type-3 LSAs. Therefore, using the same domain ID is required for an OSPF domain.

## Examples

```
# Configure the OSPF domain ID.
<Sysname> system-view
[Sysname] ospf 100 vpn-instance vpn1
[Sysname-ospf-100] domain-id 234
```

## export route-policy

### Syntax

```
export route-policy route-policy
undo export route-policy
```

### View

VPN instance view

### Default Level

2: System level

### Parameters

*route-policy*: Name of the export routing policy for the VPN instance, a string of 1 to 19 characters.

### Description

Use the **export route-policy** command to apply an export routing policy to a VPN instance.

Use the **undo export route-policy** command to remove the application.

You can configure an export routing policy when a finer control on the VPN instance routes to be redistributed is required, that is, when the control provided by the extended community attribute is not enough. An export routing policy may deny routes that are permitted by the export target attribute.

By default, all VPN instance routes permitted by the export target attribute can be redistributed.

## Examples

```
# Apply export routing policy poly-1 to VPN instance vpn1.
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] export route-policy poly-1
```

## ext-community-type

### Syntax

```
ext-community-type { domain-id type-code1 | router-id type-code2 | route-type type-code3 }
undo ext-community-type { domain-id | router-id | route-type }
```

## View

OSPF view

## Default Level

2: System level

## Parameters

**domain-id** *type-code1*: Specifies the type code for the OSPF extended community attribute of Domain ID. Valid values are 0x0005, 0x0105, 0x0205, and 0x8005.

**router-id** *type-code2*: Specifies the type code for the OSPF extended community attribute of Router ID. Valid values are 0x0107 and 0x8001.

**route-type** *type-code3*: Specifies the type code for the OSPF extended community attribute of Route Type. Valid values are 0x0306 and 0x8000.

## Description

Use the **ext-community-type** command to configure the type code of an OSPF extended community attribute.

Use the **undo ext-community-type** command to restore the default.

By default, the type codes for the OSPF extended community attributes of Domain ID, Router ID, and Route Type are 0x0005, 0x0107, and 0x0306 respectively.

## Examples

# Configure the type codes of OSPF extended community attributes Domain ID, Router ID, and Route Type as 0x8005, 0x8001, and 0x8000 respectively for OSPF process 100.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] ext-communityroute-type domain-id 8005
[Sysname-ospf-100] ext-communityroute-type router-id 8001
[Sysname-ospf-100] ext-communityroute-type route-type 8000
```

## filter-policy export

### Syntax

```
filter-policy { acl-number | ip-prefix ip-prefix-name } export [ direct | isis process-id | ospf process-id | rip process-id | static ]
undo filter-policy export [ direct | isis process-id | ospf process-id | rip process-id | static ]
```

### View

BGP-VPN instance view

### Default Level

2: System level

### Parameters

*acl-number*: IP ACL number, in the range 2000 to 3999.

*ip-prefix-name*: IP address prefix list name, a string of 1 to 19 characters.

**direct**: Filters direct routes to be advertised.

**isis** *process-id*: Filters ISIS routes to be advertised that are from a specified ISIS process. The *process-id* argument is in the range 1 to 4294967295.

**ospf** *process-id*: Filters OSPF routes to be advertised that are from a specified OSPF process. The *process-id* argument is in the range 1 to 4294967295.

**rip** *process-id*: Filters RIP routes to be advertised that are from a specified RIP process. The *process-id* argument is in the range 1 to 4294967295.

**static**: Filters static routes to be advertised.

## Description

Use the **filter-policy export** command to configure BGP to filter all or certain types of routes to be advertised.

Use the **undo filter-policy export** command to remove the configuration.

If you specify no routing protocol parameters for the **filter-policy export** command, all routes to be advertised will be filtered.

By default, BGP does not filter routes to be advertised.

Only routes that survive the filtering are advertised by BGP.

## Examples

```
# Configure BGP to filter the routes to be advertised by using ACL 2555.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] filter-policy 2555 export
```

## filter-policy import

### Syntax

```
filter-policy { acl-number | ip-prefix ip-prefix-name } import
```

```
undo filter-policy import
```

### View

BGP-VPN instance view

### Default Level

2: System level

### Parameters

*acl-number*: IP ACL number, in the range 2000 to 3999.

*ip-prefix-name*: IP address prefix list name, a string of 1 to 19 characters.

## Description

Use the **filter-policy import** command to configure BGP to filter received routes.

Use the **undo filter-policy import** command to remove the configuration.

By default, BGP does not filter received routes.

Only routes that survive the filtering are added into the BGP routing table.

## Examples

# Configure BGP to filter received routes using ACL 2255.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] filter-policy 2255 import
```

## import route-policy

### Syntax

**import route-policy** *route-policy*

**undo import route-policy**

### View

VPN instance view

### Default Level

2: System level

### Parameters

*route-policy*: Name of the import routing policy for the VPN instance, a string of 1 to 19 characters.

### Description

Use the **import route-policy** command to apply an import routing policy to a VPN instance.

Use the **undo import route-policy** command to remove the application.

You can configure an import routing policy when a finer control on the routes to be redistributed into a VPN instance is required, that is, when the control provided by the extended community attributes is not enough. An import routing policy may deny routes that are permitted by the import target attributes.

By default, all routes permitted by the import target attribute can be redistributed into the VPN instance.

## Examples

# Apply import routing policy poly-1 to VPN instance vpn1.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] import route-policy poly-1
```

## ip binding vpn-instance

### Syntax

**ip binding vpn-instance** *vpn-instance-name*

**undo ip binding vpn-instance** *vpn-instance-name*

## View

Interface view

## Default Level

2: System level

## Parameters

*vpn-instance-name*: Name of the VPN instance to be associated, a case-insensitive string of 1 to 31 characters.

## Description

Use the **ip binding vpn-instance** command to associate an interface with a VPN instance.

Use the **undo ip binding vpn-instance** command to remove the association.

By default, an interface is associated with no VPN instance; it belongs to the public network.

When configured on an interface, the **ip binding vpn-instance** command clears the IP address of the interface. Therefore, you must re-configure the IP address of the interface after configuring the command.

## Examples

# Associate Vlan-interface 1 with the VPN instance named "vpn1".

```
<Sysname> system-view
[Sysname] interface Vlan-interface1
[Sysname-Vlan-interface1] ip binding vpn-instance vpn1
```

## ip vpn-instance

### Syntax

```
ip vpn-instance vpn-instance-name
undo ip vpn-instance vpn-instance-name
```

### View

System view

### Default Level

2: System level

### Parameters

*vpn-instance-name*: Name of the VPN instance, a case-insensitive string of 1 to 31 characters.

### Description

Use the **ip vpn-instance** command to create a VPN instance and enter VPN instance view.

Use the **undo ip vpn-instance** command to delete a VPN instance.

A VPN instance takes effect only after you configure an RD for it.

Related command: **route-distinguisher**.

## Examples

```
# Create a VPN instance named vpn1.
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1]
```

## ipv4-family vpn-instance

### Syntax

```
ipv4-family vpn-instance vpn-instance-name
undo ipv4-family vpn-instance vpn-instance-name
```

### View

BGP view

### Default Level

2: System level

### Parameters

**vpn-instance** *vpn-instance-name*: Associates a VPN instance with an IPv4 address family and enters BGP VPN instance view. The *vpn-instance-name* argument is a string of 1 to 31 characters.

### Description

Use the **ipv4-family** command to enter BGP-VPN instance view.

Use the **undo ipv4-family** command to remove all the configurations performed in either of the two views.

Before entering BGP VPN instance view, make sure the corresponding VPN instance is created.

## Examples

```
# Enter BGP-VPN instance view.
<Sysname> system-view
[Sysname] bgp 100
[Sysname] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1]
```

## peer allow-as-loop

### Syntax

```
peer { group-name | ip-address } allow-as-loop [ number ]
undo peer { group-name | ip-address } allow-as-loop
```

### View

BGP-VPN instance view

### Default Level

2: System level

## Parameters

*group-name*: Name of the peer group, a string of 1 to 47 characters.

*ip-address*: IP address of the peer.

*number*: Maximum number that the local AS number can appear repeatedly in the AS-PATH attribute. It ranges from 1 to 10 and defaults to 1.

## Description

Use the **peer allow-as-loop** command to allow the local AS number to appear in the AS-PATH attribute of a received route and to set the allowed maximum number of repetitions.

Use the **undo peer allow-as-loop** command to remove the configuration.

## Examples

# Allow the local AS number to appear repeatedly in the AS-PATH attribute of a route received from peer 1.1.1.1 for up to twice.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 1.1.1.1 allow-as-loop 2
```

## peer group

### Syntax

**peer** *ip-address* **group** *group-name* [ **as-number** *as-number* ]

**undo peer** *ip-address* **group** *group-name*

### View

BGP-VPN instance view

### Default Level

2: System level

## Parameters

*ip-address*: IP address of a peer.

*group-name*: Name of a peer group, a string of 1 to 47 characters.

**as-number** *as-number*: Specifies an AS number, which ranges from 1 to 4294967295.

## Description

Use the **peer group** command to add a peer to a peer group.

Use the **undo peer group** command to remove a peer from a peer group.

## Examples

# Add the peer with the IP address 1.1.1.1 to the peer group named "test".

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
```

```
[Sysname-bgp-vpn1] peer 1.1.1.1 group test
```

## refresh bgp vpn-instance

### Syntax

```
refresh bgp vpn-instance vpn-instance-name { ip-address | all | external | group group-name }  
{ export | import }
```

### View

User view

### Default Level

1: Monitor level

### Parameters

*vpn-instance-name*: Name of a VPN instance, a string of 1 to 31 characters.

*ip-address*: IP address of a peer.

**all**: Performs a soft reset of all BGP VPN instance connections.

**external**: Performs a soft reset of EBGp sessions.

**group** *group-name*: Performs a soft reset of the connections with the specified BGP peer group. The *group-name* argument is a string of 1 to 47 characters.

**export**: Performs a soft reset in the outbound direction.

**import**: Performs a soft reset in the inbound direction.

### Description

Use the **refresh bgp vpn-instance** command to perform a soft reset of BGP connections in a VPN instance.

### Examples

```
# Perform a soft reset of all BGP connections in VPN instance vpn1 in the inbound direction to make  
new configurations take effect.
```

```
<Sysname> refresh bgp vpn-instance vpn1 all import
```

## reset bgp vpn-instance

### Syntax

```
reset bgp vpn-instance vpn-instance-name { as-number | ip-address | all | external | group  
group-name }
```

### View

User view

### Default Level

1: Monitor level

## Parameters

*vpn-instance-name*: Name of a VPN instance, a string of 1 to 31 characters.

*as-number*: AS number, in the range 1 to 4294967295.

*ip-address*: IP address of a peer.

**group** *group-name*: Resets the connections with the specified BGP peer group. The *group-name* argument is a string of 1 to 47 characters.

**all**: Resets all BGP connections.

**external**: Resets EBGP sessions.

## Description

Use the **reset bgp vpn-instance** command to reset the BGP connections of a specified VPN instance.

## Examples

```
# Reset all BGP connections of VPN instance vpn1.
```

```
<Sysname> reset bgp vpn-instance vpn1 all
```

## reset bgp vpn-instance dampening

### Syntax

```
reset bgp vpn-instance vpn-instance-name dampening [ network-address [ mask | mask-length ] ]
```

### View

User view

### Default Level

1: Monitor level

## Parameters

*vpn-instance-name*: Name of the VPN instance, a string of 1 to 31 characters.

**dampening**: Specifies route flap dampening information.

*network-address*: Network address.

*mask*: Network mask, in the format of X.X.X.X.

*mask-length*: Length of the network mask, in the range 0 to 32.

## Description

Use the **reset bgp vpn-instance dampening** command to clear the route flap dampening information of a VPN instance.

## Examples

```
# Clear the route flap dampening information of VPN instance vpn1.
```

```
<Sysname> reset bgp vpn-instance vpn1 dampening
```

## reset bgp vpn-instance flap-info

### Syntax

**reset bgp vpn-instance** *vpn-instance-name* *ip-address* **flap-info**

**reset bgp vpn-instance** *vpn-instance-name* **flap-info** [ *ip-address* [ *mask* | *mask-length* ] ] | **as-path-acl** *as-path-acl-number* | **regex** *as-path-regexp* ]

### View

User view

### Default Level

1: Monitor level

### Parameters

*vpn-instance-name*: Name of the VPN instance, a string of 1 to 31 characters.

*ip-address*: IP address of the peer.

*mask*: Network mask, in the format of X.X.X.X.

*mask-length*: Length of the network mask, in the range 0 to 32.

**as-path-acl** *as-path-acl-number*: Specifies the AS\_PATH filtering list. The *as-path-acl-number* argument ranges from 1 to 256.

**regex** *as-path-regexp*: Specifies the AS\_PATH regular expression.

### Description

Use the **reset bgp vpn-instance flap-info** command to clear the route flap history information about BGP peers of a VPN instance.

### Examples

```
# Clear route flap history information about BGP peer 2.2.2.2 of VPN instance vpn1.
```

```
<Sysname> reset bgp vpn-instance vpn1 2.2.2.2 flap-info
```

## route-distinguisher

### Syntax

**route-distinguisher** *route-distinguisher*

### View

VPN instance view

### Default Level

2: System level

### Parameters

*route-distinguisher*: Route distinguisher (RD) for the VPN instance, a string of 3 to 21 characters in either of the following two formats:

- 16-bit AS number:32-bit user-defined number. For example, 101:3.

- 32-bit IP address:16-bit user-defined number. For example, 192.168.122.15:1.

## Description

Use the **route-distinguisher** command to configure a route distinguisher (RD) for a VPN instance.

An RD is used to create the routing and forwarding table of a VPN. By prefixing an RD to an IPv4 prefix, you make the VPN IPv4 prefix unique globally.



### Note

- No RD is configured by default; you must configure an RD for each VPN instance.
  - A VPN instance takes effect only after you configure an RD for it.
  - Once you configure an RD for a VPN, you cannot remove the association.
  - You cannot change an RD directly; you can only delete the VPN instance, re-create the VPN instance, and then re-configure a new RD.
- 

## Examples

# Configure the RD of VPN instance vpn1.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] route-distinguisher 22:1
```

## routing-table limit

### Syntax

**routing-table limit** *number* { *warn-threshold* | **simply-alert** }

**undo routing-table limit**

### View

VPN instance view

### Default Level

2: System level

### Parameters

*number*: Maximum number of routes for the VPN instance to support, in the range 1 to 12288.

*warn-threshold*: Threshold for rejecting new routes. It is expressed in the percentage of the specified maximum number of routes for the VPN instance. It ranges from 1 to 100.

**simply-alert**: Specifies that when the maximum number of routes exceeds the threshold, the system still accepts routes and generates only a SYSLOG error message.

## Description

Use the **routing-table limit** command to limit the maximum number of routes in a VPN instance, preventing too many routes from being redistributed from the inbound interface of the PE.

Use the **undo routing-table limit** command to remove the limitation.

By default, there is no limit to the maximum number of routes that a VPN instance supports.

## Examples

# Specify that VPN instance vpn1 can redistribute up to 1000 routes in, and allow the VPN instance to accept new routes after the threshold is exceeded.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] route-distinguisher 100:1
[Sysname-vpn-instance-vpn1] routing-table limit 1000 simply-alert
```

## vpn-instance-capability simple

### Syntax

```
vpn-instance-capability simple
undo vpn-instance-capability
```

### View

OSPF multi-instance view

### Default Level

2: System level

### Parameters

None

### Description

Use the **vpn-instance-capability simple** command to enable multi-VPN-instance CE.

Use the **undo vpn-instance-capability** command to disable the function.

By default, the function is disabled.

## Examples

# Enable multi-VPN-instance CE.

```
<Sysname> system-view
[Sysname] ospf 100 vpn-instance vpna
[Sysname-ospf-100] vpn-instance-capability simple
```

## vpn-target

### Syntax

```
vpn-target vpn-target&<1-8> [ both | export-extcommunity | import-extcommunity ]
undo vpn-target { all | { vpn-target&<1-8> [ both | export-extcommunity | import-extcommunity ] }
```

### View

VPN instance view

## Default Level

2: System level

## Parameters

**vpn-target**<1-8>: Adds the VPN target extended community attribute to the import or export VPN target extended community list and specify the VPN target in the format nn:nn or IP-address:nn. <1-8> means that you can specify this argument for up to 8 times.

A VPN target attribute can be of 3 to 21 characters and in either of these two formats:

- 16-bit AS number:32-bit user-defined number. For example, 101:3.
- 32-bit IP address:16-bit user-defined number. For example, 192.168.122.15:1.

**both**: Specifies both the export routing information to the destination VPN extended community and the import routing information from the destination VPN extended community. This is the default.

**export-extcommunity**: Specifies the export routing information to the destination VPN extended community.

**import-extcommunity**: Specifies the import routing information from the destination VPN extended community.

**all**: Specifies all export routing information to the destination VPN extended community and import routing information from the destination VPN extended community.

## Description

Use the **vpn-target** command to associate the current VPN instance with one or more VPN targets.

Use the **undo vpn-target** command to remove the association of the current VPN instance with VPN targets.

VPN target has no default. You must configure it when creating a VPN instance.

## Examples

# Associate the current VPN instance with VPN targets.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] route-distinguisher 100:1
[Sysname-vpn-instance-vpn1] vpn-target 3:3 export-extcommunity
EVT Assignment result:
VPN-Target assignment is successful
[Sysname-vpn-instance-vpn1] vpn-target 4:4 import-extcommunity
IVT Assignment result:
VPN-Target assignment is successful
[Sysname-vpn-instance-vpn1] vpn-target 5:5 both
IVT Assignment result:
VPN-Target assignment is successful
EVT Assignment result:
VPN-Target assignment is successful
```

# IP Multicast Volume Organization

---

## Manual Version

6W100-20090120

## Product Version

Release 2202

## Organization

The IP Multicast Volume is organized as follows:

Features	Description
Multicast Routing and Forwarding	Multicast routing and forwarding refer to some policies that filter RPF routing information for IP multicast support. This document introduces the commands for Multicast Routing and Forwarding configuration.
IGMP	Internet Group Management Protocol (IGMP) is a protocol in the TCP/IP suite responsible for management of IP multicast members. This document introduces the commands for IGMP configuration.
PIM	PIM leverages the unicast routing table created by any unicast routing protocol to provide routing information for IP multicast. This document introduces the commands for PIM configuration.
MSDP	Multicast source discovery protocol (MSDP) describes interconnection mechanism of multiple PIM-SM domains. It is used is to discover multicast source information in other PIM-SM domains. This document introduces the commands for MSDP configuration.
MBGP	As a multicast extension of MP-BGP, MBGP enables BGP to provide routing information for multicast applications. This document introduces the commands for MBGP configuration.
IGMP Snooping	Running at the data link layer, IGMP Snooping is a multicast control mechanism on the Layer 2 Ethernet switch and it is used for multicast group management and control. This document introduces the commands for IGMP Snooping configuration.
Multicast VLAN	This document introduces the commands for Multicast VLAN configuration.
IPv6 Multicast Routing and Forwarding	IPv6 multicast routing and forwarding refer to some policies that filter RPF routing information for IPv6 multicast support. This document introduces the commands for IPv6 Multicast Routing and Forwarding configuration.
MLD	MLD is used by an IPv6 router or a Ethernet Switch to discover the presence of multicast listeners on directly-attached subnets. This document introduces the commands for MLD configuration.
IPv6 PIM	IPv6 PIM discovers multicast source and delivers information to the receivers. This document introduces the commands for IPv6 PIM configuration.

<b>Features</b>	<b>Description</b>
IPv6 MBGP	As an IPv6 multicast extension of MP-BGP, IPv6 MBGP enables BGP to provide routing information for IPv6 multicast applications. This document introduces the commands for IPv6 MBGP configuration.
MLD Snooping	Multicast Listener Discovery Snooping (MLD Snooping) is an IPv6 multicast constraining mechanism that runs on Layer 2 devices to manage and control IPv6 multicast groups. This document introduces the commands for MLD Snooping configuration.
IPv6 Multicast VLAN	This document introduces the commands for IPv6 Multicast VLAN configuration.

# Table of Contents

<b>1 Multicast Routing and Forwarding Configuration Commands</b> .....	<b>1-1</b>
Multicast Routing and Forwarding Configuration Commands .....	1-1
display multicast boundary .....	1-1
display multicast forwarding-table .....	1-2
display multicast routing-table .....	1-4
display multicast routing-table static.....	1-6
display multicast rpf-info.....	1-7
ip rpf-route-static.....	1-8
mtracert .....	1-9
multicast boundary .....	1-11
multicast forwarding-table downstream-limit .....	1-12
multicast forwarding-table route-limit.....	1-13
multicast load-splitting .....	1-13
multicast longest-match.....	1-14
multicast routing-enable .....	1-14
reset multicast forwarding-table .....	1-15
reset multicast routing-table .....	1-16

# 1 Multicast Routing and Forwarding Configuration Commands

---



## Note

The term “router” in this document refers to a router in the generic sense or a Layer 3 switch running an IP multicast routing protocol.

---

## Multicast Routing and Forwarding Configuration Commands

### display multicast boundary

#### Syntax

```
display multicast boundary [ group-address [ mask | mask-length ] ] [ interface interface-type interface-number ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

*group-address*: Multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

*mask*: Mask of the multicast group address, 255.255.255.255 by default.

*mask-length*: Mask length of the multicast group address, in the range of 4 to 32. The system default is 32.

*interface-type interface-number*: Specifies an interface by its type and number.

#### Description

Use the **display multicast boundary** command to view the multicast boundary information on the specified interface or all interfaces.

Related commands: **multicast boundary**.

#### Examples

```
# View the multicast boundary information on all interfaces in the public network instance.
```

```
<Sysname> display multicast boundary
```

```

Multicast boundary information
Boundary          Interface
224.1.1.0/24      Vlan1
239.2.2.0/24      Vlan2

```

**Table 1-1 display multicast boundary command output description**

Field	Description
Multicast boundary information	Multicast boundary for the public network
Boundary	Multicast group corresponding to the multicast boundary
Interface:	Boundary interface corresponding to the multicast boundary

## display multicast forwarding-table

### Syntax

```

display multicast forwarding-table [ source-address [ mask { mask | mask-length } ] | group-address
[ mask { mask | mask-length } ] | incoming-interface { interface-type interface-number | register } |
outgoing-interface { { exclude | include | match } { interface-type interface-number | register } } |
statistics | slot slot-number ] * [ port-info ]

```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*source-address*: Multicast source address.

*group-address*: Multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

*mask*: Mask of the multicast group/source address, 255.255.255.255 by default.

*mask-length*: Mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases.

**incoming-interface**: Displays forwarding entries of which the incoming interface is the specified one.

*interface-type interface-number*: Specifies the interface by its type and number.

**register**: Displays forwarding entries of which the incoming interface is the register interface of PIM-SM.

**outgoing-interface**: Displays forwarding entries of which the outgoing interface is the specified one.

**exclude**: Displays the forwarding entries of which the outgoing interface list excludes the specified interface.

**include**: Displays the forwarding entries of which the outgoing interface list includes the specified interface.

**match**: Specifies the forwarding entries of which the outgoing interface list includes and includes only the specified interface.

**statistics:** Specifies to display the statistics information of the multicast forwarding table.

**slot slot-number:** Displays forwarding entries of the interface card specified by the slot number. If you do not specify this option, this command will display the multicast forwarding table information of the main processing board.

**port-info:** Specifies to display Layer 2 port information.

## Description

Use the **display multicast forwarding-table** command to view the multicast forwarding table information.

Multicast forwarding tables are used to guide multicast forwarding. You can view the forwarding state of multicast traffic by checking the multicast forwarding table.

Related commands: **multicast forwarding-table downstream-limit**, **multicast forwarding-table route-limit**, **display multicast routing-table**.

## Examples

# View the multicast forwarding table information in the public network instance.

```
<Sysname> display multicast forwarding-table
Multicast Forwarding Table
Total 1 entry

Total 1 entry matched

00001. (172.168.0.2, 227.0.0.1)
  MID: 0, Flags: 0x0:0
  Uptime: 00:08:32, Timeout in: 00:03:26
  Incoming interface: Vlan-interface1
  List of 1 outgoing interfaces:
    1: Vlan-interface2
  Matched 19648 packets(20512512 bytes), Wrong If 0 packets
  Forwarded 19648 packets(20512512 bytes)
```

**Table 1-2** display multicast forwarding-table command output description

Field	Description
Multicast Forwarding Table	Multicast forwarding table for the public network
Total 1 entry	Total number of (S, G) entries in the multicast forwarding table
Total 1 entry matched	Total number of matched (S, G) entries in the multicast forwarding table
00001	Sequence number of the (S, G) entry
(172.168.0.2,227.0.0.1)	An (S, G) entry of the multicast forwarding table
MID	(S, G) entry ID. Each (S, G) entry has a unique MID
Flags	Current state of the (S, G) entry. Different bits are used to indicate different states of (S, G) entries. Major values of this field are described in <a href="#">Table 1-3</a> .
Uptime	Length of time for which the (S, G) entry has been up, in hours:minutes:seconds

Field	Description
Timeout in	Length of time in which the (S, G) entry will expire, in hours:minutes:seconds
Incoming interface	Incoming interface of the (S, G) entry
List of 1 outgoing interface: 1: Vlan-interface2	Outgoing interface list Interface number: outgoing interface name and number
Matched 19648 packets (20512512 bytes), Wrong If 0 packets	(S, G)-matched packets (bytes), packets with incoming interface errors
Forwarded 19648 packets (20512512 bytes)	(S, G)-forwarded packets (bytes)

**Table 1-3** Major values of the **flags** field

Value	Meaning
0x00000001	Indicates that a register-stop message must be sent
0x00000002	Indicates whether the multicast source corresponding to the (S, G) is active
0x00000004	Indicates a null forwarding entry
0x00000008	Indicates whether the RP is a PIM domain border router
0x00000010	Indicates that a register outgoing interface is available
0x00000400	Identifies an (S, G) entry to be deleted
0x00008000	Indicates that the (S, G) entry is in the smoothening process after active/standby switchover
0x00010000	Indicates that the (S, G) has been updated during the smoothening process
0x00080000	Indicates that the (S, G) entry has been repeatedly updated and needs to be deleted before a new entry is added
0x00100000	Indicates that an entry is successfully added

## display multicast routing-table

### Syntax

```
display multicast routing-table [ source-address [ mask { mask | mask-length } ] | group-address
[ mask { mask | mask-length } ] | incoming-interface { interface-type interface-number | register } |
outgoing-interface { { exclude | include | match } { interface-type interface-number | register } } ] *
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*source-address*: Multicast source address.

*group-address*: Multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

*mask*: Mask of the multicast group/source address, 255.255.255.255 by default.

*mask-length*: Mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases.

**incoming-interface**: Displays multicast routing entries of which the incoming interface is the specified one.

*interface-type interface-number*: Specifies an interface by its type and number.

**register**: Displays multicast routing entries of which the incoming interface is the specified register interface of PIM-SM.

**outgoing-interface**: Displays multicast routing entries of which the outgoing interface is the specified one.

**exclude**: Displays routing entries of which the outgoing interface list excludes the specified interface.

**include**: Displays routing entries of which the outgoing interface list includes the specified interface.

**match**: Displays routing entries of which the outgoing interface list includes only the specified interface.

## Description

Use the **display multicast routing-table** command to view the multicast routing table information.

Multicast routing tables are the basis of multicast forwarding. You can view the establishment state of an (S, G) entry by checking the multicast routing table.

Related commands: **display multicast forwarding-table**.

## Examples

# View the routing information in the multicast routing table of the public instance.

```
<Sysname> display multicast routing-table
Multicast routing table
Total 1 entry
00001. (172.168.0.2, 227.0.0.1)
    Uptime: 00:00:28
    Upstream Interface: Vlan-interface1
    List of 2 downstream interfaces
        1: Vlan-interface2
        2: Vlan-interface3
```

**Table 1-4** display multicast routing-table command output description

Field	Description
Multicast routing table	Multicast routing table for the public network
Total 1 entry	Total number of (S, G) entries in the multicast routing table
00001	Sequence number of the (S, G) entry
(172.168.0.2, 227.0.0.1)	An (S, G) entry of the multicast forwarding table
Uptime	Length of time for which the (S, G) entry has been up, in hours:minutes:seconds

Field	Description
Upstream interface	Upstream interface the (S, G) entry: multicast packets should arrive at this interface
List of 2 downstream interfaces	Downstream interface list: these interfaces need to forward multicast packets

## display multicast routing-table static

### Syntax

```
display multicast routing-table static [ config ] [ source-address { mask-length | mask } ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**config**: Displays the configuration information of static routes.

*source-address*: Multicast source address.

*mask*: Mask of the multicast source address.

*mask-length*: Mask length of the multicast source address, in the range of 0 to 32.

### Description

Use the **display multicast routing-table static** command to view the information of multicast static routes.

### Examples

# View all the multicast static routes in the public instance.

```
<Sysname> display multicast routing-table static
Multicast Routing Table
Routes : 1

Mroute 10.10.0.0/16
    Interface = Vlan-interfacel          RPF Neighbor = 2.2.2.2
    Matched routing protocol = <none>, Route-policy = <none>
    Preference = 1, Order = 1
Running Configuration = ip rpf-route-static 10.10.0.0 16 2.2.2.2 order 1
```

# View the configuration information of multicast static routes in the public instance.

```
<Sysname> display multicast routing-table static config

Multicast Routing Table
Routes : 1

Mroute 10.10.0.0/16,    RPF neighbor = 2.2.2.2
```

Matched routing protocol = <none>, Route-policy = <none>  
 Preference = 1, Order = 1

**Table 1-5** display multicast routing-table static command output description

Field	Description
Multicast Routing Table	Multicast routing table for the public network
Mroute	Multicast route source address and its mask length
Interface	Outgoing interface to the multicast source
RPF Neighbor	IP address of the RPF neighbor through which the multicast source is reachable
Matched routing protocol	If a protocol is configured, the multicast source address of the route should be the destination address of an entry in unicast routing table.
Route-policy	Routing policy. The multicast source address of the route should match the routing policy.
Preference	Route preference
Order	Sequence number of the route

## display multicast rpf-info

### Syntax

**display multicast rpf-info** *source-address* [ *group-address* ]

### View

Any view

### Default Level

1: Monitor level

### Parameters

*source-address*: Multicast source address.

*group-address*: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

### Description

Use the **display multicast rpf-info** command to view the RPF information of a multicast source.

Related commands: **display multicast routing-table**, **display multicast forwarding-table**.

### Examples

# View all the RPF information of multicast source 192.168.1.55 in the public network.

```
<Sysname> display multicast rpf-info 192.168.1.55
RPF information about source 192.168.1.55:
  RPF interface: Vlan-interface1, RPF neighbor: 10.1.1.1
  Referenced route/mask: 192.168.1.0/24
  Referenced route type: igp
```

```
Route selection rule: preference-preferred
Load splitting rule: disable
```

**Table 1-6** display multicast rpf-info command output description

Field	Description
RPF information about source 192.168.1.55	Information of the RPF path to multicast source 192.168.1.55
RPF interface	RPF interface
RPF neighbor	IP address of the RPF neighbor
Referenced route/mask	Referenced route and its mask length
Referenced route type	Type of the referenced route, which can be any of the following: <ul style="list-style-type: none"> <li>• igp: unicast route (IGP)</li> <li>• egp: unicast route (BGP)</li> <li>• unicast (direct): unicast route (directly connected)</li> <li>• unicast: other unicast route (such as unicast static route)</li> <li>• mbgp: MBGP route</li> <li>• multicast static: multicast static route</li> </ul>
Route selection rule	Rule for RPF route selection, which can be based on the preference of the routing protocol or based on the longest match on the destination address
Load splitting rule	Status of the load splitting rule (enabled/disabled)

## ip rpf-route-static

### Syntax

```
ip rpf-route-static source-address { mask | mask-length } [ protocol [ process-id ] ] [ route-policy
policy-name ] { rpf-nbr-address | interface-type interface-number } [ preference preference ] [ order
order-number ]
```

```
undo ip rpf-route-static source-address { mask | mask-length } [ protocol [ process-id ] ] [ route-policy
policy-name ]
```

### View

System view

### Default Level

2: System level

### Parameters

*source-address*: Multicast source address.

*mask*: Mask of the multicast source address.

*mask-length*: Mask length of the multicast source address, in the range of 0 to 32.

*protocol*: Routing protocol, which can have any of the following values:

- **bgp**: Specifies the BGP protocol.
- **isis**: Specifies the IS-IS protocol.
- **ospf**: Specifies the OSPF protocol.

- **rip**: Specifies the RIP protocol.
- **static**: Specifies a static route.

*process-id*: Process number of the unicast routing protocol, in the range of 1 to 65535. This argument must be provided if IS-IS, OSPF or RIP is the specified unicast routing protocol.

*policy-name*: Name of the multicast route match rule, a case sensitive string of up to 19 characters without any space.

*rpf-nbr-address*: Specifies an RPF neighbor by the IP address.

*interface-type interface-number*: Specifies the interface type and interface number.

*preference*: Route preference, in the range of 1 to 255 and defaulting to 1.

*order-number*: Match order for routes on the same segment, in the range of 1 to 100.

## Description

Use the **ip rpf-route-static** command to configure a multicast static route.

Use the **undo ip rpf-route-static** command to delete a multicast static route from the multicast static routing table.

By default, no multicast static route is configured.

Note that:

- The arguments *source-address { mask | mask-length }*, *protocol* and *policy-name* are critical elements in multicast static route configuration. The variation of any of these three arguments results in a different configuration.
- In the configuration, you can use the **display multicast routing-table static** command to check whether the multicast static route information contains this configuration. If you find a match, modify the corresponding fields without changing the configuration sequence; otherwise, add a multicast static route.
- When configuring a multicast static route, you can specify an RPF neighbor only by providing its IP address (*rpf-nbr-address*) rather than its interface type and number (*interface-type interface-number*) if the interface type of the RPF neighbor is Ethernet, Layer 3 aggregate, Loopback, RPR, or VLAN-interface.
- Because outgoing interface iteration may fail or the specified interface may be in the down state, the multicast static route configured with this command may fail to take effect. Therefore, we recommend that you use the **display multicast routing-table static** command after you configure a multicast static route to check whether the route has been successfully configured or whether the route has taken effect.

Related commands: **display multicast routing-table static**.

## Examples

# Configure a multicast static route to the multicast source 10.1.1.1/24, specifying a router with the IP address of 192.168.1.23 as its RPF neighbor.

```
<Sysname> system-view
[Sysname] ip rpf-route-static 10.1.1.1 24 192.168.1.23
```

## mtracert

### Syntax

**mtracert** *source-address* [ [ *last-hop-router-address* ] *group-address* ]

## View

Any view

## Default Level

1: Monitor level

## Parameters

*source-address*: Specifies a multicast source address.

*group-address*: Specifies a multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

*last-hop-router-address*: Specifies a last-hop router address, which is the IP address of the local router by default.

## Description

Use the **mtracert** command to trace the path down which the multicast traffic flows to the last-hop router.

Note that if the *last-hop-router-address* argument is given in the command to trace the path for a specific (S, G) multicast stream, the interface corresponding to the last-hop router address must be the outgoing interface for the (S, G) entry; otherwise the multicast traceroute will fail.

## Examples

# Trace the path down which the (6.6.6.6, 225.2.1.1) multicast traffic flows to the last-hop router with an IP address of 5.5.5.8.

```
<Sysname> mtracert 6.6.6.6 5.5.5.8 225.2.1.1
Type Ctrl+C to quit mtrace facility
Tracing reverse path of (6.6.6.6, 225.2.1.1) from last-hop router (5.5.5.8) to source via
multicast routing-table
```

```
-1 5.5.5.8
  Incoming interface address: 4.4.4.8
  Previous-hop router address: 4.4.4.7
  Input packet count on incoming interface: 17837
  Output packet count on outgoing interface: 0
  Total number of packets for this source-group pair: 8000
  Protocol: PIM
  Forwarding TTL: 0
  Forwarding code: No error
```

```
-2 4.4.4.7
  Incoming interface address: 6.6.6.7
  Previous-hop router address: 0.0.0.0
  Input packet count on incoming interface: 2
  Output packet count on outgoing interface: 259
  Total number of packets for this source-group pair: 8100
  Protocol: PIM
  Forwarding TTL: 0
  Forwarding code: No error
```

**Table 1-7 mtracert** command output description

Field	Description
(6.6.6.6, 225.2.1.1)	The (S, G) multicast stream for which the forwarding path is being traced
-1 5.5.5.8	The (S, G) outgoing interface address of each hop, starting from the last-hop router
Incoming interface address	The address of the interface on which the (S, G) packets arrive
Previous-hop router address	The IP address of the router from which this router receives packets from this source
Input packet count on incoming interface	The total number of multicast packets received on the incoming interface
Output packet count on outgoing interface	The total number of multicast packets transmitted on the outgoing interface
Total number of packets for this source-group pair	The total number of packets from the specified source forwarded by this router to the specified group
Protocol	The multicast routing protocol in use
Forwarding TTL	The minimum TTL that a packet is required to have before it can be forwarded over the outgoing interface

## multicast boundary

### Syntax

```

multicast boundary group-address { mask | mask-length }
undo multicast boundary { group-address { mask | mask-length } | all }

```

### View

Interface view

### Default Level

2: System level

### Parameters

*group-address*: Multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

*mask*: Mask of the multicast group address.

*mask-length*: Mask length of the multicast group address, in the range of 4 to 32.

**all**: Specifies to remove all forwarding boundaries configured on the interface.

### Description

Use the **multicast boundary** command to configure a multicast forwarding boundary.

Use the **undo multicast boundary** command to remove a multicast forwarding boundary.

By default, no multicast forwarding boundary is configured.

Note that:

- A multicast forwarding boundary sets the boundary condition for the multicast groups in the specified range. If the destination address of a multicast packet matches the set boundary condition, the packet will not be forwarded.
- If an interface needs to act as a forwarding boundary for multiple multicast groups, just carry out this command on the interface once for each group.
- Assume that Set A and Set B are both multicast forwarding boundary sets to be configured, and B is a subset of A. If A has been configured on an interface, it is not allowed to configure B on the interface; if B has been configured on the interface before A is configured, the previously configured B will be removed.

Related commands: **display multicast boundary**.

## Examples

```
# Configure VLAN-interface 100 to be the forwarding boundary of multicast group 239.2.0.0/16.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] multicast boundary 239.2.0.0 16
```

## multicast forwarding-table downstream-limit

### Syntax

```
multicast forwarding-table downstream-limit limit
undo multicast forwarding-table downstream-limit
```

### View

System view

### Default Level

2: System level

### Parameters

*limit*: Maximum number of downstream nodes (namely, the maximum number of outgoing interfaces) for a single multicast forwarding entry. The value ranges from 0 to 128.

### Description

Use the **multicast forwarding-table downstream-limit** command to configure the maximum number of downstream nodes for a single entry in the multicast forwarding table.

Use the **undo multicast forwarding-table downstream-limit** command to restore the system default.

By default, the maximum number of downstream nodes for a single multicast forwarding entry is 128

Related commands: **display multicast forwarding-table**.

## Examples

```
# Set the maximum number of downstream nodes for a single multicast forwarding entry of the public instance to 128.
```

```
<Sysname> system-view
[Sysname] multicast forwarding-table downstream-limit 128
```

## multicast forwarding-table route-limit

### Syntax

```
multicast forwarding-table route-limit limit  
undo multicast forwarding-table route-limit
```

### View

System view

### Default Level

2: System level

### Parameters

*limit*: Maximum number of entries in the multicast forwarding table. The value ranges 0 to **1024**.

Use the **multicast forwarding-table route-limit** command to configure the maximum number of entries in the multicast forwarding table.

Use the **undo multicast forwarding-table route-limit** command to restore the maximum number of entries in the multicast forwarding table to the system default.

By default, the maximum number of entries in the multicast forwarding table is 1024.

Related commands: **display multicast forwarding-table**.

### Examples

# Set the maximum number of entries in the multicast forwarding table of the public instance to 200.

```
<Sysname> system-view  
[Sysname] multicast forwarding-table route-limit 200
```

## multicast load-splitting

### Syntax

```
multicast load-splitting { source | source-group }  
undo multicast load-splitting
```

### View

System view

### Default Level

2: System level

### Parameters

**source**: Specifies to implement per-source load splitting.

**source-group**: Specifies to implement per-source and per-group load splitting simultaneously.

### Description

Use the **multicast load-splitting** command to enable load splitting of multicast traffic.

Use the **undo multicast load-splitting** command to disable load splitting of multicast traffic.

By default, load splitting of multicast traffic is disabled.

## Examples

```
# Enable per-source load splitting of multicast traffic in the public instance.
```

```
<Sysname> system-view  
[Sysname] multicast load-splitting source
```

## multicast longest-match

### Syntax

```
multicast longest-match  
undo multicast longest-match
```

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **multicast longest-match** command to configure the device to select the RPF route based on the longest match principle, namely to select the route with the longest mask as the RPF route.

Use the **undo multicast longest-match** command to restore the default.

By default, the device selects the route with the highest priority as the RPF route.

## Examples

```
# Configure the device to select the RPF route based on the longest match principle in the public instance.
```

```
<Sysname> system-view  
[Sysname] multicast longest-match
```

## multicast routing-enable

### Syntax

```
multicast routing-enable  
undo multicast routing-enable
```

### View

System view

### Default Level

2: System level

## Parameters

None

## Description

Use the **multicast routing-enable** command to enable IP multicast routing.

Use the **undo multicast routing-enable** command to disable IP multicast routing.

IP multicast routing is disabled by default.

Note that:

- You must enable IP multicast routing before you can carry out other Layer 3 multicast commands.
- The device does not forward any multicast packets before IP multicast routing is enabled.

## Examples

```
# Enable IP multicast routing in the public instance.
```

```
<Sysname> system-view  
[Sysname] multicast routing-enable
```

## reset multicast forwarding-table

### Syntax

```
reset multicast forwarding-table { { source-address [ mask { mask | mask-length } ] | group-address [ mask { mask | mask-length } ] | incoming-interface { interface-type interface-number | register } } * | all }
```

### View

User view

### Default Level

2: System level

## Parameters

*source-address*: Multicast source address.

*group-address*: Multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

*mask*: Mask of the multicast group/source address, 255.255.255.255 by default.

*mask-length*: Mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases.

**incoming-interface**: Specifies to clear multicast forwarding entries of which the incoming interface is the specified one.

*interface-type interface-number*: Specifies an interface by its type and number.

**register**: Specifies to clear multicast forwarding entries of which the incoming interface is the specified register interface of PIM-SM.

**all**: Specifies to clear all the forwarding entries from the multicast forwarding table.

## Description

Use the **reset multicast forwarding-table** command to clear the multicast forwarding table information.

Note that, When a forwarding entry is deleted from the multicast forwarding table, the corresponding route entry is also deleted from the multicast routing table.

Related commands: **reset multicast routing-table**, **display multicast routing-table**, **display multicast forwarding-table**.

## Examples

```
# Clear the multicast forwarding entries related to multicast group 225.5.4.3 from the multicast forwarding table of the public instance.
```

```
<Sysname> reset multicast forwarding-table 225.5.4.3
```

## reset multicast routing-table

### Syntax

```
reset multicast routing-table { { source-address [ mask { mask | mask-length } ] | group-address [ mask { mask | mask-length } ] | incoming-interface { interface-type interface-number | register } } * | all }
```

### View

User view

### Default Level

2: System level

### Parameters

*source-address*: Multicast source address.

*group-address*: Multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

*mask*: Mask of the multicast group/source address, 255.255.255.255 by default.

*mask-length*: Mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases.

**incoming-interface**: Specifies to clear the routing entries of which the incoming interface is the specified one.

*interface-type interface-number*: Specifies an interface by its type and number.

**register**: Specifies to clear the routing entries of which the incoming interface is the specified register interface of PIM-SM.

**all**: Specifies to clear all the routing entries from the multicast routing table.

## Description

Use the **reset multicast routing-table** command to clear multicast routing entries from the multicast routing table.

Note that,When a route entry is deleted from the multicast routing table, the corresponding forwarding entry is also deleted from the multicast forwarding table.

Related commands: **reset multicast forwarding-table**, **display multicast routing-table**, **display multicast forwarding-table**.

### Examples

# Clear the route entries related to multicast group 225.5.4.3 from the multicast routing table of the public instance.

```
<Sysname> reset multicast routing-table 225.5.4.3
```

# Table of Contents

<b>1 IGMP Configuration Commands</b> .....	<b>1-1</b>
IGMP Configuration Commands .....	1-1
display igmp group .....	1-1
display igmp group port-info .....	1-2
display igmp interface .....	1-4
display igmp proxying group .....	1-6
display igmp routing-table .....	1-7
display igmp ssm-mapping .....	1-9
display igmp ssm-mapping group .....	1-10
fast-leave (IGMP view) .....	1-11
igmp .....	1-12
igmp enable .....	1-13
igmp group-limit .....	1-13
igmp group-policy .....	1-14
igmp last-member-query-interval .....	1-15
igmp max-response-time .....	1-16
igmp proxying enable .....	1-16
igmp proxying forwarding .....	1-17
igmp require-router-alert .....	1-18
igmp robust-count .....	1-18
igmp send-router-alert .....	1-19
igmp ssm-mapping enable .....	1-20
igmp startup-query-count .....	1-20
igmp startup-query-interval .....	1-21
igmp static-group .....	1-22
igmp timer other-querier-present .....	1-23
igmp timer query .....	1-24
igmp version .....	1-24
last-member-query-interval (IGMP view) .....	1-25
max-response-time (IGMP view) .....	1-25
require-router-alert (IGMP view) .....	1-26
reset igmp group .....	1-27
reset igmp group port-info .....	1-28
reset igmp ssm-mapping group .....	1-28
robust-count (IGMP view) .....	1-29
send-router-alert (IGMP view) .....	1-30
ssm-mapping (IGMP view) .....	1-30
startup-query-count (IGMP view) .....	1-31
startup-query-interval (IGMP view) .....	1-32
timer other-querier-present (IGMP view) .....	1-33
timer query (IGMP view) .....	1-33
version (IGMP view) .....	1-34

# 1 IGMP Configuration Commands

---



## Note

The term "router" in this document refers to a router in a generic sense or a Layer 3 switch running an IGMP protocol.

---

## IGMP Configuration Commands

### display igmp group

#### Syntax

```
display igmp group [ group-address | interface interface-type interface-number ] [ static | verbose ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

*group-address*: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

**interface** *interface-type interface-number*: Displays the IGMP multicast group information about a particular interface.

**static**: Displays the information of statically joined IGMP multicast groups.

**verbose**: Displays the detailed information of IGMP multicast groups.

#### Description

Use the **display igmp group** command to view IGMP multicast group information.

Note that:

- If you do not specify *group-address*, this command will display the IGMP information of all the multicast groups.
- If you do not specify *interface-type interface-number*, this command will display the IGMP multicast group information on all the interfaces.
- If you do not specify the **static** keyword, this command will display the detailed information about the dynamically joined IGMP multicast groups.

## Examples

# Display the information about dynamically joined IGMP multicast groups on all interfaces.

```
<Sysname> display igmp group
Total 3 IGMP Group(s).
Vlan-interface1(20.20.20.20):
  Total 3 IGMP Groups reported
  Group Address    Last Reporter    Uptime          Expires
  225.1.1.1        20.20.20.20     00:02:04        00:01:15
  225.1.1.3        20.20.20.20     00:02:04        00:01:15
  225.1.1.2        20.20.20.20     00:02:04        00:01:17
```

# Display the detailed information of multicast group 225.1.1.1.

```
<Sysname> display igmp group 225.1.1.1 verbose
Vlan-interface1(10.10.1.20):
  Total 1 IGMP Groups reported
  Group: 225.1.1.1
  Uptime: 00:00:34
  Expires: 00:00:40
  Last reporter: 10.10.1.10
  Last-member-query-counter: 0
  Last-member-query-timer-expiry: off
  Version1-host-present-timer-expiry: off
```

**Table 1-1 display igmp group command output description**

Field	Description
Interface group report information of VPN-Instance: public net	IGMP multicast group information on a public network interface
Total 1 IGMP Groups reported	One IGMP multicast group was reported.
Group	Multicast group address
Uptime	Length of time since the multicast group was reported
Expires	Remaining time of the multicast group, where “off” means that the multicast group never times out
Last reporter	Address of the last host that reported its membership for this multicast group
Last-member-query-counter	Number of group-specific queries sent
Last-member-query-timer-expiry	Remaining time of the last member query timer, where “off” means that the timer never expires
Version1-host-present-timer-expiry	Remaining time of the IGMPv1 host present timer, where “off” means that the timer never expires

## display igmp group port-info

### Syntax

```
display igmp group port-info [ vlan vlan-id ] [ slot slot-number ] [ verbose ]
```

## View

Any view

## Default Level

1: Monitor level

## Parameters

**vlan-id:** VLAN ID, in the range of 1 to 4094. If you do not specify a VLAN, this command will display the Layer 2 port information of IGMP multicast groups in all VLANs.

**slot slot-number:** Displays the Layer 2 port information about IGMP multicast groups on the specified card. If you do not specify a slot number, this command will display the Layer 2 port information about IGMP multicast groups on the SRPU.

**verbose:** Displays the detailed information about Layer 2 ports of IGMP multicast groups.

## Description

Use the **display igmp group port-info** command to view Layer 2 port information of IGMP multicast groups.

## Examples

# View detailed Layer 2 ports information of IGMP multicast groups.

```
<Sysname> display igmp group port-info verbose
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Port flags: D-Dynamic port, S-Static port, C-Copy port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):2.
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Router port(s):total 1 port.
    GE1/0/1                (D) ( 00:01:30 )
IP group(s):the following ip group(s) match to one mac group.
IP group address:224.1.1.1
(1.1.1.1, 224.1.1.1):
Attribute:    Host Port
Host port(s):total 1 port.
    GE1/0/2                (D) ( 00:03:23 )
MAC group(s):
MAC group address:0100-5e01-0101
Host port(s):total 1 port.
    GE1/0/2
```

**Table 1-2** display igmp group port-info command output description

Field	Description
Total 1 IP Group(s).	Total number of IP multicast groups
Total 1 IP Source(s).	Total number of IP multicast sources
Total 1 MAC Group(s).	Total number of MAC multicast groups
Port flags: D-Dynamic port, S-Static port, C-Copy port	Port flags: D for a dynamic port, S for a static port, and C for a port copied from a (*, G) entry to an (S, G) entry
Subvlan flags: R-Real VLAN, C-Copy VLAN	Sub-VLAN flags: R for a real egress sub-VLAN under the current entry, and C for a sub-VLAN copied from a (*, G) entry to an (S, G) entry
Router port(s)	Number of router ports
( 00:01:30 )	Remaining time of dynamic member port or router port aging timer. On a distributed device, to get this time value of a non-aggregation port on a board other than the SRPU, you must specify the number of the slot where the corresponding board resides by using <b>slot slot-number</b> . This is not required for an aggregation port.
IP group address	Address of the IP multicast group
MAC group address	Address of the MAC multicast group
Attribute	Attribute of the IP multicast group
Host port(s)	Number of member ports

## display igmp interface

### Syntax

```
display igmp interface [ interface-type interface-number ] [ verbose ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*interface-type interface-number*: Specifies an interface to display the IGMP configuration and operation information about. If no interface is specified, this command will display the related information of all IGMP-enabled interfaces.

**verbose**: Displays the detailed IGMP configuration and operation information.

### Description

Use the **display igmp interface** command to view IGMP configuration and operation information of the specified interface or all IGMP-enabled interfaces.

### Examples

```
# View the IGMP configuration and operation information on Vlan-interface1 (downstream interface).
```

```

<Sysname> display igmp interface vlan-interface 1 verbose
Vlan-interface1(10.10.1.20):
  IGMP is enabled
  Current IGMP version is 2
  Value of query interval for IGMP(in seconds): 60
  Value of other querier present interval for IGMP(in seconds): 125
  Value of maximum query response time for IGMP(in seconds): 10
  Value of last member query interval(in seconds): 1
  Value of startup query interval(in seconds): 15
  Value of startup query count: 2
  General query timer expiry (hours:minutes:seconds): 00:00:54
  Querier for IGMP: 10.10.1.20 (this router)
  IGMP activity: 1 joins, 0 leaves
  Multicast routing on this interface: enabled
  Robustness: 2
  Require-router-alert: disabled
  Fast-leave: disabled
  Ssm-mapping: disabled
  Startup-query-timer-expiry: off
  Other-querier-present-timer-expiry: off
  Proxying interface: Vlan-interface2(20.10.1.20)
  Total 1 IGMP Group reported

```

# View the detailed IGMP configuration and operation information on Vlan-interface2 (upstream interface).

```

<Sysname> display igmp interface vlan-interface 2 verbose
Vlan-interface2(20.10.1.20):
  IGMP proxy is enabled
  Current IGMP version is 3
  Multicast routing on this interface: enabled
  Require-router-alert: disabled
  Version1-querier-present-timer-expiry: off
  Version2-querier-present-timer-expiry: off

```

**Table 1-3 display igmp interface command output description**

Field	Description
Vlan-interface1(10.10.1.20)	Interface name (IP address)
Current IGMP version	Version of IGMP currently running on the interface
Value of query interval for IGMP(in seconds)	IGMP query interval, in seconds
Value of other querier present interval for IGMP(in seconds)	Other querier present interval, in seconds
Value of maximum query response time for IGMP(in seconds)	Maximum response time for IGMP general queries, in seconds
Value of last member query interval(in seconds)	IGMP last member query interval, in seconds
Value of startup query interval(in seconds)	IGMP startup query interval, in seconds

Field	Description
Value of startup query count	Number of IGMP general queries the device sends on startup
General query timer expiry	Remaining time of the IGMP general query timer, where "off" means that the timer never expires
Querier for IGMP	IP address of the IGMP querier
IGMP activity	Statistics of IGMP activities (joins and leaves)
Robustness	Robustness variable of the IGMP querier
Require-router-alert	Dropping IGMP messages without Router-Alert (enabled/disabled)
Fast-leave	Fast leave processing status (enabled/disabled)
Ssm-mapping	IGMP SSM mapping status (enabled/disabled)
Startup-query-timer-expiry	Remaining time of the startup query timer, where "off" means that the timer never expires
Other-querier-present-timer-expiry	Remaining time of the other querier present timer, where "off" means that the timer never expires
Proxying interface	IGMP proxy interface, where "none" means that no proxy interface exists
Total 1 IGMP Group reported	Total number of IGMP groups the interface has dynamically joined
IGMP proxy is enabled	IGMP proxying is enabled
Version1-querier-present-timer-expiry	Remaining time of the IGMPv1 querier present timer, where "off" means that the timer never expires
Version2-querier-present-timer-expiry	Remaining time of the IGMPv2 querier present timer, where "off" means that the timer never expires

## display igmp proxying group

### Syntax

```
display igmp proxying group [ group-address ] [ verbose ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*group-address*: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255. With no multicast group address included, this command displays the information of all the IGMP proxying groups.

**verbose**: Displays the detailed IGMP proxying group information.

## Description

Use the **display igmp proxying group** command to view the IGMP proxying group information.

## Examples

# View the IGMP proxying group information.

```
<Sysname> display igmp proxying group
Total 1 IGMP-Proxying group record(s)
  Group Address      Member state    Expires
  225.1.1.1         Delay          00:01:15
```

# View the detailed information of IGMP proxying group 225.1.1.1.

```
<Sysname> display igmp proxying group 225.1.1.1 verbose
Total 1 IGMP-Proxying group record(s)
Group: 225.1.1.1
Group mode: include
Member state: Delay
Expires: 00:00:02
Source list (total 1 source(s))
Source: 1.1.1.1
```

**Table 1-4** display igmp proxying group command output description

Field	Description
Total 1 IGMP-Proxying group record(s)	One IGMP proxying group is recorded.
Group Address/Group	Multicast group address
Member state	Host member states: <ul style="list-style-type: none"><li>• Delay</li><li>• Idle</li></ul>
Expires	Remaining time of the multicast group, where “off” means that the multicast group never times out
Group mode	Multicast source filtering modes: <ul style="list-style-type: none"><li>• Include</li><li>• Exclude</li></ul>
Source list	A list of sources joining the same multicast group in the IGMP proxying group

## display igmp routing-table

### Syntax

```
display igmp routing-table [ source-address [ mask { mask | mask-length } ] ] | group-address [ mask { mask | mask-length } ] ] * [ flags { act | suc } ]
```

### View

Any view

### Default Level

1: Monitor level

## Parameters

*source-address*: Multicast source address.

*group-address*: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

*mask*: Subnet mask of the multicast group/source address, 255.255.255.255 by default.

*mask-length*: Subnet mask length of the multicast group/source address. For a multicast source address, this argument has an effective value range of 0 to 32; for a multicast group address, this argument has an effective value range of 4 to 32. The system default is 32 in both cases.

**Flags**: Specifies the route flag.

**act**: Specifies to view the IGMP routes with the ACT flag

**suc**: specifies to view the IGMP routes with the SUC flag.

## Description

Use the **display igmp routing-table** command to view the IGMP routing table information.

## Examples

# View IGMP routing table information.

```
<Sysname> display igmp routing-table
Routing table of VPN-Instance: public net
Total 3 entries

00001. (*, 225.1.1.1)
    List of 1 downstream interface
        Vlan-interface1 (20.1.1.1),
            Protocol: STATIC

00002. (1.1.1.1, 225.1.1.1), Flag: ACT
    List of 1 downstream interface in include mode
        Vlan-interface2 (30.1.1.1),
            Protocol: IGMP

00003. (*, 239.255.255.250)
    List of 1 downstream interface
        Vlan-interface3 (40.20.20.20),
            Protocol: IGMP
```

**Table 1-5** display igmp routing-table command output description

Field	Description
Routing table of VPN-Instance: public net	Public network IGMP routing table
00001	Sequence number of this (*, G) entry
(*, 225.1.1.1)	A (*, G) entry of the IGMP routing table

Field	Description
Flag	IGMP route flags: <ul style="list-style-type: none"> <li>• ACT: Indicates IGMP routing entries that have been used for forwarding data packets but have the multicast group address out of the SSM group range</li> <li>• SUC: Indicates IGMP routing entries that have been added to the forwarding table and have the multicast group address within the SSM group range</li> </ul>
List of 1 downstream interface	Downstream interface list, namely the interfaces to which multicast data for this group will be forwarded
in include mode	The downstream interface is in the include mode
in exclude mode	The downstream interface is in the exclude mode
Downstream interface is none	No downstream interfaces exist
Protocol	Protocol type

## display igmp ssm-mapping

### Syntax

```
display igmp ssm-mapping group-address
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*group-address*: Specifies a multicast group by its IP address, in the range of 224.0.1.0 to 239.255.255.255.

### Description

Use the **display igmp ssm-mapping** command to view the configured IGMP SSM mappings for the specified multicast group.

Related commands: **ssm-mapping**.

### Examples

```
# View the IGMP SSM mappings for multicast group 232.1.1.1.
```

```
<Sysname> display igmp ssm-mapping 232.1.1.1
Group: 232.1.1.1
Source list:
  1.2.3.4
  5.5.5.5
 10.1.1.1
100.1.1.10
```

**Table 1-6 display igmp ssm-mapping** command output description

Field	Description
VPN-Instance: public net	Public instance
Group	Multicast group address
Source list	List of multicast source addresses

## display igmp ssm-mapping group

### Syntax

```
display igmp ssm-mapping group [ group-address | interface interface-type interface-number ]  
[ verbose ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*group-address*: Specifies a multicast group by its IP address, in the range of 224.0.1.0 to 239.255.255.255.

*interface-type interface-number*: Specifies an interface by its type and number.

**verbose**: Displays the detailed multicast group information created based on the configured IGMP SSM mappings.

### Description

Use the **display igmp ssm-mapping group** command to view the multicast group information created based on the configured IGMP SSM mappings.

Note that:

- If you do not specify a multicast group, this command will display the information of all multicast groups created based on the configured IGMP SSM mappings.
- If you do not specify an interface, this command will display the multicast group information created based on the configured IGMP SSM mappings on all the interfaces.

### Examples

# View the detailed information of multicast group 232.1.1.1 created based on the configured IGMP SSM mappings.

```
<Sysname> display igmp ssm-mapping group 232.1.1.1 verbose  
Vlan-interfaces(10.10.10.10):  
  Total 1 IGMP SSM-mapping Group reported  
  Group: 232.1.1.1  
    Uptime: 00:00:31  
    Expires: off  
    Last reporter: 1.1.1.1
```

```

Version1-host-present-timer-expiry: off
Source list(Total 1 source):
  Source: 1.1.1.1
    Uptime: 00:00:31
    Expires: 00:01:39
    Last-member-query-counter: 0
    Last-member-query-timer-expiry: off

```

**Table 1-7** display igmp ssm-mapping group command output description

Field	Description
Total 1 IGMP SSM-mapping Group reported	One IGMP SSM mapping multicast group was reported.
Group	Multicast group address
Uptime	Length of time since the multicast group was reported
Expires	Remaining time of the multicast group, where “off” means that the multicast group never times out
Last reporter	Address of the last host that reported its membership for this multicast group
Version1-host-present-timer-expiry	Remaining time of the IGMPv1 host present timer, where “off” means that the timer never expires
Source list(Total 1 source)	Multicast source list (one multicast source)
Source	Multicast source address
Last-member-query-counter	Number of group-specific queries sent
Last-member-query-timer-expiry	Remaining time of the last member query timer, where “off” means that the timer never expires

## fast-leave (IGMP view)

### Syntax

```

fast-leave [ group-policy acl-number ]
undo fast-leave

```

### View

IGMP view

### Default Level

2: System level

### Parameters

*acl-number*: Basic ACL number, in the range of 2000 to 2999. If you do not include this option in your command, this command will take effect for all multicast groups.

### Description

Use the **fast-leave** command to configure fast leave processing globally.

Use the **undo fast-leave** command to disable fast leave processing globally.

By default, fast leave processing is disabled. Namely, the IGMP querier sends IGMP group-specific queries upon receiving an IGMP leave message from a host, instead of sending a leave notification directly to the upstream.

Related commands: **last-member-query-interval**.



If the device supports IGMP Snooping, this command takes effect only on Layer 3 interfaces other than VLAN interfaces when executed in IGMP view.

---

## Examples

# Enable fast leave processing globally.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] fast-leave
```

## igmp

### Syntax

```
igmp
undo igmp
```

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **igmp** command to enter IGMP view .

Use the **undo igmp** command to remove configurations performed in IGMP view.

Note that,IP multicast must be enabled in the corresponding instance before this command can take effect.

Related commands: **igmp enable**; **multicast routing-enable** in *Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*.

## Examples

# Enable IP multicast routing and enter IGMP view.

```
<Sysname> system-view
```

```
[Sysname] multicast routing-enable
[Sysname] igmp
[Sysname-igmp]
```

## igmp enable

### Syntax

```
igmp enable
undo igmp enable
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **igmp enable** command to enable IGMP on the current interface.

Use the **undo igmp enable** command to disable IGMP on the current interface.

By default, IGMP is disabled on all interfaces.

Note that:

- IP multicast must be enabled before this command can take effect.
- IGMP must be enabled on an interface before any other IGMP feature configured on the interface can take effect.

Related commands: **igmp**; **multicast routing-table** in *Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*.

### Examples

```
# Enable IP multicast routing, and then enable IGMP on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp enable
```

## igmp group-limit

### Syntax

```
igmp group-limit limit
undo igmp group-limit
```

### View

Interface view

## Default Level

2: System level

## Parameters

*limit*: The maximum number of multicast groups that can be joined on the interface, in the range of 1 to 1024.

## Description

Use the **igmp group-limit** command to configure the maximum number of multicast groups that can be joined on the current interface.

Use the **undo igmp group-limit** command to restore the default.

By default, the maximum number of multicast groups that can be joined on an interface is 1024.

Note that:

- This command is effective only for dynamically joined multicast groups but not statically joined multicast groups.
- If the configured *limit* value is smaller than the number of the existing multicast groups on the current interface, the system does not automatically remove the multicast groups in excess. To bring this configuration into effect in this case, you need to use the **reset igmp group** command to clear the IGMP multicast group information manually.
- you can also use the **igmp group-limit** command to limit the number of groups on an interface. If you configure a limit of the number of groups for ports in a VLAN while you have configured a limit of the number of groups for a VLAN interface, or vice versa, this may cause inconsistencies between Layer 2 and Layer 3 table entries. Therefore, it is recommended to configure a limit of the number of multicast groups only on the VLAN interface.

Related commands: **igmp static-group**, **reset igmp group**; **igmp-snooping group-limit** in *IGMP Snooping Commands* in the *IP Multicast Volume*.

## Examples

```
# Limit the number of the multicast groups that can be joined on VLAN-interface 100 to 128.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp group-limit 128
```

## igmp group-policy

### Syntax

```
igmp group-policy acl-number [ version-number ]
undo igmp group-policy
```

### View

Interface view

## Default Level

2: System level

## Parameters

*acl-number*: Basic or advanced ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced ACL rule is used to match the multicast source address(es) specified in IGMPv3 reports, rather than the source address in the IP packets. The system assumes that an IGMPv1 or IGMPv2 report or an IGMPv3 IS\_EX and TO\_EX report that does not carry a multicast source address carries a multicast source address of 0.0.0.0..

*version-number*: IGMP version, in the range of 1 to 3. If you do not specify an IGMP version, the configured group filter will apply to IGMP reports of all versions.

## Description

Use the **igmp group-policy** command to configure a multicast group filter on the current interface to control joins to specific multicast groups.

Use the **undo igmp group-policy** command to remove the configured multicast group filter.

By default, no multicast group filter is configured, namely a host can join any valid multicast group.

## Examples

# Configure an ACL rule so that hosts on the subnet attached to VLAN-interface 100 can join multicast group 225.1.1.1 only.

```
<Sysname> system-view
[Sysname] acl number 2005
[Sysname-acl-basic-2005] rule permit source 225.1.1.1 0
[Sysname-acl-basic-2005] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp group-policy 2005
```

## igmp last-member-query-interval

### Syntax

**igmp last-member-query-interval** *interval*

**undo igmp last-member-query-interval**

### View

Interface view

### Default Level

2: System level

### Parameters

*interval*: IGMP last member query interval in seconds, with an effective range of 1 to 5.

### Description

Use the **igmp last-member-query-interval** command to configure the last member query interval, namely the length of time the device waits between sending IGMP group-specific queries, on the current interface.

Use the **undo igmp last-member-query-interval** command to restore the system default.

By default, the IGMP last member query interval is 1 second.

Related commands: **last-member-query-interval**, **igmp robust-count**, **display igmp interface**.

## Examples

```
# Set the IGMP last member query interval to 3 seconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp last-member-query-interval 3
```

## igmp max-response-time

### Syntax

```
igmp max-response-time interval
undo igmp max-response-time
```

### View

Interface view

### Default Level

2: System level

### Parameters

*interval*: Maximum response time in seconds for IGMP general queries, with an effective range of 1 to 25.

### Description

Use the **igmp max-response-time** command to configure the maximum response time for IGMP general queries on the current interface.

Use the **undo igmp max-response-time** command to restore the system default.

By default, the maximum response time for IGMP general queries is 10 seconds.

Related commands: **max-response-time**, **igmp timer other-querier-present**, **display igmp interface**.

## Examples

```
# Set the maximum response time for IGMP general queries to 8 seconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp max-response-time 8
```

## igmp proxying enable

### Syntax

```
igmp proxying enable
undo igmp proxying enable
```

## View

Interface view

## Default Level

2: System level

## Parameters

None

## Description

Use the **igmp proxying enable** command to enable IGMP proxying on an interface.

Use the **undo igmp proxying enable** command to disable IGMP proxying on the interface.

By default, IGMP proxying is disabled.

Note that:

- This command takes effect only after IP multicast routing is enabled.
- If IGMP proxying is enabled on a loopback interface, the proxy device maintains only the IGMP routing table without adding the IGMP routes to the multicast routing table or forwarding table.

Related commands: **multicast routing-enable** in *Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*.

## Examples

# Enable IP multicast routing on the public instance and enable IGMP proxying on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp proxying enable
```

## Igmp proxying forwarding

### Syntax

**igmp proxying forwarding**

**undo igmp proxying forwarding**

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **igmp proxying forwarding** command to enable a non-querier downstream interface to forward multicast traffic.

Use the **undo igmp proxying forwarding** command to disable the forwarding capability of a non-querier downstream interface.

By default, a non-querier downstream interface does not forward multicast traffic.

## Examples

# Enable the multicast forwarding capability on VLAN-interface 100, a non-querier downstream interface on the IGMP proxy device.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp proxying forwarding
```

## igmp require-router-alert

### Syntax

```
igmp require-router-alert
undo igmp require-router-alert
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **igmp require-router-alert** command to configure the interface to discard IGMP messages that do not carry the Router-Alert option.

Use the **undo igmp require-router-alert** command to restore the default configuration.

By default, the device does not check the Router-Alert option, namely it passes all the IGMP messages it receives to the upper layer protocol for processing.

Related commands: **require-router-alert**, **igmp send-router-alert**.

## Examples

# Configure VLAN-interface 100 to discard IGMP messages that do not carry the Router-Alert option.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp require-router-alert
```

## igmp robust-count

### Syntax

```
igmp robust-count robust-value
undo igmp robust-count
```

## View

Interface view

## Default Level

2: System level

## Parameters

*robust-value*: IGMP querier robustness variable, with an effective range of 2 to 5. The IGMP robustness variable determines the default number of general queries the IGMP querier sends on startup and the number of IGMP group-specific queries the IGMP querier sends upon receiving an IGMP leave message.

## Description

Use the **igmp robust-count** command to configure the IGMP querier robustness variable on the current interface.

Use the **undo igmp robust-count** command to restore the system default.

By default, the IGMP querier robustness variable is 2.

Related commands: **robust-count**, **igmp timer query**, **igmp last-member-query-interval**, **igmp timer other-querier-present**, **display igmp interface**.

## Examples

```
# Set the IGMP querier robustness variable to 3 on VLAN-interface 100.
```

```
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] igmp robust-count 3
```

## igmp send-router-alert

### Syntax

```
igmp send-router-alert  
undo igmp send-router-alert
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **igmp send-router-alert** command on the current interface to enable insertion of the Router-Alert option in IGMP messages to be sent.

Use the **undo igmp send-router-alert** command on the current interface to disable insertion of the Router-Alert option in IGMP messages to be sent.

By default, IGMP messages are sent with the Router-Alert option.

Related commands: **send-router-alert**, **igmp require-router-alert**.

## Examples

```
# Disable insertion of the Router-Alert option into IGMP messages that leave VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo igmp send-router-alert
```

## igmp ssm-mapping enable

### Syntax

```
igmp ssm-mapping enable
undo igmp ssm-mapping enable
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **igmp ssm-mapping enable** command to enable the IGMP SSM mapping feature on the current interface.

Use the **undo igmp ssm-mapping enable** command to disable the IGMP SSM mapping feature on the current interface.

By default, the IGMP SSM mapping feature is disabled on all interfaces.

## Examples

```
# Enable the IGMP SSM mapping feature on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp ssm-mapping enable
```

## igmp startup-query-count

### Syntax

```
igmp startup-query-count value
undo igmp startup-query-count
```

### View

Interface view

## Default Level

2: System level

## Parameters

*value*: Startup query count, namely, the number of queries the IGMP querier sends on startup, with an effective range of 2 to 5.

## Description

Use the **igmp startup-query-count** command to configure the startup query count on the current interface.

Use the **undo igmp startup-query-count** command to restore the system default.

By default, the startup query count is set to the IGMP querier robustness variable.



### Note

By default, the IGMP querier robustness variable is 2, so the startup query count is also 2.

---

Related commands: **startup-query-count**, **igmp robust-count**.

## Examples

# Set the startup query count to 3 on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp startup-query-count 3
```

## igmp startup-query-interval

### Syntax

**igmp startup-query-interval** *interval*

**undo igmp startup-query-interval**

### View

Interface view

## Default Level

2: System level

## Parameters

*interval*: Startup query interval in seconds, namely, the interval between general queries the IGMP querier sends on startup, with an effective range of 1 to 18000.

## Description

Use the **igmp startup-query-interval** command to configure the startup query interval on the current interface.

Use the **undo igmp startup-query-interval** command to restore the system default.  
By default, the startup query interval is 1/4 of the IGMP query interval.



By default, the IGMP query interval is 60 seconds, so the startup query interval = 60 / 4 = 15 (seconds).

---

Related commands: **startup-query-interval**, **igmp timer query**.

### Examples

# Set the startup query interval to 5 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp startup-query-interval 5
```

### igmp static-group

#### Syntax

```
igmp static-group group-address [ source source-address ]
undo igmp static-group { all | group-address [ source source-address ] }
```

#### View

Interface view

#### Default Level

2: System level

#### Parameters

*group-address*: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

*source-address*: Multicast source address.

**all**: Specifies to remove all static multicast groups that the current interface has joined.

#### Description

Use the **igmp static-group** command to configure the current interface to be a statically connected member of the specified multicast group or multicast source and group.

Use the **undo igmp static-group** command to restore the system default.

By default, an interface is not a static member of any multicast group or multicast source and group.

If the specified multicast address is in the SSM multicast address range, you must specify a multicast source address at the same time; otherwise IGMP routing table entries cannot be established. There is no such a restriction if the specified multicast group address is not in the SSM multicast address range.

### Examples

# Configure VLAN-interface 100 to be a statically connected member of multicast group 224.1.1.1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp static-group 224.1.1.1

# Configure VLAN-interface 100 to be a statically connected member of multicast source and group
(192.168.1.1, 232.1.1.1).

<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp static-group 232.1.1.1 source 192.168.1.1
```

## igmp timer other-querier-present

### Syntax

```
igmp timer other-querier-present interval
undo igmp timer other-querier-present
```

### View

Interface view

### Default Level

2: System level

### Parameters

*interval*: IGMP other querier present interval in seconds, in the range of 60 to 300.

### Description

Use the **igmp timer other-querier-present** command to configure the IGMP other querier present interval on the current interface.

Use the **undo igmp timer other-querier-present** command to restore the system default.

By default, the IGMP other querier present interval is [ IGMP query interval ] times [ IGMP querier robustness variable ] plus [ maximum response time for IGMP general queries ] divided by two.



#### Note

By default, the three parameters in the above-mentioned formula are 60 (seconds), 2 and 10 (seconds) respectively, so the IGMP other querier present interval =  $60 \times 2 + 10 / 2 = 125$  (seconds).

---

Related commands: **timer other-querier-present**, **igmp timer query**, **igmp robust-count**, **igmp max-response-time**, **display igmp interface**.

### Examples

```
# Set the IGMP other querier present interval to 200 seconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp timer other-querier-present 200
```

## igmp timer query

### Syntax

```
igmp timer query interval  
undo igmp timer query
```

### View

Interface view

### Default Level

2: System level

### Parameters

*interval*: IGMP query interval in seconds, namely the interval between IGMP general queries, with an effective range of 1 to 18,000.

### Description

Use the **igmp timer query** command to configure the IGMP query interval on the current interface.

Use the **undo igmp timer query** command to restore the system default.

By default, the IGMP query interval is 60 seconds.

Related commands: **timer query**, **igmp timer other-querier-present**, **display igmp interface**.

### Examples

```
# Set the IGMP query interval to 125 seconds on VLAN-interface 100.
```

```
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] igmp timer query 125
```

## igmp version

### Syntax

```
igmp version version-number  
undo igmp version
```

### View

Interface view

### Default Level

2: System level

### Parameters

*version-number*: IGMP version, in the range of 1 to 3.

### Description

Use the **igmp version** command to configure the IGMP version on the current interface.

Use the **undo igmp version** command to restore the default IGMP version.

The default IGMP version is version 2.

Related commands: **version**.

## Examples

```
# Set the IGMP version to IGMPv1 on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp version 1
```

## last-member-query-interval (IGMP view)

### Syntax

```
last-member-query-interval interval
undo last-member-query-interval
```

### View

IGMP view

### Default Level

2: System level

### Parameters

*interval*: Last-member query interval in seconds, with an effective range of 1 to 5.

### Description

Use the **last-member-query-interval** command to configure the global IGMP last-member query interval.

Use the **undo last-member-query-interval** command to restore the system default.

By default, the IGMP last-member query interval is 1 second.

Related commands: **igmp last-member-query-interval**, **robust-count**, **display igmp interface**.

## Examples

```
# Set the global IGMP last-member interval to 3 seconds.
```

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] last-member-query-interval 3
```

## max-response-time (IGMP view)

### Syntax

```
max-response-time interval
undo max-response-time
```

### View

IGMP view

## Default Level

2: System level

## Parameters

*interval*: Maximum response time for IGMP general queries in seconds, with an effective range of 1 to 25.

## Description

Use the **max-response-time** command to configure the maximum response time for IGMP general queries globally.

Use the **undo max-response-time** command to restore the system default.

By default, the maximum response time for IGMP general queries is 10 seconds.

Related commands: **igmp max-response-time**, **timer other-querier-present**, **display igmp interface**.

## Examples

```
# Set the maximum response time for IGMP general queries to 8 seconds globally.
```

```
<Sysname> system-view  
[Sysname] igmp  
[Sysname-igmp] max-response-time 8
```

## require-router-alert (IGMP view)

### Syntax

```
require-router-alert  
undo require-router-alert
```

### View

IGMP view

## Default Level

2: System level

## Parameters

None

## Description

Use the **require-router-alert** command to configure globally the router to discard IGMP messages that do not carry the Router-Alert option.

Use the **undo require-router-alert** command to restore the system default.

By default, the device does not check the Router-Alert option, namely it handles all the IGMP messages it received to the upper layer protocol for processing.

Related commands: **igmp require-router-alert**, **send-router-alert**.

## Examples

```
# Globally configure the router to discard IGMP messages that do not carry the Router-Alert option.
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] require-router-alert
```

## reset igmp group

### Syntax

```
reset igmp group { all | interface interface-type interface-number } { all | group-address [ mask { mask | mask-length } ] [ source-address [ mask { mask | mask-length } ] ] }
```

### View

User view

### Default Level

2: System level

### Parameters

**all**: The first **all** specifies to clear IGMP multicast group information on all interfaces, while the second **all** specifies to clear the information of all IGMP multicast groups.

**interface** *interface-type interface-number*: Clears IGMP multicast information on the specified interface.

*group-address*: Multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

*source-address*: Multicast source address.

*mask*: Subnet mask of the multicast group/source address, 255.255.255.255 by default.

*mask-length*: Subnet mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases.

### Description

Use the **reset igmp group** command to clear IGMP multicast group information.

Note that, This command cannot clear IGMP multicast group information of static joins.

Related commands: **display igmp group**.

### Examples

```
# Clear all IGMP multicast group information on all interfaces.
```

```
<Sysname> reset igmp group all
```

```
# Clear all IGMP multicast group information on VLAN-interface 100.
```

```
<Sysname> reset igmp group interface vlan-interface 100 all
```

```
# Clear IGMP multicast group information about multicast group 225.0.0.1 on VLAN-interface 100.
```

```
<Sysname> reset igmp group interface vlan-interface 100 225.0.0.1
```

## reset igmp group port-info

### Syntax

```
reset igmp group port-info { all | group-address } [ vlan vlan-id ]
```

### View

User view

### Default Level

2: System level

### Parameters

**all**: Clears Layer 2 port information of all the IGMP multicast groups.

*group-address*: Clears Layer 2 port information of the specified IGMP multicast group. The effective range of *group-address* is 224.0.1.0 to 239.255.255.255.

*vlan-id*: Clears Layer 2 port information of IGMP multicast groups in the specified VLAN. The effective range of *vlan-id* is 1 to 4094.

### Description

Use the **reset igmp group port-info** command to clear Layer 2 port information of IGMP multicast groups.

Note that:

- Layer 2 ports for IGMP multicast groups include member ports and router ports.
- This command cannot clear Layer 2 port information about IGMP multicast groups of static joins.

Related commands: **display igmp group port-info**.

### Examples

```
# Clear Layer 2 port information of all IGMP multicast groups in all VLANs.
```

```
<Sysname> reset igmp group port-info all
```

```
# Clear Layer 2 port information of all IGMP multicast groups in VLAN 100.
```

```
<Sysname> reset igmp group port-info all vlan 100
```

```
# Clear Layer 2 port information about multicast group 225.0.0.1 in VLAN 100.
```

```
<Sysname> reset igmp group port-info 225.0.0.1 vlan 100
```

## reset igmp ssm-mapping group

### Syntax

```
reset igmp ssm-mapping group { all | interface interface-type interface-number { all | group-address  
[ mask { mask | mask-length } ] [ source-address [ mask { mask | mask-length } ] ] }
```

### View

User view

### Default Level

2: System level

## Parameters

**all**: The first **all** specifies to clear multicast group information created based on the configured IGMP SSM mappings on all interfaces, while the second **all** specifies to clear all multicast group information created based on the configured IGMP SSM mappings.

*interface-type interface-number*: Specifies an interface by its type and number.

*group-address*: Specifies a multicast group by its IP address, in the range of 224.0.0.0 to 239.255.255.255.

*source-address*: Specifies a multicast source by its IP address.

*mask*: Subnet mask of the multicast group/source address, 255.255.255.255 by default.

*mask-length*: Subnet mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a multicast source address, this argument has an effective value range of 0 to 32. For both cases, the default value is 32.

## Description

Use the **reset igmp ssm-mapping group** command to clear multicast group information created based on the configured IGMP SSM mappings.

Related commands: **display igmp ssm-mapping group**.

## Examples

# Clear all multicast group information created based on the configured IGMP SSM mappings on all interfaces.

```
<Sysname> reset igmp ssm-mapping group all
```

## robust-count (IGMP view)

### Syntax

**robust-count** *robust-value*

**undo robust-count**

### View

IGMP view

### Default Level

2: System level

### Parameters

*robust-value*: IGMP querier robustness variable, with an effective range of 2 to 5. The IGMP robustness variable determines the default number of general queries the IGMP querier sends on startup and the number of IGMP group-specific queries the IGMP querier sends upon receiving an IGMP leave message.

### Description

Use the **robust-count** command to configure the IGMP querier robustness variable globally.

Use the **undo robust-count** command to restore the system default.

By default, the IGMP querier robustness variable is 2.

Related commands: **igmp robust-count**, **timer query**, **last-member-query-interval**, **timer other-querier-present**, **display igmp interface**.

## Examples

# Set the IGMP querier robustness variable to 3 globally.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] robust-count 3
```

## send-router-alert (IGMP view)

### Syntax

```
send-router-alert
undo send-router-alert
```

### View

IGMP view

### Default Level

2: System level

### Parameters

None

### Description

Use the **send-router-alert** command to globally enable insertion of the Router-Alert option into IGMP messages to be sent.

Use the **undo send-router-alert** command to globally disable insertion of the Router-Alert option into IGMP messages to be sent.

By default, an IGMP message carries the Router-Alert option.

Related commands: **igmp send-router-alert**, **require-router-alert**.

## Examples

# Globally disable the insertion of the Router-Alert option in IGMP messages to be sent.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] undo send-router-alert
```

## ssm-mapping (IGMP view)

### Syntax

```
ssm-mapping group-address { mask | mask-length } source-address
undo ssm-mapping { group-address { mask | mask-length } source-address | all }
```

### View

IGMP view

## Default Level

2: System level

## Parameters

*group-address*: Specifies a multicast group by its IP address, in the range of 224.0.0.0 to 239.255.255.255.

*mask*: Subnet mask of the multicast group address.

*mask-length*: Subnet mask length of the multicast group address, in the range of 4 to 32.

*source-address*: Specifies a multicast source by its IP address.

**all**: Removes all IGMP SSM mappings.

## Description

Use the **ssm-mapping** command to configure an IGMP SSM mapping.

Use the **undo ssm-mapping** command to remove one or all IGMP SSM mappings.

By default, no IGMP SSM mappings are configured.

Related commands: **igmp ssm-mapping enable**, **display igmp ssm-mapping**.

## Examples

```
# Configure an IGMP SSM mapping for multicast group 225.1.1.1/32 and multicast source 125.1.1.1.
```

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] ssm-mapping 225.1.1.1 32 125.1.1.1
```

## startup-query-count (IGMP view)

### Syntax

```
startup-query-count value
```

```
undo startup-query-count
```

### View

IGMP view

## Default Level

2: System level

## Parameters

*value*: Startup query count, namely, the number of queries the IGMP querier sends on startup, with an effective range of 2 to 5.

## Description

Use the **startup-query-count** command to configure the startup query count globally.

Use the **undo startup-query-count** command to restore the system default.

By default, the startup query count is set to the IGMP querier robustness variable.



#### Note

By default, the IGMP querier robustness variable is 2, so the startup query count is also 2.

---

Related commands: **igmp startup-query-count**, **robust-count**.

#### Examples

```
# Set the startup query count to 3 globally.
```

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] startup-query-count 3
```

### startup-query-interval (IGMP view)

#### Syntax

```
startup-query-interval interval
```

```
undo startup-query-interval
```

#### View

IGMP view

#### Default Level

2: System level

#### Parameters

*interval*: Startup query interval in seconds, namely, the interval between general queries the IGMP querier sends on startup, with an effective range of 1 to 18000.

#### Description

Use the **startup-query-interval** command to configure the startup query interval globally.

Use the **undo startup-query-interval** command to restore the system default.

By default, the startup query interval is 1/4 of the “IGMP query interval”.



#### Note

By default, the IGMP query interval is 60 seconds, so the startup query interval =  $60 / 4 = 15$  (seconds).

---

Related commands: **igmp-startup-query-interval**, **timer query**.

#### Examples

```
# Set the startup query interval to 5 seconds globally.
```

```
<Sysname> system-view
```

```
[Sysname] igmp
[Sysname-igmp] startup-query-interval 5
```

## timer other-querier-present (IGMP view)

### Syntax

```
timer other-querier-present interval
undo timer other-querier-present
```

### View

IGMP view

### Default Level

2: System level

### Parameters

*interval*: IGMP other querier present interval, in the range of 60 to 300.

### Description

Use the **timer other-querier-present** command to configure the IGMP other querier present interval globally.

Use the **undo timer other-querier-present** command to restore the system default.

By default, the IGMP other querier present interval is [ IGMP query interval ] times [ IGMP querier robustness variable ] plus [ maximum response time for IGMP general queries ] divided by two.



### Note

By default, the three parameters in the above-mentioned formula are 60 (seconds), 2 (times) and 10 (seconds) respectively, so the IGMP other querier present interval =  $60 \times 2 + 10 / 2 = 125$  (seconds).

---

Related commands: **igmp timer other-querier-present**, **timer query**, **robust-count**, **max-response-time**, **display igmp interface**.

### Examples

# Set the IGMP other querier present interval to 200 seconds globally.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] timer other-querier-present 200
```

## timer query (IGMP view)

### Syntax

```
timer query interval
undo timer query
```

## View

IGMP view

## Default Level

2: System level

## Parameters

*interval*: IGMP query interval in seconds, namely interval between IGMP general queries, with an effective range of 1 to 18,000.

## Description

Use the **timer query** command to configure the IGMP query interval globally.

Use the **undo timer query** command to restore the default setting.

By default, IGMP query interval is 60 seconds.

Related commands: **igmp timer query**, **timer other-querier-present**, **display igmp interface**.

## Examples

```
# Set the IGMP query interval to 125 seconds globally.
```

```
<Sysname> system-view  
[Sysname] igmp  
[Sysname-igmp] timer query 125
```

## version (IGMP view)

### Syntax

```
version version-number  
undo version
```

### View

IGMP view

### Default Level

2: System level

### Parameters

*version-number*: IGMP version, in the range of 1 to 3.

### Description

Use the **version** command to configure the IGMP version globally.

Use the **undo version** command to restore the system default.

The default IGMP version is version 2.

Related commands: **igmp version**.

### Examples

```
# Set the global IGMP version to IGMPv1.
```

```
<Sysname> system-view  
[Sysname] igmp  
[Sysname-igmp] version 1
```

# Table of Contents

<b>1 PIM Configuration Commands</b> .....	<b>1-1</b>
PIM Configuration Commands .....	1-1
auto-rp enable .....	1-1
bsr-policy (PIM view) .....	1-2
c-bsr (PIM view) .....	1-2
c-bsr admin-scope .....	1-3
c-bsr global .....	1-4
c-bsr group .....	1-4
c-bsr hash-length (PIM view) .....	1-5
c-bsr holdtime (PIM view) .....	1-6
c-bsr interval (PIM view) .....	1-6
c-bsr priority (PIM view) .....	1-7
c-rp (PIM view) .....	1-8
c-rp advertisement-interval (PIM view) .....	1-9
c-rp holdtime (PIM view) .....	1-10
crp-policy (PIM view) .....	1-10
display pim bsr-info .....	1-11
display pim claimed-route .....	1-13
display pim control-message counters .....	1-14
display pim grafts .....	1-16
display pim interface .....	1-16
display pim join-prune .....	1-18
display pim neighbor .....	1-20
display pim routing-table .....	1-21
display pim rp-info .....	1-23
hello-option dr-priority (PIM view) .....	1-25
hello-option holdtime (PIM view) .....	1-25
hello-option lan-delay (PIM view) .....	1-26
hello-option neighbor-tracking (PIM view) .....	1-26
hello-option override-interval (PIM view) .....	1-27
holdtime assert (PIM view) .....	1-28
holdtime join-prune (PIM view) .....	1-28
jp-pkt-size (PIM view) .....	1-29
jp-queue-size (PIM view) .....	1-30
pim .....	1-30
pim bsr-boundary .....	1-31
pim dm .....	1-32
pim hello-option dr-priority .....	1-32
pim hello-option holdtime .....	1-33
pim hello-option lan-delay .....	1-34
pim hello-option neighbor-tracking .....	1-34
pim hello-option override-interval .....	1-35
pim holdtime assert .....	1-36

pim holdtime join-prune .....	1-36
pim neighbor-policy .....	1-37
pim require-genid.....	1-38
pim sm .....	1-38
pim state-refresh-capable.....	1-39
pim timer graft-retry .....	1-39
pim timer hello .....	1-40
pim timer join-prune.....	1-41
pim triggered-hello-delay .....	1-41
probe-interval (PIM view).....	1-42
register-policy (PIM view) .....	1-42
register-suppression-timeout (PIM view).....	1-43
register-whole-checksum (PIM view) .....	1-44
reset pim control-message counters .....	1-44
source-lifetime (PIM view) .....	1-45
source-policy (PIM view) .....	1-45
spt-switch-threshold (PIM view) .....	1-46
ssm-policy (PIM view).....	1-47
state-refresh-interval (PIM view) .....	1-48
state-refresh-rate-limit (PIM view) .....	1-49
state-refresh-ttl .....	1-49
static-rp (PIM view).....	1-50
timer hello (PIM view).....	1-51
timer join-prune (PIM view) .....	1-51

# 1 PIM Configuration Commands

---



## Note

The term “router” in this document refers to a router in a generic sense or a Layer 3 switch running the PIM protocol.

---

## PIM Configuration Commands

### auto-rp enable

#### Syntax

**auto-rp enable**

**undo auto-rp enable**

#### View

PIM view

#### Default Level

2: System level

#### Parameters

None

#### Description

Use the **auto-rp enable** command to enable auto-RP.

Use the **undo auto-rp enable** command to disable auto-RP.

By default, auto-RP is disabled.

Related commands: **static-rp**.

#### Examples

```
# Enable auto-RP.
```

```
<Sysname> system-view
```

```
[Sysname] pim
```

```
[Sysname-pim] auto-rp enable
```

## bsr-policy (PIM view)

### Syntax

```
bsr-policy acl-number  
undo bsr-policy
```

### View

PIM view

### Default Level

2: System level

### Parameters

*acl-number*: Basic ACL number, in the range of 2000 to 2999. When an ACL is defined, the **source** keyword in the **rule** command specifies a legal BSR source address range.

### Description

Use the **bsr-policy** command to configure a legal BSR address range to guard against BSR spoofing.

Use the **undo bsr-policy** command to remove the restriction of the BSR address range.

By default, there are no restrictions on the BSR address range, namely the bootstrap messages from any source are regarded to be valid.

### Examples

# Configure a legal BSR address range so that only routers on the segment 10.1.1.0/24 can become the BSR.

```
<Sysname> system-view  
[Sysname] acl number 2000  
[Sysname-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255  
[Sysname-acl-basic-2000] quit  
[Sysname] pim  
[Sysname-pim] bsr-policy 2000
```

## c-bsr (PIM view)

### Syntax

```
c-bsr interface-type interface-number [ hash-length [ priority ] ]  
undo c-bsr
```

### View

PIM view

### Default Level

2: System level

### Parameters

*interface-type interface-number*: Specifies an interface by its type and number.

*hash-length*: Hash mask length, in the range of 0 to 32. If you do not include this argument in your command, the corresponding global setting will be used.

*priority*: Priority of the C-BSR, in the range of 0 to 255. If you do not include this argument in your command, the corresponding global setting will be used. A larger value of this argument means a higher priority.

## Description

Use the **c-bsr** command to configure the specified interface as a C-BSR.

Use the **undo c-bsr** command to remove the related C-BSR configuration.

No C-BSR is configured by default.

Note that PIM-SM must be enabled on the interface to be configured as a C-BSR.

Related commands: **pim sm**, **c-bsr hash-length**, **c-bsr priority**, **c-rp**.

## Examples

```
# Configure VLAN-interface 100 to be a C-BSR.
```

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr vlan-interface 100
```

## c-bsr admin-scope

### Syntax

```
c-bsr admin-scope
undo c-bsr admin-scope
```

### View

PIM view

### Default Level

2: System level

### Parameters

None

## Description

Use the **c-bsr admin-scope** command to enable administrative scoping.

Use the **undo c-bsr admin-scope** command to disable administrative scoping.

By default, BSR administrative scoping is disabled, namely there is only one BSR in a PIM-SM domain.

Related commands: **c-bsr**, **c-bsr group**, **c-bsr global**.

## Examples

```
# Enable administrative scoping.
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr admin-scope
```

## c-bsr global

### Syntax

```
c-bsr global [ hash-length hash-length | priority priority ] *  
undo c-bsr global
```

### View

PIM view

### Default Level

2: System level

### Parameters

*hash-length*: Hash mask length in the global scope zone, in the range of 0 to 32. If you do not include this argument in your command, the corresponding global setting will be used.

*priority*: Priority of the C-BSR in the global scope zone, in the range of 0 to 255. If you do not include this argument in your command, the corresponding global setting will be used. A larger value of this argument means a higher priority.

### Description

Use the **c-bsr global** command to configure a C-BSR for the global scope zone.

Use the **undo c-bsr global** command to remove the C-BSR configuration for the global scope zone.

By default, no C-BSRs are configured for the global scope zone.

Related commands: **c-bsr group**, **c-bsr hash-length**, **c-bsr priority**.

### Examples

```
# Configure the router to be a C-BSR for the global scope zone, with the priority of 1.
```

```
<Sysname> system-view  
[Sysname] pim  
[Sysname-pim] c-bsr global priority 1
```

## c-bsr group

### Syntax

```
c-bsr group group-address { mask | mask-length } [ hash-length hash-length | priority priority ] *  
undo c-bsr group group-address
```

### View

PIM view

### Default Level

2: System level

### Parameters

*group-address*: Multicast group address, in the range of 239.0.0.0 to 239.255.255.255.

*mask*: Mask of the multicast group address.

*mask-length*: Mask length of the multicast group address, in the range of 8 to 32.

*hash-length*: Hash mask length in the admin-scope region corresponding to the specified multicast group, in the range of 0 to 32. If you do not include this argument in your command, the corresponding global setting will be used.

*priority*: Priority of the C-BSR in the admin-scope region corresponding to a multicast group, in the range of 0 to 255. If you do not include this argument in your command, the corresponding global setting will be used. A larger value of this argument means a higher priority.

## Description

Use the **c-bsr group** command to configure a C-BSR for the admin-scope region associated with the specified group.

Use the **undo c-bsr group** command to remove the C-BSR configuration for the admin-scope region associated with the specified group.

By default, no C-BSRs are configured for admin-scope regions.

Related commands: **c-bsr global**, **c-bsr admin-scope**, **c-bsr hash-length**, **c-bsr priority**.

## Examples

# Configure the router to be a C-BSR in the admin-scope region associated with the multicast group address 239.0.0.0/8, with the priority of 10.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr group 239.0.0.0 255.0.0.0 priority 10
```

## c-bsr hash-length (PIM view)

### Syntax

**c-bsr hash-length** *hash-length*

**undo c-bsr hash-length**

### View

PIM view

### Default Level

2: System level

### Parameters

*hash-length*: Hash mask length, in the range of 0 to 32.

## Description

Use the **c-bsr hash-length** command to configure the global Hash mask length .

Use the **undo c-bsr hash-length** command to restore the system default.

By default, the Hash mask length is 30.

Related commands: **c-bsr**, **c-bsr global**, **c-bsr group**.

## Examples

```
# Set the global Hash mask length to 16.
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr hash-length 16
```

## c-bsr holdtime (PIM view)

### Syntax

```
c-bsr holdtime interval
undo c-bsr holdtime
```

### View

PIM view

### Default Level

2: System level

### Parameters

*interval*: BS timeout in seconds, with an effective range of 1 to 2,147,483,647.

### Description

Use the **c-bsr holdtime** command to configure the BS timeout, namely the length of time a C-BSR waits before it must receive a bootstrap message from the BSR.

Use the **undo c-bsr holdtime** command to restore the system default.

By default, the bootstrap timeout value is determined by this formula: BS timeout = BS period × 2 + 10.



### Note

The default BS period is 60 seconds, so the default BS timeout = 60 × 2 + 10 = 130 (seconds).

---

Related commands: **c-bsr**, **c-bsr interval**.

## Examples

```
# Set the BS timeout time to 150 seconds.
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr holdtime 150
```

## c-bsr interval (PIM view)

### Syntax

```
c-bsr interval interval
```

## undo c-bsr interval

### View

PIM view

### Default Level

2: System level

### Parameters

*interval*: BS period in seconds, with an effective range of 1 to 2,147,483,647.

### Description

Use the **c-bsr interval** command to configure the BS period, namely the interval at which the BSR sends bootstrap messages.

Use the **undo c-bsr interval** command to restore the system default.

By default, the BS period value is determined by this formula: BS period = (BS timeout – 10) ÷ 2.



#### Note

The default BS timeout is 130 seconds, so the default BS period = (130 – 10) ÷ 2 = 60 (seconds).

---

Related commands: **c-bsr**, **c-bsr holdtime**.

### Examples

```
# Set the BS period to 30 seconds.  
<Sysname> system-view  
[Sysname] pim  
[Sysname-pim] c-bsr interval 30
```

## c-bsr priority (PIM view)

### Syntax

```
c-bsr priority priority  
undo c-bsr priority
```

### View

PIM view

### Default Level

2: System level

### Parameters

*priority*: Priority of the C-BSR, in the range of 0 to 255. A larger value of this argument means a higher priority.

## Description

Use the **c-bsr priority** command to configure the global C-BSR priority.

Use the **undo c-bsr priority** command to restore the system default.

By default, the C-BSR priority is 0.

Related commands: **c-bsr**, **c-bsr global**, **c-bsr group**.

## Examples

```
# Set the global C-BSR priority to 5.
```

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr priority 5
```

## c-rp (PIM view)

### Syntax

```
c-rp interface-type interface-number [ group-policy acl-number | priority priority | holdtime hold-interval | advertisement-interval adv-interval ] *
```

```
undo c-rp interface-type interface-number
```

### View

PIM view

### Default Level

2: System level

### Parameters

*interface-type interface-number*: Specifies an interface by its type and number.

*acl-number*: Basic ACL number, in the range of 2000 to 2999. This ACL defines a range of multicast groups the C-RP is going to serve, rather than defining a filtering rule. Any group range matching the **permit** statement in the ACL will be advertised as an RP served group, while configurations matching other statements like **deny** will not take effect.

*priority*: Priority of the C-RP, in the range of 0 to 255 and defaulting to 0. A larger value of this argument means a lower priority.

*hold-interval*: C-RP timeout time, in seconds. The effective range is 1 to 65,535. If you do not provide this argument in your command, the corresponding global setting will be used.

*adv-interval*: C-RP-Adv interval in seconds, with an effective range of 1 to 65,535. If you do not provide this argument in your command, the corresponding global setting will be used.

## Description

Use the **c-rp** command to configure the specified interface as a C-RP.

Use the **undo c-rp** command to remove the related C-RP configuration.

No C-RPs are configured by default.

Note that:

- PIM-SM must be enabled on the interface to be configured as a C-RP.

- If you do not specify a group range for the C-RP, the C-RP will serve all multicast groups.
- If you wish a router to be a C-RP for multiple group ranges, you need to include these multiple group ranges in multiple rules in the ACL corresponding to the **group-policy** keyword.
- If you carry out this command repeatedly on the same interface, the last configuration will take effect.

Related commands: **c-bsr**.

## Examples

# Configure VLAN-interface 100 to be a C-RP for multicast groups 225.1.0.0/16 and 226.2.0.0/16, with a priority of 10.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 225.1.0.0 0.0.255.255
[Sysname-acl-basic-2000] rule permit source 226.2.0.0 0.0.255.255
[Sysname-acl-basic-2000] quit
[Sysname] pim
[Sysname-pim] c-rp vlan-interface 100 group-policy 2000 priority 10
```

## c-rp advertisement-interval (PIM view)

### Syntax

**c-rp advertisement-interval** *interval*

**undo c-rp advertisement-interval**

### View

PIM view

### Default Level

2: System level

### Parameters

*interval*: C-RP-Adv interval in seconds, with an effective range of 1 to 65,535.

### Description

Use the **c-rp advertisement-interval** command to configure the interval at which C-RP-Adv messages are sent.

Use the **undo c-rp advertisement-interval** command to restore the system default.

By default, the C-RP-Adv interval is 60 seconds.

Related commands: **c-rp**.

## Examples

# Set the global C-RP-Adv interval to 30 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-rp advertisement-interval 30
```

## c-rp holdtime (PIM view)

### Syntax

```
c-rp holdtime interval  
undo c-rp holdtime
```

### View

PIM view

### Default Level

2: System level

### Parameters

*interval*: C-RP timeout in seconds, with an effective range of 1 to 65,535.

### Description

Use the **c-rp holdtime** command to configure the global C-RP timeout time, namely the length of time the BSR waits before it must receive a C-RP-Adv message.

Use the **undo c-rp holdtime** command to restore the system default.

By default, the C-RP timeout time is 150 seconds.

Because a non-BSR router refreshes its C-RP timeout time through BSR bootstrap messages, to prevent loss of C-RP information in BSR bootstrap messages, make sure that the C-RP timeout time is not smaller than the interval at which the BSR sends bootstrap messages. The recommended C-RP timeout setting is 2.5 times the BS period or longer.

Related commands: **c-rp**, **c-bsr interval**.

### Examples

# Set the global C-RP timeout time to 200 seconds.

```
<Sysname> system-view  
[Sysname] pim  
[Sysname-pim] c-rp holdtime 200
```

## crp-policy (PIM view)

### Syntax

```
crp-policy acl-number  
undo crp-policy
```

### View

PIM view

### Default Level

2: System level

## Parameters

*acl-number*: Advanced ACL number, in the range of 3000 to 3999. When the ACL is defined, the **source** keyword in the **rule** command specifies the address of a C-RP and the **destination** keyword specifies the address range of the multicast groups that the C-RP will serve.

## Description

Use the **crp-policy** command to configure a legal C-RP address range and the range of served multicast groups, so as to guard against C-RP spoofing.

Use the **undo crp-policy** command to remove the restrictions in C-RP address ranges and the ranges of served multicast groups.

By default, there are no restrictions on C-RP address ranges and the address ranges of served groups, namely all received C-RP messages are accepted.

Note that the **crp-policy** command filters the multicast group ranges advertised by C-RPs based on the group prefixes. For example, if the multicast group range advertised by a C-RP is 224.1.0.0/16 while the legal group range defined by the **crp-policy** command is 224.1.0.0/30, the multicast groups in the range of 224.1.0.0/16 are allowed to pass.

Related commands: **c-rp**.

## Examples

#Configure a C-RP address range so that only routers in the address range of 1.1.1.1/24 can be C-RPs.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule permit ip source 1.1.1.1 0.0.0.255
[Sysname-acl-adv-3000] quit
[Sysname] pim
[Sysname-pim] crp-policy 3000
```

## display pim bsr-info

### Syntax

```
display pim bsr-info
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display pim bsr-info** command to view the BSR information in the PIM domain and the locally configured C-RP information in effect.

Related commands: **c-bsr**, **c-rp**.

## Examples

# View the BSR information in the PIM-SM domain and the locally configured C-RP information in effect.

```
<Sysname> display pim bsr-info
Elected BSR Address: 12.12.12.9
    Priority: 0
    Hash mask length: 30
    State: Elected
    Scope: Global
    Uptime: 00:00:56
    Next BSR message scheduled at: 00:01:14
Candidate BSR Address: 12.12.12.9
    Priority: 0
    Hash mask length: 30
    State: Elected
    Scope: Global

Candidate RP: 12.12.12.9(LoopBack1)
    Priority: 0
    HoldTime: 150
    Advertisement Interval: 60
    Next advertisement scheduled at: 00:00:48
Candidate RP: 3.3.3.3(Vlan-interface1)
    Priority: 20
    HoldTime: 90
    Advertisement Interval: 50
    Next advertisement scheduled at: 00:00:28
Candidate RP: 5.5.5.5(Vlan-interface2)
    Priority: 0
    HoldTime: 80
    Advertisement Interval: 60
    Next advertisement scheduled at: 00:00:48
```

**Table 1-1 display pim bsr-info command output description**

Field	Description
Elected BSR Address	Address of the elected BSR
Candidate BSR Address	Address of the candidate BSR
Priority	BSR priority
Hash mask length	Hash mask length
State	BSR state
Scope	Scope of the BSR
Uptime	Length of time for which this BSR has been up, in hh:mm:ss
Next BSR message scheduled at	Length of time in which the BSR will expire, in hh:mm:ss
Candidate RP	Address of the C-RP
Priority	Priority of the C-RP

Field	Description
HoldTime	Timeout time of the C-RP
Advertisement Interval	Interval at which the C-RP sends advertisement messages
Next advertisement scheduled at	Length of time in which the C-RP will send the next advertisement message, in hh:mm:ss

## display pim claimed-route

### Syntax

**display pim claimed-route** [ *source-address* ]

### View

Any view

### Default Level

1: Monitor level

### Parameters

*source-address*: Displays the information of the unicast route to a particular multicast source. If you do not provide this argument, this command will display the information about all unicast routes used by PIM.

### Description

Use the **display pim claimed-route** command to view the information of unicast routes used by PIM.

Note that, If an (S, G) is marked SPT, this (S, G) entry uses a unicast route.

### Examples

# View the information of all unicast routes used by PIM.

```
<Sysname> display pim claimed-route
RPF information about: 172.168.0.0
  RPF interface: Vlan-interface1, RPF neighbor: 172.168.0.2
  Referenced route/mask: 172.168.0.0/24
  Referenced route type: unicast (direct)
  RPF-route selecting rule: preference-preferred
  The (S,G) or (*,G) list dependent on this route entry
  (172.168.0.12, 227.0.0.1)
```

**Table 1-2 display pim claimed-route** command output description

Field	Description
RPF information about: 172.168.0.0	Information of the route to the multicast source 172.168.0.0
RPF interface	RPF interface type and number
RPF neighbor	IP address of the RPF neighbor
Referenced route/mask	Address/mask of the referenced route

Field	Description
Referenced route type	Type of the referenced route: <ul style="list-style-type: none"> <li>• igp: IGP unicast route</li> <li>• egp: EGP unicast route</li> <li>• unicast (direct): Direct unicast route</li> <li>• unicast: Other unicast route (such as static unicast route)</li> <li>• mbgp: MBGP route</li> <li>• multicast static: Static multicast route</li> </ul>
RPF-route selecting rule	Rule of RPF route selection
The (S,G) or (*,G) list dependent on this route entry	(S,G) or (*, G) entry list dependent on this RPF route

## display pim control-message counters

### Syntax

```
display pim control-message counters [ message-type { probe | register | register-stop } |
[ interface interface-type interface-number | message-type { assert | bsr | crp | graft | graft-ack |
hello | join-prune | state-refresh } ] * ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**probe:** Displays the number of null register messages.

**register:** Displays the number of register messages.

**register-stop:** Displays the number of register-stop messages.

**interface** *interface-type interface-number*: Displays the number of PIM control messages on the specified interface.

**assert:** Displays the number of assert messages.

**bsr:** Displays the number of Bootstrap messages.

**crp:** Displays the number of C-RP-Adv messages.

**graft:** Displays the number of Graft messages.

**graft-ack:** Displays the number of Graft-ack messages.

**hello:** Displays the number of Hello messages.

**join-prune:** Displays the number of Join/prune messages.

**state-refresh:** Displays the number of state refresh messages.

### Description

Use the **display pim control-message counters** command to view the statistics information of PIM control messages.

Note that if neither **all-instance** nor **vpn-instance** is specified, this command will display the information on the public instance.

## Examples

# View the statistics information of all types of PIM control messages on all interfaces .

```
<Sysname> display pim control-message counters
PIM global control-message counters:

      Received      Sent      Invalid
Register      20      37      2
Register-Stop  25      20      1
Probe         10      5      0

PIM control-message counters for interface: Vlan-interfaces1

      Received      Sent      Invalid
Assert      10      5      0
Graft      20      37      2
Graft-Ack   25      20      1
Hello     1232      453      0
Join/Prune  15      30      21
State-Refresh  8      7      1
BSR      3243      589      1
C-RP      53      32      0
```

**Table 1-3** display pim control-message counters command output description

Field	Description
PIM global control-message counters	Statistics of PIM global control messages
PIM control-message counters for interface	Interface for which PIM control messages were counted
Received	Number of messages received
Sent	Number of messages sent
Invalid	Number of invalid messages
Register	Register messages
Register-Stop	Register-stop messages
Probe	Null register messages
Assert	Assert messages
Graft	Graft messages
Graft-Ack	Graft-ack messages
Hello	Hello messages
Join/Prune	Join/prune messages
State Refresh	State refresh messages
BSR	Bootstrap messages
C-RP	C-RP-Adv messages

## display pim grafts

### Syntax

**display pim grafts**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display pim grafts** command to view the information about unacknowledged graft messages.

### Examples

# View the information about unacknowledged graft messages.

```
<Sysname> display pim grafts
```

```
Source          Group           Age             RetransmitIn
192.168.10.1    224.1.1.1      00:00:24      00:00:02
```

**Table 1-4 display pim grafts** command output description

Field	Description
Source	Multicast source address in the graft message
Group	Multicast group address in the graft message
Age	Time in which the graft message will get aged out, in hh:mm:ss
RetransmitIn	Time in which the graft message will be retransmitted, in hh:mm:ss

## display pim interface

### Syntax

**display pim interface** [ *interface-type interface-number* ] [ **verbose** ]

### View

Any view

### Default Level

1: Monitor level

### Parameters

*interface-type interface-number*: Displays the PIM information on a particular interface.

**verbose**: Displays the detailed PIM information.

## Description

Use the **display pim interface** command to view the PIM information on the specified interface or all interfaces.

## Examples

# View the PIM information on all interfaces.

```
<Sysname> display pim interface
Interface          NbrCnt  HelloInt  DR-Pri  DR-Address
Vlan1              1        30        1       10.1.1.2
Vlan2              0        30        1       172.168.0.2  (local)
Vlan3              1        30        1       20.1.1.2
```

**Table 1-5 display pim interface** command output description

Field	Description
Interface	Interface name
NbrCnt	Number of PIM neighbors
HelloInt	Hello interval
DR-Pri	Priority for DR election
DR-Address	DR IP address

# View the detailed PIM information on Vlan-interface1.

```
<Sysname> display pim interface vlan-interface1 verbose
Interface: Vlan-interface1, 10.1.1.1
  PIM version: 2
  PIM mode: Sparse
  PIM DR: 10.1.1.2
  PIM DR Priority (configured): 1
  PIM neighbor count: 1
  PIM hello interval: 30 s
  PIM LAN delay (negotiated): 500 ms
  PIM LAN delay (configured): 500 ms
  PIM override interval (negotiated): 2500 ms
  PIM override interval (configured): 2500 ms
  PIM neighbor tracking (negotiated): disabled
  PIM neighbor tracking (configured): disabled
  PIM generation ID: 0xF5712241
  PIM require generation ID: disabled
  PIM hello hold interval: 105 s
  PIM assert hold interval: 180 s
  PIM triggered hello delay: 5 s
  PIM J/P interval: 60 s
  PIM J/P hold interval: 210 s
  PIM BSR domain border: disabled
  Number of routers on network not using DR priority: 0
  Number of routers on network not using LAN delay: 0
```

**Table 1-6** display pim interface verbose command output description

Field	Description
Interface	Interface name and its IP address
PIM version	Running PIM version
PIM mode	PIM mode, dense or sparse
PIM DR	DR IP address
PIM DR Priority (configured)	Configured priority for DR election
PIM neighbor count	Total number of PIM neighbors
PIM hello interval	Hello interval
PIM LAN delay (negotiated)	Negotiated prune delay
PIM LAN delay (configured)	Configured prune delay
PIM override interval (negotiated)	Negotiated prune override interval
PIM override interval (configured)	Configured prune override interval
PIM neighbor tracking (negotiated)	Negotiated neighbor tracking status (enabled/disabled)
PIM neighbor tracking (configured)	Configured neighbor tracking status (enabled/disabled)
PIM generation ID	Generation_ID value
PIM require generation ID	Rejection of Hello messages without Generation_ID (enabled/disabled)
PIM hello hold interval	PIM neighbor timeout time
PIM assert hold interval	Assert timeout time
PIM triggered hello delay	Maximum delay of sending hello messages
PIM J/P interval	Join/prune interval
PIM J/P hold interval	Join/prune timeout time
PIM BSR domain border	Status of PIM domain border configuration (enabled/disabled)
Number of routers on network not using DR priority	Number of routers not using the DR priority field on the subnet where the interface resides
Number of routers on network not using LAN delay	Number of routers not using the LAN delay field on the subnet where the interface resides
Number of routers on network not using neighbor tracking	Number of routers not using neighbor tracking on the subnet where the interface resides

## display pim join-prune

### Syntax

```
display pim join-prune mode { sm [ flags flag-value ] | ssm } [ interface interface-type
interface-number | neighbor neighbor-address ] * [ verbose ]
```

## View

Any view

## Default Level

1: Monitor level

## Parameters

**mode:** Displays the information of join/prune messages to send in the specified PIM mode. PIM modes include **sm** and **ssm**, which represent PIM-SM and PIM-SSM respectively.

**flags flag-value:** Displays routing entries containing the specified flag. Values and meanings of *flag-value* are as follows:

- **rpt:** Specifies routing entries on the RPT.
- **spt:** Specifies routing entries on the SPT.
- **wc:** Specifies wildcard routing entries.

*interface-type interface-number:* Displays the information of join/prune messages to send on the specified interface.

*neighbor-address:* Displays the information of join/prune messages to send to the specified PIM neighbor.

**verbose:** Displays the detailed information of join/prune messages to send.

## Description

Use the **display pim join-prune** command to view the information about the join/prune messages to send.

## Examples

# The information of join/prune messages to send in the PIM-SM mode.

```
<Sysname> display pim join-prune mode sm
  Expiry Time: 50 sec
  Upstream nbr: 10.1.1.1 (Vlan-interface1)
  1 (*, G) join(s), 0 (S, G) join(s), 1 (S, G, rpt) prune(s)
  -----
  Total (*, G) join(s): 1, (S, G) join(s): 0, (S, G, rpt) prune(s): 1
```

**Table 1-7 display pim join-prune command output description**

Field	Description
Expiry Time:	Expiry time of sending join/prune messages
Upstream nbr:	IP address of the upstream PIM neighbor and the interface connecting to it
(*, G) join(s)	Number of (*, G) joins to send
(S, G) join(s)	Number of (S, G) joins to send
(S, G, rpt) prune(s)	Number of (S, G, rpt) prunes

## display pim neighbor

### Syntax

```
display pim neighbor [ interface interface-type interface-number | neighbor-address | verbose ] *
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*interface-type interface-number*: Displays the PIM neighbor information on a particular interface.

*neighbor-address*: Displays the information of a particular PIM neighbor.

**verbose**: Displays the detailed PIM neighbor information.

### Description

Use the **display pim neighbor** command to view the PIM neighbor information.

### Examples

# View the information of all PIM neighbors.

```
<Sysname> display pim neighbor
Total Number of Neighbors = 2
```

Neighbor	Interface	Uptime	Expires	Dr-Priority
10.1.1.2	Vlan1	02:50:49	00:01:31	1
20.1.1.2	Vlan2	02:49:39	00:01:42	1

# View the detailed information of the PIM neighbor whose IP address is 11.110.0.20.

```
<Sysname> display pim neighbor 11.110.0.20 verbose
Neighbor: 11.110.0.20
  Interface: Vlan-interface1
  Uptime: 00:00:10
  Expiry time: 00:00:30
  DR Priority: 1
  Generation ID: 0x2ACEFE15
  Holdtime: 105 s
  LAN delay: 500 ms
  Override interval: 2500 ms
  State refresh interval: 60 s
  Neighbor tracking: Disabled
```

**Table 1-8 display pim neighbor** command output description

Field	Description
Total Number of Neighbors	Total number of PIM neighbors
Neighbor	IP address of the PIM neighbor

Field	Description
Interface	Interface connecting the PIM neighbor
Uptime	Length of time for which the PIM neighbor has been up, in hh:mm:ss
Expires/Expiry time	Remaining time of the PIM neighbor, in hh:mm:ss; "never" means that the PIM neighbor is always up and reachable.
Dr-Priority/DR Priority	Priority of the PIM neighbor
Generation ID	Generation ID of the PIM neighbor (a random value indicating a status change of the PIM neighbor)
Holdtime	Holdtime of the PIM neighbor; "forever" means that the PIM neighbor is always up and reachable
LAN delay	Prune delay
Override interval	Prune override interval
State refresh interval	Interval of sending state refresh messages
Neighbor tracking	Neighbor tracking status (enabled/disabled)

## display pim routing-table

### Syntax

```
display pim routing-table [ group-address [ mask { mask-length | mask } ] | source-address [ mask { mask-length | mask } ] | incoming-interface [ interface-type interface-number | register ] | outgoing-interface { include | exclude | match } { interface-type interface-number | register } | mode mode-type | flags flag-value | fsm ] *
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*group-address*: Multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

*source-address*: Multicast source address.

*mask*: Mask of the multicast group/source address, 255.255.255.255 by default.

*mask-length*: Mask length of the multicast group/source address, in the range of 0 to 32. The system default is 32.

**incoming-interface**: Displays PIM routing entries that contain the specified interface as the incoming interface.

*interface-type interface-number*: Specifies an interface by its type and number.

**register**: Specifies the register interface. This keyword is valid only if *mode-type* is not specified or is **sm**.

**outgoing-interface**: Displays PIM routing entries of which the outgoing interface is the specified interface.

**include:** Displays PIM routing entries of which the outgoing interface list includes the specified interface.

**exclude:** Displays PIM routing entries of which the outgoing interface list excludes the specified interface.

**match:** Displays PIM routing entries of which the outgoing interface list includes only the specified interface.

**mode** *mode-type*: Specifies a PIM mode, where *mode-type* can have the following values:

- **dm**: Specifies PIM-DM.
- **sm**: Specifies PIM-SM.
- **ssm**: Specifies PIM-SSM.

**flags** *flag-value*: Displays PIM routing entries containing the specified flag(s). The values of *flag-value* and their meanings are as follows:

- **2msdp**: Specifies PIM routing entries to be contained in the next SA message to notify an MSDP peer.
- **act**: Specifies PIM routing entries to which actual data has arrived.
- **del**: Specifies PIM routing entries scheduled to be deleted.
- **exprune**: Specifies PIM routing entries containing outgoing interfaces pruned by other multicast routing protocols.
- **ext**: Specifies PIM routing entries containing outgoing interfaces provided by other multicast routing protocols.
- **loc**: Specifies PIM routing entries on routers directly connecting to the same subnet with the multicast source.
- **msdp**: Specifies PIM routing entries learned from MSDP SA messages.
- **niif**: Specifies PIM routing entries containing unknown incoming interfaces.
- **nonbr**: Specifies PIM routing entries with PIM neighbor searching failure.
- **rpt**: Specifies PIM routing entries on RPT branches where (S, G) prunes have been sent to the RP.
- **rq**: Specifies PIM routing entries of the receiving side of the switch-MDT.
- **spt**: Specifies PIM routing entries on the SPT.
- **sq**: Specifies PIM routing entries of the originator side of switch-MDT switchover.
- **swt**: Specifies PIM routing entries in the process of RPT-to-SPT switchover.
- **wc**: Specifies wildcard routing entries.

**fsm**: Displays the detailed information of the finite state machine (FSM).

## Description

Use the **display pim routing-table** command to view PIM routing table information.

Related commands: **display multicast routing-table** in *Multicast Routing and Forwarding Commands of the IP Multicast Volume*.

## Examples

# View the content of the PIM routing table.

```
<Sysname> display pim routing-table  
Total 0 (*, G) entry; 1 (S, G) entry
```

```
(172.168.0.12, 227.0.0.1)  
  RP: 2.2.2.2  
  Protocol: pim-sm, Flag: SPT LOC ACT
```

```

UpTime: 02:54:43
Upstream interface: Vlan-interface1
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
Downstream interface(s) information:
Total number of downstreams: 1
    1: Vlan-interface2
        Protocol: pim-sm, UpTime: 02:54:43, Expires: 00:02:47

```

**Table 1-9 display pim routing-table command output description**

Field	Description
Total 0 (*, G) entry; 1 (S, G) entry (172.168.0.2, 227.0.0.1)	Number of (S,G) and (*, G) entries in the PIM routing table An (S, G) entry in the PIM routing table
Protocol	PIM mode, PIM-SM or PIM-DM
Flag	Flag of the (S, G) or (*, G) entry in the PIM routing table
Uptime	Length of time for which the (S, G) or (*, G) entry has been existing
Upstream interface	Upstream (incoming) interface of the (S, G) or (*, G) entry
Upstream neighbor	Upstream neighbor of the (S, G) or (*, G) entry
RPF prime neighbor	RPF neighbor of the (S, G) or (*, G) entry <ul style="list-style-type: none"> <li>For a (*, G) entry, if this router is the RP, the RPF neighbor of this (*, G) entry is NULL.</li> <li>For a (S, G) entry, if this router directly connects to the multicast source, the RPF neighbor of this (S, G) entry is NULL.</li> </ul>
Downstream interface(s) information	Information of the downstream interface(s), including: <ul style="list-style-type: none"> <li>Number of downstream interfaces</li> <li>Downstream interface name</li> <li>Protocol type on the downstream interface(s)</li> <li>Uptime of the downstream interface(s)</li> <li>Expiry time of the downstream interface(s)</li> </ul>

## display pim rp-info

### Syntax

```
display pim rp-info [ group-address ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*group-address*: Address of the multicast group of which the RP information is to be displayed, in the range of 224.0.1.0 to 239.255.255.255. If you do not provide a group address, this command will display

the RP information corresponding to all multicast groups.

## Description

Use the **display pim rp-info** command to view the RP information.

Note that:

- The RP information includes the information of RPs dynamically found by the BSR mechanism and static RPs.
- Because a non-BSR router refreshes its local RP-Set only based on the received BSR bootstrap messages, the system does not delete an RP even if its expiry time is 0. Instead, the system waits for the next bootstrap message from the BSR: if the bootstrap message does not contain information of the RP, the system will delete it.

## Examples

# View the RP information corresponding to the multicast group 224.0.1.1.

```
<Sysname> display pim rp-info 224.0.1.1
BSR RP Address is: 2.2.2.2
    Priority: 0
    HoldTime: 150
    Uptime: 03:01:10
    Expires: 00:02:30
RP mapping for this group is: 2.2.2.2
```

# View the RP information corresponding to all multicast groups.

```
<Sysname> display pim rp-info
PIM-SM BSR RP information:
Group/MaskLen: 224.0.0.0/4
    RP: 2.2.2.2
    Priority: 0
    HoldTime: 150
    Uptime: 03:01:36
    Expires: 00:02:29
```

**Table 1-10 display pim rp-info** command output description

Field	Description
BSR RP Address is	IP address of the RP
Group/MaskLen	The multicast group served by the RP
RP	IP address of the RP
Priority	RP priority
HoldTime	RP timeout time
Uptime	Length of time for which the RP has been up, in hh:mm:ss
Expires	Length of time in which the RP will expire, in hh:mm:ss
RP mapping for this group	IP address of the RP serving the current multicast group

## hello-option dr-priority (PIM view)

### Syntax

```
hello-option dr-priority priority  
undo hello-option dr-priority
```

### View

PIM view

### Default Level

2: System level

### Parameters

*priority*: Router priority for DR election, in the range of 0 to 4294967295. A larger value of this argument means a higher priority.

### Description

Use the **hello-option dr-priority** command to configure the global value of the router priority for DR election.

Use the **undo hello-option dr-priority** command to restore the system default.

By default, the router priority for DR election is 1.

Related commands: **pim hello-option dr-priority**.

### Examples

```
# Set the router priority for DR election to 3.  
<Sysname> system-view  
[Sysname] pim  
[Sysname-pim] hello-option dr-priority 3
```

## hello-option holdtime (PIM view)

### Syntax

```
hello-option holdtime interval  
undo hello-option holdtime
```

### View

PIM view

### Default Level

2: System level

### Parameters

*interval*: PIM neighbor timeout time in seconds, with an effective range of 1 to 65,535. 65,535 makes the PIM neighbor always reachable.

## Description

Use the **hello-option holdtime** command to configure the PIM neighbor timeout time.

Use the **undo hello-option holdtime** command to restore the system default.

By default, the PIM neighbor timeout time is 105 seconds.

Related commands: **pim hello-option holdtime**.

## Examples

```
# Set the global value of the PIM neighbor timeout time to 120 seconds.
```

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option holdtime 120
```

## hello-option lan-delay (PIM view)

### Syntax

```
hello-option lan-delay interval
```

```
undo hello-option lan-delay
```

### View

PIM view

### Default Level

2: System level

### Parameters

*interval*: LAN-delay time in milliseconds, with an effective range of 1 to 32,767.

## Description

Use the **hello-option lan-delay** command to configure the global value of the LAN-delay time.

Use the **undo hello-option lan-delay** command to restore the system default.

By default, the LAN-delay time is 500 milliseconds.

This command is effective for both PIM-DM and PIM-SM.

Related commands: **hello-option override-interval**, **pim hello-option override-interval**, **pim hello-option lan-delay**.

## Examples

```
# Set the LAN-delay time to 200 milliseconds globally.
```

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option lan-delay 200
```

## hello-option neighbor-tracking (PIM view)

### Syntax

```
hello-option neighbor-tracking
```

## undo hello-option neighbor-tracking

### View

PIM view

### Default Level

2: System level

### Parameters

None

### Description

Use the **hello-option neighbor-tracking** command to globally disable join suppression, namely enable neighbor tracking.

Use the **undo hello-option neighbor-tracking** command to enable join suppression.

By default, join suppression is enabled, namely neighbor tracking is disabled.

This command is effective for both PIM-DM and PIM-SM.

Related commands: **pim hello-option neighbor-tracking**.

### Examples

```
# Disable join suppression globally.  
<Sysname> system-view  
[Sysname] pim  
[Sysname-pim] hello-option neighbor-tracking
```

## hello-option override-interval (PIM view)

### Syntax

```
hello-option override-interval interval  
undo hello-option override-interval
```

### View

PIM view

### Default Level

2: System level

### Parameters

*interval*: Prune override interval in milliseconds, with an effective range of 1 to 65,535.

### Description

Use the **hello-option override-interval** command to configure the global value of the prune override interval.

Use the **undo hello-option override-interval** command to restore the system default.

By default, the prune override interval is 2,500 milliseconds.

This command is effective for both PIM-DM and PIM-SM.

Related commands: **hello-option lan-delay**, **pim hello-option lan-delay**, **pim hello-option override-interval**.

### Examples

```
# Set the prune override interval to 2,000 milliseconds globally.
```

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option override-interval 2000
```

## holdtime assert (PIM view)

### Syntax

```
holdtime assert interval
undo holdtime assert
```

### View

PIM view

### Default Level

2: System level

### Parameters

*interval*: Assert timeout time in seconds, with an effective range of 7 to 2,147,483,647.

### Description

Use the **holdtime assert** command to configure the global value of the assert timeout time.

Use the **undo holdtime assert** command to restore the system default.

By default, the assert timeout time is 180 seconds.

This command is effective for both PIM-DM and PIM-SM.

Related commands: **holdtime join-prune**, **pim holdtime join-prune**, **pim holdtime assert**.

### Examples

```
# Set the global value of the assert timeout time to 100 seconds.
```

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] holdtime assert 100
```

## holdtime join-prune (PIM view)

### Syntax

```
holdtime join-prune interval
undo holdtime join-prune
```

## View

PIM view

## Default Level

2: System level

## Parameters

*interval*: Join/prune timeout time in seconds, with an effective range of 1 to 65,535.

## Description

Use the **holdtime join-prune** command to configure the global value of the join/prune timeout time.

Use the **undo holdtime join-prune** command to restore the system default.

By default, the join/prune timeout time is 210 seconds.

Related commands: **holdtime assert**, **pim holdtime assert**, **pim holdtime join-prune**.

## Examples

```
# Set the global value of the join/prune timeout time to 280 seconds.
```

```
<Sysname> system-view  
[Sysname] pim  
[Sysname-pim] holdtime join-prune 280
```

## jp-pkt-size (PIM view)

### Syntax

```
jp-pkt-size packet-size
```

```
undo jp-pkt-size
```

### View

PIM view

### Default Level

2: System level

### Parameters

*packet-size*: Maximum size of join/prune messages in bytes, with an effective range of 100 to 8,100.

### Description

Use the **jp-pkt-size** command to configure the maximum size of join/prune messages.

Use the **undo jp-pkt-size** command to restore the system default.

By default, the maximum size of join/prune messages is 8,100 bytes.

Related commands: **jp-queue-size**.

### Examples

```
# Set the maximum size of join/prune messages to 1,500 bytes.
```

```
<Sysname> system-view
```

```
[Sysname] pim
[Sysname-pim] jp-pkt-size 1500
```

## jp-queue-size (PIM view)

### Syntax

```
jp-queue-size queue-size
undo jp-queue-size
```

### View

PIM view

### Default Level

2: System level

### Parameters

*queue-size*: Maximum number of (S, G) entries in a join/prune message, in the range of 1 to 4,096.

### Description

Use the **jp-queue-size** command to configure the maximum number of (S, G) entries in a join/prune message.

Use the **undo jp-queue-size** command to restore the system default.

By default, a join/prune messages contains a maximum of 1,020 (S, G) entries.

When you use this command, take the following into account:

- The size of the forwarding table. In a network that does not support packet fragmentation, if you configure a large queue-size, a join/prune message may contain a large number of groups, causing the message length to exceed the MTU of the network. As a result, the products that do not support fragmentation will drop the join/prune message.
- The (S, G) join/prune timeout time on the upstream device. If you configure a small queue size, the outgoing interface of the corresponding entry may have been pruned due to timeout before the last join/prune message in a queue reaches the upstream device.

Related commands: **jp-pkt-size**, **holdtime join-prune**, **pim holdtime join-prune**.

### Examples

# Configure a join/prune messages to contain a maximum of 2,000 (S, G) entries.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] jp-queue-size 2000
```

## pim

### Syntax

```
pim
undo pim
```

## View

System view

## Default Level

2: System level

## Parameters

None

## Description

Use the **pim** command to enter PIM view.

Use the **undo pim** command to remove all configurations performed in PIM view.

Note that, IP multicast routing must be enabled in the corresponding instance before this command can take effect.

Related commands: **multicast routing-enable** in *Multicast Routing and Forwarding Commands of the IP Multicast Volume*.

## Examples

# Enable IP multicast routing and enter PIM view.

```
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] pim
[Sysname-pim]
```

## pim bsr-boundary

### Syntax

```
pim bsr-boundary
undo pim bsr-boundary
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **pim bsr-boundary** command to configure a PIM domain border, namely a bootstrap message boundary.

Use the **undo pim bsr-boundary** command to remove the configured PIM domain border.

By default, no PIM domain border is configured.

Related commands: **c-bsr**; **multicast boundary** in *Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*.

## Examples

# Configure VLAN-interface 100 as a PIM domain border.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim bsr-boundary
```

## pim dm

### Syntax

```
pim dm
undo pim dm
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **pim dm** command to enable PIM-DM.

Use the **undo pim dm** command to disable PIM-DM.

By default, PIM-DM is disabled.

Note that:

- This command can take effect only after IP multicast routing is enabled.
- PIM-DM cannot be used for multicast groups in the SSM group range.

Related commands: **pim sm**; **ssm-policy**; **multicast routing-table** in the *Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*.

## Examples

# Enable IP multicast routing, and enable PIM-DM on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim dm
```

## pim hello-option dr-priority

### Syntax

```
pim hello-option dr-priority priority
```

## undo pim hello-option dr-priority

### View

Interface view

### Default Level

2: System level

### Parameters

*priority*: Router priority for DR election, in the range of 0 to 4294967295. A larger value of this argument means a higher priority.

### Description

Use the **pim hello-option dr-priority** command to configure the router priority for DR election on the current interface.

Use the **undo pim hello-option dr-priority** command to restore the system default.

By default, the router priority for DR election is 1.

Related commands: **hello-option dr-priority**.

### Examples

```
# Set the router priority for DR election to 3 on VLAN-interface 100.
```

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 100
```

```
[Sysname-Vlan-interface100] pim hello-option dr-priority 3
```

## pim hello-option holdtime

### Syntax

```
pim hello-option holdtime interval
```

```
undo pim hello-option holdtime
```

### View

Interface view

### Default Level

2: System level

### Parameters

*interval*: PIM neighbor timeout time in seconds, with an effective range of 1 to 65,535. 65,535 makes the PIM neighbor always reachable.

### Description

Use the **pim hello-option holdtime** command to configure the PIM neighbor timeout time on the current interface.

Use the **undo pim hello-option holdtime** command to restore the system default.

By default, the PIM neighbor timeout time is 105 seconds.

Related commands: **hello-option holdtime**.

## Examples

```
# Set the PIM neighbor timeout time to 120 seconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option holdtime 120
```

## pim hello-option lan-delay

### Syntax

```
pim hello-option lan-delay interval
undo pim hello-option lan-delay
```

### View

Interface view

### Default Level

2: System level

### Parameters

*interval*: LAN-delay time in milliseconds, with an effective range of 1 to 32,767.

### Description

Use the **pim hello-option lan-delay** command to configure the LAN-delay time, namely the length of time the device waits between receiving a prune message and taking a prune action, on the current interface.

Use the **undo pim hello-option lan-delay** command to restore the system default.

By default, the LAN-delay time is 500 milliseconds.

Related commands: **pim hello-option override-interval**, **hello-option override-interval**, **hello-option lan-delay**.

## Examples

```
# Set the LAN-delay time to 200 milliseconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option lan-delay 200
```

## pim hello-option neighbor-tracking

### Syntax

```
pim hello-option neighbor-tracking
undo pim hello-option neighbor-tracking
```

### View

Interface view

## Default Level

2: System level

## Parameters

None

## Description

Use the **pim hello-option neighbor-tracking** command to disable join suppression, namely enable neighbor tracking, on the current interface.

Use the **undo pim hello-option neighbor-tracking** command to enable join suppression.

By default, join suppression is enabled, namely neighbor tracking is disabled.

Related commands: **hello-option neighbor-tracking**.

## Examples

```
# Disable join suppression on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option neighbor-tracking
```

## pim hello-option override-interval

### Syntax

```
pim hello-option override-interval interval
undo pim hello-option override-interval
```

### View

Interface view

## Default Level

2: System level

## Parameters

*interval*: Prune override interval in milliseconds, with an effective range of 1 to 65,535.

## Description

Use the **pim hello-option override-interval** command to configure the prune override interval on the current interface.

Use the **undo pim hello-option override-interval** command to restore the system default.

By default, the prune override interval is 2,500 milliseconds.

Related commands: **pim hello-option lan-delay**, **hello-option lan-delay**, **hello-option override-interval**.

## Examples

```
# Set the prune override interval to 2,000 milliseconds on VLAN-interface 100.
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim hello-option override-interval 2000
```

## pim holdtime assert

### Syntax

```
pim holdtime assert interval
undo pim holdtime assert
```

### View

Interface view

### Default Level

2: System level

### Parameters

*interval*: Assert timeout time in seconds, with an effective range of 7 to 2,147,483,647.

### Description

Use the **pim holdtime assert** command to configure the assert timeout time on the current interface.

Use the **undo pim holdtime assert** command to restore the system default.

By default, the assert timeout time is 180 seconds.

Related commands: **holdtime join-prune**, **pim holdtime join-prune**, **holdtime assert**.

### Examples

```
# Set the assert timeout time to 100 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim holdtime assert 100
```

## pim holdtime join-prune

### Syntax

```
pim holdtime join-prune interval
undo pim holdtime join-prune
```

### View

Interface view

### Default Level

2: System level

### Parameters

*interval*: Join/prune timeout time in seconds, with an effective range of 1 to 65,535.

## Description

Use the **pim holdtime join-prune** command to configure the join/prune timeout time on the interface.

Use the **undo pim holdtime join-prune** command to restore the system default.

By default, the join/prune timeout time is 210 seconds.

Related commands: **holdtime assert**, **pim holdtime assert**, **holdtime join-prune**.

## Examples

```
# Set the join/prune timeout time to 280 seconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim holdtime join-prune 280
```

## pim neighbor-policy

### Syntax

```
pim neighbor-policy acl-number
```

```
undo pim neighbor-policy
```

### View

Interface view

### Default Level

2: System level

### Parameters

*acl-number*: Basic ACL number, in the range of 2000 to 2999. When the ACL is defined, the **source** keyword in the **rule** command specifies a legal source address range for hello messages.

## Description

Use the **pim neighbor-policy** command to configure a legal source address range for hello messages to guard against hello message spoofing.

Use the **undo pim neighbor-policy** command to restore the default.

By default, no source address range for hello messages is configured, that is, all the received hello messages are considered legal.

## Examples

```
# Configure a legal source address range for hello messages on VLAN-interface 100 so that only the switches on the 10.1.1.0/24 subnet can become PIM neighbors of this switch.
```

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim neighbor-policy 2000
```

## pim require-genid

### Syntax

```
pim require-genid
undo pim require-genid
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **pim require-genid** command to enable rejection of hello messages without Generation\_ID.

Use the **undo pim require-genid** command to restore the default configuration.

By default, hello messages without Generation\_ID are accepted.

### Examples

```
# Enable VLAN-interface 100 to reject hello messages without Generation_ID.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim require-genid
```

## pim sm

### Syntax

```
pim sm
undo pim sm
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **pim sm** command to enable PIM-SM.

Use the **undo pim sm** command to disable PIM-SM.

By default, PIM-SM is disabled.

Note that this command can take effect only after IP multicast routing is enabled.

Related commands: **pim dm**; **multicast routing-table** in the *Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*.

## Examples

```
# Enable IP multicast routing, and enable PIM-SM on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim sm
```

## pim state-refresh-capable

### Syntax

```
pim state-refresh-capable
undo pim state-refresh-capable
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **pim state-refresh-capable** command to enable the state fresh feature on the interface.

Use the **undo pim state-refresh-capable** command to disable the state fresh feature.

By default, the state refresh feature is enabled.

Related commands: **state-refresh-interval**, **state-refresh-rate-limit**, **state-refresh-ttl**.

## Examples

```
# Disable state refresh on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo pim state-refresh-capable
```

## pim timer graft-retry

### Syntax

```
pim timer graft-retry interval
undo pim timer graft-retry
```

### View

Interface view

## Default Level

2: System level

## Parameters

*interval*: Graft retry period in seconds, with an effective range of 1 to 65,535.

## Description

Use the **pim timer graft-retry** command to configure the graft retry period.

Use the **undo pim timer graft-retry** command to restore the system default.

By default, the graft retry period is 3 seconds.

## Examples

# Set the graft retry period to 80 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim timer graft-retry 80
```

## pim timer hello

### Syntax

**pim timer hello** *interval*

**undo pim timer hello**

### View

Interface view

## Default Level

2: System level

## Parameters

*interval*: Hello interval in seconds, with an effective range of 1 to 2,147,483,647.

## Description

Use the **pim timer hello** command to configure on the current interface the interval at which hello messages are sent.

Use the **undo pim timer hello** command to restore the system default.

By default, hello messages are sent at the interval of 30 seconds.

Related commands: **timer hello**.

## Examples

# Set the hello interval to 40 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim timer hello 40
```

## pim timer join-prune

### Syntax

```
pim timer join-prune interval  
undo pim timer join-prune
```

### View

Interface view

### Default Level

2: System level

### Parameters

*interval*: Join/prune interval in seconds, with an effective range of 1 to 2,147,483,647.

### Description

Use the **pim timer join-prune** command to configure on the current interface the interval at which join/prune messages are sent.

Use the **undo pim timer join-prune** command to restore the system default.

By default, the join/prune interval is 60 seconds.

Related commands: **timer join-prune**.

### Examples

```
# Set the join/prune interval to 80 seconds on VLAN-interface 100.
```

```
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] pim timer join-prune 80
```

## pim triggered-hello-delay

### Syntax

```
pim triggered-hello-delay interval  
undo pim triggered-hello-delay
```

### View

Interface view

### Default Level

2: System level

### Parameters

*interval*: Maximum delay in seconds between hello messages, with an effective range of 1 to 5.

### Description

Use the **pim triggered-hello-delay** command to configure the maximum delay between hello messages.

Use the **undo pim triggered-hello-delay** command to restore the system default.

By default, the maximum delay between hello messages is 5 seconds.

### Examples

```
# Set the maximum delay between hello messages to 3 seconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim triggered-hello-delay 3
```

## probe-interval (PIM view)

### Syntax

```
probe-interval interval
```

```
undo probe-interval
```

### View

PIM view

### Default Level

2: System level

### Parameters

*interval*: Register probe time in seconds, with an effective range of 1 to 1799.

### Description

Use the **probe-interval** command to configure the register probe time.

Use the **undo probe-interval** command to restore the system default.

By default, the register probe time is 5 seconds.

Related commands: **register-suppression-timeout**.

### Examples

```
# Set the register probe time to 6 seconds.
```

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] probe-interval 6
```

## register-policy (PIM view)

### Syntax

```
register-policy acl-number
```

```
undo register-policy
```

### View

PIM view

## Default Level

2: System level

## Parameters

*acl-number*: Advanced ACL number, in the range of 3000 to 3999. Only register messages that match the **permit** statement of the ACL can be accepted by the RP.

## Description

Use the **register-policy** command to configure an ACL rule to filter register messages.

Use the **undo register-policy** command to remove the configured register filtering rule.

By default, no register filtering rule is configured.

Related commands: **register-suppression-timeout**.

## Examples

# Configure the RP to accept only those register messages from multicast sources on the subnet of 10.10.0.0/16 for multicast groups on the subnet of 225.1.0.0/16.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule permit ip source 10.10.0.0 0.0.255.255 destination 225.1.0.0
0.0.255.255
[Sysname-acl-adv-3000] quit
[Sysname] pim
[Sysname-pim] register-policy 3000
```

## register-suppression-timeout (PIM view)

### Syntax

**register-suppression-timeout** *interval*

**undo register-suppression-timeout**

### View

PIM view

## Default Level

2: System level

## Parameters

*interval*: Register suppression time in seconds, in the range of 1 to 3,600.

## Description

Use the **register-suppression-timeout** command to configure the register suppression time.

Use the **undo register-suppression-timeout** command to restore the system default.

By default, the register suppression time is 60 seconds.

Related commands: **probe-interval**, **register-policy**.

## Examples

```
# Set the register suppression time to 70 seconds.
<Sysname> system-view
[Sysname] pim
[Sysname-pim] register-suppression-timeout 70
```

## register-whole-checksum (PIM view)

### Syntax

```
register-whole-checksum
undo register-whole-checksum
```

### View

PIM view

### Default Level

2: System level

### Parameters

None

### Description

Use the **register-whole-checksum** command to configure the router to calculate the checksum based on the entire register message.

Use the **undo register-whole-checksum** command to restore the default configuration.

By default, the checksum is calculated based on the header in the register message.

Related commands: **register-policy**, **register-suppression-timeout**.

## Examples

```
# Configure the router to calculate the checksum based on the entire register message.
<Sysname> system-view
[Sysname] pim
[Sysname-pim] register-whole-checksum
```

## reset pim control-message counters

### Syntax

```
reset pim control-message counters [ interface interface-type interface-number ]
```

### View

User view

### Default Level

1: Monitor level

## Parameters

**interface** *interface-type interface-number*: Specifies to reset the PIM control message counter on a particular interface. If no interface is specified, this command will clear the statistics information of PIM control messages on all interfaces.

## Description

Use the **reset pim control-message counters** command to reset PIM control message counters.

## Examples

```
# Reset PIM control message counters on all interfaces.
```

```
<Sysname> reset pim control-message counters
```

## source-lifetime (PIM view)

### Syntax

```
source-lifetime interval  
undo source-lifetime
```

### View

PIM view

### Default Level

2: System level

## Parameters

*interval*: Multicast source lifetime in seconds, with an effective range of 1 to 65,535.

## Description

Use the **source-lifetime** command to configure the multicast source lifetime.

Use the **undo source-lifetime** command to restore the system default.

By default, the lifetime of a multicast source is 210 seconds.

## Examples

```
# Set the multicast source lifetime to 200 seconds.
```

```
<Sysname> system-view  
[Sysname] pim  
[Sysname-pim] source-lifetime 200
```

## source-policy (PIM view)

### Syntax

```
source-policy acl-number  
undo source-policy
```

### View

PIM view

## Default Level

2: System level

## Parameters

*acl-number*: Basic or advanced ACL number, in the range of 2000 to 3999.

## Description

Use the **source-policy** command to configure a multicast data filter.

Use the **undo source-policy** command to remove the configured multicast data filter.

By default, no multicast data filter is configured.

Note that:

- If you specify a basic ACL, the device filters all the received multicast packets based on the source address, and discards packets that fail the source address match.
- If you specify an advanced ACL, the device filters all the received multicast packets based on the source and group addresses, and discards packets that fail the match.
- If this command is executed repeatedly, the last configuration will take effect.

## Examples

# Configure the router to accept multicast packets originated from 10.10.1.2 and discard multicast packets originated from 10.10.1.1.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.10.1.2 0
[Sysname-acl-basic-2000] rule deny source 10.10.1.1 0
[Sysname-acl-basic-2000] quit
[Sysname] pim
[Sysname-pim] source-policy 2000
```

## spt-switch-threshold (PIM view)

### Syntax

**spt-switch-threshold infinity [ group-policy *acl-number* [ order *order-value* ] ]**

**undo spt-switch-threshold [ group-policy *acl-number* ]**

### View

PIM view

## Default Level

2: System level

## Parameters

**infinity**: Disables SPT switchover.

**group-policy *acl-number***: Specifies a basic ACL, in the range of 2000 to 2999. If you do not include this option in your command, the configuration will apply on all multicast groups.

**order order-value:** Specifies the order of the ACL in the group-policy list, where *order-value* has an effective range of 1 to (the largest order value in the existing group-policy list + 1), but the value range should not include the original order value of the ACL in the group-policy list. If you have assigned an *order-value* to a certain ACL, do not specify the same *order-value* for another ACL; otherwise the system will give error information. If you do not specify an *order-value*, the order value of the ACL will remain the same in the group-policy list.

## Description

Use the **spt-switch-threshold** command to prohibit the SPT switchover.

Use the **undo spt-switch-threshold** command to restore the default configuration.

By default, the device switches to the SPT immediately after it receives the first multicast packet.

Note that:

- To adjust the order of an existing ACL in the group-policy list, you can use the *acl-number* argument to specify this ACL and set its *order-value*. This will insert the ACL to the position of *order-value* in the group-policy list. The order of the other existing ACLs in the group-policy list will remain unchanged.
- To use an ACL that does not exist in the group-policy list, you can use the *acl-number* argument to specify an ACL and set its *order-value*. This will insert the ACL to the position of *order-value* in the group-policy list. If you do not include the **order order-value** option in your command, the ACL will be appended to the end of the group-policy list.
- If you use this command multiple times on the same multicast group, the first traffic rate configuration matched in sequence will take effect.
- For a switch, once a multicast forwarding entry is created, subsequent multicast data will not be encapsulated in register messages before being forwarded even if a register outgoing interface is available. Therefore, to avoid forwarding failure, do not include the infinity keyword in the **spt-switch-threshold** command on a switch that may become an RP (namely, a static RP or a C-RP).

## Examples

```
# Prohibit SPT switchover on a switch that will never become an RP.
```

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] spt-switch-threshold infinity
```

## ssm-policy (PIM view)

### Syntax

```
ssm-policy acl-number
```

```
undo ssm-policy
```

### View

```
PIM view
```

### Default Level

```
2: System level
```

## Parameters

*acl-number*: Basic ACL number, in the range of 2000 to 2999.

## Description

Use the **ssm-policy** command to configure the SSM multicast group range.

Use the **undo ssm-policy** command to restore the system default.

By default, the SSM group range is 232.0.0.0/8.

This command allows you to define an address range of permitted or denied multicast groups. If the match succeeds, the multicast mode will be PIM-SSM; otherwise the multicast mode will be PIM-SM.

## Examples

```
# Configure the SSM group range to be 232.1.0.0/16.
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 232.1.0.0 0.0.255.255
[Sysname-acl-basic-2000] quit
[Sysname] pim
[Sysname-pim] ssm-policy 2000
```

## state-refresh-interval (PIM view)

### Syntax

```
state-refresh-interval interval
undo state-refresh-interval
```

### View

PIM view

### Default Level

2: System level

## Parameters

*interval*: State refresh interval in seconds, with an effective range of 1 to 255.

## Description

Use the **state-refresh-interval** command to configure the interval between state refresh messages.

Use the **undo state-refresh-interval** command to restore the system default.

By default, the state refresh interval is 60 seconds.

Related commands: **pim state-refresh-capable**, **state-refresh-rate-limit**, **state-refresh-ttl**.

## Examples

```
# Set the state refresh interval to 70 seconds.
<Sysname> system-view
[Sysname] pim
[Sysname-pim] state-refresh-interval 70
```

## state-refresh-rate-limit (PIM view)

### Syntax

```
state-refresh-rate-limit interval  
undo state-refresh-rate-limit
```

### View

PIM view

### Default Level

2: System level

### Parameters

*interval*: Time to wait before receiving a new refresh message, in seconds and with an effective range of 1 to 65535.

### Description

Use the **state-refresh-rate-limit** command to configure the time the router must wait before receiving a new state refresh message.

Use the **undo state-refresh-rate-limit** command to restore the system default.

By default, the device waits 30 seconds before receiving a new state refresh message.

Related commands: **pim state-refresh-capable**, **state-refresh-interval**, **state-refresh-ttl**.

### Examples

```
# Configure the device to wait 45 seconds before receiving a new state refresh message.  
<Sysname> system-view  
[Sysname] pim  
[Sysname-pim] state-refresh-rate-limit 45
```

## state-refresh-ttl

### Syntax

```
state-refresh-ttl ttl-value  
undo state-refresh-ttl
```

### View

PIM view

### Default Level

2: System level

### Parameters

*ttl-value*: TTL value of state refresh messages, in the range of 1 to 255.

### Description

Use the **state-refresh-ttl** command to configure the TTL value of state refresh messages.

Use the **undo state-refresh-ttl** command to restore the system default.

By default, the TTL value of state refresh messages is 255.

Related commands: **pim state-refresh-capable**, **state-refresh-interval**, **state-refresh-rate-limit**.

## Examples

# Configure the device to send PIM state refresh messages with a TTL of 45.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] state-refresh-ttl 45
```

## static-rp (PIM view)

### Syntax

**static-rp** *rp-address* [ *acl-number* ] [ **preferred** ]

**undo static-rp** *rp-address*

### View

PIM view

### Default Level

2: System level

### Parameters

*rp-address*: IP address of the static RP to be configured. This address must be a legal unicast IP address, rather than an address on the 127.0.0.0/8 segment.

*acl-number*: Basic ACL number, in the range of 2000 to 2999. If you provide this argument, the configured static RP will serve only those groups that pass the ACL filtering; otherwise, the configured static RP will serve the all-system group 224.0.0.0/4.

**preferred**: Specifies to give priority to the static RP if the static RP conflicts with the dynamic RP. If you do not include the **preferred** keyword in your command, the dynamic RP will be given priority, and the static RP takes effect only if no dynamic RP exists in the network or when the dynamic RP fails.

### Description

Use the **static-rp** command to configure a static RP.

Use the **undo static-rp** command to configure a static RP.

By default, no static RP is configured.

Note that:

- PIM-SM or PIM-DM cannot be enabled on an interface that serves as a static RP.
- When the ACL rule applied on a static RP changes, a new RP must be elected for all the multicast groups.
- You can configure multiple static RPs by using this command repeatedly. However, if you carry out this command multiple times and specify the same static RP address or reference the same ACL rule, the last configuration will override the previous one. If multiple static RPs have been configured for the same multicast group, the one with the highest IP address will be chosen to serve the multicast group.

- You can configure up to 50 static RPs on the same device.

Related commands: **display pim rp-info**, **auto-rp enable**.

## Examples

# Configure the interface with the IP address 11.110.0.6 to be a static RP that serves the multicast groups defined in ACL 2001, and give priority to this static RP in the case of static/dynamic RP conflict.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] static-rp 11.110.0.6 2001 preferred
```

## timer hello (PIM view)

### Syntax

```
timer hello interval
undo timer hello
```

### View

PIM view

### Default Level

2: System level

### Parameters

*interval*: Hello interval in seconds, with an effective range of 1 to 2,147,483,647.

### Description

Use the **timer hello** command to configure the hello interval globally.

Use the **undo timer hello** command to restore the system default.

By default, hello messages are sent at the interval of 30 seconds.

Related commands: **pim timer hello**.

## Examples

# Set the global hello interval to 40 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] timer hello 40
```

## timer join-prune (PIM view)

### Syntax

```
timer join-prune interval
undo timer join-prune
```

### View

PIM view

## Default Level

2: System level

## Parameters

*interval*: Join/prune interval in seconds, with an effective range of 1 to 2,147,483,647.

## Description

Use the **timer join-prune** command to configure the join/prune interval globally.

Use the **undo timer join-prune** command to restore the system default.

By default, the join/prune interval is 60 seconds.

Related commands: **pim timer join-prune**.

## Examples

# Set the global join/prune interval to 80 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] timer join-prune 80
```

# Table of Contents

<b>1 MSDP Configuration Commands</b> .....	<b>1-1</b>
MSDP Configuration Commands.....	1-1
cache-sa-enable.....	1-1
display msdp brief.....	1-2
display msdp peer-status .....	1-3
display msdp sa-cache.....	1-5
display msdp sa-count.....	1-6
encap-data-enable.....	1-7
import-source.....	1-8
msdp.....	1-9
originating-rp.....	1-10
peer connect-interface.....	1-10
peer description .....	1-11
peer mesh-group .....	1-12
peer minimum-ttl.....	1-12
peer request-sa-enable .....	1-13
peer sa-cache-maximum .....	1-14
peer sa-policy .....	1-15
peer sa-request-policy .....	1-15
reset msdp peer.....	1-16
reset msdp sa-cache .....	1-17
reset msdp statistics .....	1-17
shutdown (MSDP View).....	1-18
static-rpf-peer .....	1-18
timer retry .....	1-19

# 1 MSDP Configuration Commands

---



## Note

The term “router” in this document refers to a router in a generic sense or a Layer 3 switch running MSDP.

---

## MSDP Configuration Commands

### cache-sa-enable

#### Syntax

**cache-sa-enable**

**undo cache-sa-enable**

#### View

MSDP view

#### Default Level

2: System level

#### Parameters

None

#### Description

Use the **cache-sa-enable** command to enable the SA cache mechanism to cache the (S, G) entries contained in SA messages.

Use the **undo cache-sa-enable** command to disable the SA cache mechanism.

By default, the SA cache mechanism is enabled, that is, the device caches the (S, G) entries contained in SA messages received.

#### Examples

# Enable the SA message cache mechanism so that the device caches the (S, G) entries contained in SA messages received.

```
<Sysname> system-view
```

```
[Sysname] msdp
```

```
[Sysname-msdp] cache-sa-enable
```

## display msdp brief

### Syntax

```
display msdp brief [ state { connect | down | listen | shutdown | up } ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**state:** Displays the information of MSDP peers in the specified state.

**connect:** Displays the information of MSDP peers in the connecting state.

**down:** Displays the information of MSDP peers in the down state.

**listen:** Displays the information of MSDP peers in the listening state.

**shutdown:** Displays the information of MSDP peers in the deactivated state.

**up:** Displays the information of MSDP peers in the in-session state.

### Description

Use the **display msdp brief** command to view the brief information of MSDP peers.

### Examples

```
# View the brief information of MSDP peers in all states.
```

```
<Sysname> display msdp brief
```

```
Configured  Up           Listen      Connect     Shutdown    Down
1           1           0           0           0           0

Peer's Address  State  Up/Down time  AS    SA Count  Reset Count
20.20.20.20    Up     00:00:13     100   0         0
```

**Table 1-1 display msdp brief** command output description

Field	Description
Configured	Number of MSDP peers configured
Up	Number of MSDP peers in the up state
Listen	Number of MSDP peers in the listen state
Connect	Number of MSDP peers in the connect state
Shutdown	Number of MSDP peers in the shutdown state
Down	Number of MSDP peers in the down state
Peer's Address	MSDP peer address

Field	Description
State	MSDP peer status: Up: Session set up; MSDP peer in session Listen: Session set up; local device as server, in listening state Connect: Session not set up; local device as client, in connecting state Shutdown: Deactivated Down: Connection failed
Up/Down time	Length of time since MSDP peer connection was established/failed
AS	Number of the AS where the MSDP peer is located. "?" indicates that the system was unable to obtain the AS number.
SA Count	Number of (S, G) entries
Reset Count	MSDP peer connection reset times

## display msdp peer-status

### Syntax

```
display msdp peer-status [ peer-address ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*peer-address*: Specifies an MSDP peer by its address. If you do not provide this argument, this command will display the detailed status information of all MSDP peers.

### Description

Use the **display msdp peer-status** command to view the detailed MSDP peer status information.

Related commands: **peer connect-interface**, **peer description**, **peer mesh-group**, **peer minimum-ttl**, **peer request-sa-enable**, **peer sa-cache-maximum**, **peer sa-policy**, **peer sa-request-policy**.

### Examples

# View the detailed status information of the MSDP peer with the address of 10.110.11.11.

```
<Sysname> display msdp peer-status 10.110.11.11
MSDP Peer 20.20.20.20, AS 100
Description:
Information about connection status:
State: Up
Up/down time: 14:41:08
Resets: 0
Connection interface: LoopBack0 (20.20.20.30)
```

```

Number of sent/received messages: 867/947
Number of discarded output messages: 0
Elapsed time since last connection or counters clear: 14:42:40
Information about (Source, Group)-based SA filtering policy:
  Import policy: none
  Export policy: none
Information about SA-Requests:
  Policy to accept SA-Request messages: none
  Sending SA-Requests status: disable
Minimum TTL to forward SA with encapsulated data: 0
SAs learned from this peer: 0, SA-cache maximum for the peer: none
Input queue size: 0, Output queue size: 0
Counters for MSDP message:
  Count of RPF check failure: 0
  Incoming/outgoing SA messages: 0/0
  Incoming/outgoing SA requests: 0/0
  Incoming/outgoing SA responses: 0/0
  Incoming/outgoing data packets: 0/0

```

**Table 1-2 display msdp peer-status command output description**

Field	Description
MSDP Peer	MSDP peer address
AS	Number of the AS where the MSDP peer is located. "?" indicates that the system was unable to obtain the AS number.
State	MSDP peer status: <ul style="list-style-type: none"> <li>• Up: Session set up; MSDP peer in session</li> <li>• Listen: Session set up; local device as server, in listening state</li> <li>• Connect: Session not set up; local device as client, in connecting state</li> <li>• Shutdown: Deactivated</li> <li>• Down: Connection failed</li> </ul>
Resets	Number of times the MSDP peer connection is reset
Up/Down time	Length of time since MSDP peer connection was established/failed
Connection interface	Interface and its IP address used for setting up a TCP connection with the remote MSDP peer
Number of sent/received messages	Number of SA messages sent and received through this connection
Number of discarded output messages	Number of discarded outgoing messages
Elapsed time since last connection or counters clear	Time passed since the information of the MSDP peer was last cleared
Information about (Source, Group)-based SA filtering policy	SA message filtering list information <ul style="list-style-type: none"> <li>• Import policy: Filter list for receiving SA messages from the specified MSDP peer</li> <li>• Export policy: Filter list for forwarding SA messages from the specified MSDP peer</li> </ul>

Field	Description
Information about SA-Requests	SA requests information <ul style="list-style-type: none"> <li>Policy to accept SA-Request messages: Filtering rule for receiving or forwarding SA messages from the specified MSDP peer</li> <li>Sending SA-Requests status: Whether enabled to send an SA request message to the designated MSDP peer upon receiving a new Join message</li> </ul>
Minimum TTL to forward SA with encapsulated data	Minimum TTL of multicast packet encapsulated in SA messages
SAs learned from this peer	Number of cached (S, G) entries learned from this MSDP peer
SA-cache maximum for the peer	Maximum number of (S, G) entries learned from this MSDP peer that the device can cache
Input queue size	Data size cached in the input queue
Output queue size	Data size cached in the output queue
Counters for MSDP message	MSDP peer statistics: <ul style="list-style-type: none"> <li>Count of RPF check failure: Number of SA messages discarded due to RPF check failure</li> <li>Incoming/outgoing SA messages: Number of SA messages received and sent</li> <li>Incoming/outgoing SA requests: Number of SA request received and sent</li> <li>Incoming/outgoing SA responses: Number of SA responses received and sent</li> <li>Incoming/outgoing data packets: Number of received and sent SA messages encapsulated with multicast data</li> </ul>

## display msdp sa-cache

### Syntax

```
display msdp sa-cache [ group-address | source-address | as-number ] *
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*group-address*: Multicast group address in the (S, G) entry, in the range of 224.0.1.0 to 239.255.255.255.

*source-address*: Multicast source address in the (S, G) entry.

*as-number*: AS number, in the range of 1 to 4294967295.

### Description

Use the **display msdp sa-cache** command to view the information of (S, G) entries in the SA cache.

Note that:

- This command gives the corresponding output only after the `cache-sa-enable` command is executed.
- If you do not provide a group address, this command will display the (S, G) entry information for all multicast groups.
- If you do not provide a source address, this command will display the (S, G) entry information for all sources.
- If you provide neither a group address nor a source address, this command will display the information of all cached (S, G) entries.
- If you do not provide an AS number, this command will display the (S, G) entry information related to all ASs.

Related commands: **cache-sa-enable**.

## Examples

# View the information of (S, G) entries in the SA cache.

```
<Sysname> display msdp sa-cache
```

```
MSDP Total Source-Active Cache - 5 entries
```

```
MSDP matched 5 entries
```

```
(Source, Group)          Origin RP      Pro AS      Uptime   Expires
(10.10.1.2, 225.1.1.1)   10.10.10.10   BGP 100     00:00:11 00:05:49
(10.10.1.3, 225.1.1.1)   10.10.10.10   BGP 100     00:00:11 00:05:49
(10.10.1.2, 225.1.1.2)   10.10.10.10   BGP 100     00:00:11 00:05:49
(10.10.2.1, 225.1.1.2)   10.10.10.10   BGP 100     00:00:11 00:05:49
(10.10.1.2, 225.1.2.2)   10.10.10.10   BGP 100     00:00:11 00:05:49
```

**Table 1-3 display msdp sa-cache command output description**

Field	Description
MSDP Total Source-Active Cache - 5 entries	Total number of (S, G) entries in the SA cache
MSDP matched 5 entries	Total number of (S, G) entries matched by MSDP
(Source, Group)	(S, G) entry: (source address, group address)
Origin RP	Address of the RP that generated the (S, G) entry
Pro	Type of protocol from which the AS number is originated. "?" indicates that the system was unable to obtain the protocol type.
AS	AS number of the origin RP. "?" indicates that the system was unable to obtain the AS number.
Uptime	Length of time for which the cached (S, G) entry has been existing, in hours:minutes:seconds
Expires	Length of time in which the cached (S, G) entry will expire, in hours:minutes:seconds

## display msdp sa-count

### Syntax

```
display msdp sa-count [ as-number ]
```

## View

Any view

## Default Level

1: Monitor level

## Parameters

*as-number*: AS number, in the range of 1 to 4294967295.

## Description

Use the **display msdp sa-count** command to view the number of (S, G) entries in the SA cache.

Note that, This command gives the corresponding output only after the **cache-sa-enable** command is executed.

Related commands: **cache-sa-enable**.

## Examples

# View the number of (S, G) entries in the SA cache.

```
<Sysname> display msdp sa-count
Number of cached Source-Active entries, counted by Peer
Peer's Address      Number of SA
10.10.10.10         5

Number of source and group, counted by AS
AS      Number of source  Number of group
?       3                3

Total 5 Source-Active entries
```

**Table 1-4 display msdp sa-count** command output description

Field	Description
Number of cached Source-Active entries, counted by Peer	Number of (S, G) entries counted by peer
Peer's Address	Address of the MSDP peer that sent SA messages
Number of SA	Number of (S, G) entries from this peer
Number of source and group, counted by AS	Number of cached (S, G) entries, counted by AS
AS	AS number. "?" indicates that the system was unable to obtain the AS number.
Number of source	Number of multicast sources from this AS
Number of group	Number of multicast groups from this AS

## encap-data-enable

### Syntax

**encap-data-enable**

## **undo encap-data-enable**

### **View**

MSDP view

### **Default Level**

2: System level

### **Parameters**

None

### **Description**

Use the **encap-data-enable** command to enable register message encapsulation in SA messages.

Use the **undo encap-data-enable** command to disable register message encapsulation in SA messages.

By default, an SA message contains only an (S, G) entry. No register message is encapsulated in an SA message.

### **Examples**

# Enable register message encapsulation in SA messages.

```
<Sysname> system-view  
[Sysname] msdp  
[Sysname-msdp] encap-data-enable
```

## **import-source**

### **Syntax**

```
import-source [ acl acl-number ]
```

```
undo import-source
```

### **View**

MSDP view

### **Default Level**

2: System level

### **Parameters**

*acl-number*: Basic or advanced ACL number, in the range of 2000 to 3999. A basic ACL is used to filter multicast sources, while an advanced ACL is used to filter multicast sources or multicast groups. If you do not provide this argument in your command, no multicast source information will be advertised.



## Note

During ACL matching, the protocol ID in the ACL rule is not checked.

---

## Description

Use the **import-source** command to configure a rule of creating (S, G) entries.

Use the **undo import-source** command to remove any rule of creating (S, G) entries.

By default, when an SA message is created, there are no restrictions on the (S, G) entries to be advertised in it, namely all the (S, G) entries within the domain are advertised in the SA message.

In addition to controlling SA message creation by using this command, you can also configure a filtering rule for forwarding and receiving SA messages by using the **peer sa-policy** command.

Related commands: **peer sa-policy**.

## Examples

# Configure the MSDP peer to advertise only the (S, G) entries of multicast sources on the 10.10.0.0/16 subnet and with multicast group address of 225.1.0.0/16 when creating an SA message.

```
<Sysname> system-view
[Sysname] acl number 3101
[Sysname-acl-adv-3101] rule permit ip source 10.10.0.0 0.0.255.255 destination 225.1.0.0
0.0.255.255
[Sysname-acl-adv-3101] quit
[Sysname] msdp
[Sysname-msdp] import-source acl 3101
```

## msdp

### Syntax

**msdp**

**undo msdp**

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **msdp** command to enable MSDP and enter MSDP view.

Use the **undo msdp** command to disable MSDP and remove the configurations performed MSDP view to free the resources occupied by MSDP.

By default, MSDP is disabled.

Note that, IP multicast must be enabled in the corresponding instance before this command can take effect.

Related commands: **multicast routing-enable** in *Multicast Routing and Forwarding Commands of the Multicast Volume*.

## Examples

```
# Enable IP multicast routing, and enable MSDP to enter MSDP view.
```

```
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] msdp
[Sysname-msdp]
```

## originating-rp

### Syntax

```
originating-rp interface-type interface-number
undo originating-rp
```

### View

MSDP view

### Default Level

2: System level

### Parameters

*interface-type interface-number*. Specifies an interface by its type and number.

### Description

Use the **originating-rp** command to configure the address of the specified interface as the RP address of SA messages.

Use the **undo originating-rp** command to restore the system default.

By default, the PIM RP address is used as the RP address of SA messages.

## Examples

```
# Specify the IP address of VLAN-interface 100 as the RP address of SA messages.
```

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] originating-rp vlan-interface 100
```

## peer connect-interface

### Syntax

```
peer peer-address connect-interface interface-type interface-number
undo peer peer-address
```

## View

MSDP view

## Default Level

2: System level

## Parameters

*peer-address*: MSDP peer address.

*interface-type interface-number*: Specifies an interface by its type and number. The local device will use the IP address of the specified interface as the source IP address when setting up a TCP connection with the remote MSDP peer.

## Description

Use the **peer connect-interface** command to create an MSDP peer connection.

Use the **undo peer connect-interface** command to remove an MSDP peer connection.

No MSDP peer connection is created by default.

Be sure to carry out this command before you use any other **peer** command; otherwise the system will prompt that the peer does not exist.

Related commands: **static-rpf-peer**.

## Examples

# Configure the router with the IP address of 125.10.7.6 as the MSDP peer of the local router, with interface VLAN-interface 100 as the local connection port.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 connect-interface vlan-interface 100
```

## peer description

### Syntax

**peer** *peer-address* **description** *text*

**undo peer** *peer-address* **description**

### View

MSDP view

### Default Level

2: System level

### Parameters

*peer-address*: MSDP peer address.

*text*: Descriptive string of 1 to 80 case sensitive characters including spaces.

### Description

Use the **peer description** command to configure the description information for the specified MSDP

peer.

Use the **undo peer description** command to delete the configured description information of the specified MSDP peer.

By default, an MSDP peer has no description information.

Related commands: **display msdp peer-status**.

## Examples

# Add the descriptive text "Router CstmrA" for the router with the IP address of 125.10.7.6 to indicate that this router is Customer A.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 description Router CstmrA
```

## peer mesh-group

### Syntax

```
peer peer-address mesh-group name
```

```
undo peer peer-address mesh-group
```

### View

MSDP view

### Default Level

2: System level

### Parameters

*peer-address*: MSDP peer address.

*name*: Mesh group name, a case-sensitive string of 1 to 32 characters. A mesh group name must not contain any space.

### Description

Use the **peer mesh-group** command to configure an MSDP peer as a mesh group member.

Use the **undo peer mesh-group** command to remove an MSDP peer as a mesh group member.

By default, an MSDP peer does not belong to any mesh group.

## Examples

# Configure the MSDP peer with the IP address of 125.10.7.6 as a member of the mesh group "Grp1".

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 mesh-group Grp1
```

## peer minimum-ttl

### Syntax

```
peer peer-address minimum-ttl tvl-value
```

**undo peer** *peer-address* **minimum-ttl**

## View

MSDP view

## Default Level

2: System level

## Parameters

*peer-address*: MSDP peer address.

*tvl-value*: Time-to-Live (TTL) threshold, in the range of 0 to 255.

## Description

Use the **peer minimum-ttl** command to configure the TTL threshold for multicast data packet encapsulation in SA messages.

Use the **undo peer minimum-ttl** command to restore the system default.

By default, the TTL threshold for a multicast packet to be encapsulated in an SA message is 0.

Related commands: **display msdp peer-status**.

## Examples

# Set the TTL threshold for multicast packets to be encapsulated in SA messages to 10 so that only multicast data packets whose TTL value is larger than or equal to 10 can be encapsulated in SA messages and forwarded to the MSDP peer 110.10.10.1.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 110.10.10.1 minimum-ttl 10
```

## peer request-sa-enable

### Syntax

**peer** *peer-address* **request-sa-enable**

**undo peer** *peer-address* **request-sa-enable**

### View

MSDP view

### Default Level

2: System level

### Parameters

*peer-address*: MSDP peer address.

### Description

Use the **peer request-sa-enable** command to enable the device to send an SA request message to the specified MSDP peer upon receiving a new join message.

Use the **undo peer request-sa-enable** command to disable the device from sending an SA request message to the specified MSDP peer.

By default, upon receiving a new join message, the router does not send an SA request message to any MSDP peer; instead, it waits for the next SA message to come.

Note that before you can enable the device to send SA requests, you must disable the SA message cache mechanism.

Related commands: **cache-sa-enable**.

## Examples

# Disable the SA message cache mechanism, and enable the router to send an SA request message to the MSDP peer 125.10.7.6 upon receiving a new Join message.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] undo cache-sa-enable
[Sysname-msdp] peer 125.10.7.6 request-sa-enable
```

## peer sa-cache-maximum

### Syntax

```
peer peer-address sa-cache-maximum sa-limit
undo peer peer-address sa-cache-maximum
```

### View

MSDP view

### Default Level

2: System level

### Parameters

*peer-address*: MSDP peer address.

*sa-limit*: Maximum number of (S, G) entries that the device can cache, in the range of 1 to 8,192.

### Description

Use the **peer sa-cache-maximum** command to configure the maximum number of (S, G) entries learned from the specified MSDP peer that the device can cache.

Use the **undo peer sa-cache-maximum** command to restore the system default.

By default, the device can cache a maximum of 8,192 (S, G) entries learned from any MSDP peer.

Related commands: **display msdp sa-count**, **display msdp peer-status**, **display msdp brief**.

## Examples

# Allow the device to cache a maximum of 100 (S, G) entries learned from its MSDP peer 125.10.7.6.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 sa-cache-maximum 100
```

## peer sa-policy

### Syntax

```
peer peer-address sa-policy { import | export } [ acl acl-number ]
undo peer peer-address sa-policy { import | export }
```

### View

MSDP view

### Default Level

2: System level

### Parameters

**import**: Specifies to filter SA messages from the specified MSDP peer.

**export**: Specifies to filter SA messages forwarded to the specified MSDP peer.

*peer-address*: MSDP peer address.

*acl-number*: Advanced ACL number, in the range of 3000 to 3999. If you do not provide an ACL number, all SA messages carrying (S, G) entries will be filtered off.

### Description

Use the **peer sa-policy** command to configure a filtering rule for receiving or forwarding SA messages.

Use the **undo peer sa-policy** command to restore the default setting.

By default, SA messages received or to be forwarded are not filtered, namely, all SA messages are accepted or forwarded.

In addition to controlling SA message receiving and forwarding by using this command, you can also configure a filtering rule for creating SA messages using the **import-source** command.

Related commands: **display msdp peer-status**, **import-source**.

### Examples

```
# Configure a filtering rule so that SA messages will be forwarded to the MSDP peer 125.10.7.6 only if they match ACL 3100.
```

```
<Sysname> system-view
[Sysname] acl number 3100
[Sysname-acl-adv-3100] rule permit ip source 170.15.0.0 0.0.255.255 destination 225.1.0.0 0.0.255.255
[Sysname-acl-adv-3100] quit
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 connect-interface vlan-interface 100
[Sysname-msdp] peer 125.10.7.6 sa-policy export acl 3100
```

## peer sa-request-policy

### Syntax

```
peer peer-address sa-request-policy [ acl acl-number ]
undo peer peer-address sa-request-policy
```

## View

MSDP view

## Default Level

2: System level

## Parameters

*peer-address*: MSDP peer address.

*acl-number*: Basic ACL number, in the range of 2000 to 2999. If you provide this argument, the SA requests of only the multicast groups that match the ACL will be accepted and other SA requests will be ignored; if you do not provide this argument, all SA requests will be ignored.

## Description

Use the **peer sa-request-policy** command to configure a filtering rule for SA request messages.

Use the **undo peer sa-request-policy** command to remove the configured SA request filtering rule.

By default, SA request messages are not filtered.

Related commands: **display msdp peer-status**.

## Examples

# Configure an SA request filtering rule so that SA messages from the MSDP peer 175.58.6.5 will be accepted only if the multicast group address in the SA messages is in the range of 225.1.1.0/24.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 225.1.1.0 0.0.0.255
[Sysname-acl-basic-2001] quit
[Sysname] msdp
[Sysname-msdp] peer 175.58.6.5 sa-request-policy acl 2001
```

## reset msdp peer

### Syntax

```
reset msdp peer [ peer-address ]
```

### View

User view

### Default Level

2: System level

### Parameters

None

### Description

Use the **reset msdp peer** command to reset the TCP connection with the specified MSDP peer or the TCP connections with all MSDP peers and clear all the statistics information of the MSDP peer(s).

Related commands: **display msdp peer-status**.

## Examples

# Reset the TCP connection with the MSDP peer 125.10.7.6 and clear all the statistics information of this MSDP peer.

```
<Sysname> reset msdp peer 125.10.7.6
```

## reset msdp sa-cache

### Syntax

```
reset msdp sa-cache [ group-address ]
```

### View

User view

### Default Level

2: System level

### Parameters

None

### Description

Use the **reset msdp sa-cache** command to clear (S, G) entries from the SA cache.

Related commands: **cache-sa-enable**, **display msdp sa-cache**.

## Examples

# Clear the (S, G) entries for multicast group 225.5.4.3 from the SA cache.

```
<Sysname> reset msdp sa-cache 225.5.4.3
```

## reset msdp statistics

### Syntax

```
reset msdp statistics [ peer-address ]
```

### View

User view

### Default Level

2: System level

### Parameters

None

### Description

Use the **reset msdp statistics** command to clear the statistics information of the specified MSDP peer or all MSDP peers without resetting the MSDP peer(s).

## Examples

```
# Clear the statistics information of the MSDP peer 125.10.7.6.
<Sysname> reset msdp statistics 125.10.7.6
```

## shutdown (MSDP View)

### Syntax

```
shutdown peer-address
undo shutdown peer-address
```

### View

MSDP view

### Default Level

2: System level

### Parameters

*peer-address*: MSDP peer address.

### Description

Use the **shutdown** command to deactivate manually the connection with the specified MSDP peer.

Use the **undo shutdown** command to reactivate the connection with the specified MSDP peer.

By default, the connections with all MSDP peers are active.

Related commands: **display msdp peer-status**.

## Examples

```
# Deactivate the connection with the MSDP peer 125.10.7.6.
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] shutdown 125.10.7.6
```

## static-rpf-peer

### Syntax

```
static-rpf-peer peer-address [ rp-policy ip-prefix-name ]
undo static-rpf-peer peer-address
```

### View

MSDP view

### Default Level

2: System level

### Parameters

*peer-address*: MSDP peer address.

**rp-policy** *ip-prefix-name*: Specifies a filtering policy based on the RP address in SA messages, where *ip-prefix-name* is the filtering policy name, a case sensitive string of 1 to 19 characters. A policy name must not contain any space.

## Description

Use the **static-rpf-peer** command to configure a static RPF peer.

Use the **undo static-rpf-peer** command to remove a static RPF peer.

No static RPF peer is configured by default.

When you configure multiple static RPF peers, observe the follow rules:

- 1) If you use the **rp-policy** keyword for all the static RPF peers, all the static RPF peers take effect concurrently. SA messages will be filtered as per the configured prefix list and only those SA messages whose RP addresses pass the filtering will be accepted. If multiple static RPF peers use the same filtering policy at the same time, when a peer receives an SA message, it will forward the SA message to the other peers.
- 2) If you use the **rp-policy** keyword for none of the static RPF peers, according to the configuration sequence, only the first static RPF peer whose connection is in the UP state will be activated, and all SA messages from this peer will be accepted while the SA messages from other static RPF peers will be discarded. When this active static RPF peer fails (for example, when the configuration is removed or when the connection is torn down), still the first RPF peer whose connection is in UP state will be selected as the activated RPF peer according to the configuration sequence.

Related commands: **display msdp peer-status**, **ip prefix-list**.

## Examples

# Configure static RPF peers.

```
<Sysname> system-view
[Sysname] ip ip-prefix list1 permit 130.10.0.0 16 great-equal 16 less-equal 32
[Sysname] msdp
[Sysname-msdp] peer 130.10.7.6 connect-interface vlan-interface 100
[Sysname-msdp] static-rpf-peer 130.10.7.6 rp-policy list1
```

## timer retry

### Syntax

**timer retry** *interval*

**undo timer retry**

### View

MSDP view

### Default Level

2: System level

### Parameters

*interval*: Interval between MSDP peer connection retries, in seconds. The effective range is 1 to 60.

## Description

Use the **timer retry** command to configure the interval between MSDP peer connection retries.

Use the **undo timer retry** command to restore the default setting.

By default, the interval between MSDP peer connection retries is 30 seconds.

Related commands: **display msdp peer-status**.

## Examples

# Set the MSDP peer connection retry interval to 60 seconds.

```
<Sysname> system-view  
[Sysname] msdp  
[Sysname-msdp] timer retry 60
```

# Table of Contents

<b>1 MBGP Configuration Commands</b> .....	<b>1-1</b>
MBGP Configuration Commands.....	1-1
aggregate (MBGP family view).....	1-1
balance (MBGP family view) .....	1-2
bestroute as-path-neglect (MBGP family view).....	1-3
bestroute compare-med (MBGP family view) .....	1-4
bestroute med-confederation (MBGP family view).....	1-4
compare-different-as-med (MBGP family view) .....	1-5
dampening (MBGP family view) .....	1-6
default local-preference (MBGP family view) .....	1-6
default med (MBGP family view) .....	1-7
default-route imported (MBGP family view).....	1-8
display ip multicast routing-table .....	1-9
display ip multicast routing-table <i>ip-address</i> .....	1-11
display bgp multicast group.....	1-12
display bgp multicast network .....	1-14
display bgp multicast paths .....	1-15
display bgp multicast peer.....	1-16
display bgp multicast routing-table .....	1-18
display bgp multicast routing-table as-path-acl.....	1-19
display bgp multicast routing-table cidr .....	1-20
display bgp multicast routing-table community .....	1-21
display bgp multicast routing-table community-list.....	1-22
display bgp multicast routing-table dampened.....	1-23
display bgp multicast routing-table dampening parameter.....	1-23
display bgp multicast routing-table different-origin-as.....	1-24
display bgp multicast routing-table flap-info .....	1-25
display bgp multicast routing-table peer.....	1-26
display bgp multicast routing-table regular-expression .....	1-27
display bgp multicast routing-table statistic.....	1-28
filter-policy export (MBGP family view).....	1-28
filter-policy import (MBGP Family view) .....	1-29
import-route (MBGP family view) .....	1-30
ipv4-family multicast .....	1-31
network (MBGP family view) .....	1-31
peer advertise-community (MBGP family view) .....	1-32
peer advertise-ext-community (MBGP family view) .....	1-33
peer allow-as-loop (MBGP family view) .....	1-34
peer as-path-acl (MBGP family view).....	1-34
peer default-route-advertise (MBGP family view) .....	1-35
peer enable (MBGP family view).....	1-36
peer filter-policy (MBGP family view) .....	1-37
peer group (MBGP family view) .....	1-37

peer ip-prefix (MBGP family view).....	1-38
peer keep-all-routes (MBGP family view).....	1-39
peer next-hop-local (MBGP family view).....	1-40
peer preferred-value (MBGP family view).....	1-40
peer public-as-only (MBGP family view).....	1-41
peer reflect-client (MBGP family view).....	1-42
peer route-limit (MBGP family view).....	1-43
peer route-policy (MBGP family view).....	1-44
preference (MBGP family view).....	1-45
reflect between-clients (MBGP family view).....	1-45
reflector cluster-id (MBGP family view).....	1-46
refresh bgp ipv4 multicast.....	1-47
reset bgp ipv4 multicast.....	1-48
reset bgp ipv4 multicast dampening.....	1-48
reset bgp ipv4 multicast flap-info.....	1-49
summary automatic (MBGP family view).....	1-49

# 1 MBGP Configuration Commands

---



## Note

The term “router” in this document refers to a generic router or an Ethernet switch running routing protocols.

For information about route policy commands, refer to *Route Policy Commands* in the *IP Routing Volume*.

---

## MBGP Configuration Commands

### aggregate (MBGP family view)

#### Syntax

```
aggregate ip-address { mask | mask-length } [ as-set | attribute-policy route-policy-name |  
detail-suppressed | origin-policy route-policy-name | suppress-policy route-policy-name ] *  
undo aggregate ip-address { mask | mask-length }
```

#### View

IPv4 MBGP address family view

#### Default Level

2: System level

#### Parameters

*ip-address*: Summary address.

*mask*: Summary mask, in dotted decimal notation.

*mask-length*: Summary mask length, in the range 0 to 32.

**as-set**: Creates a summary with AS set.

**attribute-policy** *route-policy-name*: Sets the attributes of the summary route according to the route policy. The route policy name is a string of 1 to 19 characters.

**detail-suppressed**: Advertises the summary route only.

**suppress-policy** *route-policy-name*: Suppresses specific routes defined in the route policy. The route policy name is a string of 1 to 19 characters.

**origin-policy** *route-policy-name*: References the route policy to determine routes for summarization. The route policy name is a string of 1 to 19 characters.

The keywords of the command are described as follows:

**Table 1-1** Functions of the keywords

Keywords	Function
<b>as-set</b>	Used to create a summary route, whose AS path contains the AS path information of summarized routes. Use this keyword carefully when many AS paths need to be summarized, because the frequent changes of these specific routes may lead to route flaps.
<b>detail-suppressed</b>	This keyword does not suppress the summary route, but it suppresses the advertisement of all the more specific routes. To summarize only some specific routes, use the <b>peer filter-policy</b> command.
<b>suppress-policy</b>	Used to create a summary route and suppress the advertisement of some summarized routes. If you want to suppress some routes selectively and leave other routes still advertised, use the <b>if-match</b> clause of the <b>route-policy</b> command.
<b>origin-policy</b>	Selects only routes satisfying the route policy for route summarization
<b>attribute-policy</b>	Sets attributes except the AS-PATH attribute for the summary route. The same work can be done by using the <b>peer route-policy</b> command.

### Description

Use the **aggregate** command to create a summary route in the IPv4 MBGP routing table.

Use the **undo aggregate** command to remove a summary route.

By default, no summary route is configured.

### Examples

# In IPv4 MBGP address family view, create a summary of 192.213.0.0/16 in the IPv4 MBGP routing table.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul]aggregate 10.40.0.0 255.255.0.0
```

### balance (MBGP family view)

#### Syntax

**balance** *number*

**undo balance**

#### View

IPv4 MBGP address family view

#### Default Level

2: System level

#### Parameters

*number*: Number of MBGP routes for load balancing. Its range varies is 1 to 4. When it is set to 1, load balancing is disabled.

## Description

Use the **balance** command to configure the number of MBGP routes for load balancing.

Use the **undo balance** command to restore the default.

By default, no load balancing is configured.

Unlike IGP, MBGP has no explicit metric for making load balancing decision. Instead, it implements load balancing by using route selection rules.

Related commands: **display ip multicast routing-table**.

## Examples

# In IPv4 MBGP address family view, set the number of routes for BGP load balancing to 2.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul]balance 2
```

## bestroute as-path-neglect (MBGP family view)

### Syntax

**bestroute as-path-neglect**

**undo bestroute as-path-neglect**

### View

IPv4 MBGP address family view

### Default Level

2: System level

### Parameters

None

## Description

Use the **bestroute as-path-neglect** command to configure MBGP not to consider the AS\_PATH during best route selection.

Use the **undo bestroute as-path-neglect** command to restore the default.

By default, MBGP considers AS\_PATH during best route selection.

## Examples

# In IPv4 MBGP address family view, configure BGP to ignore the AS\_PATH during best route selection.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul]bestroute as-path-neglect
```

## bestroute compare-med (MBGP family view)

### Syntax

```
bestroute compare-med  
undo bestroute compare-med
```

### View

IPv4 MBGP address family view

### Default Level

2: System level

### Parameters

None

### Description

Use the **bestroute compare-med** command to enable the comparison of the MED for paths from each AS during best route selection.

Use the **undo bestroute compare-med** command to disable this comparison.

The comparison is not enabled by default.

### Examples

# In IPv4 MBGP address family view, enable the comparison of the MED for paths from each AS during best route selection.

```
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp]ipv4-family multicast  
[Sysname-bgp-af-mul] bestroute compare-med
```

## bestroute med-confederation (MBGP family view)

### Syntax

```
bestroute med-confederation  
undo bestroute med-confederation
```

### View

IPv4 MBGP address family view

### Default Level

2: System level

### Parameters

None

### Description

Use the **bestroute med-confederation** command to enable the comparison of the MED for paths from

confederation peers during best route selection.

Use the **undo bestroute med-confederation** command to disable the comparison.

The comparison is not enabled by default.

The system only compares MED values for paths from peers within the confederation. Paths from external ASs are advertised throughout the confederation without MED comparison.

## Examples

# In IPv4 MBGP address family view, enable the comparison of the MED for paths from peers within the confederation.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] bestroute med-confederation
```

## compare-different-as-med (MBGP family view)

### Syntax

```
compare-different-as-med
undo compare-different-as-med
```

### View

IPv4 MBGP address family view

### Default Level

2: System level

### Parameters

None

### Description

Use the **compare-different-as-med** command to enable the comparison of the MED for paths from peers in different ASs.

Use the **undo compare-different-as-med** command to disable the comparison.

The comparison is disabled by default.

If several paths to one destination are available, the path with the smallest MED is selected.

Do not use this command unless associated ASs adopt the same IGP and routing selection method.

## Examples

# In IPv4 MBGP address family view, enable the comparison of the MED for paths from peers in different ASs.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul]compare-different-as-med
```

## dampening (MBGP family view)

### Syntax

```
dampening [ half-life-reachable half-life-unreachable reuse suppress ceiling | route-policy  
route-policy-name ] *
```

```
undo dampening
```

### View

IPv4 MBGP address family view

### Default Level

2: System level

### Parameters

*half-life-reachable*: Specifies a half-life for active routes from 1 to 45 minutes. By default, the value is 15 minutes.

*half-life-unreachable*: Specifies a half-life for suppressed routes from 1 to 45 minutes. By default, the value is 15 minutes.

*reuse*: Specifies a reuse threshold value for suppressed routes from 1 to 20000. A suppressed route whose penalty value decreases under the value is reused. By default, the reuse value is 750.

*suppress*: Specifies a suppression threshold from 1 to 20000. The route with a penalty value higher than the threshold is suppressed. The default value is 2000.

*ceiling*: Specifies a ceiling penalty value from 1001 to 20000. The value must be greater than the *suppress* value. By default, the value is 16000.

*route-policy-name*: Route policy name, a string of 1 to 19 characters.

### Description

Use the **dampening** command to configure IPv4 MBGP route dampening.

Use the **undo dampening** command to disable route dampening.

By default, no IPv4 MBGP route dampening is configured.

The command dampens only EBGP routes rather than IBGP routes.

### Examples

# In IPv4 MBGP address family view, configure IPv4 MBGP route dampening.

```
<Sysname> system-view  
[Sysname]bgp 100  
[Sysname-bgp]ipv4-family multicast  
[Sysname-bgp-af-mul]dampening 15 15 1000 2000 10000
```

## default local-preference (MBGP family view)

### Syntax

```
default local-preference value
```

```
undo default local-preference
```

## View

IPv4 MBGP address family view

## Default Level

2: System level

## Parameters

*value*: Default local preference, in the range 0 to 4294967295. The larger the value is, the higher the preference is.

## Description

Use the **default local-preference** command to configure the default local preference.

Use the **undo default local-preference** command to restore the default.

By default, the default local preference is 100.

Using this command can affect MBGP route selection.

## Examples

# In IPv4 MBGP address family view, set the default local preference to 180.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul]default local-preference 180
```

## default med (MBGP family view)

### Syntax

**default med** *med-value*

**undo default med**

### View

IPv4 MBGP address family view

### Default Level

2: System level

### Parameters

*med-value*: Default MED value, in the range 0 to 4294967295.

### Description

Use the **default med** command to specify the default MED value.

Use the **undo default med** command to restore the default.

By default, the default MED value is 0.

Multi-exit discriminator (MED) is an external metric for routes. Different from local preference, MED is exchanged between ASs and will stay in the AS once it enters the AS. The route with a lower MED is preferred. When a router running BGP obtains several routes with an identical destination but different

next-hops from various external peers, it will select the best route depending on the MED value. In the case that all other conditions are the same, the system selects the route with the smallest MED as the best external route.

## Examples

```
# In IPv4 MBGP address family view, configure the default MED as 25.
```

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul]default med 25
```

## default-route imported (MBGP family view)

### Syntax

```
default-route imported
undo default-route imported
```

### View

IPv4 MBGP address family view

### Default Level

2: System level

### Parameters

None

### Description

Use the **default-route imported** command to allow default route redistribution into the MBGP routing table.

Use the **undo default-route imported** command to restore the default.

By default, default route redistribution is not allowed.

Using the **default-route imported** command cannot redistribute default routes. To do so, use the **import-route** command.

Related commands: **import-route**.

## Examples

```
# In IPv4 MBGP address family view, allow default route redistribution from OSPF into MBGP.
```

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] default-route imported
[Sysname-bgp-af-mul] import-route ospf 1
```

## display ip multicast routing-table

### Syntax

```
display ip multicast routing-table [ verbose]
```

### View

Any view

### Default Level

2: Monitor level

### Parameters

**verbose:** Displays the detailed information of the multicast routing table, including both inactive and active multicast routes. Without the keyword, the command displays brief information about only the active MBGP routes.

### Description

Use the **display ip multicast routing-table** command to display the multicast BGP routing table.

All the active MBGP routes in the MBGP routing table are used for RPF check, but inactive MBGP routes are not.

### Examples

# Display brief information about the active routes in the multicast BGP routing table.

```
<Sysname> display ip multicast routing-table
```

```
Routing Tables: Public
```

```
Destinations : 6          Routes : 6
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
2.2.2.0/24	Direct	0	0	2.2.2.1	Vlan1
2.2.2.1/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.80.0/24	Direct	0	0	192.168.80.10	Vlan1
192.168.80.10/32	Direct	0	0	127.0.0.1	InLoop0

**Table 1-2** display ip multicast routing-table command output description

Field	Description
Destinations	Number of destinations
Routes	Number of routes
Destination/Mask	Destination address /Mask length
Proto	Routing protocol that discovered the route
Pre	Route preference
Cost	Route cost

Field	Description
NextHop	Next hop of the route
Interface	Outgoing interface to reach the destination

# Display the detailed information of the multicast routing table.

```
<Sysname> display ip multicast routing-table verbose
Routing Table : Public
    Destinations : 2      Routes : 2

Destination: 192.168.80.0/24
    Protocol: Direct      Process ID: 0
    Preference: 0         Cost: 0
    NextHop: 192.168.80.10 Interface: Vlan-interfaces1
    RelyNextHop: 0.0.0.0  Neighbour: 0.0.0.0
    Tunnel ID: 0x0        Label: NULL
    State: Active Adv     Age: 00h14m49s
    Tag: 0

Destination: 192.168.80.10/32
    Protocol: Direct      Process ID: 0
    Preference: 0         Cost: 0
    NextHop: 127.0.0.1    Interface: InLoopBack0
    RelyNextHop: 0.0.0.0  Neighbour: 0.0.0.0
    Tunnel ID: 0x0        Label: NULL
    State: Active NoAdv   Age: 00h14m49s
    Tag: 0
```

**Table 1-3** display ip multicast routing-table verbose command output description

Field	Description
Destination	Destination/mask
Protocol	Routing protocol that discovered the route
Process ID	Process ID
Preference	Route preference
Cost	Route cost
NextHop	NextHop of the route
Interface	Outgoing interface to reach the destination
RelyNextHop	Recursive next hop
Neighbour	Neighbor address
Tunnel ID	Tunnel ID
Label	Label
State	Route state: Active, Inactive, Adv (can be advertised), NoAdv (cannot be advertised), GotQ (route recursion succeeded), WaitQ (route recursion has not succeeded yet)

Field	Description
Age	Age of the route, in the sequence of hour, minute, and second from left to right.
Tag	Route tag

## display ip multicast routing-table *ip-address*

### Syntax

**display ip multicast routing-table** *ip-address* [*mask-length* |*mask*] [ **longer-match** ] [ **verbose** ]

### View

Any view

### Default Level

2: Monitor level

### Parameters

*ip-address*: Destination IP address, in dotted decimal format.

*mask-length*: IP address mask length in the range 0 to 32.

*mask*: IP address mask in dotted decimal format.

**longer-match**: Displays the route with the longest mask.

**verbose**: Displays detailed information about both active and inactive routes. With this argument absent, the command displays only brief information about active routes.

### Description

Use the **display ip multicast routing-table** command to display information about multicast routes to a specified destination address.

Executing the command with different parameters yields different outputs:

**display ip multicast routing-table** *ip-address*

It displays all multicast routes falling into the natural network of the IP address. If no such multicast routes are available, it displays only the longest matched active multicast route.

**display ip multicast routing-table** *ip-address mask*

It displays the multicast route exactly matching the IP address and mask.

### Examples

# Display brief information about all multicast routes falling into the natural network of the IP address (A multicast route is available).

```
<Sysname> display ip multicast routing-table 169.0.0.0
```

```
Routing Table : Public
```

```
Summary Count : 1
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
169.0.0.0/16	Static	60	0	2.1.1.1	InLoop1

# Display brief information about the longest matched active multicast route (No multicast route falls into the natural network of the IP address).

```
<Sysname> display ip multicast routing-table 169.253.0.0
Routing Table : Public
Summary Count : 1
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
169.0.0.0/8	Static	60	0	2.1.1.1	InLoop1

# Display detailed information about multicast routes falling into the natural network of the IP address (A multicast route is available).

```
<Sysname> display ip multicast routing-table 2.2.2.1 verbose
Routing Table : Public
Summary Count : 1
```

```
Destination: 2.2.2.1/32
  Protocol: Direct                Process ID: 0
  Preference: 0                   Cost: 0
  NextHop: 127.0.0.1              Interface: InLoopBack0
  RelyNextHop: 0.0.0.0            Neighbour: 0.0.0.0
  Tunnel ID: 0x0                  Label: NULL
  State: Active NoAdv             Age: 05h38m46s
  Tag: 0
```

# Display detailed information about the longest matched active multicast route (No multicast route falls into the natural network of the IP address).

```
<Sysname> display ip multicast routing-table 169.253.2.1 verbose
Routing Table : Public
Summary Count : 1
```

```
Destination: 169.0.0.0/8
  Protocol: Direct                Process ID: 0
  Preference: 0                   Cost: 0
  NextHop: 169.1.1.1              Interface: Vlan-interface1
  RelyNextHop: 0.0.0.0            Neighbour: 0.0.0.0
  Tunnel ID: 0x0                  Label: NULL
  State: Active Adv               Age: 00h00m32s
  Tag: 0
```

## display bgp multicast group

### Syntax

```
display bgp multicast group [ group-name ]
```

### View

Any view

## Default Level

2: Monitor level

## Parameters

*group-name*: MBGP peer group name, a string of 1 to 47 characters.

## Description

Use the **display bgp multicast group** command to display IPv4 MBGP peer group information.

## Examples

# Display the information of the IPv4 MBGP peer group **aaa**.

```
<Sysname> display bgp multicast group aaa
BGP peer-group is aaa
remote AS 200
Type : external
Maximum allowed prefix number: 4294967295
Threshold: 75%
Configured hold timer value: 180
Keepalive timer value: 60
Minimum time between advertisement runs is 30 seconds
Peer Preferred Value: 0
No routing policy is configured
Members:
Peer           V    AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down  State
-----
2.2.2.1       4    200      0        0      0      0 00:00:35 Active
```

**Table 1-4** display bgp multicast group command output description

Field	Description
BGP peer-group	Name of the peer group
remote AS	AS number of the peer group
Type	Type of the peer group: IBGP or EBGP
Maximum allowed prefix number	Maximum allowed prefix number
Threshold	Percentage of received prefixes from the peer group to maximum prefixes allowed to receive from the peer group; If the percentage is reached, the system generates alarm messages.
Configured hold timer value	Holdtime interval
Keepalive timer value	Keepalive interval
Minimum time between advertisement runs	Minimum interval for route advertisement
Peer Preferred Value	Preferred value specified for the routes from the peer
No routing policy is configured	No route policy is configured.
Members	Detailed information of the members in the peer group

Field	Description
Peer	IPv4 address of the peer
V	BGP version running on the peer
AS	AS number of the peer
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages to be sent
PrefRcv	Number of prefixes received
Up/Down	Time elapsed
State	State machine of the peer

## display bgp multicast network

### Syntax

**display bgp multicast network**

### View

Any view

### Default Level

2: Monitor level

### Parameters

None

### Description

Use the **display bgp multicast network** command to display IPv4 MBGP routing information advertised with the **network** command.

### Examples

# Display IPv4 MBGP routing information advertised with the **network** command.

```
<Sysname> display bgp multicast network
  BGP Local Router ID is 10.1.4.2.
  Local AS Number is 400.
  Network          Mask          Route-policy      Short-cut
  100.1.2.0        255.255.255.0
  100.1.1.0        255.255.255.0      Short-cut
```

**Table 1-5** display bgp multicast network command output description

Field	Description
BGP Local Router ID	BGP Local Router ID
Local AS Number	Local AS Number

Field	Description
Network	Network address
Mask	Mask
Route-policy	Route policy referenced
Short-cut	Short-cut route

## display bgp multicast paths

### Syntax

**display bgp multicast paths** [ *as-regular-expression* ]

### View

Any view

### Default Level

2: Monitor level

### Parameters

*as-regular-expression*: AS path regular expression, a string of 1 to 80 case-sensitive characters, including spaces.

### Description

Use the **display bgp multicast paths** command to display the AS path information of IPv4 MBGP routes.

### Examples

# Display the AS path information of IPv4 MBGP routes.

```
<Sysname> display bgp multicast paths ^200
```

Address	Hash	Refcount	MED	Path/Origin
0x5917100	11	1		200 300i

**Table 1-6 display bgp multicast paths** command output description

Field	Description
Address	Route address in the local database, in dotted hexadecimal notation
Hash	Hash index
Refcount	Count of routes that reference the path
MED	MED of the path
Path	AS_PATH attribute of the path, recording the ASs it has passed to avoid routing loops

Field	Description	
Origin	Origin attribute of the path:	
	i	Indicates the route is interior to the AS. Summary routes and routes injected using the <b>network</b> command are considered IGP routes.
	e	Indicates the route is learned from the Exterior Gateway Protocol (EGP).
	?	Indicates the origin of the route is unknown. Routes redistributed from other routing protocols have this origin attribute.

## display bgp multicast peer

### Syntax

```
display bgp multicast peer [ ip-address ] [ verbose ]
```

### View

Any view

### Default Level

2: Monitor level

### Parameters

*ip-address*: IP address of an IPv4 MBGP peer to be displayed, in dotted decimal notation.

**verbose**: Displays the detailed information of the peer/peer group.

### Description

Use the **display bgp multicast peer** command to display IPv4 MBGP peer information.

### Examples

# Display the detailed information of the IPv4 MBGP peer 10.110.25.20.

```
<Sysname> display bgp multicast peer 10.110.25.20 verbose
```

```
Peer: 10.110.25.20 Local: 2.2.2.2
Type: EBGP link
BGP version 4, remote router ID 1.1.1.1
BGP current state: Established, Up for 00h01m51s
BGP current event: RecvKeepalive
BGP last state: OpenConfirm
Port: Local - 1029 Remote - 179
Configured: Active Hold Time: 180 sec Keepalive Time: 60 sec
Received : Active Hold Time: 180 sec
Negotiated: Active Hold Time: 180 sec
Peer optional capabilities:
Peer support bgp multi-protocol extended
Peer support bgp route refresh capability
```

Address family IPv4 Unicast: advertised and received

Received: Total 5 messages, Update messages 1  
 Sent: Total 4 messages, Update messages 0  
 Maximum allowed prefix number: 4294967295  
 Threshold: 75%  
 Minimum time between advertisement runs is 30 seconds  
 Optional capabilities:  
 Route refresh capability has been enabled  
 Peer Preferred Value: 0  
 BFD: Enabled

Routing policy configured:  
 No routing policy is configured

**Table 1-7 display bgp multicast peer command output description**

Field	Description
Peer	IP address of the peer
Local	Local router ID
Type	Peer type
BGP version	BGP version
remote router ID	Router ID of the peer
BGP current state	Current state of the peer
BGP current event	Current event of the peer
BGP last state	Previous state of the peer
Port	TCP port numbers
Configured: Active Hold Time	Local holdtime interval
Keepalive Time	Local keepalive interval
Received: Active Hold Time	Remote holdtime interval
Negotiated: Active Hold Time	Negotiated holdtime interval
Peer optional capabilities	Optional capabilities supported by the peer, including multiprotocol BGP extensions and route refresh
Address family IPv4 Unicast	Routes are advertised and received in IPv4 unicasts.
Received	Total numbers of received packets and updates
Sent	Total numbers of sent packets and updates
Maximum allowed prefix number	Maximum allowed prefix number
Threshold	Threshold value
Minimum time between advertisement runs	Minimum route advertisement interval
Optional capabilities	Optional capabilities enabled by the peer
Peer Preferred Value	Preferred value specified for the routes from the peer

Field	Description
BFD	Status of BGP (enabled/disabled)
Routing policy configured	Local route policy

## display bgp multicast routing-table

### Syntax

```
display bgp multicast routing-table [ ip-address [ { mask | mask-length } [ longer-prefixes ] ] ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ip-address*: Destination IP address.

*mask*: Network mask, in dotted decimal notation.

*mask-length*: Mask length, in the range 0 to 32.

**longer-prefixes**: Matches the longest prefix.

### Description

Use the **display bgp multicast routing-table** command to display IPv4 MBGP routing information.

### Examples

```
# Display the IPv4 MBGP routing table.
```

```
<Sysname> display bgp multicast routing-table
```

```
Total Number of Routes: 1
```

```
BGP Local router ID is 10.10.10.1
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

```
Origin : i - IGP, e - EGP, ? - incomplete
```

```

Network          NextHop          MED          LocPrf          PrefVal Path/Ogn
* > 40.40.40.0/24  20.20.20.1          0          200 300i

```

**Table 1-8** display bgp multicast routing-table command output description

Field	Description
Total Number of Routes	Total Number of Routes
BGP Local router ID	BGP local router ID

Field	Description	
Status codes	Status codes: * – valid > – best d – damped h – history i – internal s – suppressed S – Stale	
Origin	i – IGP (originated in the AS) e – EGP (learned through EGP) ? – incomplete (learned by some other means)	
Network	Destination network address	
Next Hop	Next hop	
MED	MULTI_EXIT_DISC attribute	
LocPrf	Local preference value	
PrefVal	Preferred value of the route	
Path	AS_PATH attribute, recording the ASs the packet has passed to avoid routing loops	
Ogn	Origin attribute of the route, which can be one of the following values:	
	i	Indicates that the route is interior to the AS. Summary routes and the routes injected with the <b>network</b> command are considered IGP routes.
	e	Indicates that the route is learned from the Exterior Gateway Protocol (EGP).
	?	Short for INCOMPLETE. It indicates that the origin of the route is unknown and the route is learned by some other means. BGP marks routes redistributed from IGP as incomplete.

## display bgp multicast routing-table as-path-acl

### Syntax

```
display bgp multicast routing-table as-path-acl as-path-acl-number
```

### View

Any view

### Default Level

2: Monitor level

### Parameters

*as-path-acl-number*: Displays IPv4 MBGP routing information matching the AS path ACL, which is specified with a number from 1 to 256.

## Description

Use the **display bgp multicast routing-table as-path-acl** command to display IPv4 MBGP routes matching an AS-path ACL.

## Examples

# Display IPv4 MBGP routes matching AS path ACL 1.

```
<Sysname> display bgp multicast routing-table as-path-acl 1

BGP Local router ID is 20.20.20.1
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete
      Network          NextHop      MED          LocPrf      PrefVal Path/Ogn
* > 40.40.40.0/24      30.30.30.1    0            0           0       300i
```

Refer to [Table 1-8](#) for description on the fields above.

## display bgp multicast routing-table cidr

### Syntax

```
display bgp multicast routing-table cidr
```

### View

Any view

### Default Level

2: Monitor level

### Parameters

None

## Description

Use the **display bgp multicast routing-table cidr** command to display IPv4 MBGP Classless Inter-Domain Routing (CIDR) routing information.

## Examples

# Display IPv4 MBGP CIDR routing information.

```
<Sysname> display bgp multicast routing-table cidr

Total Number of Routes: 1

BGP Local router ID is 20.20.20.1
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete
      Network          NextHop      MED          LocPrf      PrefVal Path/Ogn
```

```
*> 40.40.40.0/24 30.30.30.1 0 0 300i
```

Refer to [Table 1-8](#) for description on the fields above.

## display bgp multicast routing-table community

### Syntax

```
display bgp multicast routing-table community [ aa:nn ]&<1-13> [ no-advertise | no-export | no-export-subconfed ] * [ whole-match ]
```

### View

Any view

### Default Level

2: Monitor level

### Parameters

**aa:nn**: Community number. Both aa and nn are in the range 0 to 65535.

**&<1-13>**: Argument before it can be entered up to 13 times.

**no-advertise**: Displays MBGP routes that cannot be advertised to any peer.

**no-export**: Displays MBGP routes that cannot be advertised out the AS. If a confederation is configured, it displays routes that cannot be advertised out the confederation, but can be advertised to other sub ASs in the confederation.

**no-export-subconfed**: Displays MBGP routes that cannot be advertised out the AS or to other sub ASs in the confederation.

**whole-match**: Displays the MBGP routes exactly matching the specified community attributes.

### Description

Use the **display bgp multicast routing-table community** command to display IPv4 MBGP routing information with the specified BGP community attribute.

### Examples

```
# Display IPv4 MBGP routing information with the specified BGP community attribute.
```

```
<Sysname> display bgp multicast routing-table community 11:22
```

```
BGP Local router ID is 10.10.10.1
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

```
Origin : i - IGP, e - EGP, ? - incomplete
```

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*> 10.10.10.0/24	0.0.0.0	0		0	i
*> 40.40.40.0/24	20.20.20.1			0	200 300i

Refer to [Table 1-8](#) for description on the fields above.

## display bgp multicast routing-table community-list

### Syntax

```
display bgp multicast routing-table community-list { basic-community-list-number [ whole-match ]  
| adv-community-list-number }&<1-16>
```

### View

Any view

### Default Level

2: Monitor level

### Parameters

*basic-community-list-number*: Specifies a basic community-list number from 1 to 99.

*adv-community-list-number*: Specifies an advanced community-list number from 100 to 199.

**whole-match**: Displays routes exactly matching the specified *basic-community-list*.

&<1-16>: Specifies the argument before it can be entered up to 16 times.

### Description

Use the **display bgp multicast routing-table community-list** command to display IPv4 MBGP routing information matching the specified BGP community list.

### Examples

# Display MBGP routing information matching the community list 100.

```
<Sysname> display bgp multicast routing-table community-list 100  
BGP Local router ID is 1.2.3.4  
Status codes: * - valid, > - best, d - damped,  
               h - history, i - internal, s - suppressed,  
Origin codes: i - IGP, e - EGP, ? - incomplete  
      Network          NextHop      Metric      LocPrf      PrefVal Path  
*> 3.3.3.0/30          1.2.3.4          0           0           ?  
*> 4.4.0.0/20          1.2.3.4          0           0           ?  
*> 4.5.6.0/26          1.2.3.4          0           0           ?  
  
BGP Local router ID is 30.30.30.1  
Status codes: * - valid, > - best, d - damped,  
               h - history, i - internal, s - suppressed, S - Stale  
Origin : i - IGP, e - EGP, ? - incomplete  
      Network          NextHop      MED          LocPrf      PrefVal Path/Ogn  
*> 30.30.30.0/24       0.0.0.0          0           0           i  
*> 40.40.40.0/24       0.0.0.0          0           0           i
```

Refer to [Table 1-8](#) for description on the fields above.

## display bgp multicast routing-table dampened

### Syntax

**display bgp multicast routing-table dampened**

### View

Any view

### Default Level

2: Monitor level

### Parameters

None

### Description

Use the **display bgp multicast routing-table dampened** command to display dampened IPv4 MBGP routes.

### Examples

# Display dampened IPv4 MBGP routes.

```
<Sysname> display bgp multicast routing-table dampened
BGP Local router ID is 2.2.2.2
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete
   Network          From           Reuse      Path/Origin
*d  77.0.0.0        12.1.1.1      00:29:20  100?
```

**Table 1-9** display bgp multicast routing-table dampened command output description

Field	Description
From	IP address from which the route was received
Reuse	Reuse time of the route

Refer to [Table 1-8](#) for description on the other fields above.

## display bgp multicast routing-table dampening parameter

### Syntax

**display bgp multicast routing-table dampening parameter**

### View

Any view

### Default Level

2: Monitor level

## Parameters

None

## Description

Use the **display bgp multicast routing-table dampening parameter** command to display IPv4 MBGP route dampening parameters.

Related commands: **dampening**.

## Examples

# Display IPv4 MBGP route dampening parameters.

```
<Sysname> display bgp multicast routing-table dampening parameter
Maximum Suppress Time(in second) : 3069
Ceiling Value                    : 16000
Reuse Value                      : 750
Reach HalfLife Time(in second)  : 900
Unreach HalfLife Time(in second): 900
Suppress-Limit                  : 2000
```

**Table 1-10** display bgp multicast routing-table dampening parameter command output description

Field	Description
Maximum Suppress Time	Maximum Suppress Time
Ceiling Value	Ceiling penalty value
Reuse Value	Reuse value
HalfLife Time	Half-life time of active routes
Suppress-Limit	Threshold at which a route is suppressed

## display bgp multicast routing-table different-origin-as

### Syntax

```
display bgp multicast routing-table different-origin-as
```

### View

Any view

### Default Level

2: Monitor level

## Parameters

None

## Description

Use the **display bgp multicast routing-table different-origin-as** command to display IPv4 MBGP routes originating from different autonomous systems.

## Examples

```
# Display IPv4 MBGP routes originating from different autonomous systems.
<Sysname> display bgp multicast routing-table different-origin-as
BGP Local router ID is 2.2.2.2
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

```

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*> 55.0.0.0	12.1.1.1	0		0	100?
*	14.1.1.2	0		0	300?

Refer to [Table 1-8](#) for description on the fields above.

## display bgp multicast routing-table flap-info

### Syntax

```
display bgp multicast routing-table flap-info [ regular-expression as-regular-expression |
as-path-acl as-path-acl-number | ip-address [ { mask | mask-length } [ longer-match ] ] ]
```

### View

Any view

### Default Level

2: Monitor level

### Parameters

*as-regular-expression*: Displays route flap information that matches the AS path regular expression.

*as-path-acl-number*: Displays route flap information matching the AS path ACL. The number is in the range 1 to 256.

*ip-address*: Destination IP address.

*mask*: Mask, in dotted decimal notation.

*mask-length*: Mask length, in the range 0 to 32.

**longer-match**: Matches the longest prefix.

### Description

Use the **display bgp multicast routing-table flap-info** command to display IPv4 MBGP route flap statistics. If no parameter is specified, this command displays all IPv4 MBGP route flap statistics.

## Examples

```
# Display IPv4 MBGP route flap statistics.
<Sysname> display bgp multicast routing-table flap-info

BGP Local router ID is 2.2.2.2
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
```

```

Origin : i - IGP, e - EGP, ? - incomplete
Network      From      Flaps  Duration  Reuse      Path/Origin
* > 55.0.0.0  12.1.1.1  2      00:00:16          100?
*d 77.0.0.0  12.1.1.1  5      00:34:02  00:27:08  100?

```

**Table 1-11** display bgp multicast routing-table flap-info command output description

Field	Description
From	Source IP address of the route
Flaps	Number of routing flaps
Duration	Route flap duration
Reuse	Reuse time of the route

Refer to [Table 1-8](#) for description on the other fields above.

## display bgp multicast routing-table peer

### Syntax

```

display bgp multicast routing-table peer ip-address { advertised-routes | received-routes }
[ network-address [ mask | mask-length ] | statistic ]

```

### View

Any view

### Default Level

2: Monitor level

### Parameters

*ip-address*: IP address of an IPv4 MBGP peer.

**advertised-routes**: Displays routing information advertised to the specified peer.

**received-routes**: Displays routing information received from the specified peer.

*network-address*: IP address of the destination network.

*mask*: Mask of the destination network, in dotted decimal notation.

*mask-length*: Mask length, in the range 0 to 32.

**statistic**: Displays route statistics.

### Description

Use the **display bgp multicast routing-table peer** command to display IPv4 MBGP routing information advertised to or received from the specified IPv4 MBGP peer.

Related commands: display bgp multicast peer.

### Examples

```
# Display IPv4 MBGP routing information advertised to the peer 20.20.20.1.
```

```
<Sysname> display bgp multicast routing-table peer 20.20.20.1 advertised-routes
```

```
Total Number of Routes: 2
```

```
BGP Local router ID is 30.30.30.1
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

```
Origin : i - IGP, e - EGP, ? - incomplete
```

	Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*>	30.30.30.0/24	0.0.0.0	0		0	i
*>	40.40.40.0/24	0.0.0.0	0		0	i

Refer to [Table 1-8](#) for description on the fields above.

## display bgp multicast routing-table regular-expression

### Syntax

```
display bgp multicast routing-table regular-expression as-regular-expression
```

### View

Any view

### Default Level

2: Monitor level

### Parameters

*as-regular-expression*: AS path regular expression, a string of 1 to 80 case-sensitive characters, including spaces.

### Description

Use the **display bgp multicast routing-table regular-expression** command to display IPv4 MBGP routing information matching the specified AS path regular expression.

### Examples

```
# Display IPv4 MBGP routing information matching AS path regular expression 300$.
```

```
<Sysname> display bgp multicast routing-table regular-expression 300$
```

```
BGP Local router ID is 20.20.20.1
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

```
Origin : i - IGP, e - EGP, ? - incomplete
```

	Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*>	40.40.40.0/24	30.30.30.1	0		0	300i

Refer to [Table 1-8](#) for description on the fields above.

## display bgp multicast routing-table statistic

### Syntax

```
display bgp multicast routing-table statistic
```

### View

Any view

### Default Level

2: Monitor level

### Parameters

None

### Description

Use the **display bgp multicast routing-table statistic** command to display IPv4 MBGP routing statistics.

### Examples

```
# Display IPv4 MBGP routing statistics.
```

```
<Sysname> display bgp multicast routing-table statistic
```

```
Total Number of Routes: 4
```

**Table 1-12** display bgp multicast routing-table statistic command output description

Field	Description
Total Number of Routes	Total Number of Routes

## filter-policy export (MBGP family view)

### Syntax

```
filter-policy { acl-number | ip-prefix ip-prefix-name } export [ direct | isis process-id | ospf process-id | rip process-id | static ]
```

```
undo filter-policy export [ direct | isis process-id | ospf process-id | rip process-id | static ]
```

### View

IPv4 MBGP address family view

### Default Level

2: System level

### Parameters

*acl-number*: Number of an ACL used to filter outgoing routing information, ranging from 2000 to 3999.

*ip-prefix-name*: Name of an IP prefix list used to filter outgoing routing information, a string of 1 to 19 characters.

**direct:** Filters direct routes.

**isis *process-id*:** Filters outgoing routes redistributed from an ISIS process. The process ID is in the range 1 to 65535.

**ospf *process-id*:** Filters outgoing routes redistributed from the OSPF process with an ID from 1 to 65535.

**rip *process-id*:** Filters outgoing routes redistributed from a RIP process. The process ID is in the range 1 to 65535.

**static:** Filters static routes.

## Description

Use the **filter-policy export** command to configure the filtering of outgoing routes.

Use the **undo filter-policy export** command to remove the filtering.

By default, the filtering is not configured.

If no routing protocol is specified, all redistributed routes are filtered.

## Examples

# In IPv4 MBGP address family view, reference ACL 2000 to filter all outgoing routes.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] filter-policy 2000 export
```

## filter-policy import (MBGP Family view)

### Syntax

```
filter-policy { acl-number | ip-prefix ip-prefix-name } import
undo filter-policy import
```

### View

IPv4 MBGP address family view

### Default Level

2: System level

### Parameters

*acl-number*: Number of an ACL used to filter incoming routing information, ranging from 2000 to 3999.

*ip-prefix-name*: Name of an IP prefix list used to filter incoming routing information, a string of 1 to 19 characters.

## Description

Use the **filter-policy import** command to configure the filtering of incoming routing information.

Use the **undo filter-policy import** command to disable the filtering.

By default, incoming routing information is not filtered.

## Examples

```
# In IPv4 MBGP address family view, reference ACL 2000 to filter incoming routing information.
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] filter-policy 2000 import
```

## import-route (MBGP family view)

### Syntax

```
import-route protocol [ process-id [ med med-value | route-policy route-policy-name ] * ]
undo import-route protocol [ process-id ]
```

### View

IPv4 MBGP address family view

### Default Level

2: System level

### Parameters

*protocol*: Redistributes routes from the routing protocol, which can be **direct**, **isis**, **ospf**, **rip** or **static** at present.

*process-id*: Process ID, in the range 1 to 65535. It is available only when the protocol is **isis**, **ospf** or **rip**.

*med-value*: Specifies a MED value for redistributed routes, ranging from 0 to 4294967295. If the argument is not specified, the cost of a redistributed route is used as its MED in the BGP routing domain.

*route-policy-name*: Name of a route policy used to filter redistributed routes, a string of 1 to 19 characters.

### Description

Use the **import-route** command to enable route redistribution from a specified routing protocol.

Use the **undo import-route** command to disable route redistribution from a routing protocol.

By default, MBGP does not redistribute routes from other protocols.

The origin attribute of routes redistributed with the **import-route** command is incomplete.

## Examples

```
# In IPv4 MBGP address family view, enable route redistribution from RIP.
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] import-route rip
```

## ipv4-family multicast

### Syntax

```
ipv4-family multicast
undo ipv4-family multicast
```

### View

BGP view

### Default Level

2: System level

### Parameters

None

### Description

Use the **ipv4-family multicast** command to enter IPv4 MBGP address family view.

Use the **undo ipv4-family multicast** command to remove all the settings made in IPv4 MBGP address family view.

### Examples

```
# Enter IPv4 MBGP address family view.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul]
```

## network (MBGP family view)

### Syntax

```
network ip-address [ mask | mask-length ] [ short-cut | route-policy route-policy-name ]
undo network ip-address [ mask | mask-length ] [ short-cut ]
```

### View

IPv4 MBGP address family view

### Default Level

2: System level

### Parameters

*ip-address*: Destination IP address.

*mask*: Mask of the network address, in dotted decimal notation.

*mask-length*: Mask length, in the range 0 to 32.

**short-cut**: Specifies the route to use the local preference. If the route is an EBGp route whose preference is higher than the local preference, using this keyword can configure the EBGp route to use the local preference, and thus the route can hardly become the optimal route.

*route-policy-name*: Route policy applied to the route. The name is a string of 1 to 19 characters.

## Description

Use the **network** command to inject a network to the IPv4 MBGP routing table.

Use the **undo network** command to remove a network from the IPv4 MBGP routing table.

By default, no network route is injected.

Note that:

- The network route to be injected must exist in the local IP routing table, and using a route policy makes route management more flexible.
- The origin attribute of the network route injected with the **network** command is IGP.

## Examples

```
# In IPv4 MBGP address family view, inject the network 10.0.0.0/16.
```

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] network 10.0.0.1 255.255.0.0
```

## peer advertise-community (MBGP family view)

### Syntax

```
peer { group-name | ip-address } advertise-community
undo peer { group-name | ip-address } advertise-community
```

### View

IPv4 MBGP address family view

### Default Level

2: System level

### Parameters

*group-name*: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

*ip-address*: IP address of an IPv4 MBGP peer.

## Description

Use the **peer advertise-community** command to advertise the community attribute to a peer/peer group.

Use the **undo peer advertise-community** command to disable the community attribute advertisement to a peer/peer group.

By default, no community attribute is advertised to any peer group/peer.

Related commands: **ip community-list**, **if-match community**, **apply community** (refer to *Route Policy Commands* in the *IP Routing Volume*).

## Examples

```
# In IPv4 MBGP address family view, advertise the community attribute to the existing peer group test.
```

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]group test external
[Sysname-bgp]peer test as-number 200
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test advertise-community
```

## peer advertise-ext-community (MBGP family view)

### Syntax

```
peer { group-name | ip-address } advertise-ext-community
undo peer { group-name | ip-address } advertise-ext-community
```

### View

IPv4 MBGP address family view

### Default Level

2: System level

### Parameters

*group-name*: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

*ip-address*: IP address of an IPv4 MBGP peer.

### Description

Use the **peer advertise-ext-community** command to advertise the extended community attribute to a peer/peer group.

Use the **undo peer advertise-ext-community** command to disable the extended community attribute advertisement to a peer/peer group.

By default, no extended community attribute is advertised to a peer/peer group.

For related information, refer to the **ip extcommunity-list**, **if-match extcommunity** and **apply extcommunity** commands in *Route policy Commands of the IP Routing Volume*.

### Examples

# In IPv4 MBGP address family view, advertise the extended community attribute to the existing peer group **test**.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]group test external
[Sysname-bgp]peer test as-number 200
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test advertise-ext-community
```

## peer allow-as-loop (MBGP family view)

### Syntax

```
peer { group-name | ip-address } allow-as-loop [ number ]
undo peer { group-name | ip-address } allow-as-loop
```

### View

IPv4 MBGP address family view

### Default Level

2: System level

### Parameters

*group-name*: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

*ip-address*: IP address of an IPv4 MBGP peer.

*number*: Specifies the number of times the local AS number can appear in routes from the peer/peer group, in the range 1 to 10. The default number is 1.

### Description

Use the **peer allow-as-loop** command to allow the local AS number to exist in the AS\_PATH attribute of routes from a peer/peer group, and to configure the number of times the local AS number can appear.

Use the **undo peer allow-as-loop** command to remove the configuration.

By default, the local AS number is not allowed.

Related commands: **display bgp multicast routing-table peer**.

### Examples

# In IPv4 MBGP address family view, configure the number of times the local AS number can appear in routes from the peer 1.1.1.1 as 2.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] peer 1.1.1.1 as-number 200
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] peer 1.1.1.1 enable
[Sysname-bgp-af-mul] peer 1.1.1.1 allow-as-loop 2
```

## peer as-path-acl (MBGP family view)

### Syntax

```
peer { group-name | ip-address } as-path-acl as-path-acl-number { export | import }
undo peer { group-name | ip-address } as-path-acl as-path-acl-number { export | import }
```

### View

IPv4 MBGP address family view

## Default Level

2: System level

## Parameters

*group-name*: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

*ip-address*: IP address of an IPv4 MBGP peer.

*as-path-acl-number*: AS path ACL number, in the range 1 to 256.

**export**: Filters outgoing routes.

**import**: Filters incoming routes.

## Description

Use the **peer as-path-acl** command to configure the filtering of routes incoming from or outgoing to a peer/peer group based on a specified AS path ACL.

Use the **undo peer as-path-acl** command to remove the filtering.

By default, no AS path ACL based filtering is configured.

Related commands: **ip as-path**, **if-match as-path** and **apply as-path** (refer to *IP Route policy Commands* in the *IP Routing Volume*).

## Examples

# In IPv4 MBGP address family view, reference the AS path ACL 1 to filter routes outgoing to the peer group **test**.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]group test external
[Sysname-bgp]peer test as-number 200
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test as-path-acl 1 export
```

## peer default-route-advertise (MBGP family view)

### Syntax

```
peer { group-name | ip-address } default-route-advertise [ route-policy route-policy-name ]
undo peer { group-name | ip-address } default-route-advertise
```

### View

IPv4 MBGP address family view

## Default Level

2: System level

## Parameters

*group-name*: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

*ip-address*: IP address of an IPv4 MBGP peer.

*route-policy-name*: Route policy name, a string of 1 to 19 characters.

## Description

Use the **peer default-route-advertise** command to advertise a default route to a peer/peer group.

Use the **undo peer default-route-advertise** command to disable default route advertisement to a peer/peer group.

By default, no default route is advertised to a peer/peer group.

With this command used, the router unconditionally sends a default route with the next hop being itself to the peer/peer group regardless of whether the default route is available in the routing table.

## Examples

# In IPv4 MBGP address family view, advertise a default route to the existing peer group **test**.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]group test external
[Sysname-bgp]peer test as-number 200
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test default-route-advertise
```

## peer enable (MBGP family view)

### Syntax

**peer** { *group-name* | *ip-address* } **enable**

**undo peer** { *group-name* | *ip-address* } **enable**

### View

IPv4 MBGP address family view

### Default Level

2: System level

### Parameters

*group-name*: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

*ip-address*: IP address of an IPv4 MBGP peer.

## Description

Use the **peer enable** command to enable the specified peer/peer group that has been created in BGP view.

Use the **undo peer enable** command to disable the specified peer/peer group that has been created in BGP view.

If a peer is disabled, the router will not exchange routing information with the peer.

## Examples

# Enable the peer 18.10.0.9.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]peer 18.10.0.9 as-number 100
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] peer 18.10.0.9 enable
```

## peer filter-policy (MBGP family view)

### Syntax

```
peer { group-name | ip-address } filter-policy acl-number { export | import }
undo peer { group-name | ip-address } filter-policy [ acl-number ] { export | import }
```

### View

IPv4 MBGP address family view

### Default Level

2: System level

### Parameters

*group-name*: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

*ip-address*: IP address of an IPv4 MBGP peer.

*acl-number*: ACL number, in the range 2000 to 3999.

**export**: Uses the ACL to filter routes outgoing to the peer/peer group.

**import**: Uses the ACL to filter routes incoming from the peer/peer group.

### Description

Use the **peer filter-policy** command to configure an ACL-based filter policy for a peer or peer group.

Use the **undo peer filter-policy** command to remove the filtering.

By default, no ACL-based filter policy is configured for a peer or peer group.

Related commands: **peer as-path-acl**.

### Examples

# In IPv4 MBGP address family view, reference ACL 2000 to filter routes sent to the peer group test.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]group test external
[Sysname-bgp]peer test as-number 200
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test filter-policy 2000 export
```

## peer group (MBGP family view)

### Syntax

```
peer ip-address group group-name
```

**undo peer** *ip-address* **group** *group-name*

## View

IPv4 MBGP address family view

## Default Level

2: System level

## Parameters

*group-name*: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

*ip-address*: IP address of an IPv4 MBGP peer.

## Description

Use the **peer group** command to add an IPv4 MBGP peer to an IPv4 MBGP peer group.

Use the **undo peer group** command to delete a specified peer from a peer group.

By default, no peer is added into a peer group.

## Examples

# In IPv4 MBGP address family view, add the peer 10.1.1.1 to the multicast EBGP peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp]group test external
[Sysname-bgp]peer test as-number 200
[Sysname-bgp] peer 10.1.1.1 group test
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer 10.1.1.1 group test
```

## peer ip-prefix (MBGP family view)

### Syntax

**peer** { *group-name* | *ip-address* } **ip-prefix** *ip-prefix-name* { **export** | **import** }

**undo peer** { *group-name* | *ip-address* } **ip-prefix** { **export** | **import** }

### View

IPv4 MBGP address family view

### Default Level

2: System level

### Parameters

*group-name*: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

*ip-address*: IP address of an IPv4 MBGP peer.

*ip-prefix-name*: IP prefix list name, a string of 1 to 19 characters.

**export**: Applies the filter to routes outgoing to the specified peer/peer group.

**import:** Applies the filter to routes from the specified peer/peer group.

## Description

Use the **peer ip-prefix** command to reference an IP prefix list to filter routes received from or advertised to a peer or peer group.

Use the **undo peer ip-prefix** command to remove the configuration.

By default, no IP prefix list based filtering is configured.

## Examples

# In IPv4 MBGP address family view, use the IP prefix list **1** to filter routes outgoing to the peer group **test**.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]group test external
[Sysname-bgp]peer test as-number 200
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test ip-prefix list1 export
```

## peer keep-all-routes (MBGP family view)

### Syntax

```
peer { group-name | ip-address } keep-all-routes
undo peer { group-name | ip-address } keep-all-routes
```

### View

IPv4 MBGP address family view

### Default Level

2: System level

### Parameters

*group-name*: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

*ip-address*: IP address of an IPv4 MBGP peer.

## Description

Use the **peer keep-all-routes** command to save original routing information from a peer or peer group, including routes that fail to pass the inbound policy (if configured).

Use the **undo peer keep-all-routes** command to disable this feature.

By default, the feature is not enabled.

## Examples

# In IPv4 MBGP address family view, save all the routing information from peer 131.108.1.1.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] peer 131.108.1.1 as-number 100
```

```
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] peer 131.108.1.1 enable
[Sysname-bgp-af-mul] peer 131.108.1.1 keep-all-routes
```

## peer next-hop-local (MBGP family view)

### Syntax

```
peer { group-name | ip-address } next-hop-local
undo peer { group-name | ip-address } next-hop-local
```

### View

IPv4 MBGP address family view

### Default Level

2: System level

### Parameters

*group-name*: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

*ip-address*: IP address of an IPv4 MBGP peer.

### Description

Use the **peer next-hop-local** command to specify the router as the next hop for routes sent to a peer/peer group.

Use the **undo peer next-hop-local** command to remove the configuration.

By default, routes advertised to an EBGP peer/peer group take the local router as the next hop, while routes outgoing to an IBGP peer/peer group do not take the local router as the next hop.

### Examples

# In IPv4 MBGP address family view, specify the router as the next hop for routes sent to the peer group **test**.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]group test internal
[Sysname-bgp]peer test as-number 200
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test next-hop-local
```

## peer preferred-value (MBGP family view)

### Syntax

```
peer { group-name | ip-address } preferred-value value
undo peer { group-name | ip-address } preferred-value
```

### View

IPv4 MBGP address family view

## Default Level

2: System level

## Parameters

*group-name*: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

*ip-address*: IP address of an IPv4 MBGP peer.

*value*: Preferred value, in the range 0 to 65535.

## Description

Use the **peer preferred-value** command to specify a preferred value for routes received from a peer or peer group.

Use the **undo peer preferred-value** command to restore the default value.

The default preferred value is 0.

Routes learned from a peer have an initial preferred value. Among multiple routes that have the same destination/mask and are learned from different peers, the one with the greatest preferred value is selected as the route to the destination.

Note that:

If you both reference a route policy and use the **peer { group-name | ip-address } preferred-value value** command to set a preferred value for routes from a peer/peer group, the route policy sets a specified non-zero preferred value for routes matching it. Other routes not matching the route policy uses the value set with the **peer preferred-value** command. If the preferred value specified in the route policy is zero, the routes matching it will also use the value set with the command.

For information about using a route policy to set a preferred value, refer to the command **peer { group-name | ip-address } route-policy route-policy-name { export | import }** in this document, and the command **apply preferred-value preferred-value** in *Route policy Commands of the IP Routing Volume*.

## Examples

```
# In IPv4 MBGP address family view, configure the preferred value as 50 for routes from peer 131.108.1.1.
```

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] peer 131.108.1.1 as-number 100
[Sysname-bgp]ipv4-family multicast
[Sysname-bgp-af-mul] peer 131.108.1.1 enable
[Sysname-bgp-af-mul] peer 131.108.1.1 preferred-value 50
```

## peer public-as-only (MBGP family view)

### Syntax

```
peer { group-name | ip-address } public-as-only
```

```
undo peer { group-name | ip-address } public-as-only
```

### View

IPv4 MBGP address family view

## Default Level

2: System level

## Parameters

*group-name*: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

*ip-address*: IP address of an IPv4 MBGP peer.

## Description

Use the **peer public-as-only** command to not keep private AS numbers in BGP updates sent to a peer/peer group.

Use the **undo peer public-as-only** command to keep private AS numbers in BGP updates sent to a peer/peer group.

By default, outgoing BGP updates can carry private AS numbers.

The command does not take effect for BGP updates with both public and private AS numbers. The range of private AS numbers is from 64512 to 65535.

## Examples

# In IPv4 MBGP address family view, disable updates sent to the peer group **test** from carrying private AS numbers.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
[Sysname-bgp] peer test as-number 200
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test public-as-only
```

## peer reflect-client (MBGP family view)

### Syntax

```
peer { group-name | peer-address } reflect-client
undo peer { group-name | peer-address } reflect-client
```

### View

IPv4 MBGP address family view

## Default Level

2: System level

## Parameters

*group-name*: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

*peer-address*: IP address of an IPv4 MBGP peer.

## Description

Use the **peer reflect-client** command to configure the router as a route reflector and specify a peer/peer group as a client.

Use the **undo peer reflect-client** command to remove the configuration.

By default, neither the route reflector nor the client is configured.

Related commands: **reflect between-clients** and **reflect cluster-id**.

## Examples

# In IPv4 MBGP address family view, configure the local device as a route reflector and specify the IBGP peer group **test** as a client.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test internal
[Sysname-bgp] peer test as-number 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test reflect-client
```

## peer route-limit (MBGP family view)

### Syntax

```
peer { group-name | ip-address } route-limit limit [ percentage ]
```

```
undo peer { group-name | ip-address } route-limit
```

### View

IPv4 MBGP address family view

### Default Level

2: System level

### Parameters

*group-name*: Name of an IPv4 MBGP peer group, a string of 1 to 47 characters.

*ip-address*: IP address of an IPv4 MBGP peer.

*limit*: Upper limit of IP route that can be received from the peer or peer group. Its range is 1 to 12288.

*percentage*: If the number of received routes divided by the upper limit reaches the specified percentage, the system will generate alarm information. The percentage is in the range 1 to 100. The default is 75.

## Description

Use the **peer route-limit** command to set the maximum number of routes that can be received from a peer/peer group.

Use the **undo peer route-limit** command to restore the default.

The number is unlimited by default.

## Examples

# In IPv4 MBGP address family view, set the number of routes that can be received from peer 131.108.1.1 to 10000.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 131.108.1.1 as-number 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] peer 131.108.1.1 enable
[Sysname-bgp-af-mul] peer 131.108.1.1 route-limit 10000
```

## peer route-policy (MBGP family view)

### Syntax

```
peer { group-name | ip-address } route-policy route-policy-name { export | import }
undo peer { group-name | ip-address } route-policy route-policy-name { export | import }
```

### View

IPv4 MBGP address family view

### Default Level

2: System level

### Parameters

*group-name*: Peer group name, a string of 1 to 47 characters.

*ip-address*: IP address of an IPv4 MBGP peer.

*route-policy-name*: Route policy name, a string of 1 to 19 characters.

**export**: Applies the route policy to routes advertised to the peer/peer group.

**import**: Applies the route policy to routes received from the peer/peer group.

### Description

Use the **peer route-policy** command to apply a route policy to routes incoming from or outgoing to a peer or peer group.

Use the **undo peer route-policy** command to remove the configuration.

By default, no route policy is applied to routes from/to the peer/peer group.

The **peer route-policy** command does not apply the **if-match interface** clause in the referenced route policy. Refer to *Route policy Commands* in the *IP Routing Volume* for related commands.

## Examples

# In IPv4 MBGP address family view, apply the route policy **test-policy** to routes outgoing to the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
[Sysname-bgp] peer test as-number 200
[Sysname-bgp] ipv4-family multicast
```

```
[Sysname-bgp-af-mul] peer test enable
[Sysname-bgp-af-mul] peer test route-policy test-policy export
```

## preference (MBGP family view)

### Syntax

```
preference { external-preference internal-preference local-preference | route-policy
route-policy-name }
undo preference
```

### View

IPv4 MBGP address family view

### Default Level

2: System level

### Parameters

*external-preference*: Preference of EBGP routes, in the range 1 to 255.

*internal-preference*: Preference of IBGP routes, in the range 1 to 255.

*local-preference*: Preference of local routes, in the range 1 to 255.

*route-policy-name*: Route policy name, a string of 1 to 19 characters. Using a route policy can set preferences for the routes matching it. As for the unmatched routes, the default preferences are adopted.

### Description

Use the **preference** command to configure preferences for external, internal, and local routes.

Use the **undo preference** command to restore the default.

The default preference values of external, internal and local BGP routes are 255, 255, and 130, respectively

### Examples

# In IPv4 MBGP address family view, configure preferences for EBGP, IBGP, and local IPv4 MBGP routes as 20, 20, and 200.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] preference 20 20 200
```

## reflect between-clients (MBGP family view)

### Syntax

```
reflect between-clients
undo reflect between-clients
```

### View

IPv4 MBGP address family view

## Default Level

2: System level

## Parameters

None

## Description

Use the **reflect between-clients** command to enable route reflection between clients.

Use the **undo reflect between-clients** command to disable this function.

By default, route reflection between clients is enabled.

After a route reflector is configured, it reflects the routes of a client to other clients. If the clients of a route reflector are fully meshed, you need to disable route reflection between clients to reduce routing costs.

Related commands: **reflector cluster-id** and **peer reflect-client**.

## Examples

```
# Disable route reflection between clients.
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] undo reflect between-clients
```

## reflector cluster-id (MBGP family view)

### Syntax

```
reflector cluster-id { cluster-id | ip-address }
undo reflector cluster-id
```

### View

IPv4 MBGP address family view

## Default Level

2: System level

## Parameters

*cluster-id*: Cluster ID of the route reflector, in the range 1 to 4294967295.

*ip-address*: Cluster ID of the route reflector, in the format of an IP address.

## Description

Use the **reflector cluster-id** command to configure the cluster ID of the route reflector.

Use the **undo reflector cluster-id** command to remove the configured cluster ID.

By default, each route reflector uses its router ID as the cluster ID.

A route is reflected by a route reflector from a client to another client. The router ID of the route reflector is the ID of the cluster. You can configure multiple route reflectors to improve network stability. If a

cluster has multiple route reflectors, you need to use the **reflector cluster-id** command to specify the same cluster ID for these route reflectors to avoid routing loops.

Related commands: **reflect between-clients**, **peer reflect-client**.

## Examples

# Specify 80 as the cluster ID for the route reflector, which is one of multiple route reflectors in the cluster.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] reflector cluster-id 80
```

## refresh bgp ipv4 multicast

### Syntax

```
refresh bgp ipv4 multicast { all | ip-address | group group-name | external | internal } { export | import }
```

### View

User view

### Default Level

2: Monitor level

### Parameters

**all**: Soft-resets all BGP connections.

*ip-address*: IP address of an IPv4 MBGP peer.

*group-name*: Peer group name, a string of 1 to 47 characters.

**external**: Soft-resets EBGP connections.

**internal**: Soft-resets IBGP connections.

**export**: Outbound soft reset.

**import**: Inbound soft reset.

### Description

Use the **refresh bgp ipv4 multicast** command to perform soft reset on specified IPv4 MBGP connections. This method can also refresh the MBGP routing table and apply a new route policy seamlessly.

To perform BGP soft reset, all routers in the network must support route-refresh. If there is a router not supporting the route-refresh function, you need to configure the **peer keep-all-routes** command to save all the routing information of the peer before BGP soft reset.

## Examples

# Soft-reset all the IPv4 MBGP connections.

```
<Sysname> refresh bgp ipv4 multicast all import
```

## reset bgp ipv4 multicast

### Syntax

```
reset bgp ipv4 multicast { all | as-number | ip-address | group group-name | external | internal }
```

### View

System view

### Default Level

2: Monitor level

### Parameters

**all**: Resets all MBGP connections.

*as-number*: Resets MBGP connections to peers in the AS.

*ip-address*: Resets the connection with an IPv4 MBGP peer.

**group group-name**: Resets connections with the specified BGP peer group.

**external**: Resets all the multicast EBGP connections.

**internal**: Resets all the multicast IBGP connections.

### Description

Use the **reset bgp ipv4 multicast** command to reset specified MBGP connections.

### Examples

```
# Reset all the IPv4 MBGP connections.
```

```
<Sysname> reset bgp ipv4 multicast all
```

## reset bgp ipv4 multicast dampening

### Syntax

```
reset bgp ipv4 multicast dampening [ ip-address [ mask | mask-length ] ]
```

### View

User view

### Default Level

2: Monitor level

### Parameters

*ip-address*: Destination IP address.

*mask*: Mask, in dotted decimal notation. The default is 255.255.255.255.

*mask-length*: Mask length, in the range 0 to 32. The default is 32.

### Description

Use the **reset bgp ipv4 multicast dampening** command to clear route dampening information and release suppressed routes.

Related commands: **dampening**, **display bgp multicast routing-table dampened**.

## Examples

```
# Clear damping information of route 20.1.0.0/16 and release the suppressed route.
```

```
<Sysname> reset bgp ipv4 multicast dampening 20.1.0.0 255.255.0.0
```

## reset bgp ipv4 multicast flap-info

### Syntax

```
reset bgp ipv4 multicast flap-info [ regex as-path-regexp | as-path-acl as-path-acl-number |  
ip-address [ mask | mask-length ] ]
```

### View

User view

### Default Level

2: Monitor level

### Parameters

*as-path-regexp*: Clears the flap statistics of routes matching the AS path regular expression, which is a string of 1 to 80 case-sensitive characters with spaces included.

*as-path-acl-number*: Clears the flap statistics for routes matching the AS path ACL, number of which is in the range 1 to 256.

*ip-address*: Clears the flap statistics of a route.

*mask*: Mask, in dotted decimal notation. The default is 255.255.255.255.

*mask-length*: Mask length, in the range 0 to 32. The default is 32.

### Description

Use the **reset bgp ipv4 multicast flap-info** command to clear IPv4 MBGP routing flap statistics.

The flap statistics of all the routes will be cleared if no parameter is specified.

## Examples

```
# Clear the flap statistics of all IPv4 MBGP routes matching AS path ACL 10.
```

```
<Sysname> reset bgp ipv4 multicast flap-info as-path-acl 10
```

## summary automatic (MBGP family view)

### Syntax

```
summary automatic
```

```
undo summary automatic
```

### View

IPv4 MBGP address family view

### Default Level

2: System level

## Parameters

None

## Description

Use the **summary automatic** command to enable automatic summarization for redistributed subnets.

Use the **undo summary automatic** command to disable automatic summarization.

By default, automatic summarization is disabled.

Note that:

- The default routes and the routes imported with the **network** command cannot be automatically summarized.
- The **summary automatic** command helps IPv4 MBGP limit the number of routes redistributed from IGP.

## Examples

# In IPv4 MBGP address family view, enable automatic route summarization.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] ipv4-family multicast
[Sysname-bgp-af-mul] summary automatic
```

# Table of Contents

<b>1 IGMP Snooping Configuration Commands</b> .....	<b>1-1</b>
IGMP Snooping Configuration Commands .....	1-1
display igmp-snooping group .....	1-1
display igmp-snooping statistics .....	1-2
fast-leave (IGMP-Snooping view) .....	1-3
group-policy (IGMP-Snooping view) .....	1-4
host-aging-time (IGMP-Snooping view) .....	1-5
igmp-snooping .....	1-6
igmp-snooping drop-unknown .....	1-6
igmp-snooping enable .....	1-7
igmp-snooping fast-leave .....	1-8
igmp-snooping general-query source-ip .....	1-9
igmp-snooping group-limit .....	1-9
igmp-snooping group-policy .....	1-10
igmp-snooping host-aging-time .....	1-12
igmp-snooping host-join .....	1-12
igmp-snooping last-member-query-interval .....	1-13
igmp-snooping max-response-time .....	1-14
igmp-snooping overflow-replace .....	1-15
igmp-snooping querier .....	1-16
igmp-snooping query-interval .....	1-16
igmp-snooping router-aging-time .....	1-17
igmp-snooping source-deny .....	1-18
igmp-snooping special-query source-ip .....	1-18
igmp-snooping static-group .....	1-19
igmp-snooping static-router-port .....	1-20
igmp-snooping version .....	1-21
last-member-query-interval (IGMP-Snooping view) .....	1-22
max-response-time (IGMP-Snooping view) .....	1-22
overflow-replace (IGMP-Snooping view) .....	1-23
report-aggregation (IGMP-Snooping view) .....	1-24
reset igmp-snooping group .....	1-24
reset igmp-snooping statistics .....	1-25
router-aging-time (IGMP-Snooping view) .....	1-25
source-deny (IGMP-Snooping view) .....	1-26

# 1 IGMP Snooping Configuration Commands

---

## IGMP Snooping Configuration Commands

### display igmp-snooping group

#### Syntax

```
display igmp-snooping group [ vlan vlan-id ] [ slot slot-number ] [ verbose ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

**vlan *vlan-id***: Displays the IGMP Snooping multicast group information in the specified VLAN, where *vlan-id* is in the range of 1 to 4094. If you do not specify a VLAN, this command will display the IGMP Snooping multicast group information in all VLANs.

**slot *slot-number***: Displays the IGMP Snooping multicast group information for the specified card. If you do not specify a slot, this command will display the IGMP Snooping multicast group information on the SRPU.

**verbose**: Specifies to display the detailed IGMP Snooping multicast group information.

#### Description

Use the **display igmp-snooping group** command to view the IGMP Snooping multicast group information.

#### Examples

# View the detailed IGMP Snooping multicast group information in VLAN 2.

```
<Sysname> display igmp-snooping group vlan 2 verbose
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Port flags: D-Dynamic port, S-Static port, C-Copy port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):2.
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Router port(s):total 1 port.
                GE1/0/1                (D) ( 00:01:30 )
```

```

IP group(s):the following ip group(s) match to one mac group.
IP group address:224.1.1.1
(0.0.0.0, 224.1.1.1):
Attribute:      Host Port
Host port(s):total 1 port.
GE1/0/2          (D) ( 00:03:23 )
MAC group(s):
MAC group address:0100-5e01-0101
Host port(s):total 1 port.
GE1/0/2

```

**Table 1-1** display igmp-snooping group command output description

Field	Description
Total 1 IP Group(s).	Total number of IP multicast groups
Total 1 IP Source(s).	Total number of multicast sources
Total 1 MAC Group(s).	Total number of MAC multicast groups
Port flags: D-Dynamic port, S-Static port, C-Copy port	Port flags: D for dynamic port, S for static port, C for port copied from a (*, G) entry to an (S, G) entry
Subvlan flags: R-Real VLAN, C-Copy VLAN	Sub-VLAN flags: R for real egress sub-VLAN under the current entry, C for sub-VLAN copied from a (*, G) entry to an (S, G) entry
Router port(s)	Number of router ports
( 00:01:30 )	Remaining time of the dynamic member port or router port aging timer. On a distributed device, to get this time value of a non-aggregation port that does not belong to the SRPU, you must specify the number of the slot where the corresponding board resides; this is not required on an aggregation port.
IP group address	Address of IP multicast group
(0.0.0.0, 224.1.1.1)	An (S, G), where 0.0.0.0 implies any multicast source
MAC group address	Address of MAC multicast group
Attribute	Attribute of IP multicast group
Host port(s)	Number of member ports

## display igmp-snooping statistics

### Syntax

```
display igmp-snooping statistics
```

### View

Any view

### Default Level

1: Monitor level

## Parameters

None

## Description

Use the **display igmp-snooping statistics** command to view the statistics information of IGMP messages learned by IGMP Snooping.

## Examples

# View the statistics information of IGMP messages learned by IGMP Snooping.

```
<Sysname> display igmp-snooping statistics
Received IGMP general queries:0.
Received IGMPv1 reports:0.
Received IGMPv2 reports:19.
Received IGMP leaves:0.
Received IGMPv2 specific queries:0.
Sent IGMPv2 specific queries:0.
Received IGMPv3 reports:1.
Received IGMPv3 reports with right and wrong records:0.
Received IGMPv3 specific queries:0.
Received IGMPv3 specific sg queries:0.
Sent IGMPv3 specific queries:0.
Sent IGMPv3 specific sg queries:0.
Received error IGMP messages:19.
```

**Table 1-2** display igmp-snooping statistics command output description

Field	Description
general queries	General query messages
specific queries	Group-specific query messages
reports	Report messages
leaves	Leave messages
reports with right and wrong records	Report messages with correct and incorrect records
specific sg query packet(s)	Group-and-source-specific query message(s)
error IGMP messages	IGMP messages with errors

## fast-leave (IGMP-Snooping view)

### Syntax

```
fast-leave [ vlan vlan-list ]
```

```
undo fast-leave [ vlan vlan-list ]
```

### View

IGMP-Snooping view

## Default Level

2: System level

## Parameters

**vlan** *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* to *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

## Description

Use the **fast-leave** command to enable fast leave processing globally.

Use the **undo fast-leave** command to disable fast leave processing globally.

By default, fast leave processing is disabled.

Note that:

- This command works on both IGMP Snooping–enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.
- If you do not specify any VLAN, the command will take effect for all VLANs; if you specify a VLAN or multiple VLANs, the command will take effect for the specified VLAN(s) only.

Related commands: **igmp-snooping fast-leave**.

## Examples

```
# Enable fast leave processing globally in VLAN 2.
```

```
<Sysname> system-view  
[Sysname] igmp-snooping  
[Sysname-igmp-snooping] fast-leave vlan 2
```

## group-policy (IGMP-Snooping view)

### Syntax

```
group-policy acl-number [ vlan vlan-list ]
```

```
undo group-policy [ vlan vlan-list ]
```

### View

IGMP-Snooping view

## Default Level

2: System level

## Parameters

*acl-number*: Basic or advanced ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced ACL rule is used to match the multicast source address(es) specified in IGMPv3 reports, rather than the source address in the IP packets. The system assumes that an IGMPv1 or IGMPv2 report or an IGMPv3 IS\_EX or TO\_EX report that does not carry a multicast source address carries a multicast source address of 0.0.0.0.

**vlan *vlan-list***: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

## Description

Use the **group-policy** command to configure a global multicast group filter.

Use the **undo group-policy** command to remove the configured global multicast group filter.

By default, no global multicast group filter is configured, namely a host can join any valid multicast group.

Note that:

- If you do not specify any VLAN, the command will take effect for all VLANs; if you specify a VLAN or multiple VLANs, the command will take effect for the specified VLAN(s) only.
- If the specified ACL does not exist or the ACL rule is null, all multicast groups will be filtered out.
- You can configure different ACL rules for a port in different VLANs; for a given VLAN, a newly configured ACL rule will override the existing one.

Related commands: **igmp-snooping group-policy**.

## Examples

```
# Apply ACL 2000 as a multicast group filter in VLAN 2.
```

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] group-policy 2000 vlan 2
```

## host-aging-time (IGMP-Snooping view)

### Syntax

```
host-aging-time interval
```

```
undo host-aging-time
```

### View

```
IGMP-Snooping view
```

### Default Level

```
2: System level
```

### Parameters

*interval*: Dynamic member port aging time, in seconds. The effective range is 200 to 1,000.

## Description

Use the **host-aging-time** command to configure the aging time of dynamic member ports globally.

Use the **undo host-aging-time** command to restore the default setting.

By default, the aging time of dynamic member ports is 260 seconds.

This command works only on IGMP Snooping-enabled VLANs, but not on VLANs with IGMP enabled on their VLAN interfaces.

Related commands: **igmp-snooping host-aging-time**.

## Examples

```
# Set the aging time of dynamic member ports globally to 300 seconds.
```

```
<Sysname> system-view  
[Sysname] igmp-snooping  
[Sysname-igmp-snooping] host-aging-time 300
```

## igmp-snooping

### Syntax

```
igmp-snooping  
undo igmp-snooping
```

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **igmp-snooping** command to enable IGMP Snooping globally and enter IGMP-Snooping view.

Use the **undo igmp-snooping** command to disable IGMP Snooping globally.

By default, IGMP Snooping is disabled.

Related commands: **igmp-snooping enable**.

## Examples

```
# Enable IGMP Snooping globally and enter IGMP-Snooping view.
```

```
<Sysname> system-view  
[Sysname] igmp-snooping  
[Sysname-igmp-snooping]
```

## igmp-snooping drop-unknown

### Syntax

```
igmp-snooping drop-unknown  
undo igmp-snooping drop-unknown
```

### View

VLAN view

## Default Level

2: System level

## Parameters

None

## Description

Use the **igmp-snooping drop-unknown** command to enable the function of dropping unknown multicast data in the current VLAN, so that such multicast data will only be forwarded to router ports.

Use the **undo igmp-snooping drop-unknown** command to disable the function of dropping unknown multicast data in the current VLAN.

By default, this function is disabled, that is, unknown multicast data is flooded.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

Related commands: **drop-unknown**.

## Examples

```
# In VLAN 2, enable the function of dropping unknown multicast data.
```

```
<Sysname> system-view  
[Sysname] vlan 2  
[Sysname-vlan2] igmp-snooping drop-unknown
```

## igmp-snooping enable

### Syntax

```
igmp-snooping enable  
undo igmp-snooping enable
```

### View

VLAN view

## Default Level

2: System level

## Parameters

None

## Description

Use the **igmp-snooping enable** command to enable IGMP Snooping in the current VLAN.

Use the **undo igmp-snooping enable** command to disable IGMP Snooping in the current VLAN.

By default, IGMP Snooping is disabled in a VLAN.

IGMP Snooping must be enabled globally before it can be enabled in a VLAN.

Related commands: **igmp-snooping**.

## Examples

```
# Enable IGMP Snooping in VLAN 2.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
```

## igmp-snooping fast-leave

### Syntax

```
igmp-snooping fast-leave [ vlan vlan-list ]
undo igmp-snooping fast-leave [ vlan vlan-list ]
```

### View

Ethernet port view, Layer 2 aggregate port view, port group view

### Default Level

2: System level

### Parameters

**vlan** *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

### Description

Use the **igmp-snooping fast-leave** command to enable fast leave processing on the current port or group of ports.

Use the **undo igmp-snooping fast-leave** command to disable fast leave processing on the current port or group of ports.

By default, fast leave processing is disabled.

Note that:

- This command works on both IGMP Snooping-enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.
- If you do not specify any VLAN when using this command in Ethernet port view or Layer 2 aggregate port view, the command will take effect for all VLANs the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the port belongs to the specified VLAN(s).
- If you do not specify any VLAN when using this command in port group view, the command will take effect on all the ports in this group; if you specify a VLAN or multiple VLANs, the command will take effect only on those ports in this group that belong to the specified VLAN(s).

Related commands: **fast-leave**.

## Examples

```
# Enable fast leave processing on GigabitEthernet1/0/1 in VLAN 2.
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping fast-leave vlan 2
```

## igmp-snooping general-query source-ip

### Syntax

```
igmp-snooping general-query source-ip { current-interface | ip-address }
undo igmp-snooping general-query source-ip
```

### View

VLAN view

### Default Level

2: System level

### Parameters

**current-interface**: Sets the source address of IGMP general queries to the address of the current VLAN interface. If the current VLAN interface does not have an IP address, the default IP address 0.0.0.0 will be used as the source IP address of IGMP general queries.

*ip-address*: Specifies the source address of IGMP general queries, which can be any legal IP address.

### Description

Use the **igmp-snooping general-query source-ip** command to configure the source address of IGMP general queries.

Use the **undo igmp-snooping general-query source-ip** command to restore the default configuration.

By default, the source IP address of IGMP general queries is 0.0.0.0.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

## Examples

```
# In VLAN 2 specify 10.1.1.1 as the source IP address of IGMP general queries.
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping general-query source-ip 10.1.1.1
```

## igmp-snooping group-limit

### Syntax

```
igmp-snooping group-limit limit [ vlan vlan-list ]
undo igmp-snooping group-limit [ vlan vlan-list ]
```

## View

Ethernet port view, Layer 2 aggregate port view, port group view

## Default Level

2: System level

## Parameters

*limit*: Maximum number of multicast groups that can be joined on a port. The effective range is 1 to 1024.

**vlan** *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

## Description

Use the **igmp-snooping group-limit** command to configure the maximum number of multicast groups that can be joined on a port.

Use the **undo igmp-snooping group-limit** command to restore the default setting.

The default the maximum number of multicast groups is 1024.

Note that:

- You can also use the **igmp group-limit** command to limit the number of multicast groups that can be joined on an port. However, if you configure a limit of the number of groups for ports in a VLAN while you have configured a limit of the number of groups for the VLAN interface of the same VLAN, or vice versa, this may cause inconsistencies between Layer 2 and Layer 3 table entries. Therefore, it is recommended to configure a limit of the number of multicast groups only on the VLAN interface.
- If you do not specify any VLAN when using this command in Ethernet port view or Layer 2 aggregate port view, the command will take effect for all VLANs the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the port belongs to the specified VLAN(s).
- If you do not specify any VLAN when using this command in port group view, the command will take effect on all the ports in this group; if you specify a VLAN or multiple VLANs, the command will take effect only on those ports in this group that belong to the specified VLAN(s).

Related commands: **igmp group-limit** in *IGMP Commands* in the *IP Multicast Volume*.

## Examples

```
# Specify to allow a maximum of 10 multicast groups to be joined on GigabitEthernet1/0/1 in VLAN 2.
```

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping group-limit 10 vlan 2
```

## igmp-snooping group-policy

### Syntax

```
igmp-snooping group-policy acl-number [ vlan vlan-list ]
```

**undo igmp-snooping group-policy [ vlan *vlan-list* ]**

## View

Ethernet port view, Layer 2 aggregate port view, port group view

## Default Level

2: System level

## Parameters

*acl-number*: Basic or advanced ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced ACL rule is used to match the multicast source address(es) specified in IGMPv3 reports, rather than the source address in the IP packets. The system assumes that an IGMPv1 or IGMPv2 report or an IGMPv3 IS\_EX and TO\_EX report that does not carry a multicast source address carries a multicast source address of 0.0.0.0.

**vlan *vlan-list***: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

## Description

Use the **igmp-snooping group-policy** command to configure a multicast group filter on the current port(s).

Use the **undo igmp-snooping group-policy** command to remove a multicast group filter on the current port(s).

By default, no multicast group filter is configured on an port, namely a host can join any valid multicast group.

Note that:

- If you do not specify any VLAN when using this command in Ethernet port view or Layer 2 aggregate port view, the command will take effect for all VLANs the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the port belongs to the specified VLAN(s).
- If you do not specify any VLAN when using this command in port group view, the command will take effect on all the ports in this group; if you specify a VLAN or multiple VLANs, the command will take effect only on those ports in this group that belong to the specified VLAN(s).
- If the specified ACL does not exist or the ACL rule is null, all multicast groups will be filtered out.
- You can configure different ACL rules for a port in different VLANs; for a given VLAN, a newly configured ACL rule will override the existing one.

Related commands: **group-policy**.

## Examples

```
# Apply ACL 2000 as a multicast group filter on GigabitEthernet1/0/1 in VLAN 2.
```

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] igmp-snooping group-policy 2000 vlan 2
```

## igmp-snooping host-aging-time

### Syntax

```
igmp-snooping host-aging-time interval  
undo igmp-snooping host-aging-time
```

### View

VLAN view

### Default Level

2: System level

### Parameters

*interval*: Dynamic member port aging time, in seconds. The effective range is 200 to 1,000.

### Description

Use the **igmp-snooping host-aging-time** command to configure the aging time of dynamic member ports in the current VLAN.

Use the **undo igmp-snooping host-aging-time** command to restore the default setting.

By default, the aging time of dynamic member ports is 260 seconds.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

Related commands: **host-aging-time**.

### Examples

```
# Set the aging time of dynamic member ports to 300 seconds in VLAN 2.
```

```
<Sysname> system-view  
[Sysname] vlan 2  
[Sysname-vlan2] igmp-snooping host-aging-time 300
```

## igmp-snooping host-join

### Syntax

```
igmp-snooping host-join group-address [ source-ip source-address ] vlan vlan-id  
undo igmp-snooping host-join group-address [ source-ip source-address ] vlan vlan-id
```

### View

Ethernet port view, Layer 2 aggregate port view, port group view

### Default Level

2: System level

### Parameters

*group-address*: Address of the multicast group that the simulated host is to join, in the range of 224.0.1.0 to 239.255.255.255.

*source-address*: Address of the multicast source that the simulated host is to join. The value of this argument should be a valid unicast address or 0.0.0.0. If the value is 0.0.0.0, this means that no multicast source is specified.

**vlan** *vlan-id*: Specifies the VLAN that comprises the port(s), where *vlan-id* is in the range of 1 to 4094.

## Description

Use the **igmp-snooping host-join** command to configure the current port(s) as simulated member host(s) for the specified multicast group or source and group.

Use the **undo igmp-snooping host-join** command to remove the current port(s) as simulated member host(s) for the specified multicast group or source and group.

By default, this function is disabled.

Note that:

- This command works on both IGMP Snooping-enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces. The version of IGMP on the simulated host depends on the version of IGMP Snooping running in the VLAN or the version of IGMP running on the VLAN interface.
- The **source-ip** *source-address* option in the command is meaningful only for IGMP Snooping version 3. If IGMP Snooping version 2 is running, although you can include **source-ip** *source-address* in the command, the simulated host does not respond to a query message.
- If configured in Ethernet port view or Layer 2 aggregate port view, this feature takes effect only if the port belongs to the specified VLAN.
- If configured in port group view, this feature takes effect only on those ports in this port group that belong to the specified VLAN.

## Examples

# Configure GigabitEthernet1/0/1 as a simulated member host in VLAN 2 for multicast source 1.1.1.1 and multicast group 232.1.1.1.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping host-join 232.1.1.1 source-ip 1.1.1.1 vlan 2
```

## igmp-snooping last-member-query-interval

### Syntax

**igmp-snooping last-member-query-interval** *interval*

**undo igmp-snooping last-member-query-interval**

### View

VLAN view

## Default Level

2: System level

## Parameters

*interval*: Interval between IGMP last-member queries, in seconds. The effective range is 1 to 5.

## Description

Use the **igmp-snooping last-member-query-interval** command to configure the interval between IGMP last-member queries in the VLAN.

Use the **undo igmp-snooping last-member-query-interval** command to restore the default setting.

By default, the IGMP last-member query interval is 1 second.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

Related commands: **last-member-query-interval**.

## Examples

# Set the interval between IGMP last-member queries to 3 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping last-member-query-interval 3
```

## igmp-snooping max-response-time

### Syntax

```
igmp-snooping max-response-time interval
undo igmp-snooping max-response-time
```

### View

VLAN view

## Default Level

2: System level

## Parameters

*interval*: Maximum response time to IGMP general queries, in seconds. The effective range is 1 to 25.

## Description

Use the **igmp-snooping max-response-time** command to configure the maximum response time to IGMP general queries in the VLAN.

Use the **undo igmp-snooping max-response-time** command to restore the default setting.

By default, the maximum response time to IGMP general queries is 10 seconds.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

Related commands: **max-response-time**, **igmp-snooping query-interval**.

## Examples

```
# Set the maximum response time to IGMP general queries to 5 seconds in VLAN 2.
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping max-response-time 5
```

## igmp-snooping overflow-replace

### Syntax

```
igmp-snooping overflow-replace [ vlan vlan-list ]
undo igmp-snooping overflow-replace [ vlan vlan-list ]
```

### View

Ethernet port view, Layer 2 aggregate port view, port group view

### Default Level

2: System level

### Parameters

**vlan** *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

### Description

Use the **igmp-snooping overflow-replace** command to enable the multicast group replacement function on the current port(s).

Use the **undo igmp-snooping overflow-replace** command to disable the multicast group replacement function on the current port(s).

By default, the multicast group replacement function is disabled.

Note that:

- This command works on both IGMP Snooping-enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.
- If you do not specify any VLAN when using this command in Ethernet port view or Layer 2 aggregate port view, the command will take effect for all VLANs the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the port belongs to the specified VLAN(s).
- If you do not specify any VLAN when using this command in port group view, the command will take effect on all the ports in this group; if you specify a VLAN or multiple VLANs, the command will take effect only on those ports in this group that belong to the specified VLAN(s).

Related commands: **overflow-replace**.

## Examples

```
# Enable the multicast group replacement function on GigabitEthernet1/0/1 in VLAN 2.
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping overflow-replace vlan 2
```

## igmp-snooping querier

### Syntax

```
igmp-snooping querier
undo igmp-snooping querier
```

### View

VLAN view

### Default Level

2: System level

### Parameters

None

### Description

Use the **igmp-snooping querier** command to enable the IGMP Snooping querier function.

Use the **undo igmp-snooping querier** command to disable the IGMP Snooping querier function.

By default, the IGMP Snooping querier function is disabled.

Note that:

- This command takes effect only if IGMP Snooping is enabled in the VLAN.
- This command does not take effect in a sub-VLAN of a multicast VLAN.

Related commands: **subvlan** in *Multicast VLAN Commands* in the *IP Multicast Volume*.

### Examples

```
# Enable the IGMP Snooping querier function in VLAN 2.
```

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping querier
```

## igmp-snooping query-interval

### Syntax

```
igmp-snooping query-interval interval
undo igmp-snooping query-interval
```

### View

VLAN view

### Default Level

2: System level

## Parameters

*interval*: Interval between IGMP general queries, in seconds. The effective range is 2 to 300.

## Description

Use the **igmp-snooping query-interval** command to configure the interval between IGMP general queries.

Use the **undo igmp-snooping query-interval** command to restore the default setting.

By default, the IGMP general query interval is 60 seconds.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

Related commands: **igmp-snooping querier**, **igmp-snooping max-response-time**, **max-response-time**.

## Examples

```
# Set the interval between IGMP general queries to 20 seconds in VLAN 2.
```

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping query-interval 20
```

## igmp-snooping router-aging-time

### Syntax

```
igmp-snooping router-aging-time interval
undo igmp-snooping router-aging-time
```

### View

VLAN view

### Default Level

2: System level

## Parameters

*interval*: Dynamic router port aging time, in seconds. The effective range is 1 to 1,000.

## Description

Use the **igmp-snooping router-aging-time** command to configure the aging time of dynamic router ports in the current VLAN.

Use the **undo igmp-snooping router-aging-time** command to restore the default setting.

By default, the aging time of dynamic router ports is 105 seconds.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

Related commands: **router-aging-time**.

## Examples

```
# Set the aging time of dynamic router ports to 100 seconds in VLAN 2.
```

```
<Sysname> system-view
```

```
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping router-aging-time 100
```

## igmp-snooping source-deny

### Syntax

```
igmp-snooping source-deny
undo igmp-snooping source-deny
```

### View

Ethernet port view, port group view

### Default Level

2: System level

### Parameters

None

### Description

Use the **igmp-snooping source-deny** command to enable multicast source port filtering.

Use the **undo igmp-snooping source-deny** command to disable multicast source port filtering.

By default, multicast source port filtering is disabled.

This command works on both IGMP Snooping-enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.

### Examples

```
# Enable source port filtering for multicast data on GigabitEthernet1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping source-deny
```

## igmp-snooping special-query source-ip

### Syntax

```
igmp-snooping special-query source-ip { current-interface | ip-address }
undo igmp-snooping special-query source-ip
```

### View

VLAN view

### Default Level

2: System level

### Parameters

**current-interface**: Sets the source address of IGMP group-specific queries to the address of the current VLAN interface. If the current VLAN interface does not have an IP address, the default IP

address 0.0.0.0 will be used as the source IP address of IGMP group-specific queries.

*ip-address*: Sets the source address of IGMP group-specific queries to the specified address.

## Description

Use the **igmp-snooping special-query source-ip** command to configure the source IP address of IGMP group-specific queries.

Use the **undo igmp-snooping special-query source-ip** command to restore the default configuration.

By default, the source IP address of IGMP group-specific queries is 0.0.0.0.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

## Examples

# In VLAN 2 specify 10.1.1.1 as the source IP address of IGMP group-specific queries.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping special-query source-ip 10.1.1.1
```

## igmp-snooping static-group

### Syntax

```
igmp-snooping static-group group-address [ source-ip source-address ] vlan vlan-id
undo igmp-snooping static-group group-address [ source-ip source-address ] vlan vlan-id
```

### View

Ethernet port view, Layer 2 aggregate port view, port group view

### Default Level

2: System level

### Parameters

*group-address*: Address of the multicast group to be statically joined, in the range of 224.0.0.0 to 239.255.255.255.

*source-address*: Address of the multicast source to be statically joined. The value of this argument should be a valid unicast address or 0.0.0.0. If the value is 0.0.0.0, this means no multicast source is specified.

**vlan** *vlan-id*: Specifies the VLAN that comprises the port(s), where *vlan-id* is in the range of 1 to 4094.

## Description

Use the **igmp-snooping static-group** command to configure the static (\*, G) or (S, G) joining function, namely to configure the current port or port group as static multicast group or source-group member(s).

Use the **undo igmp-snooping static-group** command to restore the system default.

By default, no ports are static member ports.

Note that:

- The **source-ip** *source-address* option in the command is meaningful only for IGMP Snooping version 3. If IGMP Snooping version 2 is running, although you can include the **source-ip** *source-address* option in your command, the configuration will not take effect.
- If configured in Ethernet port view or Layer 2 aggregate port view, this feature takes effect only if the port belongs to the specified VLAN.
- If configured in port group view, this feature takes effect only on those ports in this port group that belong to the specified VLAN.

## Examples

# Configure GigabitEthernet1/0/1 in VLAN 2 to be a static member port for (1.1.1.1, 232.1.1.1).

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping static-group 232.1.1.1 source-ip 1.1.1.1 vlan
2
```

## igmp-snooping static-router-port

### Syntax

**igmp-snooping static-router-port** vlan *vlan-id*

**undo igmp-snooping static-router-port** vlan *vlan-id*

### View

Ethernet port view, Layer 2 aggregate port view, port group view

### Default Level

2: System level

### Parameters

**vlan** *vlan-id*: Specifies a VLAN in which one or more static router ports are to be configured, where *vlan-id* is in the range of 1 to 4094.

### Description

Use the **igmp-snooping static-router-port** command to configure the current port(s) as static router port(s).

Use the **undo igmp-snooping static-router-port** command to restore the system default.

By default, no ports are static router ports.

Note that:

- This command works on both IGMP Snooping-enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.
- This command does not take effect in a sub-VLAN of a multicast VLAN.

- If configured in Ethernet port view or Layer 2 aggregate port view, this feature takes effect only if the port belongs to the specified VLAN.
- If configured in port group view, this feature takes effect only on those ports in this port group that belong to the specified VLAN.

Related commands: **subvlan** in *Multicast VLAN Commands* in the *IP Multicast Volume*.

## Examples

```
# Enable the static router port function on GigabitEthernet1/0/1 in VLAN 2.
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping static-router-port vlan 2
```

## igmp-snooping version

### Syntax

```
igmp-snooping version version-number
undo igmp-snooping version
```

### View

VLAN view

### Default Level

2: System level

### Parameters

*version-number*: IGMP snooping version, in the range of 2 to 3.

### Description

Use the **igmp-snooping version** command to configure the IGMP Snooping version.

Use the **undo igmp-snooping version** command to restore the default setting.

By default, the IGMP Snooping version is 2.

Note that:

- This command can take effect only if IGMP Snooping is enabled in the VLAN.
- This command does not take effect in a sub-VLAN of a multicast VLAN.

Related commands: **igmp-snooping enable**; **subvlan** in *Multicast VLAN Commands* in the *IP Multicast Volume*.

## Examples

```
# Enable IGMP Snooping in VLAN 2, and set the IGMP Snooping version to version 3.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
```

## last-member-query-interval (IGMP-Snooping view)

### Syntax

```
last-member-query-interval interval  
undo last-member-query-interval
```

### View

IGMP-Snooping view

### Default Level

2: System level

### Parameters

*interval*: Interval between IGMP last-member queries, in seconds. The effective range is 1 to 5.

### Description

Use the **last-member-query-interval** command to configure the interval between IGMP last-member queries globally.

Use the **undo last-member-query-interval** command to restore the default setting.

By default, the interval between IGMP last-member queries is 1 second.

This command works only on IGMP Snooping-enabled VLANs, but not on VLANs with IGMP enabled on their VLAN interfaces.

Related commands: **igmp-snooping last-member-query-interval**.

### Examples

```
# Set the interval between IGMP last-member queries globally to 3 seconds.
```

```
<Sysname> system-view  
[Sysname] igmp-snooping  
[Sysname-igmp-snooping] last-member-query-interval 3
```

## max-response-time (IGMP-Snooping view)

### Syntax

```
max-response-time interval  
undo max-response-time
```

### View

IGMP-Snooping view

### Default Level

2: System level

### Parameters

*interval*: Maximum response time to IGMP general queries, in seconds. The effective range is 1 to 25.

## Description

Use the **max-response-time** command to configure the maximum response time to IGMP general queries globally.

Use the **undo max-response-time** command to restore the default value.

This command works only on IGMP Snooping–enabled VLANs, but not on VLANs with IGMP enabled on their VLAN interfaces.

Related commands: **igmp-snooping max-response-time**, **igmp-snooping query-interval**.

## Examples

```
# Set the maximum response time to IGMP general queries globally to 5 seconds.
```

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] max-response-time 5
```

## overflow-replace (IGMP-Snooping view)

### Syntax

```
overflow-replace [ vlan vlan-list ]
undo overflow-replace [ vlan vlan-list ]
```

### View

IGMP-Snooping view

### Default Level

2: System level

### Parameters

**vlan** *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* to *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

## Description

Use the **overflow-replace** command to enable the multicast group replacement function globally.

Use the **undo overflow-replace** command to disable the multicast group replacement function globally.

By default, the multicast group replacement function is disabled.

Note that:

- This command works on both IGMP Snooping–enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.
- If you do not specify any VLAN, the command will take effect for all VLANs; if you specify a VLAN or multiple VLANs, the command will take effect for the specified VLAN(s) only.

Related commands: **igmp-snooping overflow-replace**.

## Examples

```
# Enable the multicast group replacement function globally in VLAN 2.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] overflow-replace vlan 2
```

## report-aggregation (IGMP-Snooping view)

### Syntax

```
report-aggregation
undo report-aggregation
```

### View

IGMP-Snooping view

### Default Level

2: System level

### Parameters

None

### Description

Use the **report-aggregation** command to enable IGMP report suppression.

Use the **undo report-aggregation** command to disable IGMP report suppression.

By default, IGMP report suppression is enabled.

This command works on both IGMP Snooping-enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.

## Examples

```
# Disable IGMP report suppression.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] undo report-aggregation
```

## reset igmp-snooping group

### Syntax

```
reset igmp-snooping group { group-address | all } [ vlan vlan-id ]
```

### View

User view

### Default Level

2: System level

## Parameters

**group-address:** Clears the information about the specified multicast group. The value range of *group-address* is 224.0.1.0 to 239.255.255.255.

**all:** Clears all IGMP Snooping multicast group information.

**vlan *vlan-id*:** Clears the IGMP Snooping multicast group information in the specified VLAN. The effective range of *vlan-id* is 1 to 4094.

## Description

Use the **reset igmp-snooping group** command to clear IGMP Snooping multicast group information.

Note that:

- This command works only on IGMP Snooping-enabled VLANs, but not on VLANs with IGMP enabled on their VLAN interfaces.
- This command cannot clear IGMP Snooping multicast group information of static joins.

## Examples

```
# Clear all IGMP Snooping multicast group information.
```

```
<Sysname> reset igmp-snooping group all
```

## reset igmp-snooping statistics

### Syntax

```
reset igmp-snooping statistics
```

### View

User view

### Default Level

2: System level

### Parameters

None

### Description

Use the **reset igmp-snooping statistics** command to clear the statistics information of IGMP messages learned by IGMP Snooping.

### Examples

```
# Clear the statistics information of all kinds of IGMP messages learned by IGMP Snooping.
```

```
<Sysname> reset igmp-snooping statistics
```

## router-aging-time (IGMP-Snooping view)

### Syntax

```
router-aging-time interval
```

```
undo router-aging-time
```

## View

IGMP-Snooping view

## Default Level

2: System level

## Parameters

*interval*: Dynamic router port aging time, in seconds. The effective range is 1 to 1,000.

## Description

Use the **router-aging-time** command to configure the aging time of dynamic router ports globally.

Use the **undo router-aging-time** command to restore the default setting.

By default, the aging time of dynamic router ports is 105 seconds.

This command works only on IGMP Snooping-enabled VLANs, but not on VLANs with IGMP enabled on their VLAN interfaces.

Related commands: **igmp-snooping router-aging-time**.

## Examples

```
# Set the aging time of dynamic router ports globally to 100 seconds.
```

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] router-aging-time 100
```

## source-deny (IGMP-Snooping view)

### Syntax

**source-deny port** *interface-list*

**undo source-deny port** *interface-list*

### View

IGMP-Snooping view

### Default Level

2: System level

### Parameters

*interface-list*: Specifies one or multiple ports. You can provide up to ten port lists, by each of which you can specify an individual port in the form of *interface-type interface-number*, or a port range in the form of *interface-type start-interface-number to interface-type end-interface-number*, where the end interface number must be greater than the start interface number.

### Description

Use the **source-deny** command to enable multicast source port filtering so that all multicast data packets are blocked.

Use the **undo source-deny** command to disable multicast source port filtering.

By default, multicast source port filtering is not enabled.

This command works on both IGMP Snooping-enabled VLANs and VLANs with IGMP enabled on their VLAN interfaces.

### Examples

# Enable source port filtering for multicast data on interfaces GigabitEthernet1/0/1 through GigabitEthernet1/0/4.

```
<Sysname> system-view
```

```
[Sysname] igmp-snooping
```

```
[Sysname-igmp-snooping] source-deny port gigabitethernet1/0/1 to gigabitethernet1/0/4
```

# Table of Contents

<b>1 Multicast VLAN Configuration Commands</b> .....	<b>1-1</b>
Multicast VLAN Configuration Commands.....	1-1
display multicast-vlan .....	1-1
multicast-vlan.....	1-2
port (multicast VLAN view) .....	1-3
port multicast-vlan .....	1-3
subvlan (multicast VLAN view).....	1-4

# 1 Multicast VLAN Configuration Commands

## Multicast VLAN Configuration Commands

### display multicast-vlan

#### Syntax

```
display multicast-vlan [ vlan-id ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

*vlan-id*: VLAN ID of a multicast VLAN, in the range of 1 to 4094. If this argument is not provided, the information about all multicast VLANs will be displayed.

#### Description

Use the **display multicast-vlan** command to view the information about the specified multicast VLAN.

#### Examples

# View the information about all multicast VLANs.

```
<Sysname> display multicast-vlan
Total 1 multicast-vlan(s)

Multicast vlan 100
  subvlan list:
    vlan 2  4-6
  port list:
    no port
```

**Table 1-1** display multicast-vlan command output description

Field	Description
Total 1 multicast-vlan(s)	Total number of multicast VLANs
Multicast vlan	A multicast VLAN
subvlan list	List of sub-VLANs of the multicast VLAN
port list	Port list of the multicast VLAN

## multicast-vlan

### Syntax

```
multicast-vlan vlan-id  
undo multicast-vlan { all | vlan-id }
```

### View

System view

### Default Level

2: System level

### Parameters

*vlan-id*: Specifies a VLAN by its ID, in the range of 1 to 4094.

**all**: Deletes all multicast VLANs.

### Description

Use the **multicast-vlan** command to configure the specified VLAN as a multicast VLAN and enter multicast VLAN view.

Use the **undo multicast-vlan** command to remove the specified VLAN as a multicast VLAN.

The VLAN to be configured is not a multicast VLAN by default.

Note that:

- The specified VLAN to be configured as a multicast VLAN must exist.
- The multicast VLAN feature cannot be enabled on a device with IP multicast routing enabled.
- For a sub-VLAN-based multicast VLAN, you need to enable IGMP Snooping only in the multicast VLAN; for a port-based multicast VLAN, you need to enable IGMP Snooping in both the multicast VLAN and all the user VLANs.

Related commands: **multicast routing-table** in the *Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*; **igmp-snooping enable** in the *IGMP Snooping Commands* in the *IP Multicast Volume*.

### Examples

# Enable IGMP Snooping in VLAN 100. Configure it as a multicast VLAN and enter multicast VLAN view.

```
<Sysname> system-view  
[Sysname] igmp-snooping  
[Sysname-igmp-snooping] quit  
[Sysname] vlan 100  
[Sysname-vlan100] igmp-snooping enable  
[Sysname-vlan100] quit  
[Sysname] multicast-vlan 100  
[Sysname-mvlan-100]
```

## port (multicast VLAN view)

### Syntax

```
port interface-list  
undo port { all | interface-list }
```

### View

Multicast VLAN view

### Default Level

2: System level

### Parameters

*interface-list*: Specifies a port in the form of *interface-type interface-number*, or a port range in the form of *interface-type start-interface-number to interface-type end-interface-number*, where the end interface number must be greater than the start interface number.

**all**: Deletes all the ports in the current multicast VLAN.

### Description

Use the **port** command to assign the specified port(s) to the current multicast VLAN.

Use the **undo port** command to delete the specified port(s) or all ports from the current multicast VLAN.

By default, a multicast VLAN has no ports.

Note that:

- A port can belong to only one multicast VLAN.
- Only the following types of ports can be configured as multicast VLAN ports: Ethernet, or Layer 2 aggregate ports.

### Examples

```
# Assign ports GigabitEthernet1/0/1 through GigabitEthernet1/0/5 to multicast VLAN 100.  
<Sysname> system-view  
[Sysname] multicast-vlan 100  
[Sysname-mvlan-100] port gigabitethernet1/0/1 to gigabitethernet1/0/5
```

## port multicast-vlan

### Syntax

```
port multicast-vlan vlan-id  
undo port multicast-vlan
```

### View

Ethernet port view, Layer 2 aggregate port view, port group view.

### Default Level

2: System level

## Parameters

*vlan-id*: VLAN ID of the multicast VLAN you want to assign the current port(s) to, in the range of 1 to 4094.

## Description

Use the **port multicast-vlan** command to assign the current port(s) to the specified multicast VLAN.

Use the **undo port multicast-vlan** command to restore the system default.

By default, a port does not belong to any multicast VLAN.

Note that a port can belong to only one multicast VLAN.

## Examples

```
# Assign GigabitEthernet1/0/1 to multicast VLAN 100.
```

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-gigabitethernet1/0/1] port multicast-vlan 100
```

## subvlan (multicast VLAN view)

### Syntax

```
subvlan vlan-list
```

```
undo subvlan { all | vlan-list }
```

### View

Multicast VLAN view

### Default Level

2: System level

## Parameters

*vlan-list*: Specifies a VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

**all**: Deletes all the sub-VLANs of the current multicast VLAN.

## Description

Use the **subvlan** command to configure sub-VLAN(s) for the current multicast VLAN.

Use the **undo subvlan** command to remove the specified sub-VLAN(s) or all sub-VLANs from the current multicast VLAN.

A multicast VLAN has no sub-VLANs by default.

Note that:

- The VLANs to be configured as sub-VLANs of the multicast VLAN must exist and must not be multicast VLANs or sub-VLANs of another multicast VLAN.
- The number of sub-VLANs of the multicast VLAN must not exceed 127

## Examples

# Configure VLAN 10 through VLAN 15 as sub-VLANs of multicast VLAN 100.

```
<Sysname> system-view  
[Sysname] multicast-vlan 100  
[Sysname-mvlan-100] subvlan 10 to 15
```

# Table of Contents

<b>1 IPv6 Multicast Routing and Forwarding Configuration Commands .....</b>	<b>1-1</b>
IPv6 Multicast Routing and Forwarding Configuration Commands .....	1-1
display multicast ipv6 boundary .....	1-1
display multicast ipv6 forwarding-table.....	1-2
display multicast ipv6 routing-table .....	1-4
display multicast ipv6 rpf-info .....	1-6
multicast ipv6 boundary.....	1-7
multicast ipv6 forwarding-table downstream-limit .....	1-8
multicast ipv6 forwarding-table route-limit.....	1-8
multicast ipv6 load-splitting .....	1-9
multicast ipv6 longest-match .....	1-10
multicast ipv6 routing-enable.....	1-10
reset multicast ipv6 forwarding-table.....	1-11
reset multicast ipv6 routing-table.....	1-12

# 1 IPv6 Multicast Routing and Forwarding Configuration Commands

---



## Note

The term “router” in this document refers to a router in a generic sense or a Layer 3 switch running an IP multicast routing protocol.

---

## IPv6 Multicast Routing and Forwarding Configuration Commands

### display multicast ipv6 boundary

#### Syntax

```
display multicast ipv6 boundary [ ipv6-group-address [ prefix-length ] interface interface-type  
interface-number ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

*ipv6-group-address*: IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number from 0 through F.

*prefix-length*: Prefix length of an IPv6 multicast group address, in the range of 8 to 128. The system default is 128.

*interface-type interface-number*: Specifies an interface by its type and number.

#### Description

Use the **display multicast ipv6 boundary** command to display the IPv6 multicast boundary information on the specified interface or all interfaces.

Related commands: **multicast ipv6 boundary**.

#### Examples

```
# Display the IPv6 multicast boundary information configured on all interfaces.
```

```
<Sysname> display multicast ipv6 boundary
```

IPv6 multicast boundary information

Boundary	Interface
FF03::/16	Vlan1
FF09::/16	Vlan2

**Table 1-1** display multicast ipv6 boundary command output description

Field	Description
IPv6 multicast boundary information	IPv6 multicast boundary
Boundary	IPv6 multicast group corresponding to the IPv6 multicast boundary
Interface	Boundary interface corresponding to the IPv6 multicast boundary

## display multicast ipv6 forwarding-table

### Syntax

```
display multicast ipv6 forwarding-table [ ipv6-source-address [ prefix-length ] | ipv6-group-address  
[ prefix-length ] | incoming-interface { interface-type interface-number | register } |  
outgoing-interface { { exclude | include | match } { interface-type interface-number | register } } |  
statistics | slot slot-number ] * [ port-info ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ipv6-source-address*: IPv6 multicast source address.

*ipv6-group-address*: IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number from 0 through F.

*prefix-length*: Prefix length of an IPv6 multicast group address or an IPv6 multicast source address. For an IPv6 multicast group address, this argument has an effective value range of 8 to 128; for an IPv6 multicast source address, this argument has an effective value range of 0 to 128. The system default is 128 in both cases.

**incoming-interface**: Displays the forwarding entries whose incoming interface is the specified one.

*interface-type interface-number*: Specifies an interface by its type and number.

**register**: Represents a registered interface.

**outgoing-interface**: Displays the forwarding entries whose outgoing interface is the specified one.

**exclude**: Displays the forwarding entries whose outgoing interface list excludes the specified interface.

**include**: Displays the forwarding entries whose outgoing interface list includes the specified interface.

**match**: Displays the forwarding entries whose outgoing interface list includes and includes only the specified interface.

**statistics**: Specifies to display the statistics information of the IPv6 multicast forwarding table.

**slot slot-number:** Specifies the slot number of an interface card. If you do not provide this option, the multicast forwarding table information of the main processing board will be displayed.

**port-info:** Displays Layer 2 port information.

## Description

Use the **display multicast ipv6 forwarding-table** command to display information of the IPv6 multicast forwarding table.

IPv6 multicast forwarding tables are used to guide multicast forwarding. You can view the state of IPv6 multicast traffic forwarding by checking the IPv6 multicast forwarding table.

Related commands: **multicast ipv6 forwarding-table downstream-limit**, **multicast ipv6 forwarding-table route-limit**, **display multicast ipv6 routing-table**.

## Examples

# Display information of the IPv6 multicast forwarding table.

```
<Sysname> display multicast ipv6 forwarding-table
IPv6 Multicast Forwarding Table
Total 1 entry

Total 1 entry matched

00001. (2000:5::1:1000, FF1E::1234)
  MID: 0, Flags: 0x0:0
  Uptime: 04:04:37, Timeout in: 00:03:26
  Incoming interface: Vlan-interface1
  List of 1 outgoing interfaces:
    1: Vlan-interface2
  Matched 146754 packets(10272780 bytes), Wrong If 0 packets
  Forwarded 139571 packets(9769970 bytes)
```

**Table 1-2** display multicast ipv6 forwarding-table command output description

Field	Description
IPv6 Multicast Forwarding Table	IPv6 multicast forwarding table
Total 1 entry	Total number of (S, G) entries in the IPv6 multicast forwarding table
Total 1 entry matched	Total number of matched (S, G) entries in the IPv6 multicast forwarding table
00001	Sequence number of the (S, G) entry
(2000:5::1:1000, FF1E::1234)	An (S, G) entry in the IPv6 multicast forwarding table
MID	MID of the (S, G). Each (S, G) entry has a unique MID.
Flags	Current state of the (S, G) entry. Different bits are used to indicate different states of the (S, G) entry. For the values and meanings of this field, see <a href="#">Table 1-3</a> .
Uptime	Length of time for which the (S, G) entry has been up
Timeout in	Length of time in which the (S, G) entry will time out
Incoming interface	Incoming interface of the (S, G) entry

Field	Description
List of 1 outgoing interfaces: 1: Vlan-interface2	Outgoing interface list: Interface number: interface type and number
Matched 146754 packets(10272780 bytes), Wrong If 0 packets	(S, G)-matched packets (bytes), packets with incoming interface errors
Forwarded 139571 packets(9769970 bytes)	(S, G) forwarded IPv6 multicast packets (bytes)

**Table 1-3** Values and meanings of the Flags field

Value	Meaning
0x00000001	Indicates that a register-stop message needs to be sent.
0x00000002	Indicates whether the IPv6 multicast source corresponding to the (S, G) entry is active.
0x00000004	Indicates a null forwarding entry.
0x00000008	Indicates whether the RP is a border router in an IPv6 PIM domain.
0x00000010	Indicates a register outgoing interface is available.
0x00000400	Indicates an (S, G) entry to be deleted.
0x00008000	Indicates that the (S, G) entry is in smoothening process after active/standby switchover.
0x00010000	Indicates that the (S, G) entry has been updated during the smoothening process.
0x00080000	Indicates that the (S, G) entry has been repeatedly updated and need to be deleted before a new entry is added.
0x00100000	Indicates that the (S, G) entry was added successfully

## display multicast ipv6 routing-table

### Syntax

```
display multicast ipv6 routing-table [ ipv6-source-address [ prefix-length ] | ipv6-group-address
[ prefix-length ] | incoming-interface { interface-type interface-number | register } |
outgoing-interface { { exclude | include | match } { interface-type interface-number | register } } ] *
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ipv6-source-address*: Multicast source address.

*ipv6-group-address*: IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number from 0 through F.

*prefix-length*: Prefix length of a multicast group address or an IPv6 multicast source address. For an

IPv6 multicast group address, this argument has an effective value range of 8 to 128; for an IPv6 multicast source address, this argument has an effective value range of 0 to 128. The system default is 128 in both cases.

**incoming-interface:** Displays routing entries whose incoming interface is the specified one.

*interface-type interface-number:* Specifies an interface by its name and number.

**register:** Represents a registered interface.

**outgoing-interface:** Displays routing entries of which the outgoing interface is the specified one.

**exclude:** Displays routing entries whose outgoing interface list excludes the specified interface.

**include:** Displays routing entries whose outgoing interface list includes the specified interface.

**match:** Displays routing entries whose outgoing interface list includes only the specified interface.

## Description

Use the **display multicast ipv6 routing-table** command to display the information of an IPv6 multicast routing table.

IPv6 multicast routing tables are the basis of IPv6 multicast forwarding. You can view the establishment state of an (S, G) entry by checking the IPv6 multicast routing table.

Related commands: **display multicast ipv6 forwarding-table**.

## Examples

# Display the information of an IPv6 multicast routing table.

```
<Sysname> display multicast ipv6 routing-table
IPv6 multicast routing table
Total 1 entry

00001. (2001::2, FFE3::101)
  Uptime: 00:00:14
  Upstream Interface: Vlan-interface1
  List of 1 downstream interface
    1: Vlan-interface2
```

**Table 1-4** display multicast ipv6 routing-table command output description

Field	Description
IPv6 multicast routing table	IPv6 multicast routing table
Total 1 entry	Total number of (S, G) entries in the IPv6 multicast routing table
00001	Sequence number of the (S, G) entry
(2001::2, FFE3::101)	An (S, G) entry in the IPv6 multicast forwarding table
Uptime	Length of time for which the (S, G) entry has been up.
Upstream interface	Upstream interface of the (S, G) entry. Multicast packets should arrive through this interface.
List of 2 downstream interfaces	Downstream interface list. These interfaces need to forward multicast packets.

## display multicast ipv6 rpf-info

### Syntax

```
display multicast ipv6 rpf-info ipv6-source-address [ ipv6-group-address ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ipv6-source-address*: IPv6 multicast source address.

*ipv6-group-address*: IPv6 multicast group address, in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where x and y represent any hexadecimal number from 0 to F.

### Description

Use the **display multicast ipv6 rpf-info** command to display RPF information of an IPv6 multicast source.

Related commands: **display multicast ipv6 routing-table**, **display multicast ipv6 forwarding-table**.

### Examples

# Display all RPF information of the multicast source with an IPv6 address 2001::101.

```
<Sysname> display multicast ipv6 rpf-info 2001::101
RPF information about source 2001::101:
  RPF interface: Vlan-interface1, RPF neighbor: 2002::201
  Referenced prefix/prefix length: 2001::/64
  Referenced route type: igp
  Route selection rule: preference-preferred
  Load splitting rule: disable
```

**Table 1-5** display multicast ipv6 rpf-info command output description

Field	Description
RPF information about source 2001::101	RPF information of the IPv6 multicast source 2001::101
RPF interface	Indicates the interface type and number of the RPF interface
RPF neighbor	Indicate the IPv6 address of the RPF neighbor
Referenced prefix/prefix length	Referenced route and prefix length
Referenced route type	Type of the referenced route, which can be any of the following: <ul style="list-style-type: none"><li>• igp: IPv6 unicast route (IGB).</li><li>• egp: IPv6 unicast (EGP).</li><li>• unicast (direct): IPv6 unicast route (directly connected).</li><li>• unicast: other IPv6 unicast route (such as IPv6 unicast static route).</li><li>• mbgp: IPv6 MBGP route.</li></ul>

Field	Description
Route selection rule	RPF route selection rule: An RPF route can be selected by the priority of the routing protocol or by the longest match of the destination address in the routing table.
Load splitting rule	Load sharing rule

## multicast ipv6 boundary

### Syntax

```

multicast ipv6 boundary ipv6-group-address prefix-length
undo multicast ipv6 boundary { ipv6-group-address prefix-length | all }

```

### View

Interface view

### Default Level

2: System level

### Parameters

*ipv6-group-address*: IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number from 0 through F.

*prefix-length*: Prefix length of an IPv6 multicast group address, in the range of 8 to 128.

**all**: Deletes all IPv6 multicast boundaries configured on the interface.

### Description

Use the **multicast ipv6 boundary** command to configure an IPv6 multicast forwarding boundary.

Use the **undo multicast ipv6 boundary** command to delete the specified IPv6 multicast forwarding boundary or all IPv6 multicast forwarding boundaries.

By default, no multicast forwarding boundary is configured.

Note that:

- A multicast forwarding boundary sets the boundary condition for the IPv6 multicast groups in the specified range. If the destination address of an IPv6 multicast packet matches the set boundary condition, the packet will not be forwarded.
- If an interface needs to act as a forwarding boundary for multiple IPv6 multicast groups, just carry out this command on the interface once for each group.
- Assume that Set A and Set B are both multicast forwarding boundary sets to be configured, and that B is a subset of A. If A has been configured on an interface, it is not allowed to configure B on the interface; if B has been configured on the interface before A is configured, the previously configured B will be removed.

Related commands: **display multicast ipv6 boundary**.

### Examples

```
# Configure VLAN-interface 100 to be the forwarding boundary of the IPv6 multicast group FF03::101/16.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] multicast ipv6 boundary FF03::101 16
```

## multicast ipv6 forwarding-table downstream-limit

### Syntax

```
multicast ipv6 forwarding-table downstream-limit limit
undo multicast ipv6 forwarding-table downstream-limit
```

### View

System view

### Default Level

2: System level

### Parameters

*limit*: Maximum number of downstream nodes for a single entry in the IPv6 multicast forwarding table, the value ranges is 0 to 128.

### Description

Use the **multicast ipv6 forwarding-table downstream-limit** command to configure the maximum number of downstream nodes for a single entry in the IPv6 multicast forwarding table.

Use the **undo multicast ipv6 forwarding-table downstream-limit** command to restore the system default.

By default, the maximum number of downstream nodes for a single entry in the IPv6 multicast forwarding table is 128.

Related commands: **display multicast ipv6 forwarding-table**.

### Examples

# Set the maximum number of downstream nodes for a single entry in the IPv6 multicast forwarding table to 120.

```
<Sysname> system-view
[Sysname] multicast ipv6 forwarding-table downstream-limit 120
```

## multicast ipv6 forwarding-table route-limit

### Syntax

```
multicast ipv6 forwarding-table route-limit limit
undo multicast ipv6 forwarding-table route-limit
```

### View

System view

### Default Level

2: System level

## Parameters

*limit*: Maximum number of entries in the IPv6 multicast forwarding table. The value ranges from 0 to 512.

## Description

Use the **multicast ipv6 forwarding-table route-limit** command to configure the maximum number of entries in the IPv6 multicast forwarding table.

Use the **undo multicast ipv6 forwarding-table route-limit** command to restore the system default.

By default, the maximum number of entries in the IPv6 multicast forwarding table is the maximum number is 512.

The allowable maximum number of entries varies with devices.

Related commands: **display multicast ipv6 forwarding-table**.

## Examples

# Set the maximum number of entries in the IPv6 multicast forwarding table to 200.

```
<Sysname> system-view
[Sysname] multicast ipv6 forwarding-table route-limit 200
```

## multicast ipv6 load-splitting

### Syntax

```
multicast ipv6 load-splitting {source | source-group }
undo multicast ipv6 load-splitting
```

### View

System view

### Default Level

2: System level

## Parameters

**source**: Specifies to implement IPv6 multicast load splitting on a per-source basis.

**source-group**: Specifies to implement IPv6 multicast load splitting on a per-source and per-group basis.

## Description

Use the **multicast load-splitting** command to enable load splitting of IPv6 multicast traffic.

Use the **undo multicast load-splitting** command to disable load splitting of IPv6 multicast traffic.

By default, load splitting of IPv6 multicast traffic is disabled.

## Examples

# Enable load splitting of IPv6 multicast traffic on a per-source basis.

```
<Sysname> system-view
[Sysname] multicast ipv6 load-splitting source
```

## multicast ipv6 longest-match

### Syntax

```
multicast ipv6 longest-match
undo multicast ipv6 longest-match
```

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **multicast ipv6 longest-match** command to configure RPF route selection based on the longest match principle, namely to select the route with the longest prefix as the RPF route.

Use the **undo multicast ipv6 longest-match** command to restore the default.

By default, the route with the highest priority is selected as the RPF route.

### Examples

```
# Configure RPF route selection based on the longest match.
<Sysname> system-view
[Sysname] multicast ipv6 longest-match
```

## multicast ipv6 routing-enable

### Syntax

```
multicast ipv6 routing-enable
undo multicast ipv6 routing-enable
```

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **multicast ipv6 routing-enable** command to enable IPv6 multicast routing.

Use the **undo multicast ipv6 routing-enable** command to disable IPv6 multicast routing.

IPv6 multicast routing is disabled by default.

Note that:

- You must enable IPv6 multicast routing before you can carry out other Layer 3 IPv6 multicast commands.
- The device does not forward any IPv6 multicast packets before IPv6 multicast routing is enabled.

## Examples

```
# Enable IPv6 multicast routing.  
  
<Sysname> system-view  
[Sysname] multicast ipv6 routing-enable
```

## reset multicast ipv6 forwarding-table

### Syntax

```
reset multicast ipv6 forwarding-table { { ipv6-source-address [ prefix-length ] | ipv6-group-address [ prefix-length ] | incoming-interface { interface-type interface-number | register } } * | all }
```

### View

User view

### Default Level

2: System level

### Parameters

*ipv6-source-address*: IPv6 multicast source address.

*ipv6-group-address*: IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number from 0 to F.

*prefix-length*: Prefix length of an IPv6 multicast group or an IPv6 multicast source address. For an IPv6 multicast group address, this argument has an effective value range of 8 to 128; for an IPv6 multicast source address, this argument has an effective value range of 0 to 128. The system default is 128 in both cases.

**incoming-interface**: Specifies to clear IPv6 multicast forwarding entries of which the incoming interface is the specified one.

*interface-type interface-number*: Specifies an interface by its name and number.

**register**: Specifies the register interface.

**all**: Clears all forwarding entries from the IPv6 multicast forwarding table.

### Description

Use the **reset multicast ipv6 forwarding-table** command to clear forwarding entries from the IPv6 multicast forwarding table.

When a forwarding entry is deleted from the IPv6 multicast forwarding table, the corresponding routing entry is also deleted from the IPv6 multicast routing table.

Related commands: **reset multicast IPv6 routing-table**, **display multicast ipv6 routing-table**, **display multicast ipv6 forwarding-table**.

## Examples

# Clear the IPv6 multicast forwarding entries related to the IPv6 multicast group FF03::101 from the IPv6 multicast forwarding table.

```
<Sysname> reset multicast ipv6 forwarding-table ff03::101
```

## reset multicast ipv6 routing-table

### Syntax

```
reset multicast ipv6 routing-table { { ipv6-source-address [ prefix-length ] | ipv6-group-address [ prefix-length ] | incoming-interface { interface-type interface-number | register } } * | all }
```

### View

User view

### Default Level

2: System level

### Parameters

*ipv6-source-address*: IPv6 multicast source address.

*ipv6-group-address*: IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number from 0 to F.

*prefix-length*: Prefix length of an IPv6 multicast group address or an IPv6 multicast source address. For an IPv6 multicast group address, this argument has an effective value range of 8 to 128; for an IPv6 multicast source address, this argument has an effective value range of 0 to 128. The system default is 128 in both cases.

**incoming-interface**: Clears IPv6 multicast routing entries of which the incoming interface is the specified one.

*interface-type interface-number*: Specifies an interface by its name and number.

**register**: Specifies a register interface.

**all**: Clears all routing entries from the IPv6 multicast routing table.

### Description

Use the **reset multicast ipv6 routing-table** command to clear IPv6 routing entries from the IPv6 multicast routing table.

When a routing entry is deleted from the IPv6 multicast routing table, the corresponding forwarding entry is also deleted from the IPv6 multicast forwarding table.

Related commands: **reset multicast ipv6 forwarding-table**, **display multicast ipv6 forwarding-table**, **display multicast ipv6 routing-table**.

## Examples

# Clear the routing entries related to the IPv6 multicast group FF03::101 from the IPv6 multicast routing table.

```
<Sysname> reset multicast ipv6 routing-table ff03::101
```

# Table of Contents

<b>1 MLD Configuration Commands</b> .....	<b>1-1</b>
MLD Configuration Commands.....	1-1
display mld group .....	1-1
display mld group port-info .....	1-2
display mld interface.....	1-4
display mld proxying group.....	1-6
display mld routing-table.....	1-7
display mld ssm-mapping.....	1-8
display mld ssm-mapping group.....	1-9
fast-leave (MLD view).....	1-10
last-listener-query-interval (MLD view).....	1-11
max-response-time (MLD view) .....	1-12
mld .....	1-13
mld enable .....	1-13
mld group-limit .....	1-14
mld group-policy .....	1-15
mld last-listener-query-interval .....	1-16
mld max-response-time .....	1-16
mld require-router-alert.....	1-17
mld proxying enable .....	1-18
mld proxying forwarding .....	1-18
mld robust-count.....	1-19
mld send-router-alert .....	1-20
mld ssm-mapping enable .....	1-20
mld startup-query-count.....	1-21
mld startup-query-interval.....	1-22
mld static-group .....	1-23
mld timer other-querier-present.....	1-24
mld timer query.....	1-24
mld version .....	1-25
require-router-alert (MLD view) .....	1-26
reset mld group.....	1-26
reset mld group port-info .....	1-27
reset mld ssm-mapping group.....	1-28
robust-count (MLD view) .....	1-29
send-router-alert (MLD view).....	1-29
ssm-mapping (MLD view).....	1-30
startup-query-count (MLD view) .....	1-31
startup-query-interval (MLD view) .....	1-31
timer other-querier-present (MLD view) .....	1-32
timer query (MLD view) .....	1-33
version (MLD view).....	1-34

# 1 MLD Configuration Commands

---



## Note

The term “router” in this document refers to a router in a generic sense or a Layer 3 switch running MLD.

---

## MLD Configuration Commands

### display mld group

#### Syntax

```
display mld group [ ipv6-group-address | interface interface-type interface-number ] [ static | verbose ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

*ipv6-group-address*: MLD multicast group address, in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where x and y represent any hexadecimal number ranging from 0 to F.

**interface** *interface-type interface-number*: Displays the information of MLD multicast groups on the specified interface.

**static**: Displays the information of statically joined MLD multicast groups.

**verbose**: Displays detailed information of MLD multicast groups.

#### Description

Use the **display mld group** command to view information of MLD multicast groups.

Note that:

- If you do not specify an IPv6 multicast group address, this command will display the MLD information of all the multicast groups.
- If you do not specify *interface-type interface-number*, this command will display the MLD multicast group information on all the interfaces.
- If you do not specify the **static** keyword, the information of only dynamically joined MLD groups will be displayed.

## Examples

# View the detailed information of dynamically joined MLD multicast groups on all interfaces.

```
<Sysname> display mld group verbose
Interface group report information
Vlan-interface 2 (FE80::101)
  Total 1 MLD Groups reported
  Group: FF03::101
    Uptime: 00:01:46
    Expires: 00:01:30
    Last reporter: FE80::10
    Last-listener-query-counter: 0
    Last-listener-query-timer-expiry: off
    Group mode: include
    Version1-host-present-timer-expiry: off
```

**Table 1-1 display mld group command output description**

Field	Description
Interface group report information	MLD multicast group information on the interface
Total 1 MLD Groups reported	One MLD multicast group was reported.
Group	IPv6 multicast group address
Uptime	Length of time since the IPV6 multicast group was joined
Expires	Remaining time of the IPv6 multicast group, where "off" means that the multicast group never times out
Last reporter	IPv6 address of the host that last reported membership for this group
Last-listener-query-counter	Number of MLD multicast-address-specific queries sent
Last-listener-query-timer-expiry	Remaining time of the MLD last listener query timer, where "off" means that the timer never times out
Group mode	Filtering mode of multicast sources
Version1-host-present-timer-expiry	Remaining time of the MLDv1 host present timer, where "off" means that the timer never times out

## display mld group port-info

### Syntax

```
display mld group port-info [ vlan vlan-id ] [ slot slot-number ] [ verbose ]
```

### View

Any view

### Default Level

1: Monitor level

## Parameters

**vlan-id:** VLAN ID, in the range of 1 to 4094. If you do not specify a VLAN, this command will display the Layer 2 port information of MLD multicast groups in all VLANs.

**slot slot-number:** Displays the Layer 2 port information about MLD multicast groups on the specified card.

**verbose:** Displays the detailed information about Layer 2 ports of MLD multicast groups.

## Description

Use the **display mld group port-info** command to view Layer 2 port information of MLD multicast groups.

## Examples

# View detailed Layer 2 port information of MLD multicast groups.

```
<Sysname> display mld group port-info verbose
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).

Port flags: D-Dynamic port, S-Static port, C-Copy port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):2.
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Router port(s):total 1 port.
    GE1/0/1                (D) ( 00:01:30 )
IP group(s):the following ip group(s) match to one mac group.
IP group address: FF03::101
    (FE80::1, FF03::101):
Attribute:   Host Port
Host port(s):total 1 port.
    GE1/0/2                (D) ( 00:03:23 )
MAC group(s):
MAC group address:3333-0000-0101
Host port(s):total 1 port.
    GE1/0/2
```

**Table 1-2 display mld group port-info** command output description

Field	Description
Total 1 IP Group(s).	Total number of IPv6 multicast groups
Total 1 IP Source(s).	Total number of IPv6 multicast sources
Total 1 MAC Group(s).	Total number of MAC multicast groups
Port flags: D-Dynamic port, S-Static port, C-Copy port	Port flag: D stands for dynamic port, S for static port, and C for port copied from a (*, G) entry to an (S, G) entry.

Field	Description
Subvlan flags: R-Real VLAN, C-Copy VLAN	Sub-VLAN flag: R stands for real egress sub-VLAN under the current entry, and C for sub-VLAN copied from a (*, G) entry to an (S, G) entry.
Router port(s)	Number of router ports
( 00:01:30 )	Remaining time of dynamic member port or router port aging timer. On a distributed device, to get this time value of a non-aggregation port on a board other than the main processing unit, you must specify the number of the slot where the corresponding board resides by using <b>slot slot-number</b> . This is not required for an aggregation port.
IP group address	Address of an IPv6 multicast group
MAC group address	Address of a MAC multicast group
Attribute	Attribute of an IPv6 multicast group
Host port(s)	Number of member ports

## display mld interface

### Syntax

```
display mld interface [ interface-type interface-number ] [ verbose ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command will display the information of all interfaces running MLD.

**verbose**: Displays detailed MLD configuration and operation information.

### Description

Use the **display mld interface** command to view MLD configuration and operation information on the specified interface or all MLD-enabled interfaces.

### Examples

# View the detailed MLD configuration and operation information on Vlan-interface1 (downstream interface).

```
<Sysname> display mld interface vlan-interfacel verbose
vlan-interfacel (FE80::200:AFF:FE01:101):
  MLD is enabled
  Current MLD version is 1
  Value of query interval for MLD(in seconds): 125
  Value of other querier present interval for MLD(in seconds): 255
  Value of maximum query response time for MLD(in seconds): 10
```

```

Value of last listener query interval(in seconds): 1
Value of startup query interval(in seconds): 31
Value of startup query count: 2
General query timer expiry (hours:minutes:seconds): 00:00:23
Querier for MLD: FE80::200:AFF:FE01:101 (this router)
MLD activity: 1 joins, 0 leaves
Multicast ipv6 routing on this interface: enabled
Robustness: 2
Require-router-alert: disabled
Fast-leave: disabled
Ssm-mapping: disabled
Startup-query-timer-expiry: off
Other-querier-present-timer-expiry: off
Proxying interface: Vlan-interface2 (FE80::100:CEF:FE01:101)
Total 1 MLD Group reported

```

**Table 1-3 display mld group port-info command output description**

Field	Description
Vlan-interface1 (FE80::200:AFF:FE01:101)	Interface name (IPv6 link-local address)
Current MLD version	MLD version running on the interface
Value of query interval for MLD (in seconds)	MLD query interval, in seconds
Value of other querier present interval for MLD (in seconds)	MLD other querier present interval, in seconds
Value of maximum query response time for MLD (in seconds)	Maximum response delay for general query messages (in seconds)
Value of last listener query interval (in seconds)	MLD last listener query interval, in seconds
Value of startup query interval(in seconds)	MLD startup query interval, in seconds
Value of startup query count	Number of MLD general queries sent on startup
General query timer expiry	Remaining time of the MLD general query timer, where "off" means that the timer never times out
Querier for MLD	IPv6 link-local address of the MLD querier
MLD activity	MLD activity statistics (number of join and done messages)
Robustness	MLD querier robustness variable
Require-router-alert	Dropping MLD messages without Router-Alert (enabled/disabled)
Fast-leave	MLD fast leave processing status (enabled/disabled)
Ssm-mapping	MLD SSM mapping status (enabled/disabled)
Startup-query-timer-expiry	Remaining time of MLD startup query timer, where "off" means that the timer never times out
Other-querier-present-timer-expiry	Remaining time of MLD other querier present timer, where "off" means that the timer never times out
Proxying interface	The MLD proxy interface, where "none" means that no proxy interface exists

Field	Description
Total 1 MLD Group reported	Total number of MLD groups the interface has dynamically joined
MLD proxy is enabled	MLD proxying is enabled
Version1-querier-present-timer-expiry	Remaining time of the MLDv1 querier present timer, where "off" means that the timer never times out

## display mld proxying group

### Syntax

**display mld proxying group** [ *ipv6-group-address* ] [ **verbose** ]

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ipv6-group-address*: Displays the information of the specified MLD proxying group. The group address is in the form of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, through FF0y::), where x and y represent any hexadecimal number ranging from 0 to F. If this argument is not specified, this command displays the information of all the MLD proxying groups.

**verbose**: Displays the detailed MLD proxying group information.

### Description

Use the **display mld proxying group** command to view the MLD proxying group information.

### Examples

# View the MLD proxying group information of all interfaces.

```
<Sysname> display mld proxying group verbose
Proxying group record(s) information
Total 1 MLD-Proxying group record(s)
Group: FF03::101
Group mode: include
Member state: Delay
Expires: 00:00:02
Source list (total 1 source(s))
Source: 30::1
```

**Table 1-4 display mld proxying group** command output description

Field	Description
Proxying group record(s) information	Information of MLD proxying groups on the interfaces
Total 1 MLD-Proxying group record(s)	One MLD proxying group is recorded

Field	Description
Group	IPv6 multicast group address
Member state	State of the member hosts: <ul style="list-style-type: none"> <li>• Delay</li> <li>• Idle</li> </ul>
Expires	Remaining time of the IPv6 multicast group, where “off” means that the group never times out
Group mode	IPv6 multicast source filtering modes: <ul style="list-style-type: none"> <li>• include</li> <li>• exclude</li> </ul>
Source list	A list of sources joining the same multicast group in the MLD proxying group

## display mld routing-table

### Syntax

```
display mld routing-table [ ipv6-source-address [ prefix-length ] | ipv6-group-address [ prefix-length ] ]
*
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ipv6-source-address*: Specifies a multicast source by its IPv6 address.

*ipv6-group-address*: Specifies an IPv6 multicast group by its IPv6 address, in the form of FFxy::/16, where x and y represent any hexadecimal number ranging from 0 to F.

*prefix-length*: Prefix length of the multicast source or multicast group address. For a multicast source address, this argument has an effective value range of 0 to 128; for a multicast group address, it has an effective value range of 8 to 128. The system default is 128 in both cases.

### Description

Use the **display mld routing-table** command to view the information of the MLD routing table.

### Examples

# View the information of the MLD routing table.

```
<Sysname> display mld routing-table
Routing table
Total 1 entries

00001. (*, FF1E::101)
List of 1 downstream interface
Vlan-interface1 (FE80::200:5EFF:FE71:3800),
```

Protocol: MLD

00002. (100::1, FF1E::101), Flag: ACT

List of 1 downstream interface in include mode

Vlan-interface2 (FE80::100:5E16:FEC0:1010),

Protocol: MLD

**Table 1-5 display mld routing-table** command output description

Field	Description
Routing table	MLD routing table
00001	Sequence number of this (*, G) entry
(*, FF1E::101)	An (*, G) entry in the MLD routing table
Flag	MLD route flags: <ul style="list-style-type: none"><li>• ACT: Indicates MLD routing entries that have been used for forwarding data packets but have the multicast group address out of the SSM group range</li><li>• SUC: Indicates MLD routing entries that have been added to the forwarding table and have the multicast group address within the SSM group range</li></ul>
List of 1 downstream interface	List of downstream interfaces: namely the interfaces to which multicast data for this group will be forwarded
in include mode	The downstream interface is in the include mode
in exclude mode	The downstream interface is in the exclude mode
Downstream interface is none	No downstream interfaces exist
Protocol	Protocol type

## display mld ssm-mapping

### Syntax

```
display mld ssm-mapping ipv6-group-address
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ipv6-group-address*: Specifies an IPv6 multicast group by its address, in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where x and y represent any hexadecimal number ranging from 0 to F.

### Description

Use the **display mld ssm-mapping** command to view the configured MLD SSM mappings for the specified IPv6 multicast group.

Related commands: **ssm-mapping**.

## Examples

```
# View the MLD SSM mappings for multicast group FF1E::101.
```

```
<Sysname> display mld ssm-mapping ff1e::101
Group: FF1E::101
Source list:
    1::1
    1::2
    10::1
    100::10
```

**Table 1-6 display mld ssm-mapping** command output description

Field	Description
Group	IPv6 multicast group address
Source list	List of IPv6 multicast source addresses

## display mld ssm-mapping group

### Syntax

```
display mld ssm-mapping group [ ipv6-group-address | interface interface-type interface-number ]
[ verbose ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ipv6-group-address*: Specifies a multicast group by its IPv6 address, in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where x and y represent any hexadecimal number ranging from 0 to F.

*interface-type interface-number*: Specifies an interface by its type and number.

**verbose**: Displays the detailed multicast group information created based on the configured MLD SSM mappings.

### Description

Use the **display mld ssm-mapping group** command to view the multicast group information created based on the configured MLD SSM mappings.

Note that:

- If you do not specify an IPv6 multicast group, this command will display the information of all IPv6 multicast groups created based on the configured MLD SSM mappings.
- If you do not specify an interface, this command will display the multicast group information created based on the configured MLD SSM mappings on all interfaces.

## Examples

# View the detailed information of IPv6 multicast group FF3E::101 created based on the configured MLD SSM mappings on all interfaces.

```
<Sysname> display mld ssm-mapping group ff3e::101 verbose
Interface group report information
Vlan-interface1 (FE80::101):
  Total 1 MLD SSM-mapping Group reported
  Group: FF3E::101
  Uptime: 00:01:46
  Expires: off
  Last reporter: FE80::10
  Group mode: include
  Source list(Total 1 source):
    Source: 30::1
      Uptime: 00:01:46
      Expires: 00:02:34
      Last-listener-query-counter: 0
      Last-listener-query-timer-expiry: off
```

**Table 1-7** display mld ssm-mapping group command output description

Field	Description
Interface group report information	IPv6 multicast group information created based on MLD SSM mappings on the interface
Total 1 MLD SSM-mapping Group reported	One MLD SSM mapping multicast group was reported.
Group	IPv6 multicast group address
Uptime	Length of time since the IPv6 multicast group was reported
Expires	Remaining time of the IPv6 multicast group, where “off” means that the group never times out
Last reporter	IPv6 address of the host that last reported membership for this group
Group mode	IPv6 multicast sources filter mode
Source list(Total 1 source)	IPv6 multicast source list (one IPv6 multicast source)
Source	IPv6 multicast source address
Last-listener-query-counter	Number of MLD multicast-address-specific queries sent
Last-listener-query-timer-expiry	Remaining time of the MLD last listener query timer, where “off” means that the timer never expires

## fast-leave (MLD view)

### Syntax

```
fast-leave [ group-policy acl6-number ]
```

```
undo fast-leave
```

## View

MLD view

## Default Level

2: System level

## Parameters

*acl6-number*: Number of a basic IPv6 ACL, in the range of 2000 to 2999. If you do not include this option in your command, this command will take effect for all IPv6 multicast groups.

## Description

Use the **fast-leave** command to configure MLD fast leave processing globally.

Use the **undo fast-leave** command to disable MLD fast leave processing globally.

By default, MLD fast leave processing is disabled, that is, the MLD querier sends multicast-address-specific queries upon receiving an MLD done message from a host, instead of sending a leave notification directly to the upstream.

Related commands: **mld fast-leave**, **last-listener-query-interval**.



### Note

This command takes effect only on Layer 3 interfaces other than VLAN interfaces when executed in MLD view.

---

## Examples

```
# Enable MLD fast leave processing globally.
```

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] fast-leave
```

## last-listener-query-interval (MLD view)

### Syntax

```
last-listener-query-interval interval
```

```
undo last-listener-query-interval
```

### View

MLD view

### Default Level

2: System level

## Parameters

*interval*: MLD last listener query interval in seconds, namely the length of time the device waits between sending MLD multicast-address-specific queries. The effective range is 1 to 5.

## Description

Use the **last-listener-query-interval** command to configure the MLD last listener query interval globally.

Use the **undo last-listener-query-interval** command to restore the system default.

By default, the MLD last listener query interval is 1 second.

Related commands: **mld last-listener-query-interval**, **robust-count**, **display mld interface**.

## Examples

# Set the MLD last listener query interval to 3 seconds globally.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] last-listener-query-interval 3
```

## max-response-time (MLD view)

### Syntax

**max-response-time** *interval*

**undo max-response-time**

### View

MLD view

### Default Level

2: System level

## Parameters

*interval*: Maximum response delay for MLD general query messages in seconds, in the range of 1 to 25.

## Description

Use the **max-response-time** command to configure the maximum response delay for MLD general queries globally.

Use the **undo max-response-time** command to restore the system default.

By default, the maximum response delay for MLD general queries is 10 seconds.

Related commands: **mld max-response-time**, **timer other-querier-present**, **display mld interface**.

## Examples

# Set the maximum response delay for MLD general queries to 8 seconds globally.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] max-response-time 8
```

## mld

### Syntax

```
mld
undo mld
```

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **mld** command to enter MLD view.

Use the **undo mld** command to remove the configurations made in MLD view.

Note that this command can take effect only after IPv6 multicast routing is enabled on the device.

Related commands: **mld enable**; **multicast ipv6 routing-enable** in *IPv6 Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*.

### Examples

# Enable IPv6 multicast routing and enter MLD view.

```
<Sysname> system-view
[Sysname] multicast ipv6 routing-enable
[Sysname] mld
[Sysname-mld]
```

## mld enable

### Syntax

```
mld enable
undo mld enable
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **mld enable** command to enable MLD on the current interface.

Use the **undo mld enable** command to disable MLD on the current interface.

By default, MLD is disabled on the current interface.

Note that:

- This command can take effect only after IPv6 multicast routing is enabled on the device.
- Other MLD configurations performed on the interface can take effect only after MLD is enabled on the interface.

Related commands: **mld**; **multicast ipv6 routing-table** in *IPv6 Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*.

## Examples

```
# Enable IPv6 multicast routing and enable MLD on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] multicast ipv6 routing-enable
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld enable
```

## mld group-limit

### Syntax

```
mld group-limit limit
undo mld group-limit
```

### View

```
Interface view
```

### Default Level

```
2: System level
```

### Parameters

*limit*: The maximum number of IPv6 multicast groups that can be joined on the interface, in the range of 1 to 1024.

### Description

Use the **mld group-limit** command to configure the maximum number of IPv6 multicast groups that can be joined on the current interface.

Use the **undo mld group-limit** command to restore the default.

By default, the maximum number of IPv6 multicast groups that can be joined on an interface is 1024.

Note that:

- This command is effective only for dynamically joined IPv6 multicast groups but not statically joined IPv6 multicast groups.
- If the configured *limit* value is smaller than the number of the existing IPv6 multicast groups on the current interface, the system does not automatically remove the IPv6 multicast groups in excess. To bring this configuration into effect in this case, you need to use the **reset mld group** command to clear the IPv6 multicast groups information manually.

- You can also use the **mld group-limit** command to limit the number of IPv6 multicast groups on an interface. If you configure a limit of the number of groups for ports in a VLAN while you have configured a limit of the number of groups for the VLAN interface, or vice versa, this may cause inconsistencies between Layer 2 and Layer 3 table entries. Therefore, it is recommended to configure a limit of the number of IPv6 multicast groups only on the VLAN interface.

Related commands: **mld static-group**, **reset mld group**; **mld-snooping group-limit** in *MLD Snooping Commands* in the *IP Multicast Volume*.

## Examples

```
# Limit the number of IPv6 multicast groups that can be joined on VLAN-interface 100 to 128.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] igmp group-limit 128
```

## mld group-policy

### Syntax

```
mld group-policy acl6-number [ version-number ]
undo mld group-policy
```

### View

Interface view

### Default Level

2: System level

### Parameters

*acl6-number*: Number of a basic or advanced IPv6 ACL, in the range of 2000 to 3999. The source address or address range specified in the advanced IPv6 ACL rule is the IPv6 multicast source address(es) specified in MLDv2 reports, rather than the source address in the IPv6 packets. The system assumes that an MLDv1 report or an MLDv2 IS\_EX or TO\_EX report that does not carry an IPv6 multicast source address carries a IPv6 multicast source address of 0::0.

*version-number*: MLD version number, 1 or 2. If you do not specify an MLD version, the configured group filter will be effective for MLD reports of both version 1 and version 2.

### Description

Use the **mld group-policy** command to configure an IPv6 multicast group filter on the current interface to limit access to the IPv6 multicast group.

Use the **undo mld group-policy** command to remove the configured IPv6 multicast group filter.

By default, no IPv6 multicast group filter is configured by default, that is, a host can join any valid IPv6 multicast group.

## Examples

```
# Configure an IPv6 ACL so that hosts on the subnet attached to VLAN-interface 100 can join the IPv6
multicast group FF03::101 only.
<Sysname> system-view
```

```
[Sysname] acl ipv6 number 2005
[Sysname-acl6-basic-2005] rule permit source ff03::101 16
[Sysname-acl6-basic-2005] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld group-policy 2005
```

## mld last-listener-query-interval

### Syntax

```
mld last-listener-query-interval interval
undo mld last-listener-query-interval
```

### View

Interface view

### Default Level

2: System level

### Parameters

*interval*: MLD last listener query interval in seconds, in the range of 1 to 5.

### Description

Use the **mld last-listener-query-interval** command to configure the MLD last listener query interval on the current interface.

Use the **undo mld last-listener-query-interval** command to restore the system default.

By default, the MLD last listener query interval is 1 second.

Related commands: **last-listener-query-interval**, **mld robust-count**, **display mld interface**.

### Examples

# Set the MLD last listener query interval to 3 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld last-listener-query-interval 3
```

## mld max-response-time

### Syntax

```
mld max-response-time interval
undo mld max-response-time
```

### View

Interface view

### Default Level

2: System level

## Parameters

*interval*: Maximum response delay for MLD general query messages in seconds, in the range of 1 to 25.

## Description

Use the **mld max-response-time** command to configure the maximum response delay for MLD general query messages on the interface.

Use the **undo mld max-response-time** command to restore the default configuration.

By default, the maximum response delay for MLD general query messages is 10 seconds.

The maximum response delay determines the time which the device takes to detect directly attached group members in the LAN.

Related commands: **max-response-time**, **mld timer other-querier-present**, **display mld interface**.

## Examples

```
# Set the maximum response delay for MLD general query messages to 8 seconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld max-response-time 8
```

## mld require-router-alert

### Syntax

```
mld require-router-alert
undo mld require-router-alert
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **mld require-router-alert** command to configure the interface to discard MLD messages without the Router-Alert option.

Use the **undo mld require-router-alert** command to restore the default configuration.

By default, the device does not check the Router-Alert option, that is, it forwards all received MLD messages to the upper layer protocol for processing.

Related commands: **require-router-alert**, **mld send-router-alert**.

## Examples

```
# Configure VLAN-interface 100 to discard MLD messages without the Router-Alert option.
```

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld require-router-alert
```

## mld proxying enable

### Syntax

```
mld proxying enable
undo mld proxying enable
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **mld proxying enable** command to enable MLD proxying on an interface.

Use the **undo mld proxying enable** command to disable MLD proxying on the interface.

By default, MLD proxying is disabled.

Note that:

- This command takes effect only after IPv6 multicast routing is enabled
- If MLD proxying is enabled on a loopback interface, the proxy device maintains only the MLD routing table without adding the MLD routes to the multicast routing table or forwarding table.

Related commands: **multicast ipv6 routing-enable** in *IPv6 Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*.

### Examples

```
# Enable IPv6 multicast routing and enable MLD proxying on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] multicast ipv6 routing-enable
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld proxying enable
```

## mld proxying forwarding

### Syntax

```
mld proxying forwarding
undo mld proxying forwarding
```

### View

Interface view

## Default Level

2: System level

## Parameters

None

## Description

Use the **mld proxying forwarding** command to enable a non-querier downstream interface to forward multicast traffic.

Use the **undo mld proxying forwarding** command to disable the forwarding capability of a non-querier downstream interface.

By default, a non-querier downstream interface does not forward multicast traffic.

## Examples

# Enable the multicast forwarding capability on VLAN-interface 100, a non-querier downstream interface on the MLD proxy device.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld proxying forwarding
```

## mld robust-count

### Syntax

**mld robust-count** *robust-value*

**undo mld robust-count**

### View

Interface view

### Default Level

2: System level

### Parameters

*robust-value*: MLD querier robustness variable, with an effective range of 2 to 5.

### Description

Use the **mld robust-count** command to configure the MLD querier robustness variable on the current interface.

Use the **undo mld robust-count** command to restore the system default.

By default, the MLD querier robustness variable is 2.

Related commands: **robust-count**, **mld timer query**, **mld last-listener-query-interval**, **mld timer other-querier-present**, **display mld interface**.

### Examples

# Set the MLD querier robustness variable to 3 on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld robust-count 3
```

## mld send-router-alert

### Syntax

```
mld send-router-alert
undo mld send-router-alert
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **mld send-router-alert** command to enable insertion of the Router-Alert option into MLD messages to be sent from the current interface.

Use the **undo mld send-router-alert** command to disable insertion of the Router-Alert option into MLD messages to be sent from the current interface.

By default, MLD messages carry the Router-Alert option.

Related commands: **send-router-alert**, **mld require-router-alert**.

### Examples

```
# Disable insertion of the Router-Alert option into MLD messages to be sent from VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo mld send-router-alert
```

## mld ssm-mapping enable

### Syntax

```
mld ssm-mapping enable
undo mld ssm-mapping enable
```

### View

Interface view

### Default Level

2: System level

## Parameters

None

## Description

Use the **mld ssm-mapping enable** command to enable the MLD SSM mapping feature on the current interface.

Use the **undo mld ssm-mapping enable** command to disable the MLD SSM mapping feature on the current interface.

By default, the MLD SSM mapping feature is disabled on all interfaces.

## Examples

```
# Enable the MLD SSM mapping feature on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld ssm-mapping enable
```

## mld startup-query-count

### Syntax

**mld startup-query-count** *value*

**undo mld startup-query-count**

### View

Interface view

### Default Level

2: System level

## Parameters

*value*: Startup query count, namely, the number of queries the MLD querier sends on startup, with an effective range of 2 to 5.

## Description

Use the **mld startup-query-count** command to configure the startup query count on the current interface.

Use the **undo mld startup-query-count** command to restore the system default.

By default, the startup query count is set to the MLD querier robustness variable.



### Note

By default, the MLD querier robustness variable is 2, so the startup query count is also 2.

---

Related commands: **startup-query-count**, **mld robust-count**.

## Examples

```
# Set the startup query count to 3 on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld startup-query-count 3
```

## mld startup-query-interval

### Syntax

```
mld startup-query-interval interval
undo mld startup-query-interval
```

### View

Interface view

### Default Level

2: System level

### Parameters

*interval*: Startup query interval in seconds, namely, the interval between general queries the MLD querier sends on startup, with an effective range of 1 to 18000.

### Description

Use the **mld startup-query-interval** command to configure the startup query interval on the current interface.

Use the **undo mld startup-query-interval** command to restore the system default.

By default, the startup query interval is 1/4 of the MLD query interval.



#### Note

By default, the MLD query interval is 125 seconds, so the startup query interval =  $125 / 4 = 31.25$  (seconds).

---

Related commands: **startup-query-interval**, **mld timer query**.

## Examples

```
# Set the startup query interval to 5 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld startup-query-interval 5
```

## mld static-group

### Syntax

```
mld static-group ipv6-group-address [ source ipv6-source-address ]  
undo mld static-group { all | ipv6-group-address [ source ipv6-source-address ] }
```

### View

Interface view

### Default Level

2: System level

### Parameters

*ipv6-group-address*: IPv6 multicast group address, in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where x and y represent any hexadecimal number ranging from 0 to F. .

*ipv6-source-address*: IPv6 address of the specified multicast source.

**all**: Removes all static IPv6 multicast groups that the current interface has joined.

### Description

Use the **mld static-group** command to configure the current interface to be a statically-connected member of the specified IPv6 multicast group or IPv6 multicast source and group.

Use the **undo mld static-group** command to remove the configuration.

By default, an interface is not a statically-connected member of any IPv6 multicast group or IPv6 multicast source and group.

If the IPv6 multicast address is in the SSM multicast address range, you must specify an IPv6 multicast source address at the same time; otherwise MLD routing table entries cannot be established. There is no such a restriction if the specified IPv6 multicast group address is not in the SSM multicast address range.

### Examples

```
# Configure VLAN-interface 100 to be a statically-connected member of the IPv6 multicast group FF03::101.
```

```
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] mld static-group ff03::101
```

```
# Configure VLAN-interface 100 to be a statically connected member of multicast source and group (2001::101, FF3E::202).
```

```
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] mld static-group ff3e::202 source 2001::101
```

## mld timer other-querier-present

### Syntax

```
mld timer other-querier-present interval  
undo mld timer other-querier-present
```

### View

Interface view

### Default Level

2: System level

### Parameters

*interval*: MLD other querier present interval in seconds, in the range of 60 to 300.

### Description

Use the **mld timer other-querier-present** command to configure the MLD other querier present interval on the current interface.

Use the **undo mld timer other-querier-present** command to restore the system default.

By default, MLD other querier present interval = [ MLD query interval ] times [ MLD querier robustness variable ] plus [ maximum response delay for MLD general queries ] divided by two.



#### Note

By default, the values of the three parameters in the above-mentioned formula are 125, 2, and 10, respectively, so the MLD other querier present interval is  $125 \times 2 + 10 / 2 = 255$  (seconds).

---

Related commands: **timer other-querier-present**, **mld timer query**, **mld robust-count**, **mld max-response-time**, **display mld interface**.

### Examples

```
# Set the MLD other querier present interval to 200 seconds on VLAN-interface 100.
```

```
<Sysname> system-view  
[Sysname] interface vlan-interface100  
[Sysname-Vlan-interface100] mld timer other-querier-present 200
```

## mld timer query

### Syntax

```
mld timer query interval  
undo mld timer query
```

### View

Interface view

## Default Level

2: System level

## Parameters

*interval*: MLD query interval, namely the amount of time in seconds between MLD general query messages, in the range of 1 to 18,000.

## Description

Use the **mld timer query** command to configure the MLD query interval on the current interface.

Use the **undo mld timer query** command to restore the system default.

By default, the MLD query interval is 125 seconds.

Related commands: **timer query**, **mld timer other-querier-present**, **display mld interface**.

## Examples

```
# Set the MLD query interval to 200 seconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld timer query 200
```

## mld version

### Syntax

**mld version** *version-number*

**undo mld version**

### View

Interface view

### Default Level

2: System level

### Parameters

*version-number*: MLD version, 1 or 2.

### Description

Use the **mld version** command to configure the MLD version on the current interface.

Use the **undo mld version** command to restore the default MLD version.

By default, the MLD version is MLDv1.

Related commands: **version**.

### Examples

```
# Set the MLD version to MLDv2 on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld version 2
```

## require-router-alert (MLD view)

### Syntax

```
require-router-alert
undo require-router-alert
```

### View

MLD view

### Default Level

2: System level

### Parameters

None

### Description

Use the **require-router-alert** command to globally configure the device to discard MLD messages without the Router-Alert option.

Use the **undo require-router-alert** command to restore the default configuration.

By default, the device does not check the Router-Alert option, that is, it forwards all received MLD messages to the upper layer protocol for processing.

Related commands: **mld require-router-alert**, **send-router-alert**.

### Examples

```
# Globally configure the device to discard MLD messages without the Router-Alert option.
<Sysname> system-view
[Sysname] mld
[Sysname-mld] require-router-alert
```

## reset mld group

### Syntax

```
reset mld group { all | interface interface-type interface-number { all | ipv6-group-address
[ prefix-length ] [ ipv6-source-address [ prefix-length ] ] } }
```

### View

User view

### Default Level

2: System level

### Parameters

**all**: The first **all** specifies to clear MLD multicast group information on all interfaces, while the second **all** specifies to clear the information of all MLD multicast groups.

**interface** *interface-type interface-number*: Clears the MLD multicast group information on the specified interface.

*ipv6-group-address*: IPv6 multicast group address, in the range of FFxy::<16, where x and y represent any hexadecimal number ranging from 0 to F.

*ipv6-source-address*: IPv6 multicast source address.

*prefix-length*: Prefix length of the specified multicast source or multicast group. For a multicast source address, this argument has an effective value range of 0 to 128; for a multicast group address, it has an effective value range of 8 to 128. The system default is 128 in both cases.

## Description

Use the **reset mld group** command to clear MLD multicast group information.

Note that this command cannot clear MLD multicast group information of static joins.

Related commands: **display mld group**.

## Examples

# Clear all MLD multicast group information on all interfaces.

```
<Sysname> reset mld group all
```

# Clear all MLD multicast group information for VLAN-interface 100.

```
<Sysname> reset mld group interface vlan-interface 100 all
```

# Clear the information about MLD multicast group FF03::101:10 on VLAN-interface 100.

```
<Sysname> reset mld group interface vlan-interface 100 ff03::101:10
```

## reset mld group port-info

### Syntax

```
reset mld group port-info { all | ipv6-group-address } [ vlan vlan-id ]
```

### View

User view

### Default Level

2: System level

### Parameters

**all**: Clears Layer 2 port information of all the MLD multicast groups.

*ipv6-group-address*: Clears Layer 2 port information of the specified MLD multicast group. The effective range of *group-address* is FFxy::<16, where x and y represent any hexadecimal number between 0 and F, inclusive.

*vlan-id*: Clear Layer 2 port information of MLD multicast groups in the specified VLAN. The effective range of *vlan-id* is 1 to 4094.

## Description

Use the **reset mld group port-info** command to clear Layer 2 port information of MLD multicast groups.

Note that:

- Layer 2 ports for MLD multicast groups include member ports and router ports.

- This command cannot clear Layer 2 port information about MLD multicast groups of static joins.

Related commands: **display mld group port-info**.

## Examples

# Clear Layer 2 port information of all MLD multicast groups in all VLANs.

```
<Sysname> reset mld group port-info all
```

# Clear Layer 2 port information of all MLD multicast groups in VLAN 100.

```
<Sysname> reset mld group port-info all vlan 100
```

# Clear Layer 2 port information about multicast group FF03::101:10 in VLAN 100.

```
<Sysname> reset mld group port-info ff03::101:10 vlan 100
```

## reset mld ssm-mapping group

### Syntax

```
reset mld ssm-mapping group { all | interface interface-type interface-number { all | ipv6-group-address [ prefix-length ] [ ipv6-source-address [ prefix-length ] ] }
```

### View

User view

### Default Level

2: System level

### Parameters

**all**: The first **all** specifies to clear IPv6 multicast group information created based on the configured MLD SSM mappings on all interfaces, while the second **all** specifies to clear all IPv6 multicast group information created based on the configured MLD SSM mappings..

*interface-type interface-number*: Specifies an interface by its type and number.

*ipv6-group-address*: Specifies an IPv6 multicast group by its IPv6 address, in the form of FFxy::/16, where x and y represent any hexadecimal number ranging from 0 to F.

*ipv6-source-address*: Specifies a multicast source by its IPv6 address.

*prefix-length*: Prefix length of the multicast source or multicast group address. For a multicast source address, this argument has an effective value range of 0 to 128; for a multicast group address, it has an effective value range of 8 to 128. The system default is 128 in both cases.

### Description

Use the **reset mld ssm-mapping group** command to clear IPv6 multicast group information created based on the configured MLD SSM mappings.

Related commands: **display mld ssm-mapping group**.

## Examples

# Clear all IPv6 multicast group information created based on the configured MLD SSM mappings on all interfaces.

```
<Sysname> reset mld ssm-mapping group all
```

## robust-count (MLD view)

### Syntax

```
robust-count robust-value  
undo robust-count
```

### View

MLD view

### Default Level

2: System level

### Parameters

*robust-value*: MLD querier robustness variable, with an effective range of 2 to 5.

### Description

Use the **robust-count** command to configure the MLD querier robustness variable globally.

Use the **undo robust-count** command to restore the system default.

By default, the MLD querier robustness variable is 2.

Related commands: **mld robust-count**, **last-listener-query-interval**, **timer other-querier-present**, **display mld interface**.

### Examples

```
# Set the MLD querier robustness variable to 3 globally.
```

```
<Sysname> system-view  
[Sysname] mld  
[Sysname-mld] robust-count 3
```

## send-router-alert (MLD view)

### Syntax

```
send-router-alert  
undo send-router-alert
```

### View

MLD view

### Default Level

2: System level

### Parameters

None

### Description

Use the **send-router-alert** command to globally enable the insertion of the Router-Alert option into MLD messages to be sent.

Use the **undo send-router-alert** command to globally disable the insertion of the Router-Alert option into MLD messages to be sent.

By default, MLD messages carry the Router-Alert option.

Related commands: **mld send-router-alert**, **require-router-alert**.

## Examples

```
# Globally disable insertion of the Router-Alert option into MLD messages to be sent.
```

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] undo send-router-alert
```

## ssm-mapping (MLD view)

### Syntax

```
ssm-mapping ipv6-group-address prefix-length ipv6-source-address
undo ssm-mapping { ipv6-group-address prefix-length ipv6-source-address | all }
```

### View

MLD view

### Default level

2: System level

### Parameters

*ipv6-group-address*: Specifies an IPv6 multicast group by its IPv6 address, in the form of FFxy::/16, where x and y represent any hexadecimal number ranging from 0 to F.

*prefix-length*: Prefix length of the IPv6 multicast group address, in the range of 8 to 128.

*ipv6-source-address*: Specifies a multicast source by its IPv6 address.

**all**: Removes all MLD SSM mappings.

### Description

Use the **ssm-mapping** command to configure an MLD SSM mapping.

Use the **undo ssm-mapping** command to remove one or all MLD SSM mappings.

By default, no MLD SSM mappings are configured.

Related commands: **mld ssm-mapping enable**, **display mld ssm-mapping**.

## Examples

```
# Configure an MLD SSM mapping for multicast group FF1E::101/128 and multicast source 1::1.
```

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] ssm-mapping ff1e::101 128 1::1
```

## startup-query-count (MLD view)

### Syntax

```
startup-query-count value  
undo startup-query-count
```

### View

MLD view

### Default Level

2: System level

### Parameters

*value*: Startup query count, namely, the number of queries the MLD querier sends on startup, with an effective range of 2 to 5.

### Description

Use the **startup-query-count** command to configure the startup query count globally.

Use the **undo startup-query-count** command to restore the system default.

By default, the startup query count is set to the MLD querier robustness variable.



#### Note

By default, the MLD querier robustness variable is 2, so the startup query count is also 2.

---

Related commands: **mld startup-query-count**, **robust-count**.

### Examples

```
# Set the startup query count to 3 globally.  
<Sysname> system-view  
[Sysname] mld  
[Sysname-mld] startup-query-count 3
```

## startup-query-interval (MLD view)

### Syntax

```
startup-query-interval interval  
undo startup-query-interval
```

### View

MLD view

### Default Level

2: System level

## Parameters

*interval*: Startup query interval in seconds, namely, the interval between general queries the MLD querier sends on startup, with an effective range of 1 to 18000.

## Description

Use the **startup-query-interval** command to configure the startup query interval globally.

Use the **undo startup-query-interval** command to restore the system default.

By default, the startup query interval is 1/4 of the “MLD query interval”.



### Note

By default, the MLD query interval is 125 seconds, so the startup query interval =  $125 / 4 = 31.25$  (seconds).

---

Related commands: **mld startup-query-interval**, **timer query**.

## Examples

```
# Set the startup query interval to 5 seconds globally.
```

```
<Sysname> system-view
```

```
[Sysname] mld
```

```
[Sysname-mld] startup-query-interval 5
```

## timer other-querier-present (MLD view)

### Syntax

```
timer other-querier-present interval
```

```
undo timer other-querier-present
```

### View

```
MLD view
```

### Default Level

```
2: System level
```

## Parameters

*interval*: MLD other querier present interval in seconds, in the range of 60 to 300.

## Description

Use the **timer other-querier-present** command to configure the MLD other querier present interval globally.

Use the **undo timer other-querier-present** command to restore the default configuration.

By default, MLD other querier present interval = [ MLD query interval ] times [ MLD querier robustness variable ] plus [ maximum response delay for MLD general queries ] divided by two.

---



By default, the values of the three parameters in the above-mentioned formula are 125, 2, and 10, respectively, so the MLD other querier present interval is  $125 \times 2 + 10 / 2 = 255$  (seconds).

---

Related commands: **mld timer other-querier-present**, **timer query**, **robust-count**, **max-response-time**, **display mld interface**.

### Examples

# Set the MLD other querier present interval to 200 seconds globally.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] timer other-querier-present 200
```

### timer query (MLD view)

#### Syntax

```
timer query interval
undo timer query
```

#### View

MLD view

#### Default Level

2: System level

#### Parameters

*interval*: MLD query interval, namely, amount of time in seconds between MLD general queries, in the range of 1 to 18,000.

#### Description

Use the **timer query** command to configure the MLD query interval globally.

Use the **undo timer query** command to restore the system default.

By default, the MLD query interval is 125 seconds.

Related commands: **mld timer query**, **timer other-querier-present**, **display mld interface**.

### Examples

# Set the MLD query interval to 200 seconds globally.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] timer query 200
```

## version (MLD view)

### Syntax

**version** *version-number*

**undo version**

### View

MLD view

### Default Level

2: System level

### Parameters

*version-number*: MLD version number, 1 or 2.

### Description

Use the **version** command to configure the MLD version globally.

Use the **undo version** command to restore the default MLD version.

By default, the MLD version is MLDv1.

Related commands: **mld version**.

### Examples

# Globally set the MLD version to MLDv2.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] version 2
```

# Table of Contents

<b>1 IPv6 PIM Configuration Commands</b> .....	<b>1-1</b>
IPv6 PIM Configuration Commands.....	1-1
bsr-policy (IPv6 PIM view).....	1-1
c-bsr (IPv6 PIM view) .....	1-2
c-bsr hash-length (IPv6 PIM view) .....	1-2
c-bsr holdtime (IPv6 PIM view).....	1-3
c-bsr interval (IPv6 PIM view).....	1-4
c-bsr priority (IPv6 PIM view) .....	1-5
c-rp (IPv6 PIM view) .....	1-5
c-rp advertisement-interval (IPv6 PIM view).....	1-6
c-rp holdtime (IPv6 PIM view) .....	1-7
crp-policy (IPv6 PIM view).....	1-8
display pim ipv6 bsr-info.....	1-9
display pim ipv6 claimed-route .....	1-10
display pim ipv6 control-message counters .....	1-11
display pim ipv6 grafts.....	1-13
display pim ipv6 interface .....	1-14
display pim ipv6 join-prune.....	1-16
display pim ipv6 neighbor.....	1-17
display pim ipv6 routing-table.....	1-18
display pim ipv6 rp-info.....	1-20
embedded-rp .....	1-21
hello-option dr-priority (IPv6 PIM view) .....	1-22
hello-option holdtime (IPv6 PIM view) .....	1-23
hello-option lan-delay (IPv6 PIM view).....	1-24
hello-option neighbor-tracking (IPv6 PIM view).....	1-24
hello-option override-interval (IPv6 PIM view).....	1-25
holdtime assert (IPv6 PIM view).....	1-26
holdtime join-prune (IPv6 PIM view).....	1-26
jp-pkt-size (IPv6 PIM view).....	1-27
jp-queue-size (IPv6 PIM view).....	1-27
pim ipv6 .....	1-28
pim ipv6 bsr-boundary .....	1-29
pim ipv6 dm .....	1-29
pim ipv6 hello-option dr-priority .....	1-30
pim ipv6 hello-option holdtime.....	1-31
pim ipv6 hello-option lan-delay.....	1-31
pim ipv6 hello-option neighbor-tracking.....	1-32
pim ipv6 hello-option override-interval.....	1-33
pim ipv6 holdtime assert.....	1-33
pim ipv6 holdtime join-prune .....	1-34
pim ipv6 neighbor-policy.....	1-35
pim ipv6 require-genid .....	1-35

pim ipv6 sm .....	1-36
pim ipv6 state-refresh-capable .....	1-37
pim ipv6 timer graft-retry.....	1-37
pim ipv6 timer hello.....	1-38
pim ipv6 timer join-prune .....	1-38
pim ipv6 triggered-hello-delay .....	1-39
probe-interval (IPv6 PIM view) .....	1-40
register-policy (IPv6 PIM view).....	1-40
register-suppression-timeout (IPv6 PIM view).....	1-41
register-whole-checksum (IPv6 PIM view) .....	1-42
reset pim ipv6 control-message counters.....	1-42
source-lifetime (IPv6 PIM view).....	1-43
source-policy (IPv6 PIM view) .....	1-43
spt-switch-threshold (IPv6 PIM view) .....	1-44
ssm-policy (IPv6 PIM view) .....	1-45
state-refresh-hoplimit.....	1-46
state-refresh-interval (IPv6 PIM view) .....	1-47
state-refresh-rate-limit (IPv6 PIM view) .....	1-47
static-rp (IPv6 PIM view).....	1-48
timer hello (IPv6 PIM view).....	1-49
timer join-prune (IPv6 PIM view) .....	1-49

# 1 IPv6 PIM Configuration Commands

---



## Note

The term “router” in this document refers to a router in a generic sense or a Layer 3 switch running IPv6 PIM.

---

## IPv6 PIM Configuration Commands

### bsr-policy (IPv6 PIM view)

#### Syntax

```
bsr-policy acl6-number  
undo bsr-policy
```

#### View

IPv6 PIM view

#### Default Level

2: System level

#### Parameters

*acl6-number*: Basic IPv6 ACL number, in the range of 2000 to 2999. When an IPv6 ACL is defined, the **source** keyword in the **rule** command specifies a legal BSR source IPv6 address range.

#### Description

Use the **bsr-policy** command to configure a legal BSR address range to guard against BSR spoofing.

Use the **undo bsr-policy** command to remove the restriction of the BSR address range.

By default, there are no restrictions on the BSR address range, namely the BSR messages from any source are regarded to be eligible.

#### Examples

```
# Configure a legal BSR address range so that only routers on the segment 2001::2/64 can become the BSR.
```

```
<Sysname> system-view  
[Sysname] acl ipv6 number 2000  
[Sysname-acl6-basic-2000] rule permit source 2001::2 64  
[Sysname-acl6-basic-2000] quit
```

```
[Sysname] pim ipv6
[Sysname-pim6] bsr-policy 2000
```

## c-bsr (IPv6 PIM view)

### Syntax

```
c-bsr ipv6-address [ hash-length [ priority ] ]
undo c-bsr
```

### View

IPv6 PIM view

### Default Level

2: System level

### Parameters

*ipv6-address*: IPv6 address of the interface that is to act as a C-BSR.

*hash-length*: Hash mask length, in the range of 0 to 128. If you do not include this argument in your command, the corresponding global setting will be used.

*priority*: Priority of the C-BSR, in the range of 0 to 255. If you do not include this argument in your command, the corresponding global setting will be used. A larger value means a higher priority.

### Description

Use the **c-bsr** command to configure the specified interface a C-BSR.

Use the **undo c-bsr** command to remove the related C-BSR configuration.

No C-BSR is configured by default.

Note that IPv6 PIM-SM must be enabled on the interface to be configured as a C-BSR.

Related commands: **pim ipv6 sm**, **c-bsr hash-length**, **c-bsr priority**, **c-rp**.

### Examples

```
# Configure the interface with an IPv6 address of 1101::1 as a C-BSR.
```

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-bsr 1101::1
```

## c-bsr hash-length (IPv6 PIM view)

### Syntax

```
c-bsr hash-length hash-length
undo c-bsr hash-length
```

### View

IPv6 PIM view

## Default Level

2: System level

## Parameters

*hash-length*: Hash mask length, in the range of 0 to 128.

## Description

Use the **c-bsr hash-length** command to configure the global Hash mask length.

Use the **undo c-bsr hash-length** command to restore the system default.

By default, the Hash mask length is 126.

Related commands: **c-bsr**.

## Examples

```
# Set the global Hash mask length to 16.
```

```
<Sysname> system-view  
[Sysname] pim ipv6  
[Sysname-pim6] c-bsr hash-length 16
```

## c-bsr holdtime (IPv6 PIM view)

### Syntax

**c-bsr holdtime** *interval*

**undo c-bsr holdtime**

### View

IPv6 PIM view

## Default Level

2: System level

## Parameters

*interval*: BS timeout in seconds, in the range of 1 to 2,147,483,647.

## Description

Use the **c-bsr holdtime** command to configure the BS timeout, namely the length of time for which the C-BSRs wait for a bootstrap message from the BSR.

Use the **undo c-bsr holdtime** command to restore the system default.

By default, the BS timeout value is determined by this formula: BS timeout = BS period × 2 + 10.



### Note

The default BS period is 60 seconds, so the default BS timeout = 60 × 2 + 10 = 130 (seconds).

---

Related commands: **c-bsr**, **c-bsr interval**.

## Examples

```
# Set the BS timeout to 150 seconds.
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-bsr holdtime 150
```

## c-bsr interval (IPv6 PIM view)

### Syntax

```
c-bsr interval interval
undo c-bsr interval
```

### View

IPv6 PIM view

### Default Level

2: System level

### Parameters

*interval*: BS period in seconds, with an effective range of 1 to 2,147,483,647.

### Description

Use the **c-bsr interval** command to configure the BS period, namely the interval at which the BSR sends bootstrap messages.

Use the **undo c-bsr interval** command to restore the system default.

By default, the BS period value is determined by this formula: BS period = (BS timeout – 10) / 2.



The default BS timeout is 130 seconds, so the default BS period = (130 – 10) / 2 = 60 (seconds).

---

Related commands: **c-bsr**, **c-bsr holdtime**.

## Examples

```
# Set the BS period to 30 seconds.
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-bsr interval 30
```

## c-bsr priority (IPv6 PIM view)

### Syntax

```
c-bsr priority priority  
undo c-bsr priority
```

### View

IPv6 PIM view

### Default Level

2: System level

### Parameters

*priority*: Priority of the C-BSR, in the range of 0 to 255. A larger value means a higher priority.

### Description

Use the **c-bsr priority** command to configure the global C-BSR priority.

Use the **undo c-bsr priority** command to restore the system default.

By default, the C-BSR priority is 0.

Related commands: **c-bsr**.

### Examples

```
# Set the global C-BSR priority to 5.
```

```
<Sysname> system-view  
[Sysname] pim ipv6  
[Sysname-pim6] c-bsr priority 5
```

## c-rp (IPv6 PIM view)

### Syntax

```
c-rp ipv6-address [ group-policy acl6-number | priority priority | holdtime hold-interval |  
advertisement-interval adv-interval ] *  
undo c-rp ipv6-address
```

### View

IPv6 PIM view

### Default Level

2: System level

### Parameters

*ipv6-address*: IPv6 address of the interface that is to act as a C-RP.

*acl6-number*: Basic IPv6 ACL number, in the range of 2000 to 2999. This IPv6 ACL defines a range of IPv6 multicast groups the C-RP is going to serve, rather than defining a filtering rule. Any IPv6 multicast

group range that matches the **permit** statement in the ACL will be advertised as an RP served group, while configurations matching other statements like **deny** will not take effect.

*priority*: Priority of the C-RP, in the range of 0 to 255 and defaulting to 0. A larger value means a lower priority.

*hold-interval*: C-RP timeout time, in seconds. The effective range is 1 to 65,535. If you do not include this argument in your command, the corresponding global setting will be used.

*adv-interval*: C-RP-Adv interval in seconds, with an effective range of 1 to 65,535. If you do not include this argument in your command, the corresponding global setting will be used.

## Description

Use the **c-rp** command to configure the specified interface as a C-RP.

Use the **undo c-rp** command to remove the related C-RP configuration.

No C-RPs are configured by default.

Note that:

- IPv6 PIM-SM must be enabled on the interface to be configured as a C-RP.
- If you do not specify an IPv6 multicast group range for the C-RP, the C-RP will serve all IPv6 multicast groups.
- If you wish a router to be a C-RP for multiple group ranges, you need to include these group ranges in multiple rules in the IPv6 ACL corresponding to the **group-policy** keyword.
- If you carry out this command repeatedly on the same interface, the last configuration will take effect.

Related commands: **c-bsr**.

## Examples

```
# Configure the interface with the IPv6 address of 2001::1 to be a C-RP for IPv6 multicast group FF0E:0:1391::/96, with a priority of 10.
```

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source ff0e:0:1391:: 96
[Sysname-acl6-basic-2000] quit
[Sysname] pim ipv6
[Sysname-pim6] c-rp 2001::1 group-policy 2000 priority 10
```

## c-rp advertisement-interval (IPv6 PIM view)

### Syntax

```
c-rp advertisement-interval interval
```

```
undo c-rp advertisement-interval
```

### View

IPv6 PIM view

### Default Level

2: System level

## Parameters

*interval*: C-RP-Adv interval in seconds, with an effective range of 1 to 65,535.

## Description

Use the **c-rp advertisement-interval** command to configure the interval at which C-RP-Adv messages are sent.

Use the **undo c-rp advertisement-interval** command to restore the system default.

By default, the C-RP-Adv interval is 60 seconds.

Related commands: **c-rp**.

## Examples

```
# Set the global C-RP-Adv interval to 30 seconds.
```

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-rp advertisement-interval 30
```

## c-rp holdtime (IPv6 PIM view)

### Syntax

```
c-rp holdtime interval
```

```
undo c-rp holdtime
```

### View

IPv6 PIM view

### Default Level

2: System level

## Parameters

*interval*: C-RP timeout in seconds, with an effective range of 1 to 65,535.

## Description

Use the **c-rp holdtime** command to configure the global C-RP timeout time, namely the length of time for which the BSR waits for a C-RP-Adv message from C-RPs.

Use the **undo c-rp holdtime** command to restore the system default.

By default, the C-RP timeout time is 150 seconds.

Because a non-BSR router refreshes its C-RP timeout time through bootstrap messages, to prevent loss of C-RP information in bootstrap messages, make sure that the C-RP timeout time is not smaller than the interval at which the BSR sends bootstrap messages. The recommended C-RP timeout setting is 2.5 times the BS period or longer.

Related commands: **c-rp**, **c-bsr interval**.

## Examples

```
# Set the global C-RP timeout time to 200 seconds.
```

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-rp holdtime 200
```

## crp-policy (IPv6 PIM view)

### Syntax

```
crp-policy acl6-number
undo crp-policy
```

### View

IPv6 PIM view

### Default Level

2: System level

### Parameters

*acl6-number*: Advanced IPv6 ACL number, in the range of 3000 to 3999. When the IPv6 ACL is defined, the **source** keyword in the **rule** command specifies the IPv6 address of a C-RP and the **destination** keyword specifies the IPv6 address range of the IPv6 multicast groups that the C-RP will serve.

### Description

Use the **crp-policy** command to configure a legal C-RP address range and the range of served IPv6 multicast groups, so as to guard against C-RP spoofing.

Use the **undo crp-policy** command to remove the restrictions in C-RP address ranges and the ranges of served IPv6 multicast groups.

By default, there are no restrictions on C-RP address ranges and the address ranges of served groups, namely all received C-RP messages are assumed to be legal.

Note that the **crp-policy** command filters the IPv6 multicast group ranges advertised by C-RPs based on the group prefixes. For example, if the IPv6 multicast group range advertised by a C-RP is FF0E:0:1::/96 while the legal IPv6 multicast group range defined by the **crp-policy** command is FF0E:0:1::/120, the IPv6 multicast groups in the range of FF0E:0:1::/96 are allowed to pass.

Related commands: **c-rp**.

### Examples

# Configure a C-RP address range so that only routers in the IPv6 address range of 2001::2/64 can be C-RPs.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule permit ipv6 source 2001::2 64
[Sysname-acl6-adv-3000] quit
[Sysname] pim ipv6
[Sysname-pim6] crp-policy 3000
```

## display pim ipv6 bsr-info

### Syntax

**display pim ipv6 bsr-info**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display pim ipv6 bsr-info** command to view the BSR information in the IPv6 PIM domain and the locally configured C-RP information in effect.

Related commands: **c-bsr**, **c-rp**.

### Examples

# View the BSR information in the IPv6 PIM-SM domain and the locally configured C-RP information in effect.

```
<Sysname> display pim ipv6 bsr-info
Elected BSR Address: 2004::2
  Priority: 0
  Hash mask length: 126
  State: Elected
  Uptime: 00:01:10
  Next BSR message scheduled at: 00:00:48
Candidate BSR Address: 2004::2
  Priority: 0
  Hash mask length: 126
  State: Elected

Candidate RP: 2001::1(Vlan-interface1)
  Priority: 0
  HoldTime: 130
  Advertisement Interval: 60
  Next advertisement scheduled at: 00:00:48
Candidate RP: 2002::1(Ethernet1/1)
  Priority: 20
  HoldTime: 90
  Advertisement Interval: 50
  Next advertisement scheduled at: 00:00:28
Candidate RP: 2003::1(Vlan-interface2)
  Priority: 0
  HoldTime: 80
```

Advertisement Interval: 60

Next advertisement scheduled at: 00:00:48

**Table 1-1 display pim ipv6 bsr-info** command output description

Field	Description
Elected BSR Address	IPv6 address of the elected BSR
Candidate BSR Address	Address of the candidate BSR
Priority	BSR priority
Hash mask length	Hash mask length
State	BSR state
Uptime	Length of time since this BSR was elected
Next BSR message scheduled at	Remaining time of this BSR
Candidate RP	Address of the C-RP
Priority	Priority of the C-RP
HoldTime	Timeout time of the C-RP
Advertisement Interval	Interval between C-RP-Adv messages
Next BSR message scheduled at	Remaining time before the C-RP will send the next C-RP-Adv message

## display pim ipv6 claimed-route

### Syntax

```
display pim ipv6 claimed-route [ ipv6-source-address ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ipv6-source-address*: Displays the information of the IPv6 unicast route to a particular IPv6 multicast source. If you do not provide this argument, this command will display the information about all IPv6 unicast routes used by IPv6 PIM.

### Description

Use the **display pim ipv6 claimed-route** command to view the information of IPv6 unicast routes used by IPv6 PIM.

If an (S, G) is marked SPT, this (S, G) entry uses an IPv6 unicast route.

### Examples

```
# View the information of all IPv6 unicast routes used by IPv6 PIM.
```

```
<Sysname> display pim ipv6 claimed-route
```

```

RPF information about: 2001::2
  RPF interface: Vlan-interface1, RPF neighbor: FE80::A01:100:1
  Referenced prefix/prefix length: 2001::/64
  Referenced route type: igp
  RPF-route selecting rule: preference-preferred
  The (S, G) or (*, G) list dependent on this route entry
  (2001::2, FF03::101)

```

**Table 1-2** display pim ipv6 claimed-route command output description

Field	Description
RPF information about: 2001::2	Information of the RPF route to IPv6 multicast source 2001::2
RPF interface	RPF interface type and number
RPF neighbor	IPv6 address of the RPF neighbor
Referenced prefix/prefix length	Address/mask of the reference route
Referenced route type	Type of the referenced route: <ul style="list-style-type: none"> <li>• igp: IGP IPv6 unicast route</li> <li>• egp: EGP IPv6 unicast route</li> <li>• unicast (direct): Direct IPv6 unicast route</li> <li>• unicast: Other IPv6 unicast route (such as IPv6 static unicast route)</li> <li>• mbgp: IPv6 MBGP route</li> </ul>
RPF-route selecting rule	Rule of RPF route selection
The (S,G) or (*,G) list dependent on this route entry	(S, G) or (*, G) entry list dependent on this RPF route

## display pim ipv6 control-message counters

### Syntax

```

display pim ipv6 control-message counters [ message-type { probe | register | register-stop } |
[ interface interface-type interface-number | message-type { assert | bsr | crp | graft | graft-ack |
hello | join-prune | state-refresh } ] * ]

```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**probe:** Displays the number of null register messages.

**register:** Displays the number of register messages.

**register-stop:** Displays the number of register-stop messages.

*interface-type interface-number.* Displays the number of IPv6 PIM control messages on the specified interface.

- assert:** Displays the number of assert messages.
- bsr:** Displays the number of bootstrap messages.
- crp:** Displays the number of C-RP-Adv messages.
- graft:** Displays the number of graft messages.
- graft-ack:** Displays the number of graft-ack messages.
- hello:** Displays the number of hello messages.
- join-prune:** Displays the number of join/prune messages.
- state-refresh:** Displays the number of state refresh messages.

## Description

Use the **display pim ipv6 control-message counters** command to view the statistics information of IPv6 PIM control messages.

## Examples

# View the statistics information of all types of IPv6 PIM control messages on all interfaces.

```
<Sysname> display pim ipv6 control-message counters
PIM global control-message counters:
      Received      Sent      Invalid
Register          20         37         2
Register-Stop    25         20         1
Probe             10          5         0

PIM control-message counters for interface: Vlan-interface1
      Received      Sent      Invalid
Assert           10          5         0
Graft            20         37         2
Graft-Ack        25         20         1
Hello           1232        453         0
Join/Prune       15          30        21
State-Refresh     8           7         1
BSR              3243        589         1
C-RP             53          32         0
```

**Table 1-3** display pim ipv6 control-message counters command output description

Field	Description
PIM global control-message counters	Statistics of IPv6 PIM global control messages
PIM control-message counters for interface	Interface for which IPv6 PIM control messages were counted
Received	Number of messages received
Sent	Number of messages sent
Invalid	Number of invalid messages
Register	Register messages
Register-Stop	Register-stop messages

Field	Description
Probe	Null register messages
Assert	Assert messages
Graft	Graft messages
Graft-Ack	Graft-ack messages
Hello	Hello messages
Join/Prune	Join/prune messages
State Refresh	State refresh messages
BSR	Bootstrap messages
C-RP	C-RP-Adv messages

## display pim ipv6 grafts

### Syntax

```
display pim ipv6 grafts
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display pim ipv6 grafts** command to view the information about unacknowledged graft messages.

### Examples

# View the information about unacknowledged graft messages.

```
<Sysname> display pim ipv6 grafts
Source          Group           Age             RetransmitIn
1004::2         ff03::101      00:00:24       00:00:02
```

**Table 1-4 display pim ipv6 grafts command output description**

Field	Description
Source	IPv6 multicast source address in the graft message
Group	IPv6 multicast group address in the graft message
Age	Time in which the graft message will get aged out, in hours:minutes:seconds

Field	Description
RetransmitIn	Time in which the graft message will be retransmitted, in hours:minutes:seconds

## display pim ipv6 interface

### Syntax

```
display pim ipv6 interface [ interface-type interface-number ] [ verbose ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*interface-type interface-number*: Displays the IPv6 PIM information on a particular interface.

**verbose**: Displays the detailed PIM information.

### Description

Use the **display pim ipv6 interface** command to view the IPv6 PIM information on the specified interface or all interfaces.

### Examples

```
# View the detailed IPv6 PIM information on Vlan-interface1.
```

```
<Sysname> display pim ipv6 interface vlan-interface1 verbose
Interface: Vlan-interface1, FE80::200:5EFF:FE04:8700
  PIM version: 2
  PIM mode: Sparse
  PIM DR: FE80::200:AFF:FE01:101
  PIM DR Priority (configured): 1
  PIM neighbor count: 1
  PIM hello interval: 30 s
  PIM LAN delay (negotiated): 500 ms
  PIM LAN delay (configured): 500 ms
  PIM override interval (negotiated): 2500 ms
  PIM override interval (configured): 2500 ms
  PIM neighbor tracking (negotiated): disabled
  PIM neighbor tracking (configured): disabled
  PIM generation ID: 0xF5712241
  PIM require generation ID: disabled
  PIM hello hold interval: 105 s
  PIM assert hold interval: 180 s
  PIM triggered hello delay: 5 s
  PIM J/P interval: 60 s
```

```

PIM J/P hold interval: 210 s
PIM BSR domain border: disabled
Number of routers on network not using DR priority: 0
Number of routers on network not using LAN delay: 0
Number of routers on network not using neighbor tracking: 2

```

**Table 1-5 display pim ipv6 interface** command output description

Field	Description
Interface	Interface name and its IPv6 address
PIM version	IPv6 PIM version
PIM mode	IPv6 PIM mode, dense or sparse
PIM DR	IPv6 address of the DR
PIM DR Priority (configured)	Priority for DR election
PIM neighbor count	Total number of IPv6 PIM neighbors
PIM hello interval	Interval between IPv6 PIM hello messages
PIM LAN delay (negotiated)	Negotiated prune delay
PIM LAN delay (configured)	Configured prune delay
PIM override interval (negotiated)	Negotiated prune override interval
PIM override interval (configured)	Configured prune override interval
PIM neighbor tracking (negotiated)	Negotiated neighbor tracking status (enabled/disabled)
PIM neighbor tracking (configured)	Configured neighbor tracking status (enabled/disabled)
PIM generation ID	Generation_ID value
PIM require generation ID	Rejection of Hello messages without Generation_ID (enabled/disabled)
PIM hello hold interval	IPv6 PIM neighbor timeout time
PIM assert hold interval	Assert timeout time
PIM triggered hello delay	Maximum delay of sending hello messages
PIM J/P interval	Join/prune interval
PIM J/P hold interval	Join/prune timeout time
PIM BSR domain border	Status of PIM domain border configuration (enabled/disabled)
Number of routers on network not using DR priority	Number of routers not using the DR priority field on the subnet where the interface resides
Number of routers on network not using LAN delay	Number of routers not using the LAN delay field on the subnet where the interface resides
Number of routers on network not using neighbor tracking	Number of routers not using neighbor tracking on the subnet where the interface resides

## display pim ipv6 join-prune

### Syntax

```
display pim ipv6 join-prune mode { sm [ flags flag-value ] | ssm } [ interface interface-type  
interface-number | neighbor ipv6-neighbor-address ] * [ verbose ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**mode:** Displays the information of join/prune messages to send in the specified IPv6 PIM mode. IPv6 PIM modes include **sm** and **ssm**, which represent IPv6 PIM-SM and IPv6 PIM-SSM respectively.

**flags flag-value:** Specifies to display IPv6 PIM routing entries containing the specified flag(s). Values and meanings of *flag-value* are as follows:

- **rpt:** Specifies routing entries on the RPT.
- **spt:** Specifies routing entries on the SPT.
- **wc:** Specifies wildcard routing entries.

*interface-type interface-number:* Displays the information of join/prune messages to send on the specified interface.

*ipv6-neighbor-address:* Displays the information of join/prune messages to send to the specified IPv6 PIM neighbor.

**verbose:** Displays the detailed information of join/prune messages to send.

### Description

Use the **display pim join-prune** command to view the information about the join/prune messages to send.

### Examples

# View the information of join/prune messages to send in the IPv6 PIM-SM mode.

```
<Sysname> display pim ipv6 join-prune mode sm
```

```
Expiry Time: 50 sec
```

```
Upstream nbr: FE80::2E0:FCFF:FE03:1004 (Vlan-interface1)
```

```
1 (*, G) join(s), 0 (S, G) join(s), 1 (S, G, rpt) prune(s)
```

```
-----  
Total (*, G) join(s): 1, (S, G) join(s): 0, (S, G, rpt) prune(s): 1
```

**Table 1-6 display pim join-prune** command output description

Field	Description
Expiry Time:	Expiry time of sending join/prune messages
Upstream nbr:	IPv6 address of the upstream IPv6 PIM neighbor and the interface connecting to it

Field	Description
(*, G) join(s)	Number of (*, G) joins to send
(S, G) join(s)	Number of (S, G) joins to send
(S, G, rpt) prune(s)	Number of (S, G, rpt) prunes

## display pim ipv6 neighbor

### Syntax

```
display pim ipv6 neighbor [ interface interface-type interface-number | ipv6-neighbor-address |
verbose ] *
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*interface-type interface-number*: Displays the IPv6 PIM neighbor information on a particular interface.

*ipv6-neighbor-address*: Displays the information of a particular IPv6 PIM neighbor.

**verbose**: Displays the detailed IPv6 PIM neighbor information.

### Description

Use the **display pim ipv6 neighbor** command to view the IPv6 PIM neighbor information.

### Examples

# View the information of all IPv6 PIM neighbors.

```
<Sysname> display pim ipv6 neighbor
Total Number of Neighbors = 2
```

```
Neighbor          Interface          Uptime    Expires    Dr-Priority
FE80::A01:101:1   Vlan1              02:50:49  00:01:31  1
FE80::A01:102:1   Vlan2              02:49:39  00:01:42  1
```

# View the detailed information of the IPv6 PIM neighbor whose IPv6 address is FE80::1.

```
<Sysname> display pim ipv6 neighbor fe80::1 verbose
Neighbor: FE80:: 1
  Interface: Vlan-interface3
  Uptime: 00:00:10
  Expiry time: 00:00:30
  DR Priority: 1
  Generation ID: 0x2ACEFE15
  Holdtime: 105 s
  LAN delay: 500 ms
  Override interval: 2500 ms
```

State refresh interval: 60 s  
Neighbor tracking: Disabled

**Table 1-7 display pim ipv6 neighbor** command output description

Field	Description
Total Number of Neighbors	Total number of IPv6 PIM neighbors
Neighbor	IPv6 address of the PIM neighbor
Interface	Interface connecting the IPv6 PIM neighbor
Uptime	Length of time since the IPv6 PIM neighbor was discovered
Expires/Expiry time	Remaining time of the IPv6 PIM neighbor; "never" means that the IPv6 PIM neighbor is always up and reachable.
Dr-Priority/DR Priority	Priority of the IPv6 PIM neighbor
Generation ID	Generation ID of the IPv6 PIM neighbor (a random value indicating status change of the IPv6 PIM neighbor)
Holdtime	Holdtime of the IPv6 PIM neighbor; "forever" means that the IPv6 PIM neighbor is always up and reachable
LAN delay	Prune delay
Override interval	Prune override interval
State refresh interval	Interval of sending state refresh messages
Neighbor tracking	Neighbor tracking status (enabled/disabled)

## display pim ipv6 routing-table

### Syntax

```
display pim ipv6 routing-table [ ipv6-group-address [ prefix-length ] | ipv6-source-address
[ prefix-length ] | incoming-interface [ interface-type interface-number | register ] | outgoing-interface
{ include | exclude | match } { interface-type interface-number | register } | mode mode-type | flags
flag-value | fsm ] *
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ipv6-group-address*: Specifies an IPv6 multicast group by its address, in the range of FFxy::/16, where x and y represent any hexadecimal number between 0 and F, inclusive.

*ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address.

*prefix-length*: Prefix length of the IPv6 multicast group/source address prefix. For an IPv6 multicast group address, the effective range is 8 to 128 and the default value is 128; for an IPv6 multicast source address, the effective range is 0 to 128 and the default value is 128.

**incoming-interface:** Displays routing entries that contain the specified interface as the incoming interface.

*interface-type interface-number:* Specifies an interface by its type and number.

**register:** Specifies the register interface. This keyword is valid only if *mode-type* is not specified or is **sm**.

**outgoing-interface:** Displays routing entries that contain the specified interface as the outgoing interface.

**include:** Displays routing entries of which the outgoing interface list includes the specified interface.

**exclude:** Displays routing entries of which the outgoing interface list excludes the specified interface.

**match:** Displays routing entries of which the outgoing interface list includes only the specified interface.

**mode mode-type:** Specifies an IPv6 PIM mode, where *mode-type* can have the following values:

- **dm:** Specifies IPv6 PIM-DM.
- **sm:** Specifies IPv6 PIM-SM.
- **ssm:** Specifies IPv6 PIM-SSM.

**flags flag-value:** Displays IPv6 PIM routing entries containing the specified flag(s). The values of *flag-value* and their meanings are as follows:

- **act:** Specifies IPv6 multicast routing entries to which actual data has arrived.
- **del:** Specifies IPv6 multicast routing entries scheduled to be deleted.
- **exprune:** Specifies multicast routing entries containing outgoing interfaces pruned by other IPv6 multicast routing protocols.
- **ext:** Specifies IPv6 routing entries containing outgoing interfaces provided by other IPv6 multicast routing protocols.
- **loc:** Specifies IPv6 multicast routing entries on routers directly connecting to the same subnet with the IPv6 multicast source.
- **niif:** Specifies IPv6 multicast routing entries containing unknown incoming interfaces.
- **nonbr:** Specifies routing entries with IPv6 PIM neighbor searching failure.
- **rpt:** Specifies routing entries on RPT branches where (S, G) prunes have been sent to the RP.
- **spt:** Specifies routing entries on the SPT.
- **swt:** Specifies routing entries in the process of RPT-to-SPT switchover.
- **wc:** Specifies wildcard routing entries.

**fsm:** Displays the detailed information of the finite state machine (FSM).

## Description

Use the **display pim ipv6 routing-table** command to view IPv6 PIM routing table information.

Related commands: **display ipv6 multicast routing-table** in the *IPv6 Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*.

## Examples

# View the content of the IPv6 PIM routing table.

```
<Sysname> display pim ipv6 routing-table
```

```
Total 0 (*, G) entry; 1 (S, G) entry
```

```
(2001::2, FFE3::101)
```

```
Protocol: pim-dm, Flag:
```

```

UpTime: 00:04:24
Upstream interface: Vlan-interface1
    Upstream neighbor: FE80::A01:100:1
    RPF prime neighbor: FE80::A01:100:1
Downstream interface(s) information:
Total number of downstreams: 1
    1: Vlan-interface2
        Protocol: pim-dm, UpTime: 00:04:24, Expires: 00:02:47

```

**Table 1-8** display pim ipv6 routing-table command output description

Field	Description
Total 0 (*, G) entry; 1 (S, G) entry	Number of (S, G) and (*, G) entries in the IPv6 PIM routing table
(2001::2, FFE3::101)	An (S, G) entry in the IPv6 PIM routing table
Protocol	IPv6 PIM mode, IPv6 PIM-SM or IPv6 PIM-DM
Flag	Flag of the (S, G) or (*, G) entry in the IPv6 PIM routing table
Uptime	Length of time since the (S, G) or (*, G) entry was installed
Upstream interface	Upstream (incoming) interface of the (S, G) or (*, G) entry
Upstream neighbor	Upstream neighbor of the (S, G) or (*, G) entry
RPF prime neighbor	RPF neighbor of the (S, G) or (*, G) entry <ul style="list-style-type: none"> <li>For a (*, G) entry, if this router is the RP, the RPF neighbor of this (*, G) entry is NULL.</li> <li>For a (S, G) entry, if this router directly connects to the IPv6 multicast source, the RPF neighbor of this (S, G) entry is NULL.</li> </ul>
Downstream interface(s) information	Information of the downstream interface(s), including: <ul style="list-style-type: none"> <li>Number of downstream interfaces</li> <li>Downstream interface name</li> <li>Protocol type configured on the downstream interface</li> <li>Uptime of the downstream interface(s)</li> <li>Expiry time of the downstream interface(s)</li> </ul>

## display pim ipv6 rp-info

### Syntax

```
display pim ipv6 rp-info [ ipv6-group-address ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ipv6-group-address*: Specifies an IPv6 multicast group by its address, in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16 and FF0y::), where x and y represent any hexadecimal

number between 0 and F, inclusive. If you do not provide a group address, this command will display the RP information corresponding to all IPv6 multicast groups.

## Description

Use the **display pim ipv6 rp-info** command to view the RP information.

Note that:

- The RP information includes the information of RPs dynamically found by the BSR mechanism and static RPs.
- Because a non-BSR router refreshes its local RP-Set only based on the received BSR bootstrap messages, the system does not delete an RP even if its expiry time is 0. Instead, the system waits for the next bootstrap message from the BSR: if the bootstrap message does not contain information of the RP, the system will delete it.

## Examples

# View the RP information corresponding to the IPv6 multicast group FF0E::101.

```
<Sysname> display pim ipv6 rp-info ff0e::101
PIM-SM BSR RP information:
prefix/prefix length: FF0E::101/64
  RP: 2004::2
  Priority: 0
  HoldTime: 130
  Uptime: 00:05:19
  Expires: 00:02:11
```

**Table 1-9 display pim ipv6 rp-info** command output description

Field	Description
prefix/prefix length	The IPv6 multicast group served by the RP
RP	IPv6 address of the RP
Priority	RP priority
HoldTime	Timeout time of the RP
Uptime	Length of time since the RP was elected
Expires	Remaining time of the RP

## embedded-rp

### Syntax

```
embedded-rp [ acl6-number ]
undo embedded-rp [ acl6-number ]
```

### View

IPv6 PIM view

## Default Level

2: System level

## Parameters

*acl6-number*: Basic IPv6 ACL number, in the range of 2000 to 2999.

## Description

Use the **embedded-rp** command to enable embedded RP.

Use the **undo embedded-rp** command to disable embedded RP or restore the system default.

By default, embedded RP is enabled for IPv6 multicast groups in the default embedded RP address scopes.



The default embedded RP address scopes are FF7x::/12 and FFFx::/12. Here “x” refers to any legal address scope. For details of the scope field, see *Multicast Overview* of the *IP Multicast Volume*.

---

Note that:

- When you use the **embedded-rp** command without specifying *acl6-number*, the embedded RP feature will be enabled for all the IPv6 multicast groups in the default embedded RP address scopes; if you specify *acl6-number*, the embedded RP feature will be enabled for only those IPv6 multicast groups that are within the default embedded RP address scopes and pass the ACL check.
- When you use the **undo embedded-rp** command without specifying *acl6-number*, the embedded RP feature will be disabled for all the IPv6 multicast groups; if you specify *acl6-number*, this command will restore the system default.

## Examples

```
# Enable embedded RP for only those IPv6 multicast groups in the address scope  
FF7E:140:20::101/64.
```

```
<Sysname> system-view  
[Sysname] acl ipv6 number 2000  
[Sysname-acl6-basic-2000] rule permit source ff7e:140:20::101 64  
[Sysname-acl6-basic-2000] quit  
[Sysname] pim ipv6  
[Sysname-pim6] embedded-rp 2000
```

## hello-option dr-priority (IPv6 PIM view)

### Syntax

**hello-option dr-priority** *priority*

**undo hello-option dr-priority**

## View

IPv6 PIM view

## Default Level

2: System level

## Parameters

*priority*: Router priority for DR election, in the range of 0 to 4294967295. A larger value means a higher priority.

## Description

Use the **hello-option dr-priority** command to configure the global value of the router priority for DR election.

Use the **undo hello-option dr-priority** command to restore the system default.

By default, the router priority for DR election is 1.

Related commands: **pim ipv6 hello-option dr-priority**.

## Examples

# Set the router priority for DR election to 3.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] hello-option dr-priority 3
```

## hello-option holdtime (IPv6 PIM view)

### Syntax

**hello-option holdtime** *interval*

**undo hello-option holdtime**

### View

IPv6 PIM view

### Default Level

2: System level

### Parameters

*interval*: IPv6 PIM neighbor timeout time in seconds, with an effective range of 1 to 65,535. 65,535 makes the IPv6 PIM neighbor always reachable.

### Description

Use the **hello-option holdtime** command to configure the IPv6 PIM neighbor timeout time.

Use the **undo hello-option holdtime** command to restore the system default.

By default, the IPv6 PIM neighbor timeout time is 105 seconds.

Related commands: **pim ipv6 hello-option holdtime**.

## Examples

```
# Set the IPv6 PIM neighbor timeout time to 120 seconds globally.  
<Sysname> system-view  
[Sysname] pim ipv6  
[Sysname-pim6] hello-option holdtime 120
```

## hello-option lan-delay (IPv6 PIM view)

### Syntax

```
hello-option lan-delay interval  
undo hello-option lan-delay
```

### View

IPv6 PIM view

### Default Level

2: System level

### Parameters

*interval*: LAN-delay time in milliseconds, with an effective range of 1 to 32,767.

### Description

Use the **hello-option lan-delay** command to configure the global value of the LAN-delay time.

Use the **undo hello-option lan-delay** command to restore the system default.

By default, the LAN-delay time is 500 milliseconds.

Related commands: **hello-option override-interval**, **pim ipv6 hello-option override-interval**, **pim ipv6 hello-option lan-delay**.

## Examples

```
# Set the LAN-delay to 200 milliseconds globally.  
<Sysname> system-view  
[Sysname] pim ipv6  
[Sysname-pim6] hello-option lan-delay 200
```

## hello-option neighbor-tracking (IPv6 PIM view)

### Syntax

```
hello-option neighbor-tracking  
undo hello-option neighbor-tracking
```

### View

IPv6 PIM view

### Default Level

2: System level

## Parameters

None

## Description

Use the **hello-option neighbor-tracking** command to globally disable join suppression, namely enable neighbor tracking.

Use the **undo hello-option neighbor-tracking** command to enable join suppression.

By default, join suppression is enabled, namely neighbor tracking is disabled.

Related commands: **pim ipv6 hello-option neighbor-tracking**.

## Examples

```
# Disable join suppression globally.  
<Sysname> system-view  
[Sysname] pim ipv6  
[Sysname-pim6] hello-option neighbor-tracking
```

## hello-option override-interval (IPv6 PIM view)

### Syntax

```
hello-option override-interval interval  
undo hello-option override-interval
```

### View

IPv6 PIM view

### Default Level

2: System level

## Parameters

*interval*: Prune override interval in milliseconds, with an effective range of 1 to 65,535.

## Description

Use the **hello-option override-interval** command to configure the global value of the prune override interval.

Use the **undo hello-option override-interval** command to restore the system default.

By default, the prune override interval is 2,500 milliseconds.

Related commands: **hello-option lan-delay**, **pim ipv6 hello-option lan-delay**, **pim ipv6 hello-option override-interval**.

## Examples

```
# Set the prune override interval to 2,000 milliseconds globally.  
<Sysname> system-view  
[Sysname] pim ipv6  
[Sysname-pim6] hello-option override-interval 2000
```

## holdtime assert (IPv6 PIM view)

### Syntax

```
holdtime assert interval  
undo holdtime assert
```

### View

IPv6 PIM view

### Default Level

2: System level

### Parameters

*interval*: Assert timeout time in seconds, with an effective range of 7 to 2,147,483,647.

### Description

Use the **holdtime assert** command to configure the global value of the assert timeout time.

Use the **undo holdtime assert** command to restore the system default.

By default, the assert timeout time is 180 seconds.

Related commands: **holdtime join-prune**, **pim ipv6 holdtime join-prune**, **pim ipv6 holdtime assert**.

### Examples

```
# Set the global value of the assert timeout time to 100 seconds.
```

```
<Sysname> system-view  
[Sysname] pim ipv6  
[Sysname-pim6] holdtime assert 100
```

## holdtime join-prune (IPv6 PIM view)

### Syntax

```
holdtime join-prune interval  
undo holdtime join-prune
```

### View

IPv6 PIM view

### Default Level

2: System level

### Parameters

*interval*: Join/prune timeout time in seconds, with an effective range of 1 to 65,535.

### Description

Use the **holdtime join-prune** command to configure the global value of the join/prune timeout time.

Use the **undo holdtime join-prune** command to restore the system default.

By default, the join/prune timeout time is 210 seconds.

Related commands: **holdtime assert**, **pim ipv6 holdtime assert**, **pim ipv6 holdtime join-prune**.

## Examples

# Set the global value of the join/prune timeout time to 280 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] holdtime join-prune 280
```

## jp-pkt-size (IPv6 PIM view)

### Syntax

**jp-pkt-size** *packet-size*

**undo jp-pkt-size**

### View

IPv6 PIM view

### Default Level

2: System level

### Parameters

*packet-size*: Maximum size of join/prune messages in bytes, with an effective range of 100 to 64000.

### Description

Use the **jp-pkt-size** command to configure the maximum size of join/prune messages.

Use the **undo jp-pkt-size** command to restore the system default.

By default, the maximum size of join/prune messages is 8,100 bytes.

Related commands: **jp-queue-size**.

## Examples

# Set the maximum size of join/prune messages to 1,500 bytes.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] jp-pkt-size 1500
```

## jp-queue-size (IPv6 PIM view)

### Syntax

**jp-queue-size** *queue-size*

**undo jp-queue-size**

### View

IPv6 PIM view

## Default Level

2: System level

## Parameters

*queue-size*: Maximum number of (S, G) entries in a join/prune message, in the range of 1 to 4,096.

## Description

Use the **jp-queue-size** command to configure the maximum number of (S, G) entries in a join/prune message.

Use the **undo jp-queue-size** command to restore the system default.

By default, a join/prune messages contains a maximum of 1,020 (S, G) entries.

When you use this command, take the following into account:

- The size of the forwarding table. In a network that does not support packet fragmentation, if you configure a large queue-size, a join/prune message may contain a large number of groups, causing the message length to exceed the MTU of the network. As a result, the products that do not support fragmentation will drop the join/prune message.
- The (S, G) join/prune state hold time on the upstream device. If you configure a small queue size, the outgoing interface of the corresponding entry may have been pruned due to timeout before the last join/prune message in a queue reaches the upstream device.

Related commands: **jp-pkt-size**, **holdtime join-prune**, **pim holdtime join-prune**.

## Examples

# Configure a join/prune messages to contain a maximum of 2,000 (S, G) entries.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] jp-queue-size 2000
```

## pim ipv6

### Syntax

```
pim ipv6
undo pim ipv6
```

### View

System view

## Default Level

2: System level

## Parameters

None

## Description

Use the **pim ipv6** command to enter IPv6 PIM view.

Use the **undo pim ipv6** command to remove all configurations performed in IPv6 PIM view.

Note that IPv6 multicast routing must be enabled on the device before this command can take effect.

Related commands: **multicast ipv6 routing-enable** (*IPv6 Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*).

## Examples

```
# Enable IPv6 multicast routing and enter IPv6 PIM view.
```

```
<Sysname> system-view
[Sysname] multicast ipv6 routing-enable
[Sysname] pim ipv6
[Sysname-pim6]
```

## pim ipv6 bsr-boundary

### Syntax

```
pim ipv6 bsr-boundary
undo pim ipv6 bsr-boundary
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **pim ipv6 bsr-boundary** command to configure an IPv6 PIM domain border, namely a bootstrap message boundary.

Use the **undo pim ipv6 bsr-boundary** command to remove the configured IPv6 PIM domain border.

By default, no PIM domain border is configured.

Related commands: **c-bsr**; **multicast ipv6 boundary** (*IPv6 Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*).

## Examples

```
# Configure VLAN-interface 100 as a PIM domain border.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 bsr-boundary
```

## pim ipv6 dm

### Syntax

```
pim ipv6 dm
undo pim ipv6 dm
```

## View

Interface view

## Default Level

2: System level

## Parameters

None

## Description

Use the **pim ipv6 dm** command to enable IPv6 PIM-DM.

Use the **undo pim ipv6 dm** command to disable IPv6 PIM-DM.

By default, IPv6 PIM-DM is disabled.

Note that:

- This command can take effect only after IPv6 multicast routing is enabled on the device.
- IPv6 PIM-DM cannot be used for IPv6 multicast groups in the IPv6 SSM group range.

Related commands: **pim ipv6 sm**, **ssm-policy**; **multicast ipv6 routing-table** in the *IPv6 Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*.

## Examples

# Enable IPv6 multicast routing, and enable IPv6 PIM-DM on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] multicast ipv6 routing-enable
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 dm
```

## pim ipv6 hello-option dr-priority

### Syntax

**pim ipv6 hello-option dr-priority** *priority*

**undo pim ipv6 hello-option dr-priority**

### View

Interface view

### Default Level

2: System level

### Parameters

*priority*: Router priority for DR election, in the range of 0 to 4294967295. A larger value means a higher priority.

### Description

Use the **pim ipv6 hello-option dr-priority** command to configure the router priority for DR election on the current interface.

Use the **undo pim ipv6 hello-option dr-priority** command to restore the system default.

By default, the router priority for DR election is 1.

Related commands: **hello-option dr-priority**.

## Examples

# Set the router priority for DR election to 3 on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 hello-option dr-priority 3
```

## pim ipv6 hello-option holdtime

### Syntax

**pim ipv6 hello-option holdtime** *interval*

**undo pim ipv6 hello-option holdtime**

### View

Interface view

### Default Level

2: System level

### Parameters

*interval*: IPv6 PIM neighbor timeout time in seconds, with an effective range of 1 to 65,535. 65,535 makes the PIM neighbor always reachable.

### Description

Use the **pim ipv6 hello-option holdtime** command to configure the PIM neighbor timeout time on the current interface.

Use the **undo pim ipv6 hello-option holdtime** command to restore the system default.

By default, the IPv6 PIM neighbor timeout time is 105 seconds.

Related commands: **hello-option holdtime**.

## Examples

# Set the IPv6 PIM neighbor timeout time to 120 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 hello-option holdtime 120
```

## pim ipv6 hello-option lan-delay

### Syntax

**pim ipv6 hello-option lan-delay** *interval*

**undo pim ipv6 hello-option lan-delay**

## View

Interface view

## Default Level

2: System level

## Parameters

*interval*: LAN-delay time in milliseconds, with an effective range of 1 to 32,767.

## Description

Use the **pim ipv6 hello-option lan-delay** command to configure the LAN-delay time, namely the device waits between receiving a prune message and taking a prune action, on the current interface.

Use the **undo pim ipv6 hello-option lan-delay** command to restore the system default.

By default, the LAN-delay time is 500 milliseconds.

Related commands: **pim ipv6 hello-option override-interval**, **hello-option override-interval**, **hello-option lan-delay**.

## Examples

# Set the LAN-delay time to 200 milliseconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 hello-option lan-delay 200
```

## pim ipv6 hello-option neighbor-tracking

### Syntax

```
pim ipv6 hello-option neighbor-tracking
undo pim ipv6 hello-option neighbor-tracking
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **pim ipv6 hello-option neighbor-tracking** command to disable join suppression, namely enable neighbor tracking, on the current interface.

Use the **undo pim ipv6 hello-option neighbor-tracking** command to enable join suppression.

By default, join suppression is enabled, namely neighbor tracking is disabled.

Related commands: **hello-option neighbor-tracking**.

## Examples

```
# Disable join suppression on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 hello-option neighbor-tracking
```

## pim ipv6 hello-option override-interval

### Syntax

```
pim ipv6 hello-option override-interval interval
undo pim ipv6 hello-option override-interval
```

### View

Interface view

### Default Level

2: System level

### Parameters

*interval*: Prune override interval in milliseconds, with an effective range of 1 to 65,535.

### Description

Use the **pim ipv6 hello-option override-interval** command to configure the prune override interval on the current interface.

Use the **undo pim ipv6 hello-option override-interval** command to restore the system default.

By default, the prune override interval is 2,500 milliseconds.

Related commands: **pim ipv6 hello-option lan-delay**, **hello-option lan-delay**, **hello-option override-interval**.

## Examples

```
# Set the prune override interval to 2,000 milliseconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 hello-option override-interval 2000
```

## pim ipv6 holdtime assert

### Syntax

```
pim ipv6 holdtime assert interval
undo pim ipv6 holdtime assert
```

### View

Interface view

## Default Level

2: System level

## Parameters

*interval*: Assert timeout time in seconds, with an effective range of 7 to 2,147,483,647.

## Description

Use the **pim ipv6 holdtime assert** command to configure the assert timeout time on the current interface.

Use the **undo pim ipv6 holdtime assert** command to restore the system default.

By default, the assert timeout time is 180 seconds.

Related commands: **holdtime join-prune**, **pim ipv6 holdtime join-prune**, **holdtime assert**.

## Examples

```
# Set the assert timeout time to 100 seconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 holdtime assert 100
```

## pim ipv6 holdtime join-prune

### Syntax

```
pim ipv6 holdtime join-prune interval
undo pim ipv6 holdtime join-prune
```

### View

Interface view

## Default Level

2: System level

## Parameters

*interval*: Join/prune timeout time in seconds, with an effective range of 1 to 65,535.

## Description

Use the **pim ipv6 holdtime join-prune** command to configure the join/prune timeout time on the interface.

Use the **undo pim ipv6 holdtime join-prune** command to restore the system default.

By default, the join/prune timeout time is 210 seconds.

Related commands: **holdtime assert**, **pim ipv6 holdtime assert**, **holdtime join-prune**.

## Examples

```
# Set the join/prune timeout time to 280 seconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
```

```
[Sysname-Vlan-interface100] pim ipv6 holdtime join-prune 280
```

## pim ipv6 neighbor-policy

### Syntax

```
pim ipv6 neighbor-policy acl6-number  
undo pim ipv6 neighbor-policy
```

### View

Interface view

### Default Level

2: System level

### Parameters

*acl6-number*: Basic IPv6 ACL number, in the range of 2000 to 2999. When the IPv6 ACL is defined, the **source** keyword in the **rule** command specifies a legal source address range for hello messages.

### Description

Use the **pim ipv6 neighbor-policy** command to configure a legal source address range for hello messages to guard against hello message spoofing.

Use the **undo pim ipv6 neighbor-policy** command to restore the default.

By default, no source address range for hello messages is configured, that is, all the received hello messages are considered legal.

### Examples

# Configure a legal source address range for hello messages on VLAN-interface 100 so that only the switches on the FE80:101::101/64 subnet can become PIM neighbors of this switch.

```
<Sysname> system-view  
[Sysname] acl ipv6 number 2000  
[Sysname-acl6-basic-2000] rule permit source fe80:101::101 64  
[Sysname-acl6-basic-2000] quit  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] pim ipv6 neighbor-policy 2000
```

## pim ipv6 require-genid

### Syntax

```
pim ipv6 require-genid  
undo pim ipv6 require-genid
```

### View

Interface view

### Default Level

2: System level

## Parameters

None

## Description

Use the **pim ipv6 require-genid** command enable rejection of hello messages without Generation\_ID.

Use the **undo pim ipv6 require-genid** command to restore the default configuration.

By default, hello messages without Generation\_ID are accepted.

## Examples

# Enable VLAN-interface 100 to reject hello messages without Generation\_ID.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 require-genid
```

## pim ipv6 sm

### Syntax

```
pim ipv6 sm
undo pim ipv6 sm
```

### View

Interface view

### Default Level

2: System level

## Parameters

None

## Description

Use the **pim ipv6 sm** command to enable IPv6 PIM-SM.

Use the **undo pim ipv6 sm** command to disable IPv6 PIM-SM.

By default, IPv6 PIM-SM is disabled.

Note that this command can take effect only after IPv6 multicast routing is enabled on the device.

Related commands: **pim ipv6 dm**; **multicast ipv6 routing-table** in the *IPv6 Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*.

## Examples

# Enable IPv6 multicast routing, and enable IPv6 PIM-SM on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] multicast ipv6 routing-enable
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 sm
```

## pim ipv6 state-refresh-capable

### Syntax

```
pim ipv6 state-refresh-capable
undo pim ipv6 state-refresh-capable
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **pim ipv6 state-refresh-capable** command to enable the state fresh feature on the interface.

Use the **undo pim ipv6 state-refresh-capable** command to disable the state fresh feature.

By default, the state refresh feature is enabled.

Related commands: **state-refresh-interval**, **state-refresh-rate-limit**, **state-refresh-hoplimit**.

### Examples

```
# Disable state refresh on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo pim ipv6 state-refresh-capable
```

## pim ipv6 timer graft-retry

### Syntax

```
pim ipv6 timer graft-retry interval
undo pim ipv6 timer graft-retry
```

### View

Interface view

### Default Level

2: System level

### Parameters

*interval*: Graft retry period in seconds, with an effective range of 1 to 65,535.

### Description

Use the **pim ipv6 timer graft-retry** command to configure the graft retry period.

Use the **undo pim ipv6 timer graft-retry** command to restore the system default.

By default, the graft retry period is 3 seconds.

## Examples

```
# Set the graft retry period to 80 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 timer graft-retry 80
```

## pim ipv6 timer hello

### Syntax

```
pim ipv6 timer hello interval
undo pim ipv6 timer hello
```

### View

Interface view

### Default Level

2: System level

### Parameters

*interval*: Hello interval in seconds, with an effective range of 1 to 2,147,483,647.

### Description

Use the **pim ipv6 timer hello** command to configure on the current interface the interval at which hello messages are sent.

Use the **undo pim ipv6 timer hello** command to restore the system default.

By default, hello messages are sent at the interval of 30 seconds.

Related commands: **timer hello**.

## Examples

```
# Set the hello interval to 40 seconds on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 timer hello 40
```

## pim ipv6 timer join-prune

### Syntax

```
pim ipv6 timer join-prune interval
undo pim ipv6 timer join-prune
```

### View

Interface view

## Default Level

2: System level

## Parameters

*interval*: Join/prune interval in seconds, with an effective range of 1 to 2,147,483,647.

## Description

Use the **pim ipv6 timer join-prune** command to configure on the current interface the interval at which join/prune messages are sent.

Use the **undo pim ipv6 timer join-prune** command to restore the system default.

By default, the join/prune interval is 60 seconds.

Related commands: **timer join-prune**.

## Examples

```
# Set the join/prune interval to 80 seconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 timer join-prune 80
```

## pim ipv6 triggered-hello-delay

### Syntax

```
pim ipv6 triggered-hello-delay interval
undo pim ipv6 triggered-hello-delay
```

### View

Interface view

## Default Level

2: System level

## Parameters

*interval*: Maximum delay in seconds between hello messages, with an effective range of 1 to 5.

## Description

Use the **pim ipv6 triggered-hello-delay** command to configure the maximum delay between hello messages.

Use the **undo pim ipv6 triggered-hello-delay** command to restore the system default.

By default, the maximum delay between hello messages is 5 seconds.

## Examples

```
# Set the maximum delay between hello messages to 3 seconds on VLAN-interface 100.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 triggered-hello-delay 3
```

## probe-interval (IPv6 PIM view)

### Syntax

```
probe-interval interval  
undo probe-interval
```

### View

IPv6 PIM view

### Default Level

2: System level

### Parameters

*interval*: Register probe time in seconds, with an effective range of 1 to 1799.

### Description

Use the **probe-interval** command to configure the register probe time.

Use the **undo probe-interval** command to restore the system default.

By default, the register probe time is 5 seconds.

Related commands: **register-suppression-timeout**.

### Examples

```
# Set the register probe time to 6 seconds.
```

```
<Sysname> system-view  
[Sysname] pim ipv6  
[Sysname-pim6] probe-interval 6
```

## register-policy (IPv6 PIM view)

### Syntax

```
register-policy acl6-number  
undo register-policy
```

### View

IPv6 PIM view

### Default Level

2: System level

### Parameters

*acl6-number*: Advanced IPv6 ACL number, in the range of 3000 to 3999. Only register messages that match the **permit** statement of the IPv6 ACL can be accepted by the RP.

### Description

Use the **register-policy** command to configure an IPv6 ACL rule to filter register messages.

Use the **undo register-policy** command to remove the configured register filtering rule.

By default, no register filtering rule is configured.

Related commands: **register-suppression-timeout**.

## Examples

# Configure a register filtering policy on the RP so that the RP will accept only those register messages from IPv6 multicast sources on the 3:1::/64 subnet for IPv6 multicast groups on the FF0E:13::/64 subnet.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule permit ipv6 source 3:1:: 64 destination ff0e:13:: 64
[Sysname-acl6-adv-3000] quit
[Sysname] pim ipv6
[Sysname-pim6] register-policy 3000
```

## register-suppression-timeout (IPv6 PIM view)

### Syntax

```
register-suppression-timeout interval
undo register-suppression-timeout
```

### View

IPv6 PIM view

### Default Level

2: System level

### Parameters

*interval*: Register suppression time in seconds, in the range of 1 to 3,600.

### Description

Use the **register-suppression-timeout** command to configure the register suppression time.

Use the **undo register-suppression-timeout** command to restore the system default.

By default, the register suppression time is 60 seconds.

Related commands: **probe-interval**, **register-policy**.

## Examples

# Set the register suppression time to 70 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] register-suppression-timeout 70
```

## register-whole-checksum (IPv6 PIM view)

### Syntax

```
register-whole-checksum
undo register-whole-checksum
```

### View

IPv6 PIM view

### Default Level

2: System level

### Parameters

None

### Description

Use the **register-whole-checksum** command to configure the router to calculate the checksum based on the entire register message.

Use the **undo register-whole-checksum** command to restore the default configuration.

By default, the checksum is calculated based only on the header in the register message.

Related commands: **register-policy**, **register-suppression-timeout**.

### Examples

```
# Configure the router to calculate the checksum based on the entire register message.
```

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] register-whole-checksum
```

## reset pim ipv6 control-message counters

### Syntax

```
reset pim ipv6 control-message counters [ interface interface-type interface-number ]
```

### View

User view

### Default Level

1: Monitor level

### Parameters

*interface-type interface-number*: Specifies to reset the IPv6 PIM control message counter on a particular interface. If no interface is specified, this command will clear the statistics information about IPv6 PIM control messages on all interfaces.

## Description

Use the **reset pim ipv6 control-message counters** command to reset IPv6 PIM control message counters.

## Examples

```
# Reset IPv6 PIM control message counters on all interfaces.  
<Sysname> reset pim ipv6 control-message counters
```

## source-lifetime (IPv6 PIM view)

### Syntax

```
source-lifetime interval  
undo source-lifetime
```

### View

IPv6 PIM view

### Default Level

2: System level

### Parameters

*interval*: IPv6 multicast source lifetime in seconds, with an effective range of 1 to 65,535.

## Description

Use the **source-lifetime** command to configure the IPv6 multicast source lifetime.

Use the **undo source-lifetime** command to restore the system default.

By default, the lifetime of an IPv6 multicast source is 210 seconds.

## Examples

```
# Set the IPv6 multicast source lifetime to 200 seconds.  
<Sysname> system-view  
[Sysname] pim ipv6  
[Sysname-pim6] source-lifetime 200
```

## source-policy (IPv6 PIM view)

### Syntax

```
source-policy acl6-number  
undo source-policy
```

### View

IPv6 PIM view

### Default Level

2: System level

## Parameters

*acl6-number*: Basic or advanced IPv6 ACL number, in the range of 2000 to 3999.

## Description

Use the **source-policy** command to configure an IPv6 multicast data filter.

Use the **undo source-policy** command to remove the configured IPv6 multicast data filter.

By default, no IPv6 multicast data filter is configured.

Note that:

- If you specify a basic ACL, the device filters all the received IPv6 multicast packets based on the source address, and discards packets that fail the source address match.
- If you specify an advanced ACL, the device filters all the received IPv6 multicast packets based on the source and group addresses, and discards packets that fail the match.
- If this command is executed repeatedly, the last configuration will take effect.

## Examples

# Configure the router to accept IPv6 multicast packets originated from 3121::1 and discard IPv6 multicast packets originated from 3121::2.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source 3121::1 128
[Sysname-acl6-basic-2000] rule deny source 3121::2 128
[Sysname-acl6-basic-2000] quit
[Sysname] pim ipv6
[Sysname-pim6] source-policy 2000
[Sysname-pim6] quit
```

## spt-switch-threshold (IPv6 PIM view)

### Syntax

**spt-switch-threshold infinity [ group-policy *acl6-number* [ order *order-value* ] ]**

**undo spt-switch-threshold [ group-policy *acl6-number* ]**

### View

IPv6 PIM view

### Default Level

2: System level

### Parameters

**infinity**: Disables SPT switchover.

**group-policy *acl6-number***: Specifies a basic IPv6 ACL number, in the range of 2000 to 2999. If you do not include this option in your command, the configuration will apply on all IPv6 multicast groups.

**order *order-value***: Specifies the order of the IPv6 ACL in the group-policy list, where *order-value* has an effective range of 1 to (the largest order value in the existing group-policy list + 1), but the value range should not include the original order value of the IPv6 ACL in the group-policy list. If you have assigned

an *order-value* to a certain IPv6 ACL, do not specify the same *order-value* for another IPv6 ACL; otherwise the system will give error information. If you do not specify an *order-value*, the order value of the IPv6 ACL will remain the same in the group-policy list.

## Description

Use the **spt-switch-threshold** command to configure the SPT switchover.

Use the **undo spt-switch-threshold** command to restore the default configuration.

By default, the device switches to the SPT immediately after it receives the first IPv6 multicast packet.

Note that:

- To adjust the order of an IPv6 ACL that already exists in the group-policy list, you can use the *acl6-number* argument to specify this IPv6 ACL and set its *order-value*. This will insert the IPv6 ACL to the position of *order-value* in the group-policy list. The order of the other existing IPv6 ACLs in the group-policy list will remain unchanged.
- To use an IPv6 ACL that does not exist in the group-policy list, you can use the *acl6-number* argument to specify an IPv6 ACL and set its *order-value*. This will insert the IPv6 ACL to the position of *order-value* in the group-policy list. If you do not include the *order-value* option in your command, the ACL will be appended to the end of the group-policy list.
- If you use this command multiple times on the same IPv6 multicast group, the first traffic rate configuration matched in sequence will take effect.
- Once an IPv6 multicast forwarding entry is created, subsequent IPv6 multicast data will not be encapsulated in register messages before being forwarded even if a register outgoing interface is available. Therefore, to avoid forwarding failure, do not include the **infinity** keyword in the **spt-switch-threshold** command on a switch that may become an RP (namely, a static RP or a C-RP).

## Examples

```
# Prohibit SPT switchover on a switch that will never become an RP.
```

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] spt-switch-threshold infinity
```

## ssm-policy (IPv6 PIM view)

### Syntax

```
ssm-policy acl6-number
```

```
undo ssm-policy
```

### View

```
IPv6 PIM view
```

### Default Level

```
2: System level
```

### Parameters

*acl6-number*: Basic IPv6 ACL number, in the range of 2000 to 2999.

## Description

Use the **ssm-policy** command to configure the IPv6 SSM group range.

Use the **undo ssm-policy** command to restore the system default.

By default, the IPv6 SSM group range is FF3x::/32. Here x refers to any legal scope.

This command allows you to define an address range of permitted or denied IPv6 multicast groups. If the match succeeds, the running multicast mode will be IPv6 PIM-SSM; otherwise the multicast mode will be IPv6 PIM-SM.

## Examples

```
# Configure the IPv6 SSM group range to be FF3E:0:8192::/96.
```

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source ff3e:0:8192:: 96
[Sysname-acl6-basic-2000] quit
[Sysname] pim ipv6
[Sysname-pim6] ssm-policy 2000
```

## state-refresh-hoplimit

### Syntax

```
state-refresh-hoplimit hoplimit-value
```

```
undo state-refresh-hoplimit
```

### View

IPv6 PIM view

### Default Level

2: System level

### Parameters

*hoplimit-value*: Hop limit value of state refresh messages, in the range of 1 to 255.

## Description

Use the **state-refresh-hoplimit** command to configure the hop limit value of state refresh messages.

Use the **undo state-refresh-hoplimit** command to restore the system default.

By default, the hop limit value of state refresh messages is 255.

Related commands: **pim** **ipv6** **state-refresh-capable**, **state-refresh-interval**, **state-refresh-rate-limit**.

## Examples

```
# Set the hop limit value of state refresh messages to 45.
```

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] state-refresh-hoplimit 45
```

## state-refresh-interval (IPv6 PIM view)

### Syntax

```
state-refresh-interval interval  
undo state-refresh-interval
```

### View

IPv6 PIM view

### Default Level

2: System level

### Parameters

*interval*: State refresh interval in seconds, with an effective range of 1 to 255.

### Description

Use the **state-refresh-interval** command to configure the interval between state refresh messages.

Use the **undo state-refresh-interval** command to restore the system default.

By default, the state refresh interval is 60 seconds.

Related commands: **pim** **ipv6** **state-refresh-capable**, **state-refresh-rate-limit**, **state-refresh-hoplimit**.

### Examples

```
# Set the state refresh interval to 70 seconds.  
<Sysname> system-view  
[Sysname] pim ipv6  
[Sysname-pim6] state-refresh-interval 70
```

## state-refresh-rate-limit (IPv6 PIM view)

### Syntax

```
state-refresh-rate-limit interval  
undo state-refresh-rate-limit
```

### View

IPv6 PIM view

### Default Level

2: System level

### Parameters

*interval*: Time to wait before receiving a new refresh message, in seconds and with an effective range of 1 to 65535.

## Description

Use the **state-refresh-rate-limit** command to configure the time the router must wait before receiving a new state refresh message.

Use the **undo state-refresh-rate-limit** command to restore the system default.

By default, the device waits 30 seconds before receiving a new state refresh message.

Related commands: **pim ipv6 state-refresh-capable**, **state-refresh-interval**, **state-refresh-hoplimit**.

## Examples

# Configure the device to wait 45 seconds before receiving a new state refresh message.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] state-refresh-rate-limit 45
```

## static-rp (IPv6 PIM view)

### Syntax

```
static-rp ipv6-rp-address [ acl6-number ] [ preferred ]
undo static-rp ipv6-rp-address
```

### View

IPv6 PIM view

### Default Level

2: System level

### Parameters

*ipv6-rp-address*: IPv6 address of the static RP to be configured. This address must be a valid, globally scoped IPv6 unicast address.

*acl6-number*: Basic IPv6 ACL number, in the range of 2000 to 2999. If you provide this argument, the configured static RP will serve only those IPv6 multicast groups that pass the filtering; otherwise, the configured static RP will serve the all IPv6 multicast groups.

**preferred**: Specifies to give priority to the static RP if the static RP conflicts with the dynamic RP. If you do not include the **preferred** keyword in your command, the dynamic RP will be given priority, and the static RP takes effect only if no dynamic RP exists in the network or when the dynamic RP fails.

## Description

Use the **static-rp** command to configure a static RP.

Use the **undo static-rp** command to configure a static RP.

By default, no static RP is configured.

Note that:

- IPv6 PIM-SM or IPv6 PIM-DM cannot be enabled on an interface that serves as a static RP.
- When the IPv6 ACL rule applied on a static RP changes, a new RP must be elected for all IPv6 multicast groups.

- You can configure multiple static RPs by carrying out this command repeatedly. However, if you carry out this command multiple times and specify the same static RP address or reference the same IPv6 ACL rule, the last configuration will override the previous one. If multiple static RPs have been configured for the same IPv6 multicast group, the one with the highest IPv6 address will be chosen to serve the group.
- You can configure up to 50 static RPs on the same device.

Related commands: **display pim ipv6 rp-info**.

## Examples

# Configure the interface with an IPv6 address of 2001::2 as a static RP.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] static-rp 2001::2
```

## timer hello (IPv6 PIM view)

### Syntax

```
timer hello interval
undo timer hello
```

### View

IPv6 PIM view

### Default Level

2: System level

### Parameters

*interval*: Hello interval in seconds, with an effective range of 1 to 2,147,483,647.

### Description

Use the **timer hello** command to configure the hello interval globally.

Use the **undo timer hello** command to restore the system default.

By default, hello messages are sent at the interval of 30 seconds.

Related commands: **pim ipv6 timer hello**.

## Examples

# Set the global hello interval to 40 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] timer hello 40
```

## timer join-prune (IPv6 PIM view)

### Syntax

```
timer join-prune interval
```

## undo timer join-prune

### View

IPv6 PIM view

### Default Level

2: System level

### Parameters

*interval*: Join/prune interval in seconds, with an effective range of 1 to 2,147,483,647.

### Description

Use the **timer join-prune** command to configure the join/prune interval globally.

Use the **undo timer join-prune** command to restore the system default.

By default, the join/prune interval is 60 seconds.

Related commands: **pim ipv6 timer join-prune**.

### Examples

# Set the global join/prune interval to 80 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] timer join-prune 80
```

# Table of Contents

<b>1 IPv6 MBGP Configuration Commands</b> .....	<b>1-1</b>
IPv6 MBGP Configuration Commands .....	1-1
aggregate (IPv6 MBGP address family view) .....	1-1
balance (IPv6 MBGP address family view) .....	1-2
bestroute as-path-neglect (IPv6 MBGP address family view) .....	1-3
bestroute compare-med (IPv6 MBGP address family view) .....	1-3
bestroute med-confederation (IPv6 MBGP address family view) .....	1-4
compare-different-as-med (IPv6 MBGP address family view) .....	1-5
dampening (IPv6 MBGP address family view) .....	1-6
default local-preference (IPv6 MBGP address family view) .....	1-7
default med (IPv6 MBGP address family view) .....	1-7
default-route imported (IPv6 MBGP address family view) .....	1-8
display ipv6 multicast routing-table .....	1-9
display ipv6 multicast routing-table <i>ipv6-address prefix-length</i> .....	1-11
display bgp ipv6 multicast group .....	1-12
display bgp ipv6 multicast network .....	1-13
display bgp ipv6 multicast paths .....	1-14
display bgp ipv6 multicast peer .....	1-15
display bgp ipv6 multicast routing-table .....	1-16
display bgp ipv6 multicast routing-table as-path-acl .....	1-18
display bgp ipv6 multicast routing-table community .....	1-19
display bgp ipv6 multicast routing-table community-list .....	1-20
display bgp ipv6 multicast routing-table dampened .....	1-20
display bgp ipv6 multicast routing-table dampening parameter .....	1-21
display bgp ipv6 multicast routing-table different-origin-as .....	1-22
display bgp ipv6 multicast routing-table flap-info .....	1-23
display bgp ipv6 multicast routing-table peer .....	1-24
display bgp ipv6 multicast routing-table regular-expression .....	1-25
display bgp ipv6 multicast routing-table statistic .....	1-26
filter-policy export (IPv6 MBGP address family view) .....	1-26
filter-policy import (IPv6 MBGP address family view) .....	1-27
import-route (IPv6 MBGP address family view) .....	1-28
ipv6-family multicast .....	1-28
network (IPv6 MBGP address family view) .....	1-29
peer advertise-community (IPv6 MBGP address family view) .....	1-30
peer advertise-ext-community (IPv6 MBGP address family view) .....	1-31
peer allow-as-loop (IPv6 MBGP address family view) .....	1-31
peer as-path-acl (IPv6 MBGP address family view) .....	1-32
peer default-route-advertise (IPv6 MBGP address family view) .....	1-33
peer enable (IPv6 MBGP address family view) .....	1-34
peer filter-policy (IPv6 MBGP address family view) .....	1-35
peer group (IPv6 MBGP address family view) .....	1-35
peer ipv6-prefix (IPv6 MBGP address family view) .....	1-36

peer keep-all-routes (IPv6 MBGP address family view).....	1-37
peer next-hop-local (IPv6 MBGP address family view).....	1-38
peer preferred-value (IPv6 MBGP address family view).....	1-39
peer public-as-only (IPv6 MBGP address family view).....	1-40
peer reflect-client (IPv6 MBGP address family view).....	1-40
peer route-limit (IPv6 MBGP address family view).....	1-41
peer route-policy (IPv6 MBGP address family view).....	1-42
preference (IPv6 MBGP address family view).....	1-43
reflect between-clients (IPv6 MBGP address family view).....	1-44
reflector cluster-id (IPv6 MBGP address family view).....	1-45
refresh bgp ipv6 multicast.....	1-45
reset bgp ipv6 multicast.....	1-46
reset bgp ipv6 multicast dampening.....	1-47
reset bgp ipv6 multicast flap-info.....	1-47

# 1 IPv6 MBGP Configuration Commands

---

## IPv6 MBGP Configuration Commands

### aggregate (IPv6 MBGP address family view)

#### Syntax

```
aggregate ipv6-address prefix-length [ as-set | attribute-policy route-policy-name |  
detail-suppressed | origin-policy route-policy-name | suppress-policy route-policy-name ] *  
undo aggregate ipv6-address prefix-length
```

#### View

IPv6 MBGP address family view

#### Default Level

2 System level

#### Parameters

*ipv6-address*: Summary address.

*prefix-length*: Length of summary route mask, in the range 0 to 128.

**as-set**: Creates a summary with AS set.

**attribute-policy** *route-policy-name*: Sets the attributes of the summary route according to the routing policy. The routing policy name is a string of 1 to 19 characters.

**detail-suppressed**: Only advertises the summary route.

**suppress-policy** *route-policy-name*: Suppresses specific routes defined in the routing policy. The routing policy name is a string of 1 to 19 characters.

**origin-policy** *route-policy-name*: References the routing policy to specify routes for summarization. The routing policy name is a string of 1 to 19 characters.

The keywords of the command are described as follows:

**Table 1-1** Functions of the keywords

Keywords	Function
<b>as-set</b>	Used to create a summary route, whose AS path contains the AS path information of summarized routes. Use this keyword carefully when many AS paths need to be summarized, because the frequent changes of these specific routes may lead to route oscillation.
<b>detail-suppressed</b>	This keyword does not suppress the summary route, but it suppresses the advertisement of all the more specific routes. To summarize only some specific routes, use the <b>peer filter-policy</b> command.

Keywords	Function
<b>suppress-policy</b>	Used to create a summary route and suppress the advertisement of some summarized routes. If you want to suppress some routes selectively and leave other routes still advertised, use the <b>if-match</b> clause of the <b>route-policy</b> command.
<b>origin-policy</b>	Selects only routes satisfying the routing policy for route summarization.
<b>attribute-policy</b>	Sets attributes except the AS-PATH attribute for the summary route. The same work can be done by using the <b>peer route-policy</b> command.

## Description

Use the **aggregate** command to create an IPv6 summary route in the IPv6 MBGP routing table.

Use the **undo aggregate** command to remove an IPv6 summary route.

By default, no summary route is configured.

## Examples

# In IPv6 MBGP address family view, create a summary of 12::/64 in the IPv6 MBGP routing table.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] aggregate 12:: 64
```

## balance (IPv6 MBGP address family view)

### Syntax

**balance** *number*

**undo balance**

### View

IPv6 MBGP address family view

### Default Level

2: System level

### Parameters

*number*: Number of IPv6 MBGP routes for load balancing. The number range varies is 1 to 4. when the number is 1, load balancing is disabled.

## Description

Use the **balance** command to configure the number of IPv6 MBGP routes used for load balancing.

Use the **undo balance** command to disable load balancing.

By default, load balancing is disabled.

Unlike IGP, IPv6 MBGP has no explicit metric for making load balancing decisions. Instead, it implements load balancing by using IPv6 MBGP route selection rules.

Related commands: **display ipv6 multicast routing-table**.

## Examples

# In IPv6 MBGP address family view, set the number of IPv6 MBGP routes for load balancing to 2.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] balance 2
```

## bestroute as-path-neglect (IPv6 MBGP address family view)

### Syntax

```
bestroute as-path-neglect
undo bestroute as-path-neglect
```

### View

IPv6 MBGP address family view

### Default Level

2: System level

### Parameters

None

### Description

Use the **bestroute as-path-neglect** command to configure IPv6 MBGP not to consider the AS\_PATH during best route selection.

Use the **undo bestroute as-path-neglect** command to configure IPv6 MBGP to consider the AS\_PATH during best route selection.

By default, IPv6 MBGP considers the AS\_PATH during best route selection.

## Examples

# In IPv6 MBGP address family view, configure IPv6 MBGP to ignore the AS\_PATH during best route selection.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv6-family multicast
[Sysname-bgp-af-ipv6-mul]bestroute as-path-neglect
```

## bestroute compare-med (IPv6 MBGP address family view)

### Syntax

```
bestroute compare-med
undo bestroute compare-med
```

### View

IPv6 MBGP address family view

## Default Level

2: System level

## Parameters

None

## Description

Use the **bestroute compare-med** command to enable the comparison of the MED for paths from each AS.

Use the **undo bestroute compare-med** command to disable this comparison.

By default, the comparison of the MED for paths from each AS is disabled.



### Caution

After the **bestroute compare-med** command is used, the **balance** command will not take effect.

---

## Examples

# In IPv6 MBGP address family view, enable the comparison of MED for paths from each AS during best route selection.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] bestroute compare-med
```

## bestroute med-confederation (IPv6 MBGP address family view)

### Syntax

**bestroute med-confederation**

**undo bestroute med-confederation**

### View

IPv6 MBGP address family view

## Default Level

2: System level

## Parameters

None

## Description

Use the **bestroute med-confederation** command to enable the comparison of the MED for paths from confederation peers during best route selection.

Use the **undo bestroute med-confederation** command to disable the comparison.

Such comparison is disabled by default.

With this command used, the system only compares MED values for paths from peers within the confederation. Paths from external ASs are advertised throughout the confederation without MED comparison.

## Examples

# In IPv6 MBGP address family view, enable the comparison of the MED for paths from peers within the confederation.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv6-family multicast
[Sysname-bgp-af-ipv6-mul]bestroute med-confederation
```

## compare-different-as-med (IPv6 MBGP address family view)

### Syntax

```
compare-different-as-med
undo compare-different-as-med
```

### View

IPv6 MBGP address family view

### Default Level

2: System level

### Parameters

None

### Description

Use the **compare-different-as-med** command to enable the comparison of the MED for paths from peers in different ASs.

Use the **undo compare-different-as-med** command to disable the comparison.

By default, MED comparison is not allowed among the routes from the peers in different ASs.

If there are several paths for one destination available, the path with the smallest MED is selected.

Do not use this command unless associated ASs adopt the same IGP and routing selection method.

## Examples

# In IPv6 MBGP address family view, enable the comparison of the MED for paths from peers in different ASs.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv6-family multicast
[Sysname-bgp-af-ipv6-mul]compare-different-as-med
```

## dampening (IPv6 MBGP address family view)

### Syntax

```
dampening [ half-life-reachable half-life-unreachable reuse suppress ceiling | route-policy  
route-policy-name ] *
```

```
undo dampening
```

### View

IPv6 MBGP address family view

### Default Level

2: System level

### Parameters

*half-life-reachable*: Specifies the half-life for reachable routes, in the range 1 to 45 minutes. By default, the value is 15 minutes.

*half-life-unreachable*: Specifies the half-life for unreachable routes, in the range 1 to 45 minutes. By default, the value is 15 minutes.

*reuse*: Specifies the reuse threshold value for suppressed routes, in the range 1 to 20000. A suppressed route having the penalty value decreased under the value is reused. By default, the value is 750.

*suppress*: Threshold for a route to be suppressed, in the range 1 to 20000. A route is suppressed if its penalty value exceeds this value. The value must be greater than the *reuse* value. By default, the value is 2000.

*ceiling*: Specifies a ceiling penalty value from 1001 to 20000. The value must be greater than the *suppress* value. The default is 16000.

*route-policy-name*: Route policy name, a string of 1 to 19 characters.

*half-life-reachable*, *half-life-unreachable*, *reuse*, *suppress*, and *ceiling* are mutually dependent. Once any one is configured, all the others should also be specified accordingly.

### Description

Use the **dampening** command to configure IPv6 MBGP route dampening.

Use the **undo dampening** command to disable route dampening.

By default, route dampening is not configured.

Related commands: **reset bgp ipv6 dampening**, **reset bgp ipv6 flap-info**, **display bgp ipv6 multicast routing-table dampened**, **display bgp ipv6 multicast routing-table dampening parameter**, **display bgp ipv6 multicast routing-table flap-info**.

### Examples

```
# In IPv6 MBGP address family view, configure route dampening.
```

```
<Sysname> system-view  
[Sysname]bgp 100  
[Sysname-bgp]ipv6-family multicast  
[Sysname-bgp-af-ipv6-mul]dampening 15 15 1000 2000 10000
```

## default local-preference (IPv6 MBGP address family view)

### Syntax

```
default local-preference value  
undo default local-preference
```

### View

IPv6 MBGP address family view

### Default Level

2: System level

### Parameters

*value*: Default local preference, in the range 0 to 4294967295. The larger the value is, the higher the preference is.

### Description

Use the **default local-preference** command to configure the default local preference.

Use the **undo default local-preference** command to restore the default.

By default, the default local preference is 100.

Using this command can affect IPv6 MBGP route selection.

### Examples

# In IPv6 MBGP address family view, set the default local preference to 180.

```
<Sysname> system-view  
[Sysname]bgp 100  
[Sysname-bgp]ipv6-family multicast  
[Sysname-bgp-af-ipv6-mul] default local-preference 180
```

## default med (IPv6 MBGP address family view)

### Syntax

```
default med med-value  
undo default med
```

### View

IPv6 MBGP address family view

### Default Level

2: System level

### Parameters

*med-value*: Default MED value, in the range 0 to 4294967295.

### Description

Use the **default med** command to specify the default MED value.

Use the **undo default med** command to restore the default.

By default, the default *med-value* is 0.

The multi-exit discriminator (MED) is an external metric of a route. Different from the local preference, the MED is exchanged between ASs and will stay in the AS once it enters the AS. The route with a lower MED is preferred. When a router running BGP obtains several routes with an identical destination but different next-hops from various external peers, it will select the best route depending on the MED value. In the case that all the other conditions are the same, the system selects the route with the lowest MED as the best external route.

## Examples

# Devices A and B belong to AS100 and device C belongs to AS200. C is the peer of A and B. Configure the MED of A as 25 to make C select the path from B.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] default med 25
```

## default-route imported (IPv6 MBGP address family view)

### Syntax

```
default-route imported
undo default-route imported
```

### View

IPv6 MBGP address family view

### Default Level

2: System level

### Parameters

None

### Description

Use the **default-route imported** command to enable default route redistribution into the IPv6 MBGP routing table.

Use the **undo default-route imported** command to disable the redistribution.

By default, default route redistribution is disabled.

## Examples

# Enable default and OSPFv3 route redistribution into IPv6 MBGP.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] default-route imported
[Sysname-bgp-af-ipv6-mul] import-route ospfv3 1
```

## display ipv6 multicast routing-table

### Syntax

```
display ipv6 multicast routing-table [ verbose ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**verbose:** Displays detailed routing table information, including both active and inactive routes. With this argument absent, the command displays brief information about active IPv6 MBGP routes only.

### Description

Use the **display ipv6 multicast routing-table** command to display the IPv6 MBGP routing table.

There are active and inactive routes in the IPv6 MBGP routing table. Active routes are the optimal routes used for RPF check.

### Examples

```
# Display brief IPv6 MBGP routing table information.
```

```
<Sysname> display ipv6 multicast routing-table
```

```
Routing Table :
```

```
Destinations : 1      Routes : 1
```

```
Destination : ::1      PrefixLength : 128
NextHop      : ::1      Preference : 0
Interface    : InLoopBack0  Protocol : Direct
State        : Active NoAdv  Cost : 0
Tunnel ID    : 0x0       Label : NULL
Age          : 156sec
```

**Table 1-2** display ipv6 multicast routing-table command output description

Field	Description
Destination	Destination IPv6 address
PrefixLength	Prefix length of the address
Nexthop	Next hop IP address
Preference	Route preference
Interface	Outbound interface
Protocol	Routing protocol
State	Status of the route, which could be Active, Inactive, Adv, or NoAdv
Cost	Route cost

Field	Description
Tunnel ID	Tunnel ID
Label	Label
Age	Time elapsed since the route was generated

# Display detailed IPv6 MBGP routing table information.

```
<Sysname> display ipv6 multicast routing-table verbose
```

Routing Table :

Destinations : 1            Routes : 1

```

Destination      : ::1                PrefixLength : 128
NextHop          : ::1                Preference   : 0
RelayNextHop     : ::                Tag          : 0H
Neighbour        : ::                ProcessID    : 0
Interface        : InLoopBack0       Protocol     : Direct
State            : Active NoAdv       Cost         : 0
Tunnel ID        : 0x0                Label        : NULL
Age              : 17073sec

```

**Table 1-3** display ipv6 multicast routing-table verbose command output description

Field	Description
Destination	Destination IPv6 address
PrefixLength	Prefix length of the address
Nexthop	Next hop IP address
Preference	Route preference
RelayNextHop	Recursive next hop
Tag	Route tag
Neighbour	Neighbor address
ProcessID	Process ID
Interface	Outbound interface
Protocol	Routing protocol
State	Status of the route, which could be Active, Inactive, Adv, or NoAdv
Cost	Route cost
Tunnel ID	Tunnel ID
Label	Label
Age	Time elapsed since the route was generated

## display ipv6 multicast routing-table *ipv6-address prefix-length*

### Syntax

```
display ipv6 multicast routing-table ipv6-address prefix-length [ longer-match ] [ verbose ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ipv6-address*: Destination IPv6 address.

*prefix-length*: Prefix length, in the range 0 to 128.

**longer-match**: Displays routes matching the specified prefix.

**verbose**: Displays both detailed active and inactive routing information permitted by the ACL. Without this keyword, only the brief information about active routes permitted by the ACL is displayed.

### Description

Use the **display ipv6 multicast routing-table *ipv6-address prefix-length*** command to display the multicast routing information for the specified destination IPv6 address.

### Examples

# Display brief information about the specified multicast route.

```
<Sysname> display ipv6 multicast routing-table 4::1 32
Routing Table:
Summary Count 1
  Destination : 4::                               PrefixLength : 32
  NextHop     : 3::1                               Preference   : 60
  Interface   : Vlan-interface1                   Protocol     : Static
  State       : Active Adv                         Cost         : 0
  Tunnel ID   : 0x0                                Label        : NULL
  Age         : 19174sec
```

# Display the brief route information falling into the specified network.

```
<Sysname> display ipv6 multicast routing-table 4:: 16 longer-match
Routing Tables:
Summary Count 2
  Destination : 4::                               PrefixLength : 32
  NextHop     : 3::1                               Preference   : 60
  Interface   : Vlan-interface1                   Protocol     : Static
  State       : Active Adv                         Cost         : 0
  Tunnel ID   : 0x0                                Label        : NULL
  Age         : 766sec

  Destination : 4:4::                               PrefixLength : 64
  NextHop     : 3::1                               Preference   : 60
```

```
Interface      : Vlan-interface1          Protocol      : Static
State          : Active Adv              Cost          : 0
Tunnel ID      : 0x0                    Label         : NULL
Age            : 766sec
```

# Display the detailed route information falling into the specified network.

```
<Sysname> display ipv6 multicast routing-table 4:4:: 32 verbose
Routing Tables:
Summary count:1
Destination    : 4:4::                  PrefixLength  : 64
NextHop        : 3::1                   Preference    : 60
Interface      : Vlan-interface1        Protocol      : Static
State          : Active Adv              Cost          : 0
Age            : 19547sec
```

## display bgp ipv6 multicast group

### Syntax

```
display bgp ipv6 multicast group [ ipv6-group-name ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ipv6-group-name*: Peer group name, a string of 1 to 47 characters.

### Description

Use the **display bgp ipv6 multicast group** command to display IPv6 MBGP peer group information.

If no *ipv6-group-name* is specified, information about all peer groups is displayed.

### Examples

# Display information about the IPv6 MBGP peer group **aaa**.

```
<Sysname> display bgp ipv6 group aaa

BGP peer-group is aaa
remote AS number not specified
Type : external
Maximum allowed prefix number: 4294967295
Threshold: 75%
Configured hold timer value: 180
Keepalive timer value: 60
Minimum time between advertisement runs is 30 seconds
Peer Preferred Value: 0
No routing policy is configured
Members:
```

```
Peer          V    AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down  State
20:20:::20:1 4    200      170      141      0        2 02:13:35 Established
```

**Table 1-4** display bgp ipv6 multicast group command output description

Field	Description
BGP peer-group	Name of the IPv6 MBGP peer group
remote AS	AS number of the IPv6 MBGP peer group
Type	Type of the IPv6 MBGP peer group:
Maximum allowed prefix number	Maximum number of prefixes allowed to receive from the IPv6 MBGP peer group
Threshold	Threshold value
Configured hold timer value	Hold timer value
Keepalive timer value	Keepalive interval
Minimum time between advertisement runs	Minimum interval for route advertisement
Peer Preferred Value	Preferred value of the routes from the peer
Members	Group members
Peer	IPv6 address of the peer
V	Peer BGP version
AS	AS number
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages to be sent
PrefRcv	Number of prefixes received
Up/Down	The lasting time of a session/the lasting time of present state (when no session is established)
State	Peer state machine

## display bgp ipv6 multicast network

### Syntax

```
display bgp ipv6 multicast network
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

## Description

Use the **display bgp ipv6 multicast network** command to display the IPv6 MBGP routes advertised with the **network** command.

## Examples

# Display IPv6 MBGP routes advertised with the **network** command.

```
<Sysname> display bgp ipv6 multicast network
  BGP Local Router ID is 1.1.1.2.
  Local AS Number is 200.
  Network          Mask          Route-policy      Short-cut
  2002::           64
  2001::           64                      Short-cut
```

**Table 1-5** display bgp ipv6 multicast network command output description

Field	Description
BGP Local Router ID	BGP local router ID
Local AS Number	Local AS number
Network	Network address
Mask	Prefix length of the address
Route-policy	Route policy configured
Short-cut	Shortcut route

## display bgp ipv6 multicast paths

### Syntax

```
display bgp ipv6 multicast paths [ as-regular-expression ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*as-regular-expression*: AS path regular expression.

### Description

Use the **display bgp ipv6 multicast paths** command to display AS path information.

If no parameter is specified, all AS path information will be displayed.

### Examples

# Display AS path information.

```
<Sysname> display bgp ipv6 multicast paths
```

Address	Hash	Refcount	MED	Path/Origin
0x5917098	1	1	0	i
0x59171D0	9	2	0	100i

**Table 1-6** display bgp ipv6 multicast paths command output description

Field	Description	
Address	Route address in the local database, in dotted hexadecimal notation	
Hash	Hash index	
Refcount	Count of routes that referenced the path	
MED	MED of the path	
Path	AS_PATH attribute of the route, recording the ASs it has passed, used to avoid routing loops	
Origin	Origin attribute of the route:	
	I	Indicates the route is interior to the AS. Summary routes and routes injected with the <b>network</b> command are considered IGP routes.
	E	Indicates that a route is learned from the exterior gateway protocol (EGP).
	?	It indicates that the origin of the route is unknown and the route is learned by some other means. BGP sets the Origin attribute of routes learned from other IGP protocols to incomplete.

## display bgp ipv6 multicast peer

### Syntax

```
display bgp ipv6 multicast peer [ [ ipv6-address ] verbose ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ipv6-group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

*ipv4-address*: IPv4 address of a peer to be displayed.

*ipv6-address*: IPv6 address of a peer to be displayed.

**log-info**: Displays the log information of the specified peer.

**verbose**: Displays the detailed information of the peer.

### Description

Use the **display bgp ipv6 multicast peer** command to display IPv6 MBGP peer/peer group information.

If no parameter is specified, information about all IPv6 MBGP peers and peer groups is displayed.

## Examples

# Display all IPv6 MBGP peer information.

```
<Sysname> display bgp ipv6 multicast peer
```

```
BGP Local router ID : 20.0.0.1
local AS number : 100
Total number of peers : 1                Peers in established state : 1

Peer      V    AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down    State
-----
20::21   4    200  17        19        0         3  00:09:59  Established
```

**Table 1-7** display bgp ipv6 multicast peer command output description

Field	Description
Peer	IPv6 address of the peer
V	Peer BGP version
AS	AS number
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages to be sent
PrefRcv	Number of prefixes received
Up/Down	The lasting time of the session/the lasting time of the present state (when no session is established)
State	Peer state machine

## display bgp ipv6 multicast routing-table

### Syntax

```
display bgp ipv6 multicast routing-table [ ipv6-address prefix-length ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ipv6-address*: Destination IPv6 address.

*prefix-length*: Prefix length of the IPv6 address, in the range 0 to 128.

## Description

Use the **display bgp ipv6 multicast routing-table** command to display IPv6 MBGP routing information.

## Examples

# Display IPv6 MBGP routing information.

```
<Sysname> display bgp ipv6 routing-table
```

```
Total Number of Routes: 2
```

```
BGP Local router ID is 30.30.30.1
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

```
Origin : i - IGP, e - EGP, ? - incomplete
```

```
*> Network : 30:30::                               PrefixLen : 64
     NextHop : 30:30::30:1                          LocPrf    :
     PrefVal : 0                                     Label     : NULL
     MED     : 0
     Path/Ogn: i
```

```
*> Network : 40:40::                               PrefixLen : 64
     NextHop : 40:40::40:1                          LocPrf    :
     PrefVal : 0                                     Label     : NULL
     MED     : 0
     Path/Ogn: i
```

**Table 1-8** display bgp ipv6 multicast routing-table command output description

Field	Description
Local router ID	Local router ID
Status codes	Status codes: * - valid: valid route > - best: best route d - damped: dampened route h - history: history route i - internal: internal route s - suppressed: suppressed route S - Stale: stale route
Origin	i - IGP (originated in the AS) e - EGP (learned through EGP) ? - incomplete (learned by some other means)
Network	Destination network address
PrefixLen	Prefix length of the address
NextHop	Next hop IP address
MED	MULTI_EXIT_DISC attribute value

Field	Description	
LocPrf	Local precedence	
Path	AS_PATH attribute of the path, recording the ASs it has passed to avoid routing loops	
PrefVal	Preferred value for a route	
Label	Label	
Ogn	Origin attribute of the route:	
	i	Indicates the route is interior to the AS. Summary routes and routes injected with the <b>network</b> command are considered IGP routes.
	e	Indicates that the route is learned from the Exterior Gateway Protocol (EGP).
	?	It indicates that the origin of the route is unknown and the route is learned by some other means. BGP sets the Origin attribute of routes learned from other IGP protocols to incomplete.

## display bgp ipv6 multicast routing-table as-path-acl

### Syntax

```
display bgp ipv6 multicast routing-table as-path-acl as-path-acl-number
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*as-path-acl-number*: Displays routing information matching an AS path ACL numbered 1 to 256

### Description

Use the **display bgp ipv6 multicast routing-table as-path-acl** command to display the IPv6 MBGP routes matching the specified AS path ACL.

### Examples

```
# Display the IPv6 MBGP routes matching AS path ACL 20.
```

```
<Sysname> display bgp ipv6 multicast routing-table as-path-acl 20
BGP Local router ID is 30.30.30.1
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

*> Network : 30:30::                               PrefixLen : 64
    NextHop : 30:30::30:1                             LocPrf    :
    PrefVal : 0                                       Label     : NULL
```

```
MED      : 0
Path/Ogn: i
```

Refer to [Table 1-8](#) for description on the fields above.

## display bgp ipv6 multicast routing-table community

### Syntax

```
display bgp ipv6 multicast routing-table community [ aa:nn<1-13> ] [ no-advertise | no-export |
no-export-subconfed ] * [ whole-match ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*aa:nn*: Community number; both *aa* and *nn* are in the range 0 to 65535.

*<1-13>*: Indicates that you can provide up to 13 community numbers.

**no-advertise**: Displays IPv6 MBGP routes that cannot be advertised to any peer.

**no-export**: Displays IPv6 MBGP routes that cannot be advertised out the AS. If a confederation is configured, it displays routes that cannot be advertised out the confederation, but can be advertised to other sub-ASs in the confederation.

**no-export-subconfed**: Displays IPv6 MBGP routes that cannot be advertised out the local AS, or to other sub-ASs in the confederation.

**whole-match**: Displays the IPv6 MBGP routes exactly matching the specified community attribute.

### Description

Use the **display bgp ipv6 multicast routing-table community** command to display the IPv6 MBGP routing information with the specified IPv6 MBGP community attribute.

### Examples

# Display IPv6 MBGP routing information with the community attribute **no-export**.

```
<Sysname> display bgp ipv6 multicast routing-table community no-export
BGP Local router ID is 30.30.30.1
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete

*> Network : 30:30::                               PrefixLen : 64
     NextHop : 30:30::30:1                           LocPrf    :
     PrefVal : 0                                       Label     : NULL
     MED     : 0
     Path/Ogn: i
```

Refer to [Table 1-8](#) for description on the fields above.

## display bgp ipv6 multicast routing-table community-list

### Syntax

```
display bgp ipv6 multicast routing-table community-list { basic-community-list-number
[ whole-match ] | adv-community-list-number }&<1-16>
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*basic-community-list-number*: Basic community-list number, in the range 1 to 99.

*adv-community-list-number*: Advanced community-list number, in the range 100 to 199.

**whole-match**: Displays the IPv6 MBGP routes exactly matching the community attributes defined in the specified *basic-community-list*.

&<1-16>: Indicates that you can enter the preceding argument up to 16 times.

### Description

Use the **display bgp ipv6 multicast routing-table community-list** command to display the IPv6 MBGP routing information matching the specified IPv6 MBGP community list.

### Examples

```
# Display the IPv6 MBGP routing information matching the community list
```

```
<Sysname> display bgp ipv6 multicast routing-table community-list 99
```

```
BGP Local router ID is 30.30.30.1
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

```
Origin : i - IGP, e - EGP, ? - incomplete
```

```
*> Network : 30:30::                               PrefixLen : 64
NextHop   : 30:30::30:1                             LocPrf    :
PrefVal   : 0                                         Label     : NULL
MED       : 0
Path/Ogn  : i
```

Refer to [Table 1-8](#) for description on the fields above.

## display bgp ipv6 multicast routing-table dampened

### Syntax

```
display bgp ipv6 multicast routing-table dampened
```

### View

Any view

## Default Level

1: Monitor level

## Parameters

None

## Description

Use the **display bgp ipv6 multicast routing-table dampened** command to display the dampened IPv6 MBGP routes.

## Examples

```
# Display dampened IPv6 MBGP routing information
```

```
<Sysname> display bgp ipv6 multicast routing-table dampened
```

```
BGP Local router ID is 1.1.1.1
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

```
Origin : i - IGP, e - EGP, ? - incomplete
```

```
*d Network : 111:: PrefixLen : 64
```

```
From : 122::1
```

```
Reuse : 00:29:34
```

```
Path/Ogn: 200?
```

**Table 1-9** display bgp ipv6 multicast routing-table dampened command output description

Field	Description
From	IP address from which the route was received
Reuse	Route reuse time, namely, period of time before the unusable route becomes usable.

Refer to [Table 1-8](#) for description on the other fields above.

## display bgp ipv6 multicast routing-table dampening parameter

### Syntax

```
display bgp ipv6 multicast routing-table dampening parameter
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display bgp ipv6 multicast routing-table dampening parameter** command to display IPv6

MBGP routing dampening parameters.

Related commands: **dampening**.

## Examples

# Display IPv6 MBGP dampening parameter information.

```
<Sysname> display bgp ipv6 multicast routing-table dampening parameter
Maximum Suppress Time(in second)      : 3069
Ceiling Value                          : 16000
Reuse Value                            : 750
Reach HalfLife Time(in second)       : 900
Unreach HalfLife Time(in second): 900
Suppress-Limit                        : 2000
```

**Table 1-10** display bgp ipv6 multicast routing-table dampening parameter command output description

Field	Description
Maximum Suppress Time	Maximum suppress time
Ceiling Value	Ceiling penalty value
Reuse Value	Limit for a route to be desuppressed
Reach HalfLife Time(in second)	Half-life of reachable routes
Unreach HalfLife Time(in second)	Half-life of unreachable routes
Suppress-Limit	Limit for routes to be suppressed

## display bgp ipv6 multicast routing-table different-origin-as

### Syntax

```
display bgp ipv6 multicast routing-table different-origin-as
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display bgp ipv6 multicast routing-table different-origin-as** command to display IPv6 MBGP routes originating from different autonomous systems.

## Examples

# Display IPv6 MBGP routing information from different ASs

```
<Sysname> display bgp ipv6 multicast routing-table different-origin-as
```

```

BGP Local router ID is 2.2.2.2
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

*> Network : 222::                                PrefixLen : 64
    NextHop : 122::2                               LocPrf   :
    PrefVal  : 0                                   Label    : NULL
    MED      : 0
    Path/Ogn: 100 ?

```

For details about the displayed information, see [Table 1-8](#).

## display bgp ipv6 multicast routing-table flap-info

### Syntax

```

display bgp ipv6 multicast routing-table flap-info [ regular-expression as-regular-expression |
as-path-acl as-path-acl-number | ipv6-address [ prefix-length [ longer-match ] ] ]

```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*as-regular-expression*: AS path regular expression to be matched.

*as-path-acl-number*: Number of the specified AS path ACL to be matched, ranging from 1 to 256.

*ipv6-address*: IPv6 address of a route to be displayed.

*prefix-length*: Prefix length of the IPv6 address, in the range 1 to 128.

**longer-match**: Matches the longest prefix.

### Description

Use the **display bgp ipv6 multicast routing-table flap-info** command to display IPv6 MBGP route flap statistics.

### Examples

```
# Display IPv6 MBGP routing flap statistics
```

```
<Sysname> display bgp ipv6 multicast routing-table flap-info
```

```

BGP Local router ID is 1.1.1.1
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

*d Network : 111::                                PrefixLen : 64
  From     : 122::1                               Flaps     : 3

```

Duration : 00:13:47

Reuse : 00:16:36

Path/Ogn : 200?

**Table 1-11** display bgp ipv6 multicast routing-table flap-info command output description

Field	Description
Flaps	Number of flaps
Duration	Duration of the flapping
Reuse	Reuse value

Refer to [Table 1-8](#) for description on the other fields above.

## display bgp ipv6 multicast routing-table peer

### Syntax

```
display bgp ipv6 multicast routing-table peer ipv6-address { advertised-routes | received-routes }  
[ network-address prefix-length | statistic ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*ipv6-address*: Specifies the IPv6 peer to be displayed.

**advertised-routes**: Routing information advertised to the specified peer.

**received-routes**: Routing information received from the specified peer.

*network-address prefix-length*: IPv6 address and prefix length. The prefix length ranges from 0 to 128.

**statistic**: Displays route statistics.

### Description

Use the **display bgp ipv6 multicast routing-table peer** command to display the routing information advertised to or received from the specified IPv6 MBGP peer.

### Examples

```
# Display the routing information advertised to the specified IPv6 MBGP peer.
```

```
<Sysname> display bgp ipv6 multicast routing-table peer 10:10::10:1 advertised-routes
```

```
Total Number of Routes: 2
```

```
BGP Local router ID is 20.20.20.1
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

```
Origin : i - IGP, e - EGP, ? - incomplete
```

```
*> Network : 20:20::
```

```
PrefixLen : 64
```

```

NextHop : 20:20::20:1
PrefVal : 0
MED : 0
Path/Ogn: i

LocPrf :
Label : NULL

*> Network : 40:40::
NextHop : 30:30::30:1
PrefVal : 0
MED : 0
Path/Ogn: 300 i

PrefixLen : 64
LocPrf :
Label : NULL

```

Refer to [Table 1-8](#) for description on the fields above.

## display bgp ipv6 multicast routing-table regular-expression

### Syntax

```
display bgp ipv6 multicast routing-table regular-expression as-regular-expression
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*as-regular-expression*: AS path regular expression.

### Description

Use the **display bgp ipv6 multicast routing-table regular-expression** command to display the IPv6 MBGP routes matching the specified AS regular expression.

### Examples

# Display IPv6 MBGP routing information matching the specified AS regular expression.

```
<Sysname> display bgp ipv6 multicast routing-table regular-expression ^100
```

```

BGP Local router ID is 20.20.20.1
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete

*> Network : 50:50::
NextHop : 10:10::10:1
PrefVal : 0
MED : 0
Path/Ogn: 100 i

PrefixLen : 64
LocPrf :
Label : NULL

```

Refer to [Table 1-8](#) for description on the fields above.

## display bgp ipv6 multicast routing-table statistic

### Syntax

```
display bgp ipv6 multicast routing-table statistic
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display bgp ipv6 multicast routing-table statistic** command to display IPv6 MBGP routing statistics.

### Examples

```
# Display IPv6 MBGP routing statistics
<Sysname> display bgp ipv6 multicast routing-table statistic

Total Number of Routes: 1
```

## filter-policy export (IPv6 MBGP address family view)

### Syntax

```
filter-policy { acl6-number | ipv6-prefix ipv6-prefix-name } export [ protocol process-id ]
undo filter-policy export [ protocol process-id ]
```

### View

IPv6 MBGP address family view

### Default Level

2: System level

### Parameters

*acl6-number*: Specifies the number of a basic or advanced ACL used to match against the destination of routing information. The number is in the range 2000 to 3999.

*ipv6-prefix-name*: Specifies the name of an IPv6 prefix list used to match against the destination of routing information. The name is a string of 1 to 19 characters.

*protocol*: Filters routes redistributed from the routing protocol. It can be **direct**, **isisv6**, **ospfv3**, **ripng**, or **static** at present. If no protocol is specified, all routes will be filtered when advertised.

*process-id*: Process ID of the routing protocol, ranging from 1 to 65535. This argument is available when the protocol is **isisv6**, **ospfv3**, or **ripng**.

## Description

Use the **filter-policy export** command to filter outgoing routes using a specified filter.

Use the **undo filter-policy export** command to cancel the filtering of outgoing routes.

By default, no outgoing routing information is filtered.

If a protocol is specified, only routes redistributed from the specified protocol are filtered. If no protocol is specified, all redistributed routes are filtered.

## Examples

```
# Reference IPv6 ACL 2001 to filter all outgoing IPv6 MBGP routes.
```

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv6-family multicast
[Sysname-bgp-af-ipv6-mul]filter-policy 2001 export
```

## filter-policy import (IPv6 MBGP address family view)

### Syntax

```
filter-policy { acl6-number | ipv6-prefix ipv6-prefix-name } import
undo filter-policy import
```

### View

IPv6 MBGP address family view

### Default Level

2: System level

### Parameters

*acl6-number*: Specifies the number of a basic or advanced IPv6 ACL used to match against the destination of routing information. The number is in the range 2000 to 3999.

*ipv6-prefix-name*: Specifies the name of an IPv6 prefix list used to match against the destination of routing information. The name is a string of 1 to 19 characters.

## Description

Use the **filter-policy import** command to configure the filtering of inbound routing information using a specified filter.

Use the **undo filter-policy import** command to cancel the filtering of inbound routing information.

By default, inbound IPv6 MBGP routes are not filtered.

## Examples

```
# Reference IPv6 ACL 2000 to filter all inbound IPv6 MBGP routes.
```

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] filter-policy 2000 import
```

## import-route (IPv6 MBGP address family view)

### Syntax

```
import-route protocol [ process-id ] [ med med-value | route-policy route-policy-name ] *  
undo import-route protocol [ process-id ]
```

### View

IPv6 MBGP address family view

### Default Level

2: System level

### Parameters

*protocol*: Redistributes routes from the protocol, which can be **direct**, **isisv6**, **ospfv3**, **ripng** or **static** at present.

*process-id*: Process ID. It ranges from 1 to 65535. This argument is available when the protocol is **isisv6**, **ospfv3**, or **ripng**.

*med-value*: Default MED value, in the range 0 to 4294967295. If no MED is specified, the cost of a redistributed route will be used as its MED in the BGP routing domain.

*route-policy-name*: Name of a route policy used to filter redistributed routes, a string of 1 to 19 characters.

### Description

Use the **import-route** command to redistribute routes from another routing protocol.

Use the **undo import-route** command to disable route redistribution from a routing protocol.

By default, IPv6 MBGP does not redistribute routes from any routing protocol.

The origin attribute of routes redistributed with the **import-route** command is incomplete.

### Examples

```
# Redistribute routes from RIPng 1.  
<Sysname> system-view  
[Sysname]bgp 100  
[Sysname-bgp]ipv6-family multicast  
[Sysname-bgp-af-ipv6-mul] import-route ripng 1
```

## ipv6-family multicast

### Syntax

```
ipv6-family multicast  
undo ipv6-family multicast
```

### View

BGP view

## Default Level

2: System level

## Parameters

None

## Description

Use the **ipv6-family** command to enter IPv6 MBGP address family view.

Use the **undo ipv6-family** command to remove all the configurations in the IPv6 MBGP address family view.

IPv4 BGP unicast view is the default.

## Examples

# Enter IPv6 MBGP address family view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul]
```

## network (IPv6 MBGP address family view)

### Syntax

**network** *ipv6-address prefix-length* [ **route-policy** *route-policy-name* | **short-cut** ]

**undo network** *ipv6-address prefix-length* [ **short-cut** ]

### View

IPv6 MBGP address family view

## Default Level

2: System level

## Parameters

*ipv6-address*: IPv6 address prefix.

*prefix-length*: Prefix length of the IPv6 address, in the range 0 to 128.

**short-cut**: If the keyword is specified for an IPv6 multicast eBGP route, the route will use the local preference rather than its own preference, and therefore it will hardly become the optimal route.

*route-policy-name*: Name of a route policy, a string of 1 to 19 characters.

## Description

Use the **network** command to inject a network to the IPv6 MBGP routing table.

Use the **undo network** command to remove a network from the routing table.

By default, no network is injected.

Note the following:

- The network to be injected must exist in the local IPv6 routing table. You can use a route policy to control the advertisement of the route with more flexibility.
- The route injected with the **network** command has the IGP origin attribute.

## Examples

```
# inject the network 2002::/16.
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp]ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] network 2002:: 16
```

## peer advertise-community (IPv6 MBGP address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } advertise-community
undo peer { ipv6-group-name | ipv6-address } advertise-community
```

### View

IPv6 MBGP address family view

### Default Level

2: System level

### Parameters

*group-name*: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of an IPv6 MBGP peer.

### Description

Use the **peer advertise-community** command to advertise the community attribute to an IPv6 MBGP peer/peer group.

Use the **undo peer advertise-community** command to remove the configuration.

By default, no community attribute is advertised to any IPv6 MBGP peer group/peer.

## Examples

```
# Advertise the community attribute to the IPv6 MBGP peer 1:2::3:4.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 advertise-community
```

## peer advertise-ext-community (IPv6 MBGP address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } advertise-ext-community
undo peer { ipv6-group-name | ipv6-address } advertise-ext-community
```

### View

IPv6 MBGP address family view

### Default Level

2: System level

### Parameters

*group-name*: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of an IPv6 MBGP peer.

### Description

Use the **peer advertise-ext-community** command to advertise the extended community attribute to an IPv6 MBGP peer/peer group.

Use the **undo peer advertise-ext-community** command to remove the configuration.

By default, no extended community attribute is advertised to any IPv6 MBGP peer/peer group.

### Examples

```
# Advertise the extended community attribute to the IPv6 MBGP peer 1:2::3:4.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 advertise-ext-community
```

## peer allow-as-loop (IPv6 MBGP address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } allow-as-loop [ number ]
undo peer { ipv6-group-name | ipv6-address } allow-as-loop
```

### View

IPv6 MBGP address family view

### Default Level

2: System level

## Parameters

*ipv6-group-name*: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of an IPv6 MBGP peer.

*number*: Specifies the number of times for which the local AS number can appear in the AS PATH of routes from the peer/peer group, in the range 1 to 10. The default number is 1.

## Description

Use the **peer allow-as-loop** command to allow the local AS number to exist in the AS\_PATH attribute of routes from a peer/peer group, and to configure the times for which the local AS number can appear.

Use the **undo peer allow-as-loop** command to disable the function.

The local AS number cannot appear in routes from the peer/peer group.

## Examples

# Configure the number of times for which the local AS number can appear in the AS PATH of routes from the peer as 2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 allow-as-loop 2
```

## peer as-path-acl (IPv6 MBGP address family view)

### Syntax

```
peer { ipv6-address | ipv6-group-name } as-path-acl as-path-acl-number { export | import }
undo peer { ipv6-address | ipv6-group-name } as-path-acl as-path-acl-number { export | import }
```

### View

IPv6 MBGP address family view

### Default Level

2: System level

## Parameters

*ipv6-group-name*: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of an IPv6 MBGP peer.

*as-path-acl-number*: AS path ACL number, in the range 1 to 256.

**import**: Filters incoming IPv6 MBGP routes.

**export**: Filters outgoing IPv6 MBGP routes.

## Description

Use the **peer as-path-acl** command to specify an AS path ACL to filter routes incoming from or outgoing to an IPv6 MBGP peer/peer group.

Use the **undo peer as-path-acl** command to remove the configuration.

By default, no AS path ACL is specified for filtering the routes from/to an IPv6 MBGP peer/peer group.

## Examples

# Specify AS path ACL 3 to filter routes outgoing to the IPv6 MBGP peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 as-path-acl 3 export
```

## peer default-route-advertise (IPv6 MBGP address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } default-route-advertise [ route-policy route-policy-name ]
undo peer { ipv6-group-name | ipv6-address } default-route-advertise
```

### View

IPv6 MBGP address family view

### Default Level

2: System level

### Parameters

*ipv6-group-name*: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of an IPv6 MBGP peer.

*route-policy-name*: Route policy name, a string of 1 to 19 characters.

## Description

Use the **peer default-route-advertise** command to advertise a default route to an IPv6 MBGP peer/peer group.

Use the **undo peer default-route-advertise** command to disable default route advertisement to an IPv6 MBGP peer/peer group.

By default, no default route is advertised to any IPv6 MBGP peer/peer group.

With this command used, the router unconditionally sends a default route with the next hop being itself to the IPv6 MBGP peer/peer group regardless of whether the default route is available in the routing table.

## Examples

```
# Advertise a default route to the IPv6 MBGP peer 1:2::3:4.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 default-route-advertise
```

## peer enable (IPv6 MBGP address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } enable
undo peer { ipv6-group-name | ipv6-address } enable
```

### View

IPv6 MBGP address family view

### Default Level

2: System level

### Parameters

*ipv6-group-name*: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters. The IPv6 MBGP peer group must be created in IPv6 MBGP view before being activated here.

*ipv6-address*: IPv6 address of an IPv6 MBGP peer.

### Description

Use the **peer enable** command to enable an IPv6 MBGP peer or peer group.

Use the **undo peer enable** command to disable an IPv6 MBGP peer or peer group.

By default, no IPv6 MBGP peer or peer group is enabled.

If an IPv6 MBGP peer or peer group is disabled, the router will not exchange routing information with it.

## Examples

```
# Enable IPv6 MBGP peer 1:2::3:4.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
```

## peer filter-policy (IPv6 MBGP address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } filter-policy acl6-number { import | export }  
undo peer { ipv6-group-name | ipv6-address } filter-policy [ acl6-number ] { import | export }
```

### View

IPv6 MBGP address family view

### Default Level

2: System level

### Parameters

*ipv6-group-name*: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of an IPv6 MBGP peer.

*acl6-number*: IPv6 ACL number, in the range 2000 to 3999.

**import**: Applies the filter to routes received from the IPv6 MBGP peer/peer group.

**export**: Applies the filter to routes advertised to the IPv6 MBGP peer/peer group.

### Description

Use the **peer filter-policy** command to configure an IPv6 ACL-based filter policy for an IPv6 MBGP peer or peer group.

Use the **undo peer filter-policy** command to remove the configuration.

By default, no IPv6 ACL-based filter policy is configured for any IPv6 MBGP peer or peer group.

### Examples

# Apply IPv6 ACL 2000 to filter routes advertised to the IPv6 MBGP peer 1:2::3:4.

```
<Sysname> system-view  
[Sysname] acl ipv6 number 2000  
[Sysname-acl6-basic-2000] rule permit source 2001:1:: 64  
[Sysname-acl6-basic-2000] quit  
[Sysname] bgp 100  
[Sysname-bgp] ipv6-family  
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100  
[Sysname-bgp-af-ipv6] quit  
[Sysname-bgp] ipv6-family multicast  
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable  
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 filter-policy 2000 export
```

## peer group (IPv6 MBGP address family view)

### Syntax

```
peer ipv6-address group ipv6-group-name  
undo peer ipv6-address group ipv6-group-name
```

## View

IPv6 MBGP address family view

## Default Level

2: System level

## Parameters

*ipv6-group-name*: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of an IPv6 MBGP peer.

## Description

Use the **peer group** command to add an IPv6 MBGP peer to a configured IPv6 MBGP peer group.

Use the **undo peer group** command to delete a specified IPv6 MBGP peer from an IPv6 MBGP peer group.

By default, no IPv6 MBGP peer is added into any IPv6 MBGP peer group.

## Examples

# Create an IPv6 MBGP peer group named **test** and add the IPv6 MBGP peer 1:2::3:4 to the peer group.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 200
[Sysname-bgp-af-ipv6] peer 1:2::3:4 group test
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer test enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 group test
```

## peer ipv6-prefix (IPv6 MBGP address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } ipv6-prefix ipv6-prefix-name { import | export }
undo peer { ipv6-group-name | ipv6-address } ipv6-prefix { import | export }
```

## View

IPv6 MBGP address family view

## Default Level

2: System level

## Parameters

*ipv6-group-name*: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of an IPv6 MBGP peer.

*ipv6-prefix-name*: IPv6 prefix list name, a string of 1 to 19 characters.

**import**: Applies the IPv6 prefix list to filter routes received from the IPv6 MBGP peer/peer group.

**export**: Applies the IPv6 prefix list to filter routes advertised to the specified IPv6 MBGP peer/peer group.

## Description

Use the **peer ipv6-prefix** command to specify an IPv6 prefix list to filter routes incoming from or outgoing to an IPv6 MBGP peer or peer group.

Use the **undo peer ipv6-prefix** command to remove the configuration.

By default, no IPv6 prefix list based filtering is configured.

## Examples

# Apply the IPv6 ACL **list1** to filter routes advertised to the IPv6 MBGP peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] ip ipv6-prefix list1 permit 2002:: 64
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 ipv6-prefix list1 export
```

## peer keep-all-routes (IPv6 MBGP address family view)

### Syntax

**peer** { *ipv6-group-name* | *ipv6-address* } **keep-all-routes**

**undo peer** { *ipv6-group-name* | *ipv6-address* } **keep-all-routes**

### View

IPv6 MBGP address family view

### Default Level

2: System level

### Parameters

*ipv6-group-name*: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of a IPv6 MBGP peer.

## Description

Use the **peer keep-all-routes** command to save the original routing information from an IPv6 MBGP peer or peer group, including routes that fail to pass the inbound filtering policy (if configured).

Use the **undo peer keep-all-routes** command to disable this function.

By default, the original routing information from an IPv6 MBGP peer or peer group is not saved.

## Examples

```
# Save the original routing information from IPv6 MBGP peer 1:2::3:4.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 keep-all-routes
```

## peer next-hop-local (IPv6 MBGP address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } next-hop-local
undo peer { ipv6-group-name | ipv6-address } next-hop-local
```

### View

IPv6 MBGP address family view

### Default Level

2: System level

### Parameters

*ipv6-group-name*: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of an IPv6 MBGP peer.

### Description

Use the **peer next-hop-local** command to configure the next hop of routes advertised to an IPv6 MBGP peer/peer group as the local router.

Use the **undo peer next-hop-local** command to restore the default.

By default, an IPv6 MBGP speaker specifies itself as the next hop for routes outgoing to an IPv6 multicast eBGP peer/peer group rather than an IPv6 multicast iBGP peer/peer group.

## Examples

```
# Set the next hop of routes advertised to iBGP peer group test to the advertising router.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test internal
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer test enable
[Sysname-bgp-af-ipv6-mul] peer test next-hop-local
```

## peer preferred-value (IPv6 MBGP address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } preferred-value value
undo peer { ipv6-group-name | ipv6-address } preferred-value
```

### View

IPv6 MBGP address family view

### Default Level

2: System level

### Parameters

*ipv6-group-name*: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of an IPv6 MBGP peer.

*value*: Preferred value, in the range 0 to 65535.

### Description

Use the **peer preferred-value** command to assign a preferred value to routes received from an IPv6 MBGP peer or peer group.

Use the **undo peer preferred-value** command to restore the default.

The preferred value defaults to 0.

Routes learned from peers each have a preferred value. Among multiple routes to the same destination, the route with the greatest preferred value is selected.

Note the following:

If you both reference a route policy and use the **peer { ipv6-group-name | ipv6-address } preferred-value value** command to set a preferred value for routes from a peer, the route policy sets a specified non-zero preferred value for routes matching it. Other routes not matching the route policy uses the value set with the **peer preferred-value** command. If the preferred value specified in the route policy is zero, the routes matching it will also use the value set with the command. For information about using a route policy to set a preferred value, refer to the command **peer { group-name | ipv6-address } route-policy route-policy-name { import | export }** in this document, and the command **apply preferred-value preferred-value** in *Route Policy Commands of the IP Routing Volume*.

### Examples

```
# Configure a preferred value of 50 for routes from IPv6 MBGP peer 1:2::3:4.
```

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 preferred-value 50
```

## peer public-as-only (IPv6 MBGP address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } public-as-only  
undo peer { ipv6-group-name | ipv6-address } public-as-only
```

### View

IPv6 MBGP address family view

### Default Level

2: System level

### Parameters

*ipv6-group-name*: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of an IPv6 MBGP peer.

### Description

Use the **peer public-as-only** command to disable IPv6 MBGP updates to a peer/peer group from carrying private AS numbers.

Use the **undo peer public-as-only** command to allow IPv6 MBGP updates to a peer/peer group to carry private AS numbers.

By default, private AS numbers can be carried in outbound IPv6 MBGP update packets.

The command does not take effect for IPv6 MBGP updates with both public and private AS numbers. The range of private AS numbers is from 64512 to 65535.

### Examples

```
# Disable updates sent to IPv6 MBGP peer 1:2::3:4 from carrying private AS numbers.
```

```
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp] ipv6-family  
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100  
[Sysname-bgp-af-ipv6] quit  
[Sysname-bgp] ipv6-family multicast  
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable  
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 public-as-only
```

## peer reflect-client (IPv6 MBGP address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } reflect-client  
undo peer { ipv6-group-name | ipv6-address } reflect-client
```

### View

IPv6 MBGP address family view

## Default Level

2: System level

## Parameters

*ipv6-group-name*: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of an IPv6 MBGP peer.

## Description

Use the **peer reflect-client** command to configure the router as a route reflector and specify an IPv6 MBGP peer/peer group as its client.

Use the **undo peer reflect-client** command to remove the configuration.

By default, neither route reflector nor client is configured.

Related commands: **reflect between-clients**, **reflector cluster-id**.

## Examples

# Configure the local device as a route reflector and specify the peer group **test** as a client.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test internal
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer test enable
[Sysname-bgp-af-ipv6-mul] peer test reflect-client
```

## peer route-limit (IPv6 MBGP address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } route-limit limit [ percentage ]
undo peer { ipv6-group-name | ipv6-address } route-limit
```

### View

IPv6 MBGP address family view

## Default Level

2: System level

## Parameters

*ipv6-group-name*: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of an IPv6 MBGP peer.

*limit*: Specifies the upper limit of IPv6 address prefixes that can be received from the peer or peer group. The value is in the range 1 to 6144.

*percentage*: If the number of received routes divided by the upper limit reaches the specified percentage, the system will generate alarm information. The percentage is in the range 1 to 100. The default is 75.

## Description

Use the **peer route-limit** command to set the maximum number of IPv6 prefixes that can be received from an IPv6 MBGP peer/peer group.

Use the **undo peer route-limit** command to restore the default.

By default, the IPv6 prefixes from an IPv6 MBGP peer/peer group are unlimited.

The router will tear down the TCP connection when the number of IPv6 prefixes received from the peer exceeds the limit.

## Examples

# Set the number of IPv6 address prefixes allowed to receive from the IPv6 MBGP peer 1:2::3:4 to 1000.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 enable
[Sysname-bgp-af-ipv6-mul] peer 1:2::3:4 route-limit 1000
```

## peer route-policy (IPv6 MBGP address family view)

### Syntax

```
peer { ipv6-group-name | ipv6-address } route-policy route-policy-name { import | export }
undo peer { ipv6-group-name | ipv6-address } route-policy route-policy-name { import | export }
```

### View

IPv6 MBGP address family view

### Default Level

2: System level

### Parameters

*ipv6-group-name*: Name of an IPv6 MBGP peer group, a string of 1 to 47 characters.

*ipv6-address*: IPv6 address of an IPv6 MBGP peer.

*route-policy-name*: Route policy name, a string of 1 to 19 characters.

**import**: Applies the route-policy to routes received from the IPv6 MBGP peer/peer group.

**export**: Applies the route-policy to routes advertised to the IPv6 MBGP peer/peer group.

## Description

Use the **peer route-policy** command to apply a route policy to routes incoming from or outgoing to an IPv6 MBGP peer or peer group.

Use the **undo peer route-policy** command to remove the configuration.

By default, no route policy is applied to the routes incoming from or outgoing to an IPv6 MBGP peer or peer group.

The **if-match interface** clause in the route policy referenced by the **peer route-policy** command will not be applied.

Refer to *Route Policy Commands* in the *IP Routing Volume* for related information.

## Examples

# Apply the route policy **test-policy** to routes received from the IPv6 MBGP peer group **test**.

```
<Sysname> system-view
[Sysname] route-policy test-policy permit node 10
[Sysname-route-policy] if-match cost 10
[Sysname-route-policy] apply cost 65535
[Sysname-route-policy] quit
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] quit
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] peer test enable
[Sysname-bgp-af-ipv6-mul] peer test route-policy test-policy import
```

## preference (IPv6 MBGP address family view)

### Syntax

```
preference { external-preference internal-preference local-preference | route-policy
route-policy-name }
```

```
undo preference
```

### View

IPv6 MBGP address family view

### Default Level

2: System level

### Parameters

*external-preference*: Preference of IPv6 multicast eBGP routes, in the range 1 to 255. An IPv6 multicast eBGP route is learned from an IPv6 multicast eBGP peer.

*internal-preference*: Preference of IPv6 multicast iBGP routes, in the range 1 to 255. An IPv6 multicast iBGP route is learned from an IPv6 multicast iBGP peer.

*local-preference*: Preference of locally generated IPv6 MBGP routes, in the range 1 to 255.

*route-policy-name*: Route policy name, a string of 1 to 19 characters. Using a route policy, you can configure the preferences for the routes that match the filtering conditions. As for the unmatched routes, the default preferences are adopted.

## Description

Use the **preference** command to configure preferences for IPv6 multicast eBGP, IPv6 multicast iBGP, and local IPv6 MBGP routes.

Use the **undo preference** command to restore the default.

The default preference values of external, internal and local IPv6 MBGP routes are 255, 255, and 130, respectively.

The greater the preference value is, the lower the preference is.

## Examples

# Configure preferences for IPv6 multicast eBGP, IPv6 multicast iBGP, and local IPv6 MBGP routes as 20, 20, and 200.

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] ipv6-family multicast
[Sysname-bgp-af-ipv6-mul] preference 20 20 200
```

## reflect between-clients (IPv6 MBGP address family view)

### Syntax

**reflect between-clients**

**undo reflect between-clients**

### View

IPv6 MBGP address family view

### Default Level

2: System level

### Parameters

None

## Description

Use the **reflect between-clients** command to enable route reflection between clients.

Use the **undo reflect between-clients** command to disable this function.

By default, route reflection between clients is enabled.

After a route reflector is configured, it reflects the routes of a client to the other clients. If the clients of a route reflector are fully meshed, you need to disable route reflection between clients to reduce routing costs.

Related commands: **reflector cluster-id** and **peer reflect-client**.

## Examples

# Enable route reflection between clients

```
<Sysname> system-view
[Sysname]bgp 100
[Sysname-bgp] ipv6-family multicast
```

```
[Sysname-bgp-af-ipv6-mul] reflect between-clients
```

## reflector cluster-id (IPv6 MBGP address family view)

### Syntax

```
reflector cluster-id cluster-id  
undo reflector cluster-id
```

### View

IPv6 MBGP address family view

### Default Level

2: System level

### Parameters

*cluster-id*: Cluster ID of the route reflector, an integer from 1 to 4294967295 (the system translates it into an IPv4 address) or an IPv4 address.

### Description

Use the **reflector cluster-id** command to configure the cluster ID of the route reflector.

Use the **undo reflector cluster-id** command to remove the configured cluster ID.

By default, each route reflector uses its router ID as the cluster ID.

The router ID of the route reflector is the ID of the cluster. You can configure multiple route reflectors to improve network stability. If a cluster has multiple route reflectors, you need to use the **reflector cluster-id** command to specify the same cluster ID for these route reflectors to avoid routing loops.

Related commands: **reflect between-clients**, **peer reflect-client**.

### Examples

# Set 50 as the cluster ID for the route reflector, which is one of multiple route reflectors in the cluster.

```
<Sysname> system-view  
[Sysname]bgp 100  
[Sysname-bgp] ipv6-family multicast  
[Sysname-bgp-af-ipv6-mul] reflector cluster-id 50
```

## refresh bgp ipv6 multicast

### Syntax

```
refresh bgp ipv6 multicast { ipv6-address | all | external | group ipv6-group-name | internal }  
{ export | import }
```

### View

User view

### Default Level

1: Monitor level

## Parameters

*ipv6-address*: Soft-resets the connection to the specified IPv6 MBGP peer.

**all**: Soft-resets all IPv6 MBGP connections.

**external**: Soft-resets IPv6 multicast eBGP connections.

**group** *ipv6-group-name*: Soft-resets connections to an IPv6 multicast peer group. The name of the peer group is a string of 1 to 47 characters.

**internal**: Soft-resets IPv6 multicast iBGP connections.

**export**: Performs soft-reset in outbound direction.

**import**: Performs soft-reset in inbound direction.

## Description

Use the **refresh bgp ipv6 multicast** command to soft-reset specified IPv6 MBGP connections. With this feature, you can refresh the IPv6 MBGP routing table and apply a new policy without tearing down IPv6 MBGP connections.

To perform IPv6 MBGP soft-reset, all routers in the network should support route-refresh. If a peer not supporting route refresh exists in the network, you need to use the **peer keep-all-routes** command on the local router to save all route updates from the peer before performing soft reset.

## Examples

```
# Soft-reset inbound IPv6 MBGP connections.
```

```
<Sysname> refresh bgp ipv6 multicast all import
```

## reset bgp ipv6 multicast

### Syntax

```
reset bgp ipv6 multicast { as-number | ipv6-address | all | group ipv6-group-name | external | internal }
```

### View

User view

### Default Level

2: System level

## Parameters

*as-number*: Resets the connections to IPv6 MBGP peers in the specified AS.

*ipv6-address*: Resets the connection to the specified peer.

**flap-info**: Clears routing flap information.

**all**: Resets all IPv6 MBGP connections.

**group** *ipv6-group-name*: Resets the connections to the specified IPv6 MBGP peer group.

**external**: Resets all the IPv6 multicast eBGP connections.

**internal**: Resets all the IPv6 multicast iBGP connections.

## Description

Use the **reset bgp ipv6 multicast** command to reset specified IPv6 MBGP connections to reconnect to the peers.

## Examples

```
# Reset all the IPv6 MBGP connections.  
<Sysname> reset bgp ipv6 multicast all
```

## reset bgp ipv6 multicast dampening

### Syntax

```
reset bgp ipv6 multicast dampening [ ipv6-address prefix-length ]
```

### View

User view

### Default Level

1: Monitor level

### Parameters

*ipv6-address*: Destination IPv6 address..

*prefix-length*: Prefix length of the IPv6 address, in the range 0 to 128.

## Description

Use the **reset bgp ipv6 multicast dampening** command to clear route dampening information and release suppressed routes.

If no *ipv6-address prefix-length* is specified, all IPv6 MBGP route dampening information will be cleared.

## Examples

```
# Clear the damping information of the route 2345::/64 and release the suppressed route.  
<Sysname> reset bgp ipv6 multicast dampening 2345::64
```

## reset bgp ipv6 multicast flap-info

### Syntax

```
reset bgp ipv6 multicast flap-info [ ipv6-address/prefix-length | regexp as-path-regexp | as-path-acl as-path-acl-number ]
```

### View

User view

### Default Level

1: Monitor level

## Parameters

*ipv6-address*: Clears the routing flap statistics for the specified IPv6 address.

*prefix-length*: Prefix length of the IPv6 address, in the range 1 to 128.

*as-path-regexp*: Clears the routing flap statistics for routes matching the AS path regular expression.

*as-path-acl-number*: Clears the routing flap statistics for routes matching the AS path ACL. The value of this argument is in the range of 1 to 256.

## Description

Use the **reset bgp ipv6 multicast flap-info** command to clear IPv6 MBGP routing flap statistics.

If no parameters are specified, the flap statistics of all the routes will be cleared

## Examples

# Clear the flap statistics of all routes matching AS path ACL 10.

```
<Sysname> reset bgp ipv6 multicast flap-info as-path-acl 10
```

# Table of Contents

<b>1 MLD Snooping Configuration Commands</b> .....	<b>1-1</b>
MLD Snooping Configuration Commands .....	1-1
display mld-snooping group .....	1-1
display mld-snooping statistics .....	1-2
fast-leave (MLD-Snooping view) .....	1-3
group-policy (MLD-Snooping view) .....	1-4
host-aging-time (MLD-Snooping view) .....	1-5
last-listener-query-interval (MLD-Snooping view) .....	1-6
max-response-time (MLD-Snooping view) .....	1-6
mld-snooping .....	1-7
mld-snooping drop-unknown .....	1-8
mld-snooping enable .....	1-8
mld-snooping fast-leave .....	1-9
mld-snooping general-query source-ip .....	1-10
mld-snooping group-limit .....	1-11
mld-snooping group-policy .....	1-12
mld-snooping host-aging-time .....	1-13
mld-snooping host-join .....	1-13
mld-snooping last-listener-query-interval .....	1-15
mld-snooping max-response-time .....	1-15
mld-snooping overflow-replace .....	1-16
mld-snooping querier .....	1-17
mld-snooping query-interval .....	1-17
mld-snooping router-aging-time .....	1-18
mld-snooping source-deny .....	1-19
mld-snooping special-query source-ip .....	1-19
mld-snooping static-group .....	1-20
mld-snooping static-router-port .....	1-21
mld-snooping version .....	1-22
overflow-replace (MLD-Snooping view) .....	1-23
report-aggregation (MLD-Snooping view) .....	1-24
reset mld-snooping group .....	1-24
reset mld-snooping statistics .....	1-25
router-aging-time (MLD-Snooping view) .....	1-25
source-deny (MLD-Snooping view) .....	1-26

# 1 MLD Snooping Configuration Commands

---

## MLD Snooping Configuration Commands

### display mld-snooping group

#### Syntax

```
display mld-snooping group [ vlan vlan-id ] [ slot slot-number ] [ verbose ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

**vlan** *vlan-id*: Displays the MLD Snooping multicast group information in the specified VLAN, where *vlan-id* is in the range of 1 to 4094. If you do not specify a VLAN, this command will display the MLD Snooping multicast group information in all VLANs.

**slot** *slot-number*: Displays the MLD Snooping multicast group information for the specified card.

**verbose**: Displays the detailed MLD Snooping multicast group information.

#### Description

Use the **display mld-snooping group** command to view the MLD Snooping multicast group information.

#### Examples

```
# View the detailed MLD Snooping multicast group information in VLAN 2.
```

```
<Sysname> display mld-snooping group vlan 2 verbose
```

```
Total 1 IP Group(s).
```

```
Total 1 IP Source(s).
```

```
Total 1 MAC Group(s).
```

```
Port flags: D-Dynamic port, S-Static port, C-Copy port
```

```
Subvlan flags: R-Real VLAN, C-Copy VLAN
```

```
Vlan(id):2.
```

```
Total 1 IP Group(s).
```

```
Total 1 IP Source(s).
```

```
Total 1 MAC Group(s).
```

```
Router port(s):total 1 port.
```

```
GE1/0/1 (D) ( 00:01:30 )
```

```
IP group(s):the following ip group(s) match to one mac group.
```

```

IP group address:FF1E::101
 (::, FF1E::101):
  Attribute:      Host Port
  Host port(s):total 1 port.
    GE1/0/2              (D) ( 00:03:23 )
MAC group(s):
  MAC group address:3333-0000-0101
  Host port(s):total 1 port.
    GE1/0/2

```

**Table 1-1** display mld-snooping group command output description

Field	Description
Total 1 IP Group(s).	Total number of IPv6 multicast groups
Total 1 IP Source(s).	Total number of IPv6 multicast sources
Total 1 MAC Group(s).	Total number of MAC multicast groups
Port flags: D-Dynamic port, S-Static port, C-Copy port	Port flags: D for dynamic port, S for static port, C for port copied from a (*, G) entry to an (S, G) entry
Subvlan flags: R-Real VLAN, C-Copy VLAN	Sub-VLAN flags: R for real egress sub-VLAN under the current entry, C for sub-VLAN copied from a (*, G) entry to an (S, G) entry
Router port(s)	Number of router ports
( 00:01:30 )	Remaining time of the dynamic member port or router port aging timer. On a distributed device, to get this time value of a non-aggregation port that does not belong to the SRPU, you must specify the number of the slot where the corresponding board resides; this is not required on an aggregation port.
IP group address	Address of IPv6 multicast group
::, FF1E::101)	(S, G) entry, :: represents all the multicast sources
MAC group address	Address of MAC multicast group
Attribute	Attribute of IPv6 multicast group
Host port(s)	Number of member ports

## display mld-snooping statistics

### Syntax

**display mld-snooping statistics**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

## Description

Use the **display mld-snooping statistics** command to view the statistics information of MLD messages learned by MLD Snooping.

## Examples

# View the statistics information of all kinds of MLD messages learned by MLD Snooping.

```
<Sysname> display mld-snooping statistics
Received MLD general queries:0.
Received MLDv1 specific queries:0.
Received MLDv1 reports:0.
Received MLD dones:0.
Sent MLDv1 specific queries:0.
Received MLDv2 reports:0.
Received MLDv2 reports with right and wrong records:0.
Received MLDv2 specific queries:0.
Received MLDv2 specific sg queries:0.
Sent MLDv2 specific queries:0.
Sent MLDv2 specific sg queries:0.
Received error MLD messages:0.
```

**Table 1-2 display mld-snooping statistics** command output description

Field	Description
general queries	General query messages
specific queries	Multicast-address-specific query messages
reports	Report messages
dones	Done messages
reports with right and wrong records	Reports containing correct and incorrect records
specific sg queries	Multicast-address-and-source-specific queries
error MLD messages	Error MLD messages

## fast-leave (MLD-Snooping view)

### Syntax

```
fast-leave [ vlan vlan-list ]
```

```
undo fast-leave [ vlan vlan-list ]
```

### View

MLD-Snooping view

### Default Level

2: System level

## Parameters

**vlan** *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

## Description

Use the **fast-leave** command to enable fast leave processing globally.

Use the **undo fast-leave** command to disable fast leave processing globally.

By default, fast leave processing is disabled.

Note that:

- This command works on both MLD Snooping-enabled VLANs and VLANs with MLD enabled on their VLAN interfaces.
- If you do not specify any VLAN, the command will take effect for all VLANs; if you specify a VLAN or multiple VLANs, the command will take effect for the specified VLAN(s) only.

Related commands: **mld-snooping fast-leave**.

## Examples

```
# Enable fast leave processing globally in VLAN 2.
```

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] fast-leave vlan 2
```

## group-policy (MLD-Snooping view)

### Syntax

```
group-policy acl6-number [ vlan vlan-list ]
undo group-policy [ vlan vlan-list ]
```

### View

MLD-Snooping view

### Default Level

2: System level

## Parameters

*Acl6-number*: Basic or advanced IPv6 ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced IPv6 ACL rule is used to match the IPv6 multicast source address(es) specified in MLDv2 reports, rather than the source address in the IPv6 packets. The system assumes that an MLDv1 report or an MLDv2 IS\_EX or TO\_EX report that does not carry an IPv6 multicast source address carries an IPv6 multicast source address of 0::0.

**vlan** *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

## Description

Use the **group-policy** command to configure a global IPv6 multicast group filter.

Use the **undo group-policy** command to remove the configured global IPv6 multicast group filter.

By default, no IPv6 multicast group filter is configured globally, namely any host can join any valid IPv6 multicast group.

Note that:

- If you do not specify any VLAN, the command will take effect for all VLANs; if you specify a VLAN or multiple VLANs, the command will take effect for the specified VLAN(s) only.
- If the specified IPv6 ACL does not exist or the ACL rule is null, all IPv6 multicast groups will be filtered out.
- You can configure different IPv6 ACL rules for each port in different VLANs; for a given VLAN, a newly configured IPv6 ACL rule will override the existing one.

Related commands: **mld-snooping group-policy**.

## Examples

```
# Apply ACL 2000 as an IPv6 multicast group filter in VLAN 2.
```

```
<Sysname> system-view  
[Sysname] mld-snooping  
[Sysname-mld-snooping] group-policy 2000 vlan 2
```

## host-aging-time (MLD-Snooping view)

### Syntax

```
host-aging-time interval  
undo host-aging-time
```

### View

MLD-Snooping view

### Default Level

2: System level

### Parameters

*interval*: Dynamic member port aging time, in units of seconds. The effective range is 200 to 1,000.

## Description

Use the **host-aging-time** command to configure the aging time of dynamic member ports globally.

Use the **undo host-aging-time** command to restore the default setting.

By default, the aging time of dynamic member ports is 260 seconds.

This command works only on MLD Snooping-enabled VLANs, but not on VLANs with MLD enabled on their VLAN interfaces.

Related commands: **mld-snooping host-aging-time**.

## Examples

```
# Set the aging time of dynamic member ports globally to 300 seconds.
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] host-aging-time 300
```

## last-listener-query-interval (MLD-Snooping view)

### Syntax

```
last-listener-query-interval interval
undo last-listener-query-interval
```

### View

MLD-Snooping view

### Default Level

2: System level

### Parameters

*interval*: MLD last listener query interval in units of seconds, namely the length of time the device waits between sending MLD multicast-address-specific queries. The effective range is 1 to 5.

### Description

Use the **last-listener-query-interval** command to configure the MLD last listener query interval globally.

Use the **undo last-listener-query-interval** command to restore the system default.

By default, the MLD last listener query interval is 1 second.

This command works only on MLD Snooping-enabled VLANs, but not on VLANs with MLD enabled on their VLAN interfaces.

Related commands: **mld-snooping last-listener-query-interval**.

## Examples

```
# Set the MLD last listener query interval to 3 seconds globally.
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] last-listener-query-interval 3
```

## max-response-time (MLD-Snooping view)

### Syntax

```
max-response-time interval
undo max-response-time
```

### View

MLD-Snooping view

## Default Level

2: System level

## Parameters

*interval*: Maximum response time for MLD general queries, in units of seconds. The effective range is 1 to 25.

## Description

Use the **max-response-time** command to configure the maximum response time for MLD general queries globally.

Use the **undo max-response-time** command to restore the system default.

By default, the maximum response time for MLD general queries is 10 seconds.

This command works only on MLD Snooping-enabled VLANs, but not on VLANs with MLD enabled on their VLAN interfaces.

Related commands: **mld-snooping max-response-time**, **mld-snooping query-interval**.

## Examples

# Set the maximum response time for MLD general queries globally to 5 seconds.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] max-response-time 5
```

## mld-snooping

### Syntax

```
mld-snooping
undo mld-snooping
```

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **mld-snooping** command to enable MLD Snooping globally and enter MLD-Snooping view.

Use the **undo mld-snooping** command to disable MLD Snooping globally.

By default, MLD Snooping is disabled.

Related commands: **mld-snooping enable**.

### Examples

# Enable MLD Snooping globally and enter MLD-Snooping view.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping]
```

## mld-snooping drop-unknown

### Syntax

```
mld-snooping drop-unknown
undo mld-snooping drop-unknown
```

### View

VLAN view

### Default Level

2: System level

### Parameters

None

### Description

Use the **mld-snooping drop-unknown** command to enable dropping unknown IPv6 multicast data in the current VLAN.

Use the **undo mld-snooping drop-unknown** command to disable dropping unknown IPv6 multicast data in the current VLAN.

By default, this function is disabled, unknown IPv6 multicast data is flooded in the VLAN.

This command takes effect only if MLD Snooping is enabled in the VLAN.

Related commands: **drop-unknown**.

### Examples

```
# Enable dropping unknown IPv6 multicast data in VLAN 2.
```

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping drop-unknown
```

## mld-snooping enable

### Syntax

```
mld-snooping enable
undo mld-snooping enable
```

### View

VLAN view

### Default Level

2: System level

## Parameters

None

## Description

Use the **mld-snooping enable** command to enable MLD Snooping in the current VLAN.

Use the **undo mld-snooping enable** command to disable MLD Snooping in the current VLAN.

By default, MLD Snooping is disabled in a VLAN.

MLD Snooping must be enabled globally before it can be enabled in a VLAN

Related commands: **mld-snooping**.

## Examples

```
# Enable MLD Snooping in VLAN 2.
```

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
```

## mld-snooping fast-leave

### Syntax

```
mld-snooping fast-leave [ vlan vlan-list ]
```

```
undo mld-snooping fast-leave [ vlan vlan-list ]
```

### View

Ethernet port view, Layer 2 aggregate port view, port group view

### Default Level

2: System level

## Parameters

**vlan** *vlan-list*. Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

## Description

Use the **mld-snooping fast-leave** command to enable fast leave processing on the current port or group of ports.

Use the **undo mld-snooping fast-leave** command to disable fast leave processing on the current port or group of ports.

By default, fast leave processing is disabled.

Note that:

- This command works on both MLD Snooping-enabled VLANs and VLANs with MLD enabled on their VLAN interfaces.

- If you do not specify any VLAN when using this command in Ethernet port view or Layer 2 aggregate port view, the command will take effect for all VLANs the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the port belongs to the specified VLAN(s).
- If you do not specify any VLAN when using this command in port group view, the command will take effect on all the ports in this group; if you specify a VLAN or multiple VLANs, the command will take effect only on those ports in this group that belong to the specified VLAN(s).

Related commands: **fast-leave**.

## Examples

```
# Enable fast leave processing on GigabitEthernet 1/0/1 in VLAN 2.
```

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping fast-leave vlan 2
```

## mld-snooping general-query source-ip

### Syntax

```
mld-snooping general-query source-ip { current-interface | ipv6-address }
undo mld-snooping general-query source-ip
```

### View

VLAN view

### Default Level

2: System level

### Parameters

**current-interface**: Sets the source IPv6 link-local address of MLD general queries to the IPv6 address of the current VLAN interface. If the current VLAN interface does not have an IPv6 address, the default IPv6 address FE80::02FF:FFFF:FE00:0001 will be used as the source IPv6 address of MLD general queries.

*ipv6-address*: Specifies the source IPv6 address of MLD general queries, which can be any legal IPv6 link-local address.

### Description

Use the **mld-snooping general-query source-ip** command to configure the source IPv6 address of MLD general queries.

Use the **undo mld-snooping general-query source-ip** command to restore the default configuration.

By default, the source IPv6 address of MLD general queries is FE80::02FF:FFFF:FE00:0001.

This command takes effect only if MLD Snooping is enabled in the VLAN.

## Examples

```
# In VLAN 2, specify FE80:0:0:1::1 as the source IPv6 address of MLD general queries.
```

```
<Sysname> system-view
[Sysname] vlan 2
```

```
[Sysname-vlan2] mld-snooping general-query source-ip fe80:0:0:1::1
```

## mld-snooping group-limit

### Syntax

```
mld-snooping group-limit limit [ vlan vlan-list ]  
undo mld-snooping group-limit [ vlan vlan-list ]
```

### View

Ethernet port view, Layer 2 aggregate port view, port group view

### Default Level

2: System level

### Parameters

*limit*: Maximum number of IPv6 multicast groups that can be joined on a port. The value is in the range 1 to 512.

**vlan** *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* to *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

### Description

Use the **mld-snooping group-limit** command to configure the maximum number of IPv6 multicast groups that can be joined on a port.

Use the **undo mld-snooping group-limit** command to restore the default setting.

By default, maximum number of IPv6 multicast groups that can be joined on a port is 512.

Note that:

- You can also use the **mld group-limit** command to limit the number of IPv6 multicast groups that can be joined on an port. If you configure a limit of the number of groups for ports in a VLAN while you have configured a limit of the number of groups for the VLAN interface, or vice versa, this may cause inconsistencies between Layer 2 and Layer 3 table entries. Therefore, it is recommended to configure a limit of the number of groups only on the VLAN interface.
- If you do not specify any VLAN when using this command in Ethernet port view or Layer 2 aggregate port view, the command will take effect for all VLANs the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the port belongs to the specified VLAN(s).
- If you do not specify any VLAN when using this command in port group view, the command will take effect on all the ports in this group; if you specify a VLAN or multiple VLANs, the command will take effect only on those ports in this group that belong to the specified VLAN(s).

Related commands: **mld group-limit** in *MLD Commands* in the *IP Multicast Volume*.

### Examples

```
# Specify to allow a maximum of 10 IPv6 multicast groups to be joined on GigabitEthernet 1/0/1 in VLAN 2.
```

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet 1/0/1] mld-snooping group-limit 10 vlan 2
```

## mld-snooping group-policy

### Syntax

```
mld-snooping group-policy acl6-number [ vlan vlan-list ]
undo mld-snooping group-policy [ vlan vlan-list ]
```

### View

Ethernet port view, Layer 2 aggregate port view, port group view

### Default Level

2: System level

### Parameters

*acl6-number*: Basic or advanced IPv6 ACL number, in the range of 2000 to 3999. The IPv6 source address or address range specified in the advanced IPv6 ACL rule is the IPv6 multicast source address(es) specified in MLDv2 reports, rather than the source address in the IPv6 packets. The system assumes that an MLDv1 report or an MLDv2 IS\_EX or TO\_EX report that does not carry an IPv6 multicast source address carries an IPv6 multicast source address of 0::0.

**vlan** *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

### Description

Use the **mld-snooping group-policy** command to configure an IPv6 multicast group filter on the current port(s).

Use the **undo mld-snooping group-policy** command to remove the configured IPv6 multicast group filter on the current port(s).

By default, no IPv6 multicast group filter is configured on a port, namely a host can join any valid IPv6 multicast group.

Note that:

- If you do not specify any VLAN when using this command in Ethernet port view or Layer 2 aggregate port view, the command will take effect for all VLANs the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the port belongs to the specified VLAN(s).
- If you do not specify any VLAN when using this command in port group view, the command will take effect on all the ports in this group; if you specify a VLAN or multiple VLANs, the command will take effect only on those ports in this group that belong to the specified VLAN(s).
- If the specified ACL does not exist or the ACL rule is null, all IPv6 multicast groups will be filtered out.
- You can configure different IPv6 ACL rules for each port in different VLANs; for a given VLAN, a newly configured IPv6 ACL rule will override the existing one.

Related commands: **group-policy**.

## Examples

```
# Apply ACL 2000 as an IPv6 multicast group filter on GigabitEthernet 1/0/1 in VLAN 2.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet 1/0/1] mld-snooping group-policy 2000 vlan 2
```

## mld-snooping host-aging-time

### Syntax

```
mld-snooping host-aging-time interval
undo mld-snooping host-aging-time
```

### View

VLAN view

### Default Level

2: System level

### Parameters

*interval*: Dynamic member port aging time, in seconds. The effective range is 200 to 1,000.

### Description

Use the **mld-snooping host-aging-time** command to configure the aging time of dynamic member ports in the current VLAN.

Use the **undo mld-snooping host-aging-time** command to restore the system default.

By default, the dynamic member port aging time is 260 seconds.

This command takes effect only if MLD Snooping is enabled in the VLAN.

Related commands: **host-aging-time**.

## Examples

```
# Set the aging time of dynamic member ports to 300 seconds in VLAN 2.
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping host-aging-time 300
```

## mld-snooping host-join

### Syntax

```
mld-snooping host-join ipv6-group-address [ source-ip ipv6-source-address ] vlan vlan-id
undo mld-snooping host-join ipv6-group-address [ source-ip ipv6-source-address ] vlan vlan-id
```

### View

Ethernet port view, Layer 2 aggregate port view, port group view

## Default Level

2: System level

## Parameters

*ipv6-group-address*: Address of IPv6 multicast group which the simulated host is to join. The effective range is FFxy::<16 (excluding FFx0::<16, FFx1::<16, FFx2::<16 and FF0y::), where x and y represent any hexadecimal number between 0 and F, inclusive.

*ipv6-source-address*: Address of the IPv6 multicast source that the simulated host is to join.

**vlan** *vlan-id*: Specifies a VLAN that comprises the port(s), where *vlan-id* is in the range of 1 to 4094.

## Description

Use the **mld-snooping host-join** command to configure the current port(s) as simulated member host(s) for the specified IPv6 multicast group or source and group.

Use the **undo mld-snooping host-join** command to remove the current port(s) as simulated member host(s) for the specified IPv6 multicast group or source and group.

By default, no ports are configured as static member ports for any IPv6 multicast group or source and group.

Note that:

- This command works on both MLD Snooping-enabled VLANs and VLANs with MLD enabled on their VLAN interfaces, and the version of MLD on the simulated host depends on the version of MLD Snooping running in the VLAN or the version of MLD running on the VLAN interface.
- The **source-ip** *ipv6-source-address* option in the command is meaningful only for MLD Snooping version 2. If MLD Snooping version 1 is running, although you can include **source-ip** *ipv6-source-address* in your command, the simulated host responds with only an MLDv1 report when receiving a query message.
- If configured in Ethernet port view or Layer 2 aggregate port view, this feature takes effect only if the port belongs to the specified VLAN.
- If configured in port group view, this feature takes effect only on those ports in this port group that belong to the specified VLAN.

## Examples

# Configure GigabitEthernet 1/0/1 in VLAN 2 to join (2002::<22, FF3E::101) as a simulated host.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping version 2
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet 1/0/1] mld-snooping host-join ff3e::101 source-ip 2002::22 vlan 2
```

## mld-snooping last-listener-query-interval

### Syntax

```
mld-snooping last-listener-query-interval interval  
undo mld-snooping last-listener-query-interval
```

### View

VLAN view

### Default Level

2: System level

### Parameters

*interval*: MLD last listener query interval in units of seconds, namely the length of time the device waits between sending IGMP multicast-address-specific queries. The effective range is 1 to 5.

### Description

Use the **mld-snooping last-listener-query-interval** command to configure the MLD last-listener query interval in the VLAN.

Use the **undo mld-snooping last-listener-query-interval** command to restore the system default.

By default, the MLD last listener query interval is 1 second.

This command takes effect only if MLD Snooping is enabled in the VLAN.

Related commands: **last-listener-query-interval**.

### Examples

```
# Set the MLD last-listener query interval to 3 seconds in VLAN 2.  
<Sysname> system-view  
[Sysname] vlan 2  
[Sysname-vlan2] mld-snooping last-listener-query-interval 3
```

## mld-snooping max-response-time

### Syntax

```
mld-snooping max-response-time interval  
undo mld-snooping max-response-time
```

### View

VLAN view

### Default Level

2: System level

### Parameters

*interval*: Maximum response time for MLD general queries, in units of seconds. The effective range is 1 to 25.

## Description

Use the **mld-snooping max-response-time** command to configure the maximum response time for MLD general queries in the VLAN.

Use the **undo mld-snooping max-response-time** command to restore the default setting.

By default, the maximum response time for MLD general queries is 10 seconds.

This command takes effect only if MLD Snooping is enabled in the VLAN.

Related commands: **max-response-time**, **mld-snooping query-interval**.

## Examples

```
# Set the maximum response time for MLD general queries to 5 seconds in VLAN 2.
```

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping max-response-time 5
```

## mld-snooping overflow-replace

### Syntax

```
mld-snooping overflow-replace [ vlan vlan-list ]
undo mld-snooping overflow-replace [ vlan vlan-list ]
```

### View

Ethernet port view, Layer 2 aggregate port view, port group view

### Default Level

2: System level

### Parameters

**vlan** *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* to *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

## Description

Use the **mld-snooping overflow-replace** command to enable the IPv6 multicast group replacement function on the current port(s).

Use the **undo mld-snooping overflow-replace** command to disable the IPv6 multicast group replacement function on the current port(s).

By default, the IPv6 multicast group replacement function is disabled.

Note that:

- This command works on both MLD Snooping-enabled VLANs and VLANs with MLD enabled on their VLAN interfaces.
- If you do not specify any VLAN when using this command in Ethernet port view or Layer 2 aggregate port view, the command will take effect for all VLANs the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the port belongs to the specified VLAN(s).

- If you do not specify any VLAN when using this command in port group view, the command will take effect on all the ports in this group; if you specify a VLAN or multiple VLANs, the command will take effect only on those ports in this group that belong to the specified VLAN(s).

Related commands: **overflow-replace**.

## Examples

# Enable the IPv6 multicast group replacement function on GigabitEthernet 1/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitEthernet 1/0/1
[Sysname-GigabitEthernet 1/0/1] mld-snooping overflow-replace vlan 2
```

## mld-snooping querier

### Syntax

```
mld-snooping querier
undo mld-snooping querier
```

### View

VLAN view

### Default Level

2: System level

### Parameters

None

### Description

Use the **mld-snooping querier** command to enable the MLD Snooping querier function.

Use the **undo mld-snooping querier** command to disable the MLD Snooping querier function.

By default, the MLD Snooping querier function is disabled.

Note that:

- This command takes effect only if MLD Snooping is enabled in the VLAN.
- This command does not take effect in a sub-VLAN of an IPv6 multicast VLAN.

Related commands: **subvlan** command in *IPv6 Multicast VLAN Commands* in the *IP Multicast Volume*.

## Examples

# Enable the MLD Snooping querier function in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping querier
```

## mld-snooping query-interval

### Syntax

```
mld-snooping query-interval interval
```

**undo mld-snooping query-interval**

### View

VLAN view

### Default Level

2: System level

### Parameters

*interval*: MLD query interval in seconds, namely the length of time the device waits between sending MLD general queries. The effective range is 2 to 300.

### Description

Use the **mld-snooping query-interval** command to configure the MLD query interval.

Use the **undo mld-snooping query-interval** command to restore the system default.

By default, the MLD query interval is 125 seconds.

This command takes effect only if MLD Snooping is enabled in the VLAN.

Related commands: **mld-snooping querier**, **mld-snooping max-response-time**, **max-response-time**.

### Examples

```
# Set the MLD query interval to 20 seconds in VLAN 2.
```

```
<Sysname> system-view  
[Sysname] vlan 2  
[Sysname-vlan2] mld-snooping query-interval 20
```

## mld-snooping router-aging-time

### Syntax

```
mld-snooping router-aging-time interval  
undo mld-snooping router-aging-time
```

### View

VLAN view

### Default Level

2: System level

### Parameters

*interval*: Dynamic router port aging time, in seconds. The effective range is 1 to 1,000.

### Description

Use the **mld-snooping router-aging-time** command to configure the aging time of dynamic router ports in the current VLAN.

Use the **undo mld-snooping router-aging-time** command to restore the default setting.

By default, the dynamic router port aging time is 260 seconds.

This command takes effect only if MLD Snooping is enabled in the VLAN.

Related commands: **router-aging-time**.

## Examples

```
# Set the aging time of dynamic router ports to 100 seconds in VLAN 2.
```

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping router-aging-time 100
```

## mld-snooping source-deny

### Syntax

```
mld-snooping source-deny
undo mld-snooping source-deny
```

### View

Ethernet port view, port group view

### Default Level

2: System level

### Parameters

None

### Description

Use the **mld-snooping source-deny** command to enable IPv6 multicast source port filtering.

Use the **undo mld-snooping source-deny** command to disable IPv6 multicast source port filtering.

By default, IPv6 multicast source port filtering is disabled.

For a switch that supports both MLD Snooping and MLD, this command works on both MLD Snooping-enabled VLANs and VLANs with MLD enabled on their VLAN interfaces.

## Examples

```
# Enable source port filtering for IPv6 multicast data on GigabitEthernet 1/0/1.
```

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet 1/0/1] mld-snooping source-deny
```

## mld-snooping special-query source-ip

### Syntax

```
mld-snooping special-query source-ip { current-interface | ipv6-address }
undo mld-snooping special-query source-ip
```

### View

VLAN view

## Default Level

2: System level

## Parameters

**current-interface:** Specifies the source IPv6 link-local address of the VLAN interface of the current VLAN as the source IPv6 address of MLD multicast-address-specific queries. If the current VLAN interface does not have an IPv6 address, the default IPv6 address FE80::02FF:FFFF:FE00:0001 will be used as the source IPv6 address of MLD multicast-address-specific queries.

*ipv6-address:* Specifies an IPv6 link-local address as the source IPv6 address of MLD multicast-address-specific queries.

## Description

Use the **mld-snooping special-query source-ip** command to configure the source IPv6 address of MLD multicast-address-specific queries.

Use the **undo mld-snooping special-query source-ip** command to restore the default configuration.

By default, the source IPv6 address of MLD multicast-address-specific queries is FE80::02FF:FFFF:FE00:0001.

This command takes effect only if MLD Snooping is enabled in the VLAN.

## Examples

# In VLAN 2, specify FE80:0:0:1::1 as the source IPv6 address of MLD multicast-address-specific queries.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping special-query source-ip fe80:0:0:1::1
```

## mld-snooping static-group

### Syntax

**mld-snooping static-group** *ipv6-group-address* [ **source-ip** *ipv6-source-address* ] **vlan** *vlan-id*

**undo mld-snooping static-group** *ipv6-group-address* [ **source-ip** *ipv6-source-address* ] **vlan** *vlan-id*

### View

Ethernet port view, Layer 2 aggregate port view, port group view

## Default Level

2: System level

## Parameters

*ipv6-group-address:* Address of a IPv6 multicast group the port(s) will be configured to join as static member port(s). The effective range is FFx0::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16 and FF0y::), where x and y represent any hexadecimal number between 0 and F, inclusive.

*ipv6-source-address:* Address of the IPv6 multicast source the port(s) will be configured to join as static member port(s).

**vlan *vlan-id***: Specifies the VLAN that comprises the Ethernet port(s), where *vlan-id* is in the range of 1 to 4094.

## Description

Use the **mld-snooping static-group** command to configure the static IPv6 (\*, G) or (S, G) joining function, namely to configure the port or port group as static IPv6 multicast group or source-group member(s).

Use the **undo mld-snooping static-group** command to restore the system default.

By default, no ports are static member ports.

Note that:

- The **source-ip *ipv6-source-address*** option in the command is meaningful only for MLD Snooping version 2. If MLD Snooping version 1 is running, although you can include **source-ip *ipv6-source-address*** in your command, the simulated host responses with only an MLDv1 report when receiving a query message.
- If configured in Ethernet port view or Layer 2 aggregate port view, this feature takes effect only if the port belongs to the specified VLAN.
- If configured in port group view, this feature takes effect only on those ports in this port group that belong to the specified VLAN.

## Examples

# Configure GigabitEthernet 1/0/1 in VLAN 2 to be a static member port for (2002::22, FF3E::101).

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping version 2
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet 1/0/1] mld-snooping static-group ff3e::101 source-ip 2002::22 vlan
2
```

## mld-snooping static-router-port

### Syntax

**mld-snooping static-router-port vlan *vlan-id***

**undo mld-snooping static-router-port vlan *vlan-id***

### View

Ethernet port view, Layer 2 aggregate port view, port group view

### Default Level

2: System level

## Parameters

**vlan *vlan-id***: Specifies a VLAN in which one or more static router ports are to be configured, where *vlan-id* is in the range of 1 to 4094.

## Description

Use the **mld-snooping static-router-port** command to configure the current port(s) as static router port(s).

Use the **undo mld-snooping static-router-port** command to restore the system default.

By default, no ports are static router ports.

Note that:

- This command works on both MLD Snooping-enabled VLANs and VLANs with MLD enabled on their VLAN interfaces.
- This command does not take effect in a sub-VLAN of an IPv6 multicast VLAN.
- If configured in Ethernet port view or Layer 2 aggregate port view, this feature takes effect only if the port belongs to the specified VLAN.
- If configured in port group view, this feature takes effect only on those ports in this port group that belong to the specified VLAN.

Related commands: **subvlan** command in *IPv6 Multicast VLAN Commands* in the *IP Multicast Volume*.

## Examples

# Enable the static router port function on GigabitEthernet 1/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname- GigabitEthernet 1/0/1] mld-snooping static-router-port vlan 2
```

## mld-snooping version

### Syntax

**mld-snooping version *version-number***

**undo mld-snooping version**

### View

VLAN view

### Default Level

2: System level

### Parameters

*version-number*: MLD snooping version, in the range of 1 to 2.

### Description

Use the **mld-snooping version** command to configure the MLD Snooping version.

Use the **undo mld-snooping version** command to restore the default setting.

By default, the MLD version is 1.

Note that:

- This command can take effect only if MLD Snooping is enabled in the VLAN.
- This command does not take effect in a sub-VLAN of an IPv6 multicast VLAN.

Related commands: **mld-snooping enable**; **subvlan** in *IPv6 Multicast VLAN Commands* in the *IP Multicast Volume*.

## Examples

# Enable MLD Snooping in VLAN 2, and set the MLD Snooping version to version 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping version 2
```

## overflow-replace (MLD-Snooping view)

### Syntax

```
overflow-replace [ vlan vlan-list ]
undo overflow-replace [ vlan vlan-list ]
```

### View

MLD-Snooping view

### Default Level

2: System level

### Parameters

**vlan** *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

### Description

Use the **overflow-replace** command to enable the IPv6 multicast group replacement function globally.

Use the **undo overflow-replace** command to disable the IPv6 multicast group replacement function globally.

By default, the IPv6 multicast group replacement function is disabled globally.

Note that:

- This command works on both MLD Snooping-enabled VLANs and VLANs with MLD enabled on their VLAN interfaces.
- If you do not specify any VLAN, the command will take effect for all VLANs; if you specify a VLAN or multiple VLANs, the command will take effect for the specified VLAN(s) only.

Related commands: **mld-snooping overflow-replace**.

## Examples

# Enable the IPv6 multicast group replacement function globally in VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] overflow-replace vlan 2
```

## report-aggregation (MLD-Snooping view)

### Syntax

```
report-aggregation
undo report-aggregation
```

### View

MLD-Snooping view

### Default Level

2: System level

### Parameters

None

### Description

Use the **mld-snooping report-aggregation** command to enable MLD report suppression.

Use the **undo mld-snooping report-aggregation** command to disable MLD report suppression.

By default, MLD report suppression is enabled.

This command works on both MLD Snooping-enabled VLANs and VLANs with MLD enabled on their VLAN interfaces.

### Examples

```
# Disable MLD report suppression.
```

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] undo report-aggregation
```

## reset mld-snooping group

### Syntax

```
reset mld-snooping group { ipv6-group-address | all } [ vlan vlan-id ]
```

### View

User view

### Default Level

2: System level

## Parameters

*ipv6-group-address*: Clears the information about the specified multicast group. The effective range of *ipv6-group-address* is FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16 and FF0y::), where x and y represent any hexadecimal number between 0 and F, inclusive.

**all**: Clears all MLD Snooping multicast group information.

**vlan** *vlan-id*: Clears the MLD Snooping multicast group information in the specified VLAN. The effective range of *vlan-id* is 1 to 4094.

## Description

Use the **reset mld-snooping group** command to clear MLD Snooping multicast group information.

Note that:

- This command works only on MLD Snooping-enabled VLANs, but not on VLANs with MLD enabled on their VLAN interfaces.
- This command cannot clear MLD Snooping multicast group information of static joining.

## Examples

```
# Clear all MLD Snooping multicast group information.
```

```
<Sysname> reset mld-snooping group all
```

## reset mld-snooping statistics

### Syntax

```
reset mld-snooping statistics
```

### View

User view

### Default Level

2: System level

### Parameters

None

### Description

Use the **reset mld-snooping statistics** command to clear the statistics information of MLD messages learned by MLD Snooping.

## Examples

```
# Clear the statistics information of all kinds of MLD messages learned by MLD Snooping.
```

```
<Sysname> reset mld-snooping statistics
```

## router-aging-time (MLD-Snooping view)

### Syntax

```
router-aging-time interval
```

## undo router-aging-time

### View

MLD-Snooping view

### Default Level

2: System level

### Parameters

*interval*: Dynamic router port aging time, in seconds. The effective range is 1 to 1,000.

### Description

Use the **router-aging-time** command to configure the aging time of dynamic router ports globally.

Use the **undo router-aging-time** command to restore the default setting.

By default, the dynamic router port aging time is 260 seconds.

This command works only on MLD Snooping-enabled VLANs, but not on VLANs with MLD enabled on their VLAN interfaces.

Related commands: **mld-snooping router-aging-time**.

### Examples

# Set the aging time of dynamic router ports globally to 100 seconds.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] router-aging-time 100
```

## source-deny (MLD-Snooping view)

### Syntax

**source-deny port** *interface-list*

**undo source-deny port** *interface-list*

### View

MLD-Snooping view

### Default Level

2: System level

### Parameters

*interface-list*: Port list. You can specify multiple ports or port ranges by providing the this argument in the form of *interface-list* = { *interface-type interface-number* [ **to** *interface-type interface-number* ] }, where *interface-type* is port type and *interface-number* is port number.

### Description

Use the **source-deny** command to enable IPv6 multicast source port filtering, namely to filter out all the received IPv6 multicast packets.

Use the **undo source-deny** command to disable IPv6 multicast source port filtering.

By default, IPv6 multicast source port filtering is disabled.

This command works on both MLD Snooping-enabled VLANs and VLANs with MLD enabled on their VLAN interfaces.

### Examples

# Enable source port filtering for IPv6 multicast data on interfaces GigabitEthernet1/0/1 through GigabitEthernet1/0/4.

```
<Sysname> system-view
```

```
[Sysname] mld-snooping
```

```
[Sysname-mld-snooping] source-deny port gigabitethernet1/0/1 to gigabitethernet1/0/4
```

# Table of Contents

<b>1 IPv6 Multicast VLAN Configuration Commands .....</b>	<b>1-1</b>
IPv6 Multicast VLAN Configuration Commands .....	1-1
display multicast-vlan ipv6.....	1-1
multicast-vlan ipv6 .....	1-2
port (IPv6 multicast VLAN view).....	1-3
port multicast-vlan ipv6.....	1-3
subvlan (IPv6 multicast VLAN view).....	1-4

# 1 IPv6 Multicast VLAN Configuration Commands

---

## IPv6 Multicast VLAN Configuration Commands

### display multicast-vlan ipv6

#### Syntax

```
display multicast-vlan ipv6 [ vlan-id ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

*vlan-id*: VLAN ID of an IPv6 multicast VLAN, in the range of 1 to 4094. If this argument is not provided, the information about all IPv6 multicast VLANs will be displayed.

#### Description

Use the **display multicast-vlan ipv6** command to view the information about the specified IPv6 multicast VLAN or all IPv6 multicast VLANs.

#### Examples

# View the information about all IPv6 multicast VLANs.

```
<Sysname> display multicast-vlan ipv6
Total 1 IPv6 multicast-vlan(s)
IPv6 Multicast vlan 100
  subvlan list:
    vlan 2  4-6
  port list:
    no port
```

**Table 1-1 display multicast-vlan ipv6 command output description**

Field	Description
Total 1 IPv6 multicast-vlan(s)	Total number of IPv6 multicast VLANs
IPv6 Multicast vlan	An IPv6 multicast VLAN
subvlan list	List of sub-VLANs of the IPv6 multicast VLAN
port list	Port list of the IPv6 multicast VLAN

## multicast-vlan ipv6

### Syntax

```
multicast-vlan ipv6 vlan-id  
undo multicast-vlan ipv6 { all | vlan-id }
```

### View

System view

### Default Level

2: System level

### Parameters

*vlan-id*: Specifies a VLAN by its ID, in the range of 1 to 4094.

**all**: Deletes all IPv6 multicast VLANs.

### Description

Use the **multicast-vlan ipv6** command to configure the specified VLAN as an IPv6 multicast VLAN and enter IPv6 multicast VLAN view.

Use the **undo multicast-vlan ipv6** command to remove the specified VLAN as an IPv6 multicast VLAN.

No VLAN is an IPv6 multicast VLAN by default.

Note that:

- The specified VLAN to be configured as an IPv6 multicast VLAN must exist.
- The IPv6 multicast VLAN feature cannot be enabled on a device with IPv6 multicast routing enabled.
- For a sub-VLAN-based IPv6 multicast VLAN, you need to enable MLD Snooping only in the IPv6 multicast VLAN; for a port-based IPv6 multicast VLAN, you need to enable MLD Snooping in both the IPv6 multicast VLAN and all the user VLANs.

Related commands: **multicast ipv6 routing-table** in the *IPv6 Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*; **mld-snooping enable** in the *MLD Snooping Commands* in the *IP Multicast Volume*.

### Examples

# Enable MLD Snooping in VLAN 100. Configure it as an IPv6 multicast VLAN and enter IPv6 multicast VLAN view.

```
<Sysname> system-view  
[Sysname] mld-snooping  
[Sysname-mld-snooping] quit  
[Sysname] vlan 100  
[Sysname-vlan100] mld-snooping enable  
[Sysname-vlan100] quit  
[Sysname] multicast-vlan ipv6 100  
[Sysname-ipv6-mvlan-100]
```

## port (IPv6 multicast VLAN view)

### Syntax

```
port interface-list
undo port { all | interface-list }
```

### View

IPv6 multicast VLAN view

### Default Level

2: System level

### Parameters

*interface-list*: Specifies a port in the form of *interface-type interface-number*, or a port range in the form of *interface-type start-interface-number to interface-type end-interface-number*, where the end interface number must be greater than the start interface number.

**all**: Deletes all the ports in the current IPv6 multicast VLAN.

### Description

Use the **port** command to assign port(s) to the current IPv6 multicast VLAN.

Use the **undo port** command to delete port(s) from the current IPv6 multicast VLAN.

By default, an IPv6 multicast VLAN has no ports.

Note that:

- A port can belong to only one IPv6 multicast VLAN.
- Only the following types of ports can be configured as IPv6 multicast VLAN ports: Ethernet, and Layer 2 aggregate ports.

### Examples

```
# Assign ports GigabitEthernet1/0/1 through GigabitEthernet1/0/5 to IPv6 multicast VLAN 100.
```

```
<Sysname> system-view
[Sysname] multicast-vlan ipv6 100
[Sysname-ipv6-mvlan-100] port gigabitethernet1/0/1 to gigabitethernet1/0/5
```

## port multicast-vlan ipv6

### Syntax

```
port multicast-vlan ipv6 vlan-id
undo port multicast-vlan ipv6
```

### View

Ethernet port view, Layer 2 aggregate port view, port group view.

### Default Level

2: System level

## Parameters

*vlan-id*: VLAN ID of the IPv6 multicast VLAN you want to assign the current port(s) to, in the range of 1 to 4094.

## Description

Use the **port multicast-vlan ipv6** command to assign the current port(s) to the specified IPv6 multicast VLAN.

Use the **undo port multicast-vlan ipv6** command to restore the system default.

By default, a port does not belong to any IPv6 multicast VLAN.

Note that a port can belong to only one IPv6 multicast VLAN.

## Examples

# Assign GigabitEthernet1/0/1 to IPv6 multicast VLAN 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] port multicast-vlan ipv6 100
```

## subvlan (IPv6 multicast VLAN view)

### Syntax

**subvlan** *vlan-list*

**undo subvlan** { **all** | *vlan-list* }

### View

IPv6 multicast VLAN view

### Default Level

2: System level

## Parameters

*vlan-list*: Specifies a VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

**all**: Deletes all the sub-VLANs of the current IPv6 multicast VLAN.

## Description

Use the **subvlan** command to configure sub-VLAN(s) for the current IPv6 multicast VLAN.

Use the **undo subvlan** command to remove the specified sub-VLAN(s) or all sub-VLANs from the current IPv6 multicast VLAN.

An IPv6 multicast VLAN has no sub-VLANs by default.

Note that:

- The VLANs to be configured as the sub-VLANs of the IPv6 multicast VLAN must exist and must not be IPv6 multicast VLANs or sub-VLANs of another IPv6 multicast VLAN.
- The number of sub-VLANs of the multicast VLAN must not exceed 127.

## Examples

# Configure VLAN 10 through VLAN 15 as sub-VLANs of IPv6 multicast VLAN 100.

```
<Sysname> system-view
```

```
[Sysname] multicast-vlan ipv6 100
```

```
[Sysname-ipv6-mvlan-100] subvlan 10 to 15
```

# QoS Volume Organization

---

## Manual Version

6W100-20090120

## Product Version

Release 2202

## Organization

The QoS Volume is organized as follows:

Features	Description
QoS	<p>Quality of Service (QoS) reflects the ability to meet customer needs. This documentation mainly describes the commands for:</p> <ul style="list-style-type: none"><li>• traffic classification configuration</li><li>• traffic policing configuration</li><li>• traffic shaping configuration</li><li>• line rate configuration</li><li>• QoS policy configuration</li><li>• congestion management configuration</li><li>• congestion avoidance configuration</li><li>• priority mapping configuration</li><li>• traffic mirroring configuration</li></ul>
User Profile	<p>User profile provides a configuration template to save predefined configurations. This document introduces the commands for:</p> <ul style="list-style-type: none"><li>• Creating a User Profile</li><li>• Configuring a User Profile</li><li>• Enabling a User Profile</li></ul>

# Table of Contents

<b>1 QoS Policy Configuration Commands</b> .....	<b>1-1</b>
Commands for Defining Classes .....	1-1
display traffic classifier.....	1-1
if-match.....	1-2
traffic classifier.....	1-5
Traffic Behavior Configuration Commands.....	1-6
accounting .....	1-6
car.....	1-6
display traffic behavior.....	1-8
filter.....	1-9
nest.....	1-9
redirect.....	1-10
remark customer-vlan-id.....	1-11
remark dot1p .....	1-12
remark drop-precedence .....	1-12
remark dscp.....	1-13
remark ip-precedence.....	1-14
remark local-precedence.....	1-15
remark service-vlan-id .....	1-15
traffic behavior .....	1-16
QoS Policy Configuration Commands .....	1-17
classifier behavior.....	1-17
display qos policy .....	1-18
display qos policy global.....	1-19
display qos policy interface .....	1-20
display qos vlan-policy.....	1-21
qos apply policy.....	1-23
qos apply policy global .....	1-24
qos policy.....	1-25
qos vlan-policy.....	1-26
reset qos policy global.....	1-27
reset qos vlan-policy.....	1-27
<b>2 Priority Mapping Configuration Commands</b> .....	<b>2-1</b>
Priority Mapping Table Configuration Commands .....	2-1
display qos map-table.....	2-1
qos map-table.....	2-2
import.....	2-2
Port Priority Configuration Commands .....	2-3
qos priority .....	2-3
Port Priority Trust Mode Configuration Commands .....	2-4
display qos trust interface.....	2-4
qos trust.....	2-5

<b>3 Traffic Shaping and Line Rate Configuration Commands .....</b>	<b>3-1</b>
Traffic Shaping Configuration Commands .....	3-1
display qos gts interface .....	3-1
qos gts .....	3-2
Line Rate Configuration Commands .....	3-2
display qos lr interface .....	3-2
qos lr outbound .....	3-3
<b>4 Congestion Management Configuration Commands .....</b>	<b>4-1</b>
Congestion Management Configuration Commands .....	4-1
display qos sp interface .....	4-1
display qos wfq interface .....	4-1
display qos wrr interface .....	4-2
qos bandwidth queue .....	4-4
qos sp .....	4-4
qos wfq .....	4-5
qos wfq weight .....	4-6
qos wrr .....	4-6
qos wrr group .....	4-7
<b>5 Congestion Avoidance Configuration Commands .....</b>	<b>5-1</b>
Congestion Avoidance Configuration Commands .....	5-1
display qos wred interface .....	5-1
display qos wred table .....	5-1
qos wred apply .....	5-2
qos wred queue table .....	5-3
queue .....	5-4
<b>6 Traffic Mirroring Configuration Commands .....</b>	<b>6-1</b>
Traffic Mirroring Configuration Commands .....	6-1
mirror-to .....	6-1

# 1 QoS Policy Configuration Commands

---

## Commands for Defining Classes

### display traffic classifier

#### Syntax

```
display traffic classifier user-defined [ classifier-name ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

*classifier-name*: Class name.

#### Description

Use the **display traffic classifier** command to display the information about a class.

If no class name is provided, this command displays the information about all the user-defined classes.

#### Examples

# Display the information about the user-defined classes.

```
<Sysname> display traffic classifier user-defined
User Defined Classifier Information:
Classifier: p
Operator: AND
Rule(s) : If-match acl 2001
```

**Table 1-1** display traffic classifier user-defined command output description

Field	Description
User Defined Classifier Information	The information about the user-defined classes is displayed.
Classifier	Class name and its contents, which could be of multiple types
Operator	Logical relationship among the classification rules
Rule	Classification rules

## if-match

### Syntax

**if-match** *match-criteria*

**undo if-match** *match-criteria*

### View

Class view

### Default Level

2: System Level

### Parameters

*match-criteria*: Matching rule to be defined. [Table 1-2](#) describes the available forms of this argument.

**Table 1-2** The forms of the *match-criteria* argument

Field	Description
<b>acl</b> <i>access-list-number</i>	Specifies an ACL to match packets. The <i>access-list-number</i> argument is a number in the range 2000 to 4999 or an ACL name. In a class configured with the operator <b>and</b> , the logical relationship between rules defined in the referenced IPv4 ACL is <b>or</b> .
<b>acl ipv6</b> <i>access-list-number</i>	Specifies an IPv6 ACL to match IPv6 packets. The <i>access-list-number</i> argument is a number in the range 2000 to 3999 or an ACL name. In a class configured with the operator <b>and</b> , the logical relationship between rules defined in the referenced IPv6 ACL is <b>or</b> .
<b>any</b>	Specifies to match all packets.
<b>customer-dot1p</b> <i>802 1p-list</i>	Specifies to match packets by 802.1p precedence of the customer network. The <i>802 1p-list</i> argument is a list of CoS values, in the range of 0 to 7.  <b>Note</b> <i>Even though you can provide up to eight space-separated CoS values for this argument, the Switch 4800G supports only one CoS value in a rule. If you configure multiple CoS values in a rule, the rule cannot be issued.</i>
<b>customer-vlan-id</b> <i>vlan-id-list</i>	Specifies to match the packets of specified VLANs of user networks. The <i>vlan-id-list</i> argument specifies a list of VLAN IDs, in the form of <i>vlan-id to vlan-id</i> or multiple discontinuous VLAN IDs (separated by space). You can specify up to eight VLAN IDs for this argument at a time. VLAN ID is in the range 1 to 4094. In a class configured with the operator <b>and</b> , the logical relationship between the customer VLAN IDs specified for the <b>customer-vlan-id</b> keyword is <b>or</b> .

Field	Description
<b>dscp</b> <i>dscp-list</i>	<p>Specifies to match packets by DSCP precedence. The <i>dscp-list</i> argument is a list of DSCP values in the range of 0 to 63 or keywords shown in <a href="#">Table 1-4</a>.</p> <p> <b>Note</b>  <i>Even though you can provide up to eight space-separated DSCP values for this argument, the Switch 4800G supports only one DSCP value in a rule. If you configure multiple DSCP values in a rule, the rule cannot be issued.</i></p>
<b>destination-mac</b> <i>mac-address</i>	<p>Specifies to match the packets with a specified destination MAC address.</p>
<b>ip-precedence</b> <i>ip-precedence-list</i>	<p>Specifies to match packets by IP precedence. The <i>ip-precedence-list</i> argument is a list of IP precedence values in the range of 0 to 7.</p> <p> <b>Note</b>  <i>Even though you can provide up to eight space-separated IP precedence values for this argument, the Switch 4800G supports only one IP precedence value in a rule. If you configure multiple IP precedence values in a rule, the rule cannot be issued.</i></p>
<b>protocol</b> <i>protocol-name</i>	<p>Specifies to match the packets of a specified protocol. The <i>protocol-name</i> argument can be IP or IPv6.</p>
<b>service-dot1p</b> <i>802 1p-list</i>	<p>Specifies to match packets by 802.1p precedence of the service provider network. The <i>802 1p-list</i> argument is a list of CoS values in the range of 0 to 7.</p> <p> <b>Note</b>  <i>Even though you can provide up to eight space-separated CoS values for this argument, the Switch 4800G supports only one CoS value in a rule. If you configure multiple CoS values in a rule, the rule cannot be issued.</i></p>
<b>service-vlan-id</b> <i>vlan-id-list</i>	<p>Specifies to match the packets of specified VLANs of the operator's network. The <i>vlan-id-list</i> argument is a list of VLAN IDs, in the form of <i>vlan-id</i> to <i>vlan-id</i> or multiple discontinuous VLAN IDs (separated by space). You can specify up to eight VLAN IDs for this argument at a time. VLAN ID is in the range 1 to 4094.</p> <p>In a class configured with the operator <b>and</b>, the logical relationship between the service VLAN IDs specified for the <b>service-vlan-id</b> keyword is <b>or</b>.</p>
<b>source-mac</b> <i>mac-address</i>	<p>Specifies to match the packets with a specified source MAC address.</p>

## Description

Use the **if-match** command to define a rule to match a specific type of packets.

Use the **undo if-match** command to remove a matching rule.



## Note

Suppose the logical relationship between classification rules is **and**. Note the following when using the **if-match** command to define matching rules.

- If multiple matching rules with the **acl** or **acl ipv6** keyword specified are defined in a class, the actual logical relationship between these rules is **or** when the policy is applied.
  - If multiple matching rules with the **customer-vlan-id** or **service-vlan-id** keyword specified are defined in a class, the actual logical relationship between these rules is **or** when the policy is applied.
- 

## Examples

# Define a rule for class1 to match the packets with their destination MAC addresses being 0050-ba27-bed3.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match destination-mac 0050-ba27-bed3
```

# Define a rule for class2 to match the packets with their source MAC addresses being 0050-ba27-bed2.

```
<Sysname> system-view
[Sysname] traffic classifier class2
[Sysname-classifier-class2] if-match source-mac 0050-ba27-bed2
```

# Define a rule for class3 to match the advanced IPv4 ACL 3101.

```
<Sysname> system-view
[Sysname] traffic classifier class3
[Sysname-classifier-class3] if-match acl 3101
```

# Define a rule for class4 to match the advanced IPv6 ACL 3101.

```
<Sysname> system-view
[Sysname] traffic classifier class4
[Sysname-classifier-class4] if-match acl ipv6 3101
```

# Define a rule for class5 to match all the packets.

```
<Sysname> system-view
[Sysname] traffic classifier class5
[Sysname-classifier-class5] if-match any
```

# Define a rule for class6 to match the packets with their DSCP precedence values being 1.

```
<Sysname> system-view
[Sysname] traffic classifier class6
[Sysname-classifier-class6] if-match dscp 1
```

# Define a rule for class7 to match the packets with their IP precedence values being 1.

```
<Sysname> system-view
[Sysname] traffic classifier class7
[Sysname-classifier-class7] if-match ip-precedence 1
```

# Define a rule for class8 to match IP packets.

```

<Sysname> system-view
[Sysname] traffic classifier class8
[Sysname-classifier-class8] if-match protocol ip

# Define a rule for class9 to match the packets with the customer network 802.1p precedence 2.

<Sysname> system-view
[Sysname] traffic classifier class9
[Sysname-classifier-class9] if-match customer-dot1p 2

# Define a rule for class10 to match the packets with the service provider network 802.1p precedence 5.

<Sysname> system-view
[Sysname] traffic classifier class10
[Sysname-classifier-class10] if-match service-dot1p 5

# Define a rule for class11 to match the packets of customer VLAN 1024.

<Sysname> system-view
[Sysname] traffic classifier class11
[Sysname-classifier-class11] if-match customer-vlan-id 1024

# Define a rule for class12 to match the packets of service VLAN 1000.

<Sysname> system-view
[Sysname] traffic classifier class12
[Sysname-classifier-class12] if-match service-vlan-id 1000

```

## traffic classifier

### Syntax

```

traffic classifier classifier-name [ operator { and | or } ]
undo traffic classifier classifier-name

```

### View

System view

### Default Level

2: System Level

### Parameters

**and**: Specifies the relationship among the rules in the class as logic AND. That is, a packet is matched only when it matches all the rules defined for the class.

**or**: Specifies the relationship among the rules in the class as logic OR. That is, a packet is matched if it matches a rule defined for the class.

*classifier-name*: Name of the class to be created.

### Description

Use the **traffic classifier** command to create a class. This command also leads you to class view.

Use the **undo traffic classifier** command to remove a class.

By default, a packet is matched only when it matches all the rules configured for the class.

## Examples

```
# Create a class named class 1.
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1]
```

# Traffic Behavior Configuration Commands

## accounting

### Syntax

```
accounting
undo accounting
```

### View

Traffic behavior view

### Default Level

2: System Level

### Parameters

None

### Description

Use the **accounting** command to configure the traffic accounting action for a traffic behavior.

Use the **undo accounting** command to remove the traffic accounting action.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

## Examples

```
# Configure the traffic accounting action for a traffic behavior.
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] accounting
```

## car

### Syntax

```
car cir committed-information-rate [ cbs committed-burst-size [ ebs excess-burst-size ] ] [ pir peak-information-rate ] [ green action ] [ red action ] [ yellow action ]
undo car
```

### View

Traffic behavior view

### Default Level

2: System Level

## Parameters

**cir** *committed-information-rate*: Specifies the committed information rate (CIR) in kbps. The *committed-information-rate* argument ranges from 64 to 32000000 and must be a multiple of 64.

**cbs** *committed-burst-size*: Specifies the committed burst size (CBS) in bytes. The *committed-burst-size* argument ranges from 4000 to 16000000, the default is 4000.

**ebs** *excess-burst-size*: Specifies excess burst size (EBS) in bytes. The *excess-burst-size* argument ranges from 0 to 16000000, the default is 4000.

**pir** *peak-information-rate*: Specifies the peak information rate (PIR) in kbps. The *peak-information-rate* argument ranges from 64 to 32000000 and must be a multiple of 64.

**green** *action*: Specifies the action to be conducted for the traffic conforming to CIR. The *action* argument can be:

- **discard**: Drops the packets.
- **pass**: Forwards the packets.
- **remark-dscp-pass** *new-dscp*: Marks the packets with a new DSCP precedence and forwards them to their destinations. The *new-dscp* argument is in the range 0 to 63.

By default, packets conforming to CIR are forwarded.

**red** *action*: Specifies the action to be conducted for the traffic conforms to neither CIR nor PIR. The *action* argument can be:

- **discard**: Drops the packets.
- **pass**: Forwards the packets.
- **remark-dscp-pass** *new-dscp*: Marks the packets with a new DSCP precedence and forwards them to their destinations. The *new-dscp* argument is in the range 0 to 63.

By default, packets conforming to neither CIR nor PIR are dropped.

**yellow** *action*: Specifies the action to be conducted for the traffic conforms to PIR but does not conform to CIR. The *action* argument can be:

- **discard**: Drops the packets.
- **pass**: Forwards the packets.
- **remark-dscp-pass** *new-dscp*: Marks the packets with a new DSCP precedence and forwards them to their destinations. The *new-dscp* argument is in the range 0 to 63.

By default, packets conforming to PIR but not conforming to CIR are forwarded.

## Description

Use the **car** command to configure TP action for a traffic behavior.

Use the **undo car** command to remove the TP action.

Note that, if you configure the TP action for a traffic behavior for multiple times, only the last configuration takes effect.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

## Examples

# Configure TP action for a traffic behavior. When the traffic rate is lower than 6400 kbps, packets are forwarded normally. When the traffic rate exceeds 6400 kbps, the packets beyond 6400 kbps are dropped.

```
<Sysname> system-view
```

```
[Sysname] traffic behavior database
[Sysname-behavior-database] car cir 6400 red discard
```

## display traffic behavior

### Syntax

```
display traffic behavior user-defined [ behavior-name ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*behavior-name*: Name of a user defined traffic behavior.

### Description

Use the **display traffic behavior** command to display the information about a user defined traffic behavior.

If no behavior name is provided, this command displays the information about all the user-defined behaviors.

### Examples

# Display the information about all the user defined traffic behaviors.

```
<Sysname> display traffic behavior user-defined
User Defined Behavior Information:
Behavior: test
Marking:
  Remark dot1p COS 4
Committed Access Rate:
  CIR 64 (kbps), CBS 4000 (byte), EBS 4000 (byte), PIR 640 (kbps)
Green Action: pass
Red Action: discard
Yellow Action: pass
```

**Table 1-3** display traffic behavior user-defined command output description

Field	Description
User Defined Behavior Information	The information about user defined traffic behaviors is displayed
Behavior	Name of a traffic behavior, which can be of multiple types
Marking	Information about priority marking
Committed Access Rate	Information about traffic rate limit
CIR	Committed information rate in bytes
CBS	Committed burst size in bytes

Field	Description
EBS	Excessive burst size in bytes
PIR	Peak information rate in bytes
Green Action	Action conducted to packets conforming to CIR
Red Action	Action conducted for packets conforming to neither CIR nor PIR
Yellow Action	Action conducted to packets conforming to PIR but not conforming to CIR

## filter

### Syntax

```
filter { deny | permit }
undo filter
```

### View

Traffic behavior view

### Default Level

2: System Level

### Parameters

**deny:** Drops packets.  
**permit:** Forwards packets.

### Description

Use the **filter** command to configure traffic filtering action for a traffic behavior.

Use the **undo filter** command to remove the traffic filtering action.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

### Examples

```
# Configure traffic filtering action for a traffic behavior.
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] filter deny
```

## nest

### Syntax

```
nest top-most vlan-id vlan-id
undo nest top-most
```

### View

Traffic behavior view

## Default Level

2: System Level

## Parameters

**vlan-id** *vlan-id*: ID of the VLAN. The *vlan-id* argument is in the range 1 to 4094.

## Description

Use the **nest** command to configure an outer VLAN tag for a traffic behavior.

Use the **undo nest** command to remove the outer VLAN tag.

Note that:

- The action of creating an outer VLAN tag cannot be configured simultaneously with any other action except the traffic filtering action or the action of setting 802.1p precedence in the same traffic behavior. And the action of creating an outer VLAN tag must be applied to basic QinQ-enabled ports or port groups. Otherwise, the corresponding QoS policy cannot be applied successfully.
- The **nest** action cannot be applied to a VLAN or globally.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

## Examples

# Configure an outer VLAN tag for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] nest top-most vlan-id 100
```

## redirect

### Syntax

```
redirect { cpu | interface interface-type interface-number | next-hop { ipv4-add [ ipv4-add ] | ipv6-add [ interface-type interface-number ] [ ipv6-add [ interface-type interface-number ] ] } }
```

```
undo redirect { cpu | interface interface-type interface-number | next-hop }
```

### View

Traffic behavior view

## Default Level

2: System Level

## Parameters

**cpu**: Redirects traffic to the CPU.

**interface** *interface-type interface-number*: Redirects traffic to an interface identified by its type and number.

**next-hop**: Specifies the next hop to redirect the traffic to.

*ipv4-add*: IPv4 address of the next hop.

*ipv6-add*: IPv6 address of the next hop. The *interface-type interface-number* argument is a VLAN interface number. If the IPv6 address is a link-local address, you must specify a VLAN interface for the

IPv6 address of the next hop; if the IPv6 address is not a link-local address, you need not specify a VLAN interface for the IPv6 address of the next hop.

### Description

Use the **redirect** command to configure traffic redirecting action for a traffic behavior.

Use the **undo redirect** command to remove the traffic redirecting action.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

### Examples

# Configure the redirecting action to redirect traffic to GigabitEthernet 1/0/1 port.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] redirect interface GigabitEthernet 1/0/1
```

## remark customer-vlan-id

### Syntax

**remark customer-vlan-id** *vlan-id-value*

**undo remark customer-vlan-id**

### View

Traffic behavior view

### Default Level

2: System Level

### Parameters

*vlan-id-value*: VLAN ID to be set for packets, in the range of 1 to 4094.

### Description

Use the **remark customer-vlan-id** command to configure the action of setting the customer network VLAN ID for a traffic behavior.

Use the **undo remark customer-vlan-id** command to remove the action of setting the customer network VLAN ID.

Note that the action of setting the customer network VLAN ID cannot be applied to a VLAN or applied globally.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

### Examples

# Configure the action of setting the customer network VLAN ID to 2 for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark customer-vlan-id 2
```

## remark dot1p

### Syntax

```
remark dot1p 8021p
undo remark dot1p
```

### View

Traffic behavior view

### Default Level

2: System Level

### Parameters

*8021p*: 802.1p precedence to be set for packets, in the range 0 to 7.

### Description

Use the **remark dot1p** command to configure the action of setting 802.1p precedence for a traffic behavior.

Use the **undo remark dot1p** command to remove the action of setting 802.1p precedence

Note that, when the **remark dot1p** command is used together with the **remark local-precedence** command, the 802.1p precedence to be set for packets must be the same as the local precedence to be set for packets. Otherwise, the corresponding policy cannot be applied successfully.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

### Examples

# Configure the action to set 802.1p precedence to 2 for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dot1p 2
```

## remark drop-precedence

### Syntax

```
remark drop-precedence drop-precedence-value
undo remark drop-precedence
```

### View

Traffic behavior view

### Default Level

2: System Level

### Parameters

*drop-precedence-value*: Drop precedence to be set for packets, in the range 0 to 2.

## Description

Use the **remark drop-precedence** command to configure the action of setting drop precedence for a traffic behavior.

Use the **undo remark drop-precedence** command to remove the action of setting drop precedence.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

## Examples

# Configure the action to set drop precedence to 2 for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark drop-precedence 2
```

## remark dscp

### Syntax

**remark dscp** *dscp-value*

**undo remark dscp**

### View

Traffic behavior view

### Default Level

2: System Level

### Parameters

*dscp-value*: DSCP precedence to be set for packets, in the range of 0 to 63. This argument can also be the keywords listed in [Table 1-4](#).

**Table 1-4** DSCP keywords and values

Keyword	DSCP value (binary)	DSCP value (decimal)
default	000000	0
af11	001010	10
af12	001100	12
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22
af31	011010	26
af32	011100	28
af33	011110	30
af41	100010	34
af42	100100	36

Keyword	DSCP value (binary)	DSCP value (decimal)
af43	100110	38
cs1	001000	8
cs2	010000	16
cs3	011000	24
cs4	100000	32
cs5	101000	40
cs6	110000	48
cs7	111000	56
ef	101110	46

### Description

Use the **remark dscp** command to configure the action of setting DSCP precedence for a traffic behavior.

Use the **undo remark dscp** command to remove the action of setting DSCP precedence.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

### Examples

# Configure the action to set DSCP precedence to 6 for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dscp 6
```

## remark ip-precedence

### Syntax

**remark ip-precedence** *ip-precedence-value*

**undo remark ip-precedence**

### View

Traffic behavior view

### Default Level

2: System Level

### Parameters

*ip-precedence-value*: IP precedence to be set for packets, in the range of 0 to 7.

### Description

Use the **remark ip-precedence** command to configure the action of setting IP precedence for a traffic behavior.

Use the **undo remark ip-precedence** command to remove the action of setting IP precedence.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

## Examples

```
# Configure the action to set IP precedence to 6 for a traffic behavior.
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark ip-precedence 6
```

## remark local-precedence

### Syntax

```
remark local-precedence local-precedence
undo remark local-precedence
```

### View

Traffic behavior view

### Default Level

2: System Level

### Parameters

*local-precedence*: Local precedence to be set for packets, in the range of 0 to 7.

### Description

Use the **remark local-precedence** command to configure the action of setting local precedence for a traffic behavior.

Use the **undo remark local-precedence** command to remove the action of remarking local precedence.

Note that, when the **remark dot1p** command is used together with the **remark local-precedence** command, the 802.1p precedence to be set for packets must be the same as the local precedence to be set for packets. Otherwise, the corresponding policy cannot be applied successfully.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

## Examples

```
# Configure the action to set local precedence to 2 for a traffic behavior.
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark local-precedence 2
```

## remark service-vlan-id

### Syntax

```
remark service-vlan-id vlan-id-value
undo remark service-vlan-id
```

## View

Traffic behavior view

## Default Level

2: System Level

## Parameters

*vlan-id-value*: VLAN ID to be set for packets, in the range of 1 to 4094.

## Description

Use the **remark service-vlan-id** command to configure the action of setting the service provider network VLAN ID for a traffic behavior.

Use the **undo remark service-vlan-id** command to remove the action of setting the service provider network VLAN ID.

Note that:

- If the **remark service-vlan-id** action will be applied to the inbound direction of a port or port group, any other actions except **filer** and **remark dot1p** cannot be configured in the traffic behavior.
- The **remark service-vlan-id** action cannot be applied to a VLAN or applied globally.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

## Examples

# Configure the action of setting the service provider network VLAN ID to 2 for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark service-vlan-id 2
```

## traffic behavior

### Syntax

**traffic behavior** *behavior-name*

**undo traffic behavior** *behavior-name*

### View

System view

### Default Level

2: System Level

### Parameters

*behavior-name*: Name of the traffic behavior to be created, a case-sensitive string of 1 to 31 characters. No spaces are allowed in a traffic behavior name.

### Description

Use the **traffic behavior** command to create a traffic behavior. This command also leads you to traffic behavior view.

Use the **undo traffic classifier** command to remove a traffic behavior.

Related commands: **qos policy**, **qos apply policy**, **classifier behavior**.

## Examples

```
# Define a traffic behavior named behavior1.  
<Sysname> system-view  
[Sysname] traffic behavior behavior1  
[Sysname-behavior-behavior1]
```

# QoS Policy Configuration Commands

## classifier behavior

### Syntax

```
classifier classifier-name behavior behavior-name [ mode do1q-tag-manipulation ]  
undo classifier classifier-name
```

### View

Policy view

### Default Level

2: System Level

### Parameters

*classifier-name*: Name of an existing class, a case-sensitive string of 1 to 31 characters. No spaces are allowed in a class name.

*behavior-name*: Name of an existing traffic behavior, a case-sensitive string of 1 to 31 characters. No spaces are allowed in a behavior name.

**mode dot1q-tag-manipulation**: Specifies that the classifier-behavior association is used for the many-to-one VLAN mapping function.

### Description

Use the **classifier behavior** command to associate a traffic behavior with a class.

Use the **undo classifier** command to remove a class from a policy.

Note that each class can be associated with only one traffic behavior.

Related commands: **qos policy**.



### Note

In a QoS policy with multiple class-to-traffic-behavior associations, if the action of creating an outer VLAN tag, the action of setting customer network VLAN ID, or the action of setting service provider network VLAN ID is configured in a traffic behavior, we recommend you not to configure any other action in this traffic behavior. Otherwise, the QoS policy may not function as expected after it is applied.

---

## Examples

```
# Associate the behavior named test with the class named database in the policy user1.
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1] classifier database behavior test
```

## display qos policy

### Syntax

```
display qos policy user-defined [ policy-name [ classifier classifier-name ] ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*policy-name*: Policy name, a case-sensitive string of 1 to 31 characters. No spaces are allowed in a policy name. If no policy is specified, the configuration of all user defined policies is displayed.

*classifier-name*: Name of a class in the policy, a case-sensitive string of 1 to 31 characters. No spaces are allowed in a class name. If no class is specified, all the classes in the policy are specified.

### Description

Use the **display qos policy** command to display the configuration of a user-defined policy, including the configuration of the classes and the associated traffic behaviors in the policy.

## Examples

```
# Display the configuration of all the user specified policies.
```

```
<Sysname> display qos policy user-defined
```

```
User Defined QoS Policy Information:
```

```
Policy: test
```

```
Classifier: test
```

```
Behavior: test
```

```
Accounting Enable
```

```
Committed Access Rate:
```

```
CIR 64 (kbps), CBS 4000 (byte), EBS 4000 (byte), PIR 640 (kbps)
```

```
Green Action: pass
```

```
Red Action: discard
```

```
Yellow Action: pass
```

**Table 1-5 display qos policy command output description**

Field	Description
Policy	Policy name
Classifier	Class name and the corresponding configuration information
Behavior	Traffic behavior name and the corresponding configuration information

## display qos policy global

### Syntax

```
display qos policy global [ slot slot-number ] [ inbound | outbound ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**inbound:** Displays the QoS policy applied globally in the inbound direction of all ports.

**outbound:** Displays the QoS policy applied globally in the outbound direction of all ports.

**slot *slot-number*:** Displays the global QoS policy configuration of the specified device in the IRF stack. If the *slot-number* argument is not specified, the global QoS policy configuration of all devices in the IRF stack is displayed. If no IRF stack is formed, the global QoS policy configuration of the current device is displayed. The range for the *slot-number* argument depends on the number of devices and the numbering of the devices in the IRF stack.

### Description

Use the **display qos policy global** command to display information about a global QoS policy.

### Examples

# Display information about the global QoS policy in the inbound direction.

```
<Sysname> display qos policy global inbound
```

```
Direction: Inbound
```

```
Policy: abc_policy
```

```
Classifier: abc
```

```
Operator: AND
```

```
Rule(s) : If-match dscp cs1
```

```
Behavior: abc
```

```
Committed Access Rate:
```

```
CIR 640 (kbps), CBS 4000 (byte), EBS 4000 (byte)
```

```
Green Action: pass
```

```
Red Action: discard
```

Yellow Action: pass

Green : 0(Packets)

**Table 1-6 display qos policy global** command output description

Field	Description
Direction	Direction in which the policy is applied globally
Policy	Policy name
Classifier	Class name <b>Failed</b> indicates that the policy is not successfully applied
Operator	Logical relationship between match criteria
Rule(s)	Match criteria
Behavior	Name and the corresponding configuration information of a behavior
Committed Access Rate	Rate limiting information
CIR	Committed information rate in kbps
CBS	Committed burst size in bytes, that is, the depth of the token bucket for holding burst traffic
EBS	Excess burst size in bytes, that is, the traffic exceeding CBS when two token buckets are used
Green Action	Action to conduct for green packets
Red Action	Action to conduct for red packets
Yellow Action	Action to conduct for yellow packets
Green	Traffic statistics on green packets

## display qos policy interface

### Syntax

```
display qos policy interface [ interface-type interface-number ] [ inbound | outbound ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*interface-type*: Port type.

*interface-number*: Port number.

**inbound**: Specifies the inbound direction.

**outbound**: Specifies the outbound direction.

## Description

Use the **display qos policy interface** command to display the configuration and statistics information about the policy applied on a port.

If no interface is provided, the configuration and statistics information about the policies applied on all the ports is displayed.

## Examples

# Display the configuration and statistics information about the policy applied to port GigabitEthernet 1/0/1.

```
<Sysname> display qos policy interface GigabitEthernet 1/0/1
```

```
Interface: GigabitEthernet1/0/1

Direction: Inbound

Policy: abc_policy
Classifier: abc
Operator: AND
Rule(s) : If-match dscp cs1
Behavior: abc
Committed Access Rate:
  CIR 64 (kbps), CBS 4000 (byte), EBS 4000 (byte)
Green Action: pass
Red Action: discard
Yellow Action: pass
Green : 0(Packets)
```

**Table 1-7** display qos policy interface command output description

Field	Description
Interface	Port name, comprising of port type and port number
Direction	Direction of the port where the policy is applied
Policy	Name and configuration information of the policy
Classifier	Name and configuration information of the class <b>Failed</b> indicates that the policy is not successfully applied
Operator	Logical relationship among the classification rules in a class
Rule(s)	Classification rules in the class
Behavior	Name and configuration information of the behavior

## display qos vlan-policy

### Syntax

```
display qos vlan-policy { name policy-name | vlan [ vlan-id ] } [ slot slot-number ] [ inbound | outbound ]
```

## View

Any view

## Default Level

1: Monitor level

## Parameters

**name** *policy-name*: Specifies to display the information about the VLAN policy with the specified name, a case-sensitive string of 1 to 31 characters. No spaces are allowed in a VLAN policy name.

**vlan** *vlan-id*: Specifies to display the information about the VLAN policy applied to the specified VLAN. If no VLAN ID is specified, the VLAN policy information of all VLANs is displayed.

*slot-number*: Specifies to display VLAN QoS policy information about the specified device in the IRF stack. If the *slot-number* argument is not specified, the VLAN QoS policy information of all devices in the IRF stack is displayed. If no IRF stack is formed, the VLAN QoS policy information of the current device is displayed. The range for the *slot-number* argument depends on the number of devices and the numbering of the devices in the IRF stack.

## Description

Use the **display qos vlan-policy** command to display the information about VLAN QoS policies.

## Examples

# Display the information about the VLAN QoS policy **test**.

```
<Sysname> display qos vlan-policy name test
Policy test
Vlan 300: inbound
```

**Table 1-8 display qos vlan-policy** command output description

Field	Description
Policy	Name of the VLAN policy
Vlan 300	ID of the VLAN where the VLAN policy is applied
inbound	VLAN policy is applied in the inbound direction of the VLAN.

# Display the information about the VLAN policy applied to VLAN 300.

```
<Sysname> display qos vlan-policy vlan 300

Vlan 300

Direction: Inbound

Policy: test
Classifier: test
Operator: AND
Rule(s) : If-match customer-vlan-id 3
Behavior: test
Accounting Enable:
```

```

0 (Packets)
Committed Access Rate:
  CIR 6400 (kbps), CBS 4000 (byte), EBS 4000 (byte)
Green Action: pass
Red Action: discard
Yellow Action: pass
Green : 0(Packets)

```

**Table 1-9 display qos vlan-policy command output description**

Field	Description
Vlan 300	ID of the VLAN where the VLAN policy is applied
Inbound	VLAN policy is applied in the inbound direction of the VLAN.
Classifier	Name of the class in the policy and its configuration
Operator	Logical relationship between classification rules
Rule(s)	Classification rules
Behavior	Name of the behavior in the policy and its configuration
Accounting	Traffic accounting action
Committed Access Rate	Rate limiting information
CIR	Committed information rate in kbps
CBS	Committed burst size in bytes, that is, the depth of the token bucket for holding burst traffic
EBS	Excess burst size in bytes, namely, the traffic exceeding CBS when two token buckets are used
Green Action	Action to conduct for green packets
Red Action	Action to conduct for red packets
Yellow Action	Action to conduct for yellow packets
Green	Traffic statistics about green packets

## qos apply policy

### Syntax

```

qos apply policy policy-name { inbound | outbound }
undo qos apply policy { inbound | outbound }

```

### View

Ethernet interface view, port group view

### Default Level

2: System Level

### Parameters

**inbound:** Specifies the inbound direction.

**outbound:** Specifies the outbound direction.

*policy-name:* Specifies a QoS policy name, a case-sensitive string of 1 to 31 characters. No spaces are allowed in a QoS policy name.

## Description

Use the **qos apply policy** command to apply a QoS policy on a port or a port group.

Use the **undo qos apply policy** command to remove the policy applied on a port or a port group.

When you apply a policy by using the **qos apply policy** command, whether or not the **inbound/outbound** keyword can take effect depends on the actions defined in the traffic behavior, as described in [Table 1-10](#).

**Table 1-10** The support for the inbound direction and the outbound direction

Action	Inbound	Outbound
Traffic accounting	Supported	Supported
TP	Supported	Supported
Traffic filtering	Supported	Supported
Traffic mirroring	Supported	Supported
Configuring the outer VLAN tag	Supported	Not supported
Traffic redirecting	Supported	Not supported
Remarking the customer network VLAN ID for packets	Not supported	Supported
Remarking the 802.1p precedence for packets	Supported	Supported
Remarking the drop precedence for packets	Supported	Not supported
Remarking the DSCP precedence for packets	Supported	Supported
Remarking the IP precedence for packets	Supported	Supported
Remarking the local precedence for packets	Supported	Not supported
Remarking the service provider network VLAN ID for packets	Supported	Supported

## Examples

# Apply the policy named test in the inbound direction of GigabitEthernet1/0/1 port.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos apply policy test inbound
```

## qos apply policy global

### Syntax

```
qos apply policy policy-name global { inbound | outbound }
```

```
undo qos apply policy global { inbound | outbound }
```

## View

System view

## Default Level

2: System Level

## Parameters

*policy-name*: Policy name, a case-sensitive string of 1 to 31 characters. No spaces are allowed in a QoS policy name.

**inbound**: Applies the QoS policy to the incoming packets on all ports.

**outbound**: Applies the QoS policy to the outgoing packets on all ports.

## Description

Use the **qos apply policy global** command to apply a QoS policy globally. A QoS policy applied globally takes effect on all inbound or outbound traffic depending on the direction in which the policy is applied.

Use the **undo qos apply policy global** command to cancel the global application of the QoS policy.

Note that, when you apply a QoS policy with the **qos apply policy global** command, support for the **inbound/outbound** keyword depends on the actions defined in the traffic behavior, as described in [Table 1-10](#).

## Examples

# Apply the QoS policy **user1** in the inbound direction globally.

```
<Sysname> system-view  
[Sysname] qos apply policy user1 global inbound
```

## qos policy

### Syntax

**qos policy** *policy-name*

**undo qos policy** *policy-name*

### View

System view

### Default Level

2: System Level

### Parameters

*policy-name*: Name of the policy to be created, a case-sensitive string of 1 to 31 characters. No spaces are allowed in a policy name.

### Description

Use the **qos policy** command to create a policy. This command also leads you to policy view.

Use the **undo qos policy** command to remove a policy.

To remove a policy that is currently applied on a port, you need to disable it on the port first.

Related commands: **classifier behavior**, **qos apply policy**.

## Examples

```
# Create a policy named user1.  
<Sysname> system-view  
[Sysname] qos policy user1  
[Sysname-qospolicy-user1]
```

## qos vlan-policy

### Syntax

```
qos vlan-policy policy-name vlan vlan-id-list { inbound | outbound }  
undo qos vlan-policy vlan vlan-id-list { inbound | outbound }
```

### View

System view

### Default Level

2: System Level

### Parameters

*policy-name*: Policy name, a case-sensitive string of 1 to 31 characters. No spaces are allowed in a policy name.

*vlan-id-list*: List of VLAN IDs, presented in the form of *vlan-id* **to** *vlan-id* or discontinuous VLAN IDs. Up to eight VLAN IDs can be specified at a time.

**inbound**: Specifies to apply the VLAN policy in the inbound direction of the VLAN.

**outbound**: Specifies to apply the VLAN policy in the outbound direction of the VLAN.

### Description

Use the **qos vlan-policy** command to apply the VLAN policy to the specific VLAN(s).

Use the **undo qos vlan-policy** command to remove the VLAN policy from the specific VLAN(s).

Note that, when you apply a QoS policy with the **qos vlan-policy** command, support for the **inbound/outbound** keyword varies with the actions defined in the traffic behavior, as described in [Table 1-10](#).



#### Note

Do not apply policies to a VLAN and the ports in the VLAN at the same time.

---

## Examples

```
# Apply the VLAN policy named test in the inbound direction of VLAN 200, VLAN 300, VLAN 400, VLAN 500, VLAN 600, VLAN 700, VLAN 800, and VLAN 900.
```

```
<Sysname> system-view
[Sysname] qos vlan-policy test vlan 200 300 400 500 600 700 800 900 inbound
```

## reset qos policy global

### Syntax

```
reset qos policy global [ inbound | outbound ]
```

### View

User view

### Default Level

1: Monitor level

### Parameters

**inbound**: Specifies the inbound direction.

**outbound**: Specifies the outbound direction.

### Description

Use the **reset qos vlan-policy** command to clear the statistics of a global QoS policy. If no direction is specified, all global QoS policy statistics are cleared.

### Examples

# Clear the statistics of the global QoS policy in the inbound direction.

```
<Sysname> reset qos policy global inbound
```

## reset qos vlan-policy

### Syntax

```
reset qos vlan-policy [ vlan vlan-id ] [ inbound | outbound ]
```

### View

User view

### Default Level

1: Monitor level

### Parameters

*vlan-id*: VLAN ID, in the range 1 to 4,094.

**inbound**: Clears the QoS policy statistics in the inbound direction of the specified VLAN.

**outbound**: Clears the QoS policy statistics in the outbound direction of the specified VLAN.

### Description

Use the **reset qos vlan-policy** command to clear the statistics information about VLAN QoS policies. If no VLAN ID is specified, QoS policy statistics of all VLANs are cleared.

## Examples

# Clear the statistics information about the QoS policy applied to VLAN 2.

```
<Sysname> reset qos vlan-policy vlan 2
```

# 2 Priority Mapping Configuration Commands

---

## Priority Mapping Table Configuration Commands

### display qos map-table

#### Syntax

```
display qos map-table [ dot1p-dp | dot1p-lp | dscp-dot1p | dscp-dp | dscp-dscp ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

**dot1p-lp**: Specifies the 802.1p precedence-to-local precedence mapping table.

**dot1p-dp**: Specifies the 802.1p precedence-to-drop precedence mapping table.

**dscp-dp**: Specifies the DSCP-to-drop precedence mapping table.

**dscp-dot1p**: Specifies the DSCP-to-802.1p precedence mapping table.

**dscp-dscp**: Specifies the DSCP-to-DSCP mapping table.

#### Description

Use the **display qos map-table** command to display the configuration of a priority mapping table.

If the type of the priority mapping table is not specified, the configuration of all the priority mapping tables is displayed.

Related commands: **qos map-table**.

#### Examples

```
# Display the configuration of the 802.1p precedence-to-drop precedence mapping table.
```

```
<Sysname> display qos map-table dot1p-dp
MAP-TABLE NAME: dot1p-dp   TYPE: pre-define
IMPORT   :   EXPORT
  0     :     2
  1     :     2
  2     :     2
  3     :     1
  4     :     1
  5     :     1
  6     :     0
  7     :     0
```

**Table 2-1 display qos map-table command output description**

Field	Description
MAP-TABLE NAME	Name of the mapping table
TYPE	Type of the mapping table
IMPORT	Input entries of the mapping table
EXPORT	Output entries of the mapping table

## qos map-table

### Syntax

```
qos map-table { dot1p-dp | dot1p-lp | dscp-dot1p | dscp-dp | dscp-dscp }
```

### View

System view

### Default Level

2: System Level

### Parameters

**dot1p-lp**: Specifies the 802.1p precedence-to-local precedence mapping table.

**dot1p-dp**: Specifies the 802.1p precedence-to-drop precedence mapping table.

**dscp-dp**: Specifies the DSCP-to-drop precedence mapping table.

**dscp-dot1p**: Specifies the DSCP-to-802.1p precedence mapping table.

**dscp-dscp**: Specifies the DSCP-to-DSCP mapping table.

### Description

Use the **qos map-table** command to enter specific priority mapping table view.

Related commands: **display qos map-table**.

### Examples

```
# Enter 802.1p precedence-to-drop precedence mapping table view.
```

```
<Sysname> system-view
[Sysname] qos map-table dot1p-dp
[Sysname-maptbl-dot1p-dp]
```

## import

### Syntax

```
import import-value-list export export-value
```

```
undo import { import-value-list | all }
```

### View

Priority mapping table view

## Default Level

2: System Level

## Parameters

*import-value-list*: List of input parameters, in the range of 0 to 7.

*export-value*: Output parameter in the mapping table, in the range of 0 to 2.

**all**: Removes all the parameters in the priority mapping table.

## Description

Use the **import** command to configure entries for a priority mapping table, that is, to define one or more mapping rules.

Use the **undo import** command to restore specific entries of a priority mapping table to the default.

Note that, you cannot configure to map any DSCP value to drop precedence 1.

Related commands: **display qos map-table**.

## Examples

# Configure the 802.1p precedence-to-drop precedence mapping table to map 802.1p precedence 4 and 5 to drop precedence 1.

```
<Sysname> system-view
[Sysname] qos map-table dot1p-dp
[Sysname-maptbl-dot1p-dp] import 4 5 export 1
```

# Port Priority Configuration Commands

## qos priority

### Syntax

**qos priority** *priority-value*

**undo qos priority**

### View

Ethernet interface view, port group view

### Default Level

2: System Level

### Parameters

*priority-value*: Port priority to be configured. This argument is in the range 0 to 7.

### Description

Use the **qos priority** command to set the port priority for a port.

Use the **undo qos priority** command to restore the default port priority.

By default, the port priority is 0.

Note that, if a port receives packets without an 802.1q tag, the switch takes the priority of the receiving port as the 802.1p precedence of the packets and then searches the **dot1p-dp/ip** mapping table for the local/drop precedence for the packets according to the priority of the receiving port.

## Examples

```
# Set the port priority of GigabitEthernet1/0/1 port to 2.
```

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos priority 2
```

## Port Priority Trust Mode Configuration Commands

### display qos trust interface

#### Syntax

```
display qos trust interface [ interface-type interface-number ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

*interface-type*: Port type.

*interface-number*: Port number.

#### Description

Use the **display qos trust interface** command to display the port priority trust mode of a port.

If no port is specified, this command displays the port priority trust modes of all the ports.

## Examples

```
# Display the port priority trust mode of GigabitEthernet1/0/1 port.
```

```
<Sysname> display qos trust interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
Port priority information
Port priority :0
Port priority trust type : dscp
```

**Table 2-2** display qos trust interface command output description

Field	Description
Interface	Port name, comprising of port type and port number
Port priority	Port priority

Field	Description
Port priority trust type	Port priority trust mode <ul style="list-style-type: none"> <li>• dscp indicates that the DSCP precedence of the received packets is trusted</li> <li>• dot1p indicates that the 802.1p precedence of the received packets is trusted</li> <li>• untrust indicates that the port priority is trusted</li> </ul>

## qos trust

### Syntax

```
qos trust { dot1p | dscp }
undo qos trust
```

### View

Ethernet interface view, port group view

### Default Level

2: System Level

### Parameters

**dscp**: Specifies to trust DSCP precedence carried in the packet and adopt this priority for priority mapping.

**dot1p**: Specifies to trust 802.1p precedence carried in the packet and adopt this priority for priority mapping.

### Description

Use the **qos trust** command to configure the port priority trust mode.

Use the **undo qos trust** command to restore the default port priority trust mode.

By default, the port priority is trusted.

### Examples

# Specify to trust the DSCP precedence carried in packets on GigabitEthernet1/0/1 port.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos trust dscp
```

# 3 Traffic Shaping and Line Rate Configuration Commands

---

## Traffic Shaping Configuration Commands

### display qos gts interface

#### Syntax

**display qos gts interface** [ *interface-type interface-number* ]

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

*interface-type*: Port type.

*interface-number*: Port number.

#### Description

Use the **display qos gts interface** command to display traffic shaping configuration information. If no port is specified, traffic shaping configuration information of all ports is displayed.

#### Examples

# Display traffic shaping configuration information of all ports.

```
<Sysname> display qos gts interface
Interface: GigabitEthernet1/0/1
Rule(s): If-match queue 2
CIR 640 (kbps), CBS 40960 (byte)
```

**Table 3-1 display qos gts command output description**

Field	Description
Interface	Port name identified by port type and port number
Rule(s)	Match criteria. "If-match queue 2" indicates that traffic shaping is performed for traffic in queue 2.
CIR	Committed information rate (CIR) in kbps
CBS	Committed burst size (CBS) in bytes

## qos gts

### Syntax

```
qos gts queue queue-number cir committed-information-rate [ cbs committed-burst-size ]  
undo qos gts queue queue-number
```

### View

Ethernet interface view, port group view

### Default Level

2: System level

### Parameters

**queue** *queue-number*: Specifies a queue by its number, which ranges from 0 to 7.

**cir** *committed-information-rate*: Specifies the committed information rate (CIR) in kbps, which must be a multiple of 64, and CIR ranges from 64 to 16777216.

**cbs** *committed-burst-size*: Specifies the CBS (in bytes), which ranges from 4096 to 16777216 and must be a multiple of 4096.

If the **cbs** keyword is not specified, the default CBS is  $62.5 \text{ ms} \times \textit{committed-information-rate}$  and must be a multiple of 4096. If  $62.5 \text{ ms} \times \textit{committed-information-rate}$  is not a multiple of 4096, the default CBS is the multiple of 4096 that is bigger than and nearest to  $62.5 \text{ ms} \times \textit{committed-information-rate}$ . The maximum CBS is 16777216. For example, if the CIR is 640 kbps, then  $62.5 \text{ ms} \times \text{CIR}$  is  $62.5 \text{ ms} \times 640 = 40000$ . As 40000 is not a multiple of 4096, 40960, which is the multiple of 4096 that is bigger than and nearest to 40000, is taken as the default CBS.

### Description

Use the **qos gts** command to configure traffic shaping.

Use the **undo qos gts** command to remove the traffic shaping configuration.

In Ethernet interface view, the configuration takes effect on the current port. In port group view, the configuration takes effect on all ports in the port group.

### Examples

```
# Configure traffic shaping on GigabitEthernet 1/0/1 to limit the outgoing traffic rate of queue 2 to 640 kbps.
```

```
<Sysname> system-view  
[Sysname] interface GigabitEthernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] qos gts queue 2 cir 640
```

## Line Rate Configuration Commands

### display qos lr interface

#### Syntax

```
display qos lr interface [ interface-type interface-number ]
```

## View

Any view

## Default Level

1: Monitor level

## Parameters

*interface-type*: Port type.

*interface-number*: Port number.

## Description

Use the **display qos lr interface** command to display the line rate configuration information of the specified port or all ports if no port is specified.

## Examples

# Display the line rate configuration and statistics information of all the interfaces.

```
<Sysname> display qos lr interface
Interface: GigabitEthernet1/0/1
Direction: Outbound
CIR 6400 (kbps), CBS 400000 (byte)
```

**Table 3-2 display qos lr command output description**

Field	Description
Interface	Port name, composed of port type and port number
Direction	Specify the direction of limited rate as outbound
CIR	Committed information rate, in kbps
CBS	Committed burst size, in byte

## qos lr outbound

### Syntax

```
qos lr outbound cir committed-information-rate [ cbs committed-burst-size ]
undo qos lr outbound
```

### View

Ethernet interface view, port group view

### Default Level

2: System Level

### Parameters

**outbound**: Limits the rate of the outbound traffic.

**cir** *committed-information-rate*: Specifies the committed information rate (CIR) in kbps. The range of CIR varies with port types as follows:

- GigabitEthernet port: 64 to 1000000
- Ten-GigabitEthernet port: 64 to 10000000

Note that the *committed-information-rate* argument must be a multiple of 64.

**cbs** *committed-burst-size*: Specifies the committed burst size in bytes.

- The *committed-burst-size* argument ranges from 4000 to 16000000.
- If the **cbs** keyword is not used, the system uses the default committed burst size, that is, 62.5 ms x *committed-information-rate*, or 16000000 if the multiplication is more than 16000000.

## Description

Use the **qos lr outbound** command to limit the rate of outbound traffic via physical interfaces.

Use the **undo qos lr outbound** command to cancel the limit.

## Examples

# Limit the outbound traffic rate on GigabitEthernet 1/0/1 within 640 kbps.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos lr outbound cir 640
```

# 4 Congestion Management Configuration

## Commands

---

### Congestion Management Configuration Commands

#### display qos sp interface

##### Syntax

```
display qos sp interface [ interface-type interface-number ]
```

##### View

Any view

##### Default Level

1: Monitor level

##### Parameters

*interface-type*: Port type.

*interface-number*: Port number.

##### Description

Use the **display qos sp interface** command to display the strict priority (SP) queuing configuration on a specified port.

If no port is specified, this command displays the SP queuing configuration on all ports.

Related commands: **qos sp**.

##### Examples

```
# Display the SP queuing configuration on GigabitEthernet 1/0/1.
```

```
<Sysname> display qos sp interface GigabitEthernet 1/0/1
```

```
Interface: GigabitEthernet1/0/1
```

```
Output queue: Strict-priority queue
```

#### display qos wfq interface

##### Syntax

```
display qos wfq interface [ interface-type interface-number ]
```

##### View

Any view

## Default Level

1: Monitor level

## Parameters

*interface-type*: Port type.

*interface-number*: Port number.

## Description

Use the **display qos wfq interface** command to display the configuration of Weighted Fair Queuing (WFQ) queues of a port.

If no port number is specified, the command displays the configurations of WFQ queues of all ports.

Related commands: **qos wfq**.

## Examples

# Display the configuration of the WFQ queues on port GigabitEthernet 1/0/1.

```
<Sysname> display qos wfq interface GigabitEthernet 1/0/1
```

```
Interface: GigabitEthernet1/0/1
```

```
Output queue: Hardware weighted fair queue
```

Queue ID	Weight	Min-Bandwidth
0	1	64
1	2	64
2	4	64
3	6	64
4	8	64
5	10	64
6	12	64
7	14	64

**Table 4-1 display qos wfq interface** command output description

Field	Description
Interface	Port name, composed of port type and port number
Output queue	The type of the current output queue
Queue ID	ID of the queue
Weight	The weight of each queue during scheduling.
Min-Bandwidth	Minimum guaranteed bandwidth of the queue

## display qos wrr interface

### Syntax

```
display qos wrr interface [ interface-type interface-number ]
```

## View

Any view

## Default Level

1: Monitor level

## Parameters

*interface-type*: Port type.

*interface-number*: Port number.

## Description

Use the **display qos wrr interface** command to display the configuration of weighted round robin (WRR) queues of a port.

If no port number is specified, the command displays the configurations of WRR queues of all ports.

Related commands: **qos wrr**.

## Examples

# Display the configuration of WRR queues of GigabitEthernet 1/0/1.

```
<Sysname> display qos wrr interface GigabitEthernet 1/0/1
```

```
Interface: GigabitEthernet1/0/1
```

```
Output queue: Weighted round robin queue
```

```
Queue ID    Group    Weight
```

```
-----
```

```
0           sp      N/A
1           sp      N/A
2           1       3
3           1       4
4           1       5
5           1       6
6           1       7
7           1       8
```

**Table 4-2 display qos wrr interface** command output description

Field	Description
Interface	Port name, composed of port type and port number
Output queue	The type of the current output queue
Queue ID	ID of the queue
Group	Group ID, indicating which group a queue belongs to.
Weight	The weight of each queue during scheduling. N/A indicates that SP queue scheduling algorithm is adopted.

## qos bandwidth queue

### Syntax

```
qos bandwidth queue queue-id min bandwidth-value  
undo qos bandwidth queue queue-id [min bandwidth-value ]
```

### View

Ethernet interface view, port group view

### Default Level

2: System level

### Parameters

*queue-id*: Queue ID, in the range of 0 to 7.

*bandwidth-value*: Minimum guaranteed bandwidth (in kbps), that is, the minimum bandwidth guaranteed for a queue when the port is congested. The range for the *bandwidth-value* argument is 64 to 1048576.

### Description

Use the **qos bandwidth queue** command to set the minimum guaranteed bandwidth for a specified queue on the port or ports in the port group.

Use the **undo qos bandwidth queue** command to remove the configuration.

By default, the minimum guaranteed bandwidth of a queue is 64 kbps.

Note that:

- In Ethernet interface view, the configuration takes effect only on the current port; in port group view, the configuration takes effect on all ports in the port group.
- To configure minimum guaranteed bandwidth for queues on a port/port group, enable WFQ on the port/port group first.

### Examples

```
# Set the minimum guaranteed bandwidth to 100 kbps for queue 0 on GigabitEthernet 1/0/1.
```

```
<Sysname> system-view  
[Sysname] interface GigabitEthernet 1/0/1  
[Sysname-GigabitEthernet 1/0/1] qos wfq  
[Sysname-GigabitEthernet 1/0/1] qos bandwidth queue 0 min 100
```

## qos sp

### Syntax

```
qos sp  
undo qos sp
```

### View

Ethernet interface view, port group view

## Default Level

2: System Level

## Parameters

None

## Description

Use the **qos sp** command to configure SP queuing on the current port.

Use the **undo qos sp** command to restore the default queuing algorithm on the port.

By default, all the ports adopt the WRR queue scheduling algorithm, with the weight values assigned to queue 0 through queue 7 being 1, 2, 3, 4, 5, 9, 13, and 15.

Related commands: **display qos sp interface**.

## Examples

```
# Configure SP queuing on GigabitEthernet1/0/1.  
<Sysname> system-view  
[Sysname] interface GigabitEthernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] qos sp
```

## qos wfq

### Syntax

**qos wfq**

**undo qos wfq**

### View

Ethernet interface view, port group view

## Default Level

2: System Level

## Parameters

None

## Description

Use the **qos wfq** command to enable weighted fair queuing (WFQ) on a port or port group.

Use the **undo qos wfq** command to restore the default.

By default, all the ports adopt the WRR queue scheduling algorithm, with the weight values assigned to queue 0 through queue 7 being 1, 2, 3, 4, 5, 9, 13, and 15.

Related commands: **display qos wrr interface**.

## Examples

```
# Enable WFQ on GigabitEthernet 1/0/1.  
<Sysname> system-view  
[Sysname] interface GigabitEthernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] qos wfq
```

## qos wfq weight

### Syntax

```
qos wfq queue-id weight schedule-value  
undo qos wfq queue-id weight
```

### View

Ethernet interface view, port group view

### Default Level

2: System Level

### Parameters

*queue-id*: ID of the queue, in the range of 0 to 7.

**weight** *schedule-value*: Specifies the scheduling weight of a queue, ranges from 0 to 15, and each queue is allocated with part of the allocable bandwidth based on its scheduling weight.

### Description

Use the **qos wfq** command to enable weighted fair queuing (WFQ) on a port or port group and configure a scheduling weight for the specified queue.

Use the **undo qos wfq** command to restore the default.

On a WFQ-enable port/port group, the scheduling weight of a queue is 1 by default.

Related commands: **display qos wfq interface**, **qos bandwidth queue**.

### Examples

# Enable WFQ on GigabitEthernet 1/0/1 and assign weight values 1, 2, 4, 6, 8, 10, 12, and 14 to queues 0 through 7.

```
<Sysname> system-view  
[Sysname] interface GigabitEthernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] qos wfq  
[Sysname-GigabitEthernet1/0/1] qos wfq 0 weight 1  
[Sysname-GigabitEthernet1/0/1] qos wfq 1 weight 2  
[Sysname-GigabitEthernet1/0/1] qos wfq 2 weight 4  
[Sysname-GigabitEthernet1/0/1] qos wfq 3 weight 6  
[Sysname-GigabitEthernet1/0/1] qos wfq 4 weight 8  
[Sysname-GigabitEthernet1/0/1] qos wfq 5 weight 10  
[Sysname-GigabitEthernet1/0/1] qos wfq 6 weight 12  
[Sysname-GigabitEthernet1/0/1] qos wfq 7 weight 14
```

## qos wrr

### Syntax

```
qos wrr  
undo qos wrr
```

## View

Ethernet interface view, port group view

## Default Level

2: System Level

## Parameters

None

## Description

Use the **qos wrr** command to enable weighted round robin (WRR) on a port or port group.

Use the **undo qos wrr** command to restore the default.

By default, all the ports adopt the WRR queue scheduling algorithm, with the weight values assigned to queue 0 through queue 7 being 1, 2, 3, 4, 5, 9, 13, and 15.

Related commands: **display qos wrr interface**.

## Examples

```
# Enable WRR on GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr
```

## qos wrr group

### Syntax

```
qos wrr queue-id group { sp | group-id weight schedule-value }
undo qos wrr
```

### View

Ethernet interface view, port group view

### Default Level

2: System Level

### Parameters

*queue-id*: ID of the queue, in the range of 0 to 7.

*group-id*: It can only be 1.

**weight** *schedule-value*: Specifies the scheduling weight of a queue, rang from 1 to 15.

**sp**: Configures SP queuing.

### Description

Use the **qos wrr** command to configure Weighted Round Robin (WRR) queue scheduling algorithm or the SP + WRR queue scheduling algorithm on a port or port group.

Use the **undo qos wrr** command to restore the default queue-scheduling algorithm on the port.

By default, all the ports adopt the WRR queue scheduling algorithm, with the weight values assigned to queue 0 through queue 7 being 1, 2, 3, 4, 5, 9, 13, and 15.

As required, you can configure part of the queues on the port to adopt the SP queue-scheduling algorithm and parts of queues to adopt the WRR queue-scheduling algorithm. Through adding the queues on a port to the SP scheduling group and WRR scheduling group (namely, group 1), the SP + WRR queue scheduling is implemented. During the queue scheduling process, the queues in the SP scheduling group is scheduled preferentially. When no packet is to be sent in the queues in the SP scheduling group, the queues in the WRR scheduling group are scheduled. The queues in the SP scheduling group are scheduled according to the strict priority of each queue, while the queues in the WRR queue scheduling group are scheduled according the weight value of each queue.

Related commands: **display qos wrr interface**.

## Examples

# Configure SP+WRR queue scheduling algorithm on GigabitEthernet 1/0/1 as follows: assign queue 0, queue 1, queue 2, and queue 3 to the SP scheduling group; and assign queue 4, queue 5, queue 5, and queue 7 to WRR scheduling group, with the weight 2, 4, 6, and 8.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr
[Sysname-GigabitEthernet1/0/1] qos wrr 0 group sp
[Sysname-GigabitEthernet1/0/1] qos wrr 1 group sp
[Sysname-GigabitEthernet1/0/1] qos wrr 2 group sp
[Sysname-GigabitEthernet1/0/1] qos wrr 3 group sp
[Sysname-GigabitEthernet1/0/1] qos wrr 4 group 1 weight 2
[Sysname-GigabitEthernet1/0/1] qos wrr 5 group 1 weight 4
[Sysname-GigabitEthernet1/0/1] qos wrr 6 group 1 weight 6
[Sysname-GigabitEthernet1/0/1] qos wrr 7 group 1 weight 8
```

# 5 Congestion Avoidance Configuration Commands

---

## Congestion Avoidance Configuration Commands

### display qos wred interface

#### Syntax

```
display qos wred interface [ interface-type interface-number ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

*interface-type*: Port type.

*interface-number*: Port number.

#### Description

Use the **display qos wred interface** command to display the WRED configuration of a port.

If no port number is specified, the command displays the WRED configurations of all ports.

Related commands: **qos wred apply**.

#### Examples

```
# Display the WRED configuration of GigabitEthernet 1/0/1.
```

```
<Sysname> display qos wred interface GigabitEthernet 1/0/1
```

```
Interface: GigabitEthernet1/0/1
```

```
Current WRED configuration:
```

```
Applied WRED table name: queue-table1
```

### display qos wred table

#### Syntax

```
display qos wred table [ table-name ]
```

#### View

Any view

#### Default Level

1: Monitor level

## Parameters

*table-name*: Name of the WRED table to be displayed, a string of 1 to 32 characters.

## Description

Use the **display qos wred table** command to display the WRED table configuration information.

If no WRED table name is specified, the configuration of all the WRED tables is displayed.

Related commands: **queue**.

## Examples

# Display the configuration of WRED table queue-table1.

```
<Sysname> display qos wred table queue-table1
```

```
Table Name: queue-table1
```

```
Table Type: Queue based WRED
```

```
QID:  gmin  gmax  gprob  ymin  ymax  yprob
```

```
-----  
0   10   NA   10   10   NA   10  
1   10   NA   10   10   NA   10  
2   10   NA   10   10   NA   10  
3   10   NA   10   10   NA   10  
4   10   NA   10   10   NA   10  
5   10   NA   10   10   NA   10  
6   10   NA   10   10   NA   10  
7   10   NA   10   10   NA   10
```

**Table 5-1** display qos wred table command output description

Field	Description
Table name	Name of a WRED table
Table type	Type of a WRED table
QID	ID of the queue
gmin	Lower threshold configured for green packets, whose drop precedence is 0
gmax	Upper threshold configured for green packets, whose drop precedence is 0
gprob	Drop probability slope configured for green packets, whose drop precedence is 0
ymin	Lower threshold configured for yellow packets, whose drop precedence is 1
ymax	Upper threshold configured for yellow packets, whose drop precedence is 1
yprob	Drop probability slope configured for yellow packets, whose drop precedence is 1

## qos wred apply

### Syntax

```
qos wred apply table-name
```

```
undo qos wred apply
```

## View

Ethernet interface view, port group view

## Default Level

2: System Level

## Parameters

*table-name*: Name of a global WRED table, a string of 1 to 32 characters.

## Description

Use the **qos wred apply** command to apply a WRED table to the current port or port group.

Use the **undo qos wred apply** command to cancel the application.

By default, no WRED table is applied to any port or port group.

Related commands: **display qos wred interface**.

## Examples

```
# Apply the WRED table queue-table1 to port GigabitEthernet 1/0/1.
```

```
<Sysname> system-view
```

```
[Sysname] interface GigabitEthernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] qos wred apply queue-table1
```

## qos wred queue table

### Syntax

```
qos wred queue table table-name
```

```
undo qos wred table table-name
```

### View

System view

### Default Level

2: System Level

### Parameters

**table** *table-name*: Specifies a name for the table, a string of 1 to 32 characters.

### Description

Use the **qos wred queue table** command to create a WRED table and enter WRED table view.

Use the **undo qos wred table** command to remove a WRED table.

By default, no WRED table is created.

A WRED table in use cannot be removed.

Related commands: **queue**.

### Examples

```
# Create a WRED table named queue-table1.
```

```
<Sysname> system-view
[Sysname] qos wred queue table queue-table1
[Sysname-wred-table-queue-table1]
```

## queue

### Syntax

```
queue queue-id [ drop-level drop-level ] low-limit low-limit [ discard-probability discard-prob ]
undo queue { queue-id | all }
```

### View

WRED table view

### Default Level

2: System Level

### Parameters

*queue-id*: ID of the queue, in the range of 0 to 7.

**drop-level** *drop-level*: Specifies a drop level, in the range of 0 to 1. If this argument is not specified, the subsequent configuration takes effect on the packets in the queue regardless of the drop level.

**low-limit** *low-limit*: Specifies a lower threshold. When the queue length exceeds the lower threshold, WRED begins to drop packets. The *low-limit* argument ranges from 0 to 100 and defaults to 10.

**discard-probability** *discard-prob*: Specifies the *discard-prob* argument, which ranges from 0 to 128 and defaults to 10. Each drop level is configured with an independent drop probability.

The actual drop probability is the reciprocal of the *discard-prob* argument. The argument corresponds to the drop probability as follows:

- 0 corresponds to 100%
- 1 through 8 corresponds to 1/8
- 9 through 16 corresponds to 1/16
- 17 through 32 corresponds to 1/32
- 33 through 64 corresponds to 1/64
- 65 through 128 corresponds to 1/128

### Description

Use the **queue** command to configure the drop-related parameters for a specified queue in the WRED table.

Use the **undo queue** command to restore the default.

By default, the lower threshold is 10 and the *discard-prob* argument is 10 for all the drop levels in the WRED table.

Related commands: **qos wred queue table**.

### Examples

```
# Modify drop parameters for queue 1 in the WRED table queue-table1: set the lower threshold to 10
and the discard-prob argument to 30 for packets with drop level 1 in queue 1.
```

```
<Sysname> system-view
```

```
[Sysname] qos wred queue table queue-table1
```

```
[Sysname-wred-table-queue-table1] queue 1 drop-level 1 low-limit 10 discard-probability 30
```

# 6 Traffic Mirroring Configuration Commands

---

## Traffic Mirroring Configuration Commands

### mirror-to

#### Syntax

```
mirror-to { cpu | interface interface-type interface-number }  
undo mirror-to { cpu | interface interface-type interface-number }
```

#### View

Traffic behavior view

#### Default Level

2: System Level

#### Parameters

**cpu**: Redirects packets to the CPU.

**interface** *interface-type interface-number*: Port type and port number of the destination port for the traffic mirroring action.

#### Description

Use the **mirror-to** command to configure traffic mirroring action for a traffic behavior.

Use the **undo mirror-to** command to remove the traffic mirroring action.

Note that when the action of mirroring traffic is applied in the outbound direction, any other action cannot be configured in the same traffic behavior. Otherwise, the corresponding QoS policy cannot be applied successfully.

#### Examples

# Configure traffic behavior 1 and define the action of mirroring traffic to GigabitEthernet1/0/2 in the traffic behavior.

```
<Sysname> system-view  
[Sysname] traffic behavior 1  
[Sysname-behavior-1] mirror-to interface GigabitEthernet 1/0/2
```

# Table of Contents

<b>1 User Profile Configuration Commands .....</b>	<b>1-1</b>
User Profile Configuration Commands .....	1-1
display user-profile .....	1-1
user-profile enable .....	1-2
user-profile .....	1-3

# 1 User Profile Configuration Commands

---

## User Profile Configuration Commands

### display user-profile

#### Syntax

**display user-profile**

#### View

Any view

#### Default Level

2: System level

#### Parameters

None

#### Description

Use the **display user-profile** command to display information of all the user profiles that have been created.

#### Examples

# Display information of all the user profiles that have been created.

```
<Sysname> display user-profile
Status      User profile                AuthType
disabled   a123                          PORTAL
enabled    b123                          DOT1X
-----Total user profiles:      2-----
-----Enabled user profiles:    1-----
```

**Table 1-1 display user-profile** command output description

Field	Description
Status	Status of the current user profile: <ul style="list-style-type: none"><li>• enabled</li><li>• disabled</li></ul>
User profile	User profile name

Field	Description
AuthType	Authentication type of the current user profile, which may take the following values: DOT1X: 802.1X authentication PORTAL: portal authentication
Total user profiles	Total number of user profiles that have been created
Enabled user profiles	Total number of user profiles that have been enabled

## user-profile enable

### Syntax

**user-profile** *profile-name* **enable**

**undo user-profile** *profile-name* **enable**

### View

System view

### Default Level

2: System level

### Parameters

*profile-name*: Use profile name, a string of 1 to 31 characters, case sensitive. It can only contain English letters, numbers, underlines, and must start with an English letter.

### Description

Use the **user-profile enable** command to enable a user profile.

Use the **undo user-profile enable** command to disable the specified user profile.

By default, a created user profile is disabled.

Note that:

- When you execute the command, the specified user profile must be created; otherwise, the command fails.
- Only an enabled user profile can be used by users. You cannot modify or remove the configuration items in a user profile until the user profile is disabled.
- Disabling a user profile logs out the users using the user profile.

### Examples

# Enable user profile **a123**.

```
<Sysname> system-view
```

```
[Sysname] user-profile a123 enable
```

## user-profile

### Syntax

```
user-profile profile-name [ dot1x | portal ]
```

```
undo user-profile profile-name [ dot1x | portal ]
```

### View

System view

### Default Level

2: System level

### Parameters

*profile-name*: Use profile name, a string of 1 to 31 characters, case sensitive. It can only contain English letters, numbers, underlines, and must start with an English letter. A user profile name must be globally unique.

**dot1x**: Uses 802.1X authentication when users access the device. Refer to *802.1X Configuration* in the *Security Volume* for the detailed information about 802.1X.

**portal**: Uses portal authentication when users access the device. Refer to *Portal Configuration* in the *Security Volume* for the detailed information about portal.

### Description

Use the **user-profile** command to create a user profile and enter the corresponding user profile view. If the specified user profile already exists, you will directly enter the corresponding user profile view, without the need to create a user profile. Use the **undo user-profile** command to remove an existing, disabled user profile.

By default, no user profiles exist on the device.

Note that:

- You must provide the **dot1x**, or **portal** keyword when creating a user profile.
- If you provide the **dot1x**, or **portal**, keyword, the value must be the same with that provided when you create the user profile; otherwise, the command fails.
- If you provide the **dot1x**, or **portal** keyword when you remove a user profile, the value must be the same with that provided when you create the user profile; otherwise, the command fails.
- An enabled user profile cannot be removed.

Related commands: **user-profile enable**.

### Examples

```
# Create a user profile a123, using portal authentication.
```

```
<Sysname> system-view  
[Sysname] user-profile a123 portal  
[Sysname-user-profile-PORTAL-a123]
```

# Enter the corresponding user profile view of **a123**.

```
<Sysname> system-view
```

```
[Sysname] user-profile a123
```

```
[Sysname-user-profile-PORTAL-a123]
```

# Security Volume Organization

---

## Manual Version

6W100-20090120

## Product Version

Release 2202

## Organization

The Security Volume is organized as follows:

Features	Description
AAA	Authentication, Authorization and Accounting (AAA) provide a uniform framework used for configuring these three security functions to implement the network security management. This document introduces the commands for AAA configuration.
802.1X	IEEE 802.1X (hereinafter simplified as 802.1X) is a port-based network access control protocol that is used as the standard for LAN user access authentication. This document introduces the commands for 802.1X configuration.
HABP	On an HABP-capable switch, HABP packets can bypass 802.1X authentication and MAC authentication, allowing communication among switches in a cluster. This document introduces the commands for HABP configuration.
MAC Authentication	MAC authentication provides a way for authenticating users based on ports and MAC addresses; it requires no client software to be installed on the hosts. This document introduces the commands for MAC Authentication configuration.
Portal	Portal authentication, as its name implies, helps control access to the Internet. This document introduces the commands for Portal configuration.
Port Security	Port security is a MAC address-based security mechanism for network access controlling. It is an extension to the existing 802.1X authentication and MAC authentication. This document introduces the commands for Port Security configuration.
IP Source Guard	By filtering packets on a per-port basis, IP source guard prevents illegal packets from traveling through, thus improving the network security. This document introduces the commands for IP Source Guard configuration.
SSH2.0	SSH ensures secure login to a remote device in a non-secure network environment. By encryption and strong authentication, it protects the device against attacks. This document introduces the commands for SSH2.0 configuration.
PKI	The Public Key Infrastructure (PKI) is a hierarchical framework designed for providing information security through public key technologies and digital certificates and verifying the identities of the digital certificate owners. This document introduces the commands for PKI configuration.

<b>Features</b>	<b>Description</b>
SSL	Secure Sockets Layer (SSL) is a security protocol providing secure connection service for TCP-based application layer protocols, this document introduces the commands for SSL configuration.
Public Key	This document introduces the commands for Public Key Configuration.
ACL	An ACL is used for identifying traffic based on a series of preset matching criteria. This document introduces the commands for ACL configuration.

# Table of Contents

<b>1 AAA Configuration Commands</b> .....	<b>1-1</b>
AAA Configuration Commands.....	1-1
access-limit enable.....	1-1
access-limit.....	1-1
accounting default.....	1-2
accounting lan-access.....	1-3
accounting login.....	1-4
accounting optional.....	1-5
accounting portal.....	1-6
authentication default.....	1-7
authentication lan-access.....	1-8
authentication login.....	1-8
authentication portal.....	1-9
authorization command.....	1-10
authorization default.....	1-11
authorization lan-access.....	1-12
authorization login.....	1-13
authorization portal.....	1-14
authorization-attribute.....	1-15
bind-attribute.....	1-17
cut connection.....	1-18
display connection.....	1-19
display domain.....	1-20
display local-user.....	1-21
display user-group.....	1-23
domain.....	1-24
domain default enable.....	1-25
expiration-date.....	1-25
group.....	1-26
idle-cut enable.....	1-27
local-user.....	1-27
local-user password-display-mode.....	1-28
password.....	1-29
self-service-url enable.....	1-30
service-type.....	1-31
state.....	1-32
user-group.....	1-32
<b>2 RADIUS Configuration Commands</b> .....	<b>2-1</b>
RADIUS Configuration Commands.....	2-1
data-flow-format (RADIUS scheme view).....	2-1
display radius scheme.....	2-2
display radius statistics.....	2-4
display stop-accounting-buffer.....	2-7

key (RADIUS scheme view) .....	2-7
nas-ip (RADIUS scheme view) .....	2-8
primary accounting (RADIUS scheme view) .....	2-9
primary authentication (RADIUS scheme view) .....	2-10
radius client .....	2-11
radius nas-ip .....	2-12
radius scheme .....	2-13
radius trap .....	2-13
reset radius statistics .....	2-14
reset stop-accounting-buffer .....	2-15
retry .....	2-16
retry realtime-accounting .....	2-16
retry stop-accounting (RADIUS scheme view) .....	2-17
secondary accounting (RADIUS scheme view) .....	2-18
secondary authentication (RADIUS scheme view) .....	2-19
security-policy-server .....	2-20
server-type .....	2-21
state .....	2-22
stop-accounting-buffer enable (RADIUS scheme view) .....	2-23
timer quiet (RADIUS scheme view) .....	2-23
timer realtime-accounting (RADIUS scheme view) .....	2-24
timer response-timeout (RADIUS scheme view) .....	2-25
user-name-format (RADIUS scheme view) .....	2-26

### **3 HWTACACS Configuration Commands .....3-1**

HWTACACS Configuration Commands .....	3-1
data-flow-format (HWTACACS scheme view) .....	3-1
display hwtacacs .....	3-1
display stop-accounting-buffer .....	3-4
hwtacacs nas-ip .....	3-4
hwtacacs scheme .....	3-5
key (HWTACACS scheme view) .....	3-6
nas-ip (HWTACACS scheme view) .....	3-6
primary accounting (HWTACACS scheme view) .....	3-7
primary authentication (HWTACACS scheme view) .....	3-8
primary authorization .....	3-9
reset hwtacacs statistics .....	3-10
reset stop-accounting-buffer .....	3-10
retry stop-accounting (HWTACACS scheme view) .....	3-11
secondary accounting (HWTACACS scheme view) .....	3-12
secondary authentication (HWTACACS scheme view) .....	3-12
secondary authorization .....	3-13
stop-accounting-buffer enable (HWTACACS scheme view) .....	3-14
timer quiet (HWTACACS scheme view) .....	3-15
timer realtime-accounting (HWTACACS scheme view) .....	3-16
timer response-timeout (HWTACACS scheme view) .....	3-17
user-name-format (HWTACACS scheme view) .....	3-17

# 1 AAA Configuration Commands

---

## AAA Configuration Commands

### access-limit enable

#### Syntax

**access-limit enable** *max-user-number*

**undo access-limit enable**

#### View

ISP domain view

#### Default Level

2: System level

#### Parameters

*max-user-number*: Maximum number of user connections for the current ISP domain. The valid range from 1 to 2147483646.

#### Description

Use the **access-limit enable** command to enable the limit on the number of user connections in an ISP domain and set the allowed maximum number. After the number of user connections reaches the maximum number allowed, no more users will be accepted.

Use the **undo access-limit enable** command to restore the default.

By default, there is no limit to the number of user connections in an ISP domain.

As user connections may compete for network resources, setting a proper limit to the number of user connections helps provide a reliable system performance.

#### Examples

# Set a limit of 500 user connections for ISP domain **aabbcc.net**.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] access-limit enable 500
```

### access-limit

#### Syntax

**access-limit** *max-user-number*

**undo access-limit**

## View

Local user view

## Default Level

3: Manage level

## Parameters

*max-user-number*: Maximum number of user connections using the current username, in the range 1 to 1024.

## Description

Use the **access-limit** command to enable the limit on the number of user connections using the current username and set the allowed maximum number.

Use the **undo access-limit** command to remove the limitation.

By default, there is no limit to the number of user connections using the same username.

Note that the **access-limit** command takes effect only when local accounting is configured.

Related commands: **display local-user**.

## Examples

# Enable the limit on the number of user connections using the username **abc** and set the allowed maximum number to 5.

```
<Sysname> system-view
[Sysname] local-user abc
[Sysname-luser-abc] access-limit 5
```

## accounting default

### Syntax

```
accounting default { hwtacacs-scheme hwtacacs-scheme-name [ local ] | local | none | radius-scheme radius-scheme-name [ local ] }
```

```
undo accounting default
```

### View

ISP domain view

### Default Level

2: System level

### Parameters

**hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

**local**: Performs local accounting.

**none**: Does not perform any accounting.

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

## Description

Use the **accounting default** command to configure the default accounting method for all types of users.

Use the **undo accounting default** command to restore the default.

By default, the accounting method is **local**.

Note that:

- The RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.
- The accounting method configured with the **accounting default** command is for all types of users and has a priority lower than that for a specific access mode.
- Local accounting is only for managing the local user connection number; it does not provide the statistics function. The local user connection number management is only for local accounting; it does not affect local authentication and authorization.

Related commands: **authentication default**, **authorization default**, **hwtacacs scheme**, **radius scheme**.

## Examples

# Configure the default ISP domain **system** to use the local accounting method for all types of users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting default local
```

# Configure the default ISP domain **system** to use RADIUS accounting scheme **rd** for all types of users and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting default radius-scheme rd local
```

## accounting lan-access

### Syntax

```
accounting lan-access { local | none | radius-scheme radius-scheme-name [ local ] }
undo accounting lan-access
```

### View

ISP domain view

### Default Level

2: System level

### Parameters

**local**: Performs local accounting.

**none**: Does not perform any accounting.

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

## Description

Use the **accounting lan-access** command to configure the accounting method for LAN access users.

Use the **undo accounting lan-access** command to restore the default.

By default, the default accounting method that the **accounting default** command prescribes is used for LAN access users.

Note that the RADIUS scheme specified for the current ISP domain must have been configured.

Related commands: **accounting default**, **radius scheme**.

## Examples

# Configure the default ISP domain **system** to use the local accounting method for LAN access users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting lan-access local
```

# Configure the default ISP domain **system** to use RADIUS accounting scheme **rd** for LAN access users and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting lan-access radius-scheme rd local
```

## accounting login

### Syntax

```
accounting login { hwtacacs-scheme hwtacacs-scheme-name [ local ] | local | none | radius-scheme radius-scheme-name [ local ] }
```

```
undo accounting login
```

### View

ISP domain view

### Default Level

2: System level

### Parameters

**hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

**local**: Performs local accounting. It is not used for charging purposes, but for collecting statistics on and limiting the number of local user connections.

**none**: Does not perform any accounting.

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

## Description

Use the **accounting login** command to configure the accounting method for login users.

Use the **undo accounting login** command to restore the default.

By default, the default accounting method is used for login users.

Note that:

- The RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.
- Accounting is not supported for login users' FTP services.

Related commands: **accounting default**, **hwtacacs scheme**, **radius scheme**.

## Examples

# Configure the default ISP domain **system** to use the local accounting method for login users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting login local
```

# Configure the default ISP domain **system** to use RADIUS accounting scheme **rd** for login users and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting login radius-scheme rd local
```

## accounting optional

### Syntax

**accounting optional**

**undo accounting optional**

### View

ISP domain view

### Default Level

2: System level

### Parameters

None

### Description

Use the **accounting optional** command to enable the accounting optional feature.

Use the **undo accounting optional** command to disable the feature.

By default, the feature is disabled.

Note that with the **accounting optional** command configured for a domain:

- A user that will be disconnected otherwise can use the network resources even when there is no accounting server available or communication with the current accounting server fails. This command applies to scenarios where authentication is required but accounting is not.
- If accounting for a user in the domain fails, the device will not send real-time accounting updates for the user any more.
- The limit on the number of local user connections configured by using the **access-limit** command in local user view is not effective.

## Examples

```
# Enable the accounting optional feature for users in domain aabbcc.net.
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] accounting optional
```

## accounting portal

### Syntax

```
accounting portal { local | none | radius-scheme radius-scheme-name [ local ] }
undo accounting portal
```

### View

ISP domain view

### Default Level

2: System level

### Parameters

**local**: Performs local accounting.

**none**: Does not perform any accounting.

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

### Description

Use the **accounting portal** command to configure the accounting method for portal users.

Use the **undo accounting portal** command to restore the default.

By default, the default accounting method is used for portal users.

Note that the RADIUS scheme specified for the current ISP domain must have been configured.

Related commands: **accounting default**, **radius scheme**.

## Examples

```
# Configure the default ISP domain system to use RADIUS scheme rd for accounting on portal users.
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting portal radius-scheme rd

# Configure the default ISP domain system to use RADIUS scheme rd for accounting on portal users
and use local accounting as the backup.
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting portal radius-scheme rd local
```

## authentication default

### Syntax

```
authentication default { hwtacacs-scheme hwtacacs-scheme-name [ local ] | local | none |  
radius-scheme radius-scheme-name [ local ] }
```

```
undo authentication default
```

### View

ISP domain view

### Default Level

2: System level

### Parameters

**hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

**local**: Performs local authentication.

**none**: Does not perform any authentication.

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

### Description

Use the **authentication default** command to configure the default authentication method for all types of users.

Use the **undo authentication default** command to restore the default.

By default, the authentication method is **local**.

Note that:

- The RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.
- The authentication method specified with the **authentication default** command is for all types of users and has a priority lower than that for a specific access mode.

Related commands: **authorization default**, **accounting default**, **hwtacacs scheme**, **radius scheme**.

### Examples

# Configure the default ISP domain **system** to use local authentication for all types of users.

```
<Sysname> system-view  
[Sysname] domain system  
[Sysname-isp-system] authentication default local
```

# Configure the default ISP domain **system** to use RADIUS authentication scheme **rd** for all types of users and use local authentication as the backup.

```
<Sysname> system-view  
[Sysname] domain system  
[Sysname-isp-system] authentication default radius-scheme rd local
```

## authentication lan-access

### Syntax

```
authentication lan-access { local | none | radius-scheme radius-scheme-name [ local ] }  
undo authentication lan-access
```

### View

ISP domain view

### Default Level

2: System level

### Parameters

**local**: Performs local authentication.

**none**: Does not perform any authentication.

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

### Description

Use the **authentication lan-access** command to configure the authentication method for LAN access users.

Use the **undo authentication login** command to restore the default.

By default, the default authentication method is used for LAN access users.

Note that the RADIUS scheme specified for the current ISP domain must have been configured.

Related commands: **authentication default**, **radius scheme**.

### Examples

# Configure the default ISP domain **system** to use local authentication for LAN access users.

```
<Sysname> system-view  
[Sysname] domain system  
[Sysname-isp-system] authentication lan-access local
```

# Configure the default ISP domain **system** to use RADIUS authentication scheme **rd** for LAN access users and use local authentication as the backup.

```
<Sysname> system-view  
[Sysname] domain system  
[Sysname-isp-system] authentication lan-access radius-scheme rd local
```

## authentication login

### Syntax

```
authentication login { hwtacacs-scheme hwtacacs-scheme-name [ local ] | local | none |  
radius-scheme radius-scheme-name [ local ] }  
undo authentication login
```

## View

ISP domain view

## Default Level

2: System level

## Parameters

**hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

**local**: Performs local authentication.

**none**: Does not perform any authentication.

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

## Description

Use the **authentication login** command to configure the authentication method for login users.

Use the **undo authentication login** command to restore the default.

By default, the default authentication method is used for login users.

Note that the RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.

Related commands: **authentication default**, **hwtacacs scheme**, **radius scheme**.

## Examples

# Configure the default ISP domain **system** to use local authentication for login users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication login local
```

# Configure the default ISP domain **system** to use RADIUS authentication scheme **rd** for login users and use local authentication as the backup.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication login radius-scheme rd local
```

## authentication portal

### Syntax

**authentication portal** { **local** | **none** | **radius-scheme** *radius-scheme-name* [ **local** ] }

**undo authentication portal**

### View

ISP domain view

### Default Level

2: System level

## Parameters

**local:** Performs local authentication.

**none:** Does not perform any authentication.

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

## Description

Use the **authentication portal** command to configure the authentication method for portal users.

Use the **undo authentication portal** command to restore the default.

By default, the default authentication method is used for portal users.

Note that the RADIUS scheme specified for the current ISP domain must have been configured.

Related commands: **authentication default**, **radius scheme**.

## Examples

# Configure the default ISP domain **system** to use RADIUS scheme **rd** for authentication of portal users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication portal radius-scheme rd
```

# Configure the default ISP domain **system** to use RADIUS scheme **rd** for authentication of portal users and use local authentication as the backup.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication portal radius-scheme rd local
```

## authorization command

### Syntax

**authorization command** { **hwtacacs-scheme** *hwtacacs-scheme-name* [ **local** | **none** ] | **local** | **none** }

**undo authorization command**

### View

ISP domain view

### Default Level

2: System level

## Parameters

**hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

**local:** Performs local authorization.

**none:** Does not perform any authorization. In this case, an authenticated user is automatically authorized with the corresponding default rights.

## Description

Use the **authorization command** command to configure the authorization method for command line users.

Use the **undo authorization command** command to restore the default.

By default, the default authorization method is used for command line users.

Note that:

- The HWTACACS scheme specified for the current ISP domain must have been configured.
- For local authorization, the local users must have been configured for the command line users on the device, and the level of the commands authorized to a local user must be lower than or equal to that of the local user. Otherwise, local authorization will fail.

Related commands: **authorization default**, **hwtacacs scheme**.

## Examples

# Configure the default ISP domain **system** to use HWTACACS authorization scheme **hw** for command line users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization command hwtacacs-scheme hw
```

# Configure the default ISP domain **system** to use HWTACACS authorization scheme **hw** for command line users and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization command hwtacacs-scheme hw local
```

## authorization default

### Syntax

```
authorization default { hwtacacs-scheme hwtacacs-scheme-name [ local ] | local | none | radius-scheme radius-scheme-name [ local ] }
```

```
undo authorization default
```

### View

ISP domain view

### Default Level

2: System level

### Parameters

**hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

**local**: Performs local authorization.

**none**: Does not perform any authorization. In this case, an authenticated user is automatically authorized with the corresponding default rights.

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

## Description

Use the **authorization default** command to configure the authorization method for all types of users.

Use the **undo authorization default** command to restore the default.

By default, the authorization method for all types of users is **local**.

Note that:

- The RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.
- The authorization method specified with the **authorization default** command is for all types of users and has a priority lower than that for a specific access mode.
- RADIUS authorization is special in that it takes effect only when the RADIUS authorization scheme is the same as the RADIUS authentication scheme. If the RADIUS authorization scheme is different from the RADIUS authentication scheme, RADIUS authorization will fail. In addition, if a RADIUS authorization fails, the error message returned to the NAS says that the server is not responding.

Related commands: **authentication default**, **accounting default**, **hwtacacs scheme**, **radius scheme**.

## Examples

# Configure the default ISP domain **system** to use local authorization for all types of users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization default local
```

# Configure the default ISP domain **system** to use RADIUS authorization scheme **rd** for all types of users and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization default radius-scheme rd local
```

## authorization lan-access

### Syntax

```
authorization lan-access { local | none | radius-scheme radius-scheme-name [ local ] }
undo authorization lan-access
```

### View

ISP domain view

### Default Level

2: System level

### Parameters

**local**: Performs local authorization.

**none:** Does not perform any authorization. In this case, an authenticated user is automatically authorized with the default rights.

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

## Description

Use the **authorization lan-access** command to configure the authorization method for LAN access users.

Use the **undo authorization lan-access** command to restore the default.

By default, the default authorization method is used for LAN access users.

Note that:

- The RADIUS scheme specified for the current ISP domain must have been configured.
- RADIUS authorization is special in that it takes effect only when the RADIUS authorization scheme is the same as the RADIUS authentication scheme. If the RADIUS authorization scheme is different from the RADIUS authentication scheme, RADIUS authorization will fail.

Related commands: **authorization default**, **radius scheme**.

## Examples

# Configure the default ISP domain **system** to use local authorization for LAN access users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system]authorization lan-access local
```

# Configure the default ISP domain **system** to use RADIUS authorization scheme **rd** for LAN access users and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization lan-access radius-scheme rd local
```

## authorization login

### Syntax

```
authorization login { hwtacacs-scheme hwtacacs-scheme-name [ local ] | local | none | radius-scheme radius-scheme-name [ local ] }
```

```
undo authorization login
```

### View

ISP domain view

### Default Level

2: System level

### Parameters

**hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

**local**: Performs local authorization.

**none:** Does not perform any authorization. In this case, an authenticated user is automatically authorized with the default rights.

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

## Description

Use the **authorization login** command to configure the authorization method for login users.

Use the **undo authorization login** command to restore the default.

By default, the default authorization method is used for login users.

Note that:

- The RADIUS, HWTACACS, or LDAP scheme specified for the current ISP domain must have been configured.
- RADIUS authorization is special in that it takes effect only when the RADIUS authorization scheme is the same as the RADIUS authentication scheme. If the RADIUS authorization scheme is different from the RADIUS authentication scheme, RADIUS authorization will fail.

Related commands: **authorization default**, **hwtacacs scheme**, **radius scheme**.

## Examples

# Configure the default ISP domain **system** to use local authorization for login users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization login local
```

# Configure the default ISP domain **system** to use RADIUS authorization scheme **rd** for login users and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization login radius-scheme rd local
```

## authorization portal

### Syntax

```
authorization portal { local | none | radius-scheme radius-scheme-name [ local ] }
```

```
undo authorization portal
```

### View

ISP domain view

### Default Level

2: System level

### Parameters

**local:** Performs local authorization.

**none:** None authorization, which means the user is trusted completely. Here, the user is assigned with the default privilege.

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

## Description

Use the **authorization portal** command to configure the authorization method for portal users.

Use the **undo authorization portal** command to restore the default.

By default, the default authorization method is used for portal users.

Note that:

- The RADIUS scheme specified for the current ISP domain must have been configured.
- RADIUS authorization is special in that it takes effect only when the RADIUS authorization scheme is the same as the RADIUS authentication scheme. If the RADIUS authorization scheme is different from the RADIUS authentication scheme, RADIUS authorization will fail.

Related commands: **authorization default**, **radius scheme**.

## Examples

# Configure the default ISP domain **system** to use RADIUS scheme **rd** for authorization of portal users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization portal radius-scheme rd
```

# Configure the default ISP domain **system** to use RADIUS scheme **rd** for authorization of portal users and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization portal radius-scheme rd local
```

## authorization-attribute

### Syntax

**authorization-attribute** { **acl** *acl-number* | **callback-number** *callback-number* | **idle-cut** *minute* | **level** *level* | **user-profile** *profile-name* | **vlan** *vlan-id* | **work-directory** *directory-name* } \*

**undo authorization-attribute** { **acl** | **callback-number** | **idle-cut** | **level** | **user-profile** | **vlan** | **work-directory** } \*

### View

Local user view, user group view

### Default Level

3: Manage level

### Parameters

**acl**: Specifies the authorized ACL of the local user(s).

*acl-number*: Authorized ACL for the local user(s), in the range 2000 to 5999.

**callback-number**: Specifies the authorization PPP callback number of the local user(s).

*callback-number*: Authorization PPP callback number for the local user(s), a case-sensitive string of 1 to 64 characters.

**idle-cut:** Specifies the idle cut function for the local user(s). With the idle cut function enabled, an online user whose idle period exceeds the specified idle time will be logged out.

*minute:* Idle time allowed, in the range 1 to 120 minutes.

**level:** Specifies the level of the local user(s).

*level:* Level of the local user(s), which can be 0 for visit level, 1 for monitor level, 2 for system level, and 3 for manage level. A smaller number means a lower level. The default is 0.

**user-profile:** Specifies the authorization user profile of the local user(s).

*profile-name:* Name of the authorization user profile for the local user(s), a case-sensitive string of 1 to 32 characters. It can consist of English letters, digits, and underlines and must start with an English letter.

**vlan:** Specifies the authorized VLAN of the local user(s).

*vlan-id:* Authorized VLAN for the local user(s), in the range 1 to 4094.

**work-directory:** Specifies the authorized work directory of the local user(s), if the user or users are authorized the FTP or SFTP service type.

*directory-name:* Authorized work directory, a case-insensitive string of 1 to 135 characters. This directory must already exist.

## Description

Use the **authorization-attribute** command to configure authorization attributes for the local user or user group. After the local user or a local user of the user group passes authentication, the device will assign these attributes to the user.

Use the **undo authorization-attribute** command to remove authorization attributes.

By default, no authorization attribute is configured for a local user or user group.

Note that:

- Every configurable authorization attribute has its definite application environments and purposes. However, the assignment of local user authorization attributes does not take the service type into account. Therefore, when configuring authorization attributes for a local user, consider what attributes are needed.
- Authorization attributes configured for a user group are effective on all local users of the group.
- An authorization attribute configured in local user view takes precedence over the same attribute configured in user group view.
- If you specify to perform no authentication or perform password authentication, the levels of commands that a user can access after login depends on the level of the user interface. For information about user interface login authentication method, refer to the **authentication-mode** command in *Login Commands* of the *System Volume*. If the authentication method requires users to provide usernames and passwords, the levels of commands that a user can access after login depends on the level of the user. For an SSH user authenticated with an RSA public key, available commands depend on the level specified on the user interface.
- If you remove the specified work directory from the file system, the FTP/SFTP user(s) will not be able to access the directory.
- If the specified work directory carries slot information, the FTP/SFTP user(s) will not be able to access the directory after a switchover occurs. Therefore, specifying slot information for the work directory is not recommended.

## Examples

```
# Configure the authorized VLAN of user group abc as VLAN 3.
<Sysname> system-view
[Sysname] user-group abc
[Sysname-ugroup-abc] authorization-attribute vlan 3
```

## bind-attribute

### Syntax

```
bind-attribute { call-number call-number [ : subcall-number ] | ip ip-address | location port
slot-number subslot-number port-number | mac mac-address | vlan vlan-id } *
undo bind-attribute { call-number | ip | location | mac | vlan } *
```

### View

Local user view

### Default Level

3: Manage level

### Parameters

**call-number** *call-number*: Specifies a calling number for ISDN user authentication. The *call-number* argument is a string of 1 to 64 characters.

*subcall-number*: Specifies the sub-calling number. The total length of the calling number and the sub-calling number cannot be more than 62 characters.

**ip** *ip-address*: Specifies the IP address of the user.

**location**: Specifies the port binding attribute of the user.

**port** *slot-number subslot-number port-number*: Specifies the port to which the user is bound. The *slot-number* argument is in the range 0 to 15, the *subslot-number* argument is in the range 0 to 15, and the *port-number* argument is in the range 0 to 255. Only the numbers make sense here; port types are not taken into account.

**mac** *mac-address*: Specifies the MAC address of the user in the format of H-H-H.

**vlan** *vlan-id*: Specifies the VLAN to which the user belongs. The *vlan-id* argument is in the range 1 to 4094.

### Description

Use the **bind-attribute** command to configure binding attributes for a local user.

Use the **undo bind-attribute** command to remove binding attributes of a local user.

By default, no binding attribute is configured for a local user.

Note that:

- Binding attributes are checked upon authentication of a local user. If the binding attributes of a local user do not match the configured ones, the checking will fail and the user will fail the authentication as a result. In addition, such binding attribute checking does not take the service types of the users into account. That is, a configured binding attribute is effective on all types of users. Therefore, be cautious when deciding which binding attributes should be configured for which type of local users.

- The **bind-attribute ip** command applies only when the authentication method (802.1X, for example) supports IP address upload. If you configure the command when the authentication method (MAC address authentication, for example) does not support IP address upload, local authentication will fail.

## Examples

```
# Configure the bound IP of local user abc as 3.3.3.3.
```

```
<Sysname> system-view
[Sysname] local-user abc
[Sysname-luser-abc] bind-attribute ip 3.3.3.3
```

## cut connection

### Syntax

```
cut connection { all | domain isp-name | ucibindex ucib-index | user-name user-name } [ slot slot-number ]
```

### View

System view

### Default Level

2: System level

### Parameters

**all**: Specifies all user connections.

**domain** *isp-name*: Specifies all user connections of an ISP domain. The *isp-name* argument refers to the name of an existing ISP domain and is a string of 1 to 24 characters.

**ucibindex** *ucib-index*: Specifies a user connection by connection index. The value range from 0 to 4294967295.

**user-name** *user-name*: Specifies a user connection by username. The *user-name* argument is a case-sensitive string of 1 to 80 characters and must contain the domain name. If you enter a username without any domain name, the system assumes that the default domain name is used for the username.

**slot** *slot-number*: Specifies the connections on a specified member device in an IRF stack. The *slot-number* argument indicates the member device ID.

### Description

Use the **cut connection** command to tear down the specified connections forcibly.

At present, this command applies to only LAN access and portal user connections.

Related commands: **display connection**, **service-type**.

### Examples

```
# Tear down all connections in ISP domain aabbcc.net.
```

```
<Sysname> system-view
[Sysname] cut connection domain aabbcc.net
```

## display connection

### Syntax

```
display connection [ domain isp-name | ucibindex ucib-index | user-name user-name ] [ slot  
slot-number ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**domain** *isp-name*: Specifies all user connections of an ISP domain. The *isp-name* argument refers to the name of an existing ISP domain and is a case-insensitive string of 1 to 24 characters.

**ucibindex** *ucib-index*: Specifies all user connections using the specified connection index. The value range from 0 to 4294967295.

**user-name** *user-name*: Specifies all user connections using the specified username. The *user-name* argument is a case-sensitive string of 1 to 80 characters and must contain the domain name. If you enter a username without any domain name, the system assumes that the default domain name is used for the username.

**slot** *slot-number*: Specifies the connections on a specified member device in an IRF stack. The *slot-number* argument indicates the member device ID.

### Description

Use the **display connection** command to display information about specified or all AAA user connections.

Note that:

- With no parameter specified, the command displays brief information about all AAA user connections.
- If you specify the **ucibindex** *ucib-index* combination, the command displays detailed information; otherwise, the command displays brief information.
- This command does not apply to FTP user connections.

Related commands: **cut connection**.

### Examples

# Display information about all AAA user connections.

```
<Sysname> display connection
```

```
Index=1      ,Username=telnet@system  
IP=10.0.0.1  
Total 1 connection(s) matched.
```

**Table 1-1 display connection** command output description

Field	Description
Index	Index number
Username	Username of the connection, in the format <i>username@domain</i>
IP	IP address of the user
Total 1 connection(s) matched.	Total number of user connections

## display domain

### Syntax

```
display domain [ isp-name ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*isp-name*: Name of an existing ISP domain, a string of 1 to 24 characters.

### Description

Use the **display domain** command to display the configuration information of a specified ISP domain or all ISP domains.

Related commands: **access-limit enable**, **domain**, **state**.

### Examples

# Display the configuration information of all ISP domains.

```
<Sysname> display domain
0 Domain = system
  State = Active
  Access-limit = Disable
  Accounting method = Required
  Default authentication scheme      : local
  Default authorization scheme      : local
  Default accounting scheme         : local
  Domain User Template:
  Idle-cut = Disabled
  Self-service = Disabled

1 Domain = aabbcc
  State = Active
  Access-limit = Disable
  Accounting method = Required
```

```

Default authentication scheme      : local
Default authorization scheme      : local
Default accounting scheme        : local
Lan-access authentication scheme  : radius=test, local
Lan-access authorization scheme  : hwtacacs=hw, local
Lan-access accounting scheme     : local

Domain User Template:
Idle-cut = Disabled
Self-service = Disabled

```

Default Domain Name: system

Total 2 domain(s)

**Table 1-2 display domain command output description**

Field	Description
Domain	Domain name
State	Status of the domain (active or block)
Access-limit	Limit on the number of user connections
Accounting method	Accounting method (either required or optional)
Default authentication scheme	Default authentication method
Default authorization scheme	Default authorization method
Default accounting scheme	Default accounting method
Lan-access authentication scheme	Authentication method for LAN users
Lan-access authorization scheme	Authentication method for LAN users
Lan-access accounting scheme	Accounting method for LAN users
Domain User Template	Template for users in the domain
Idle-cut	Whether idle cut is enabled
Self-service	Whether self service is enabled
Default Domain Name	Default ISP domain name
Total 2 domain(s).	2 ISP domains in total

## display local-user

### Syntax

```

display local-user [ idle-cut { disable | enable } | service-type { ftp | lan-access | portal | ssh | telnet
| terminal } | state { active | block } | user-name user-name | vlan vlan-id ] [ slot slot-number ]

```

### View

Any view

## Default Level

1: Monitor level

## Parameters

**idle-cut** { **disable** | **enable** }: Specifies local users with the idle cut function disabled or enabled.

**service-type**: Specifies the local users of a type.

- **ftp** refers to users using FTP.
- **lan-access** refers to users accessing the network through an Ethernet, such as 802.1X users.
- **portal** refers to users using Portal.
- **ssh** refers to users using SSH.
- **telnet** refers to users using Telnet.
- **terminal** refers to users logging in through the console port or AUX port.
- **state** { **active** | **block** }: Specifies all local users in the state of active or block. A local user in the state of active can access network services, while a local user in the state of blocked cannot.

**user-name** *user-name*: Specifies all local users using the specified username. The username is a case-sensitive string of 1 to 55 characters and does not contain the domain name.

**vlan** *vlan-id*: Specifies all local users in a VLAN. The VLAN ID ranges from 1 to 4094.

**slot** *slot-number*: Specifies all local users on a specified member device in an IRF stack. The *slot-number* argument indicates the member device ID.

## Description

Use the **display local-user** command to display information about specified or all local users.

Related commands: **local-user**.

## Examples

# Display the information of local user **bbb** on the specified Unit ID.

```
<Sysname> display local-user user-name bbb slot 1
Slot: 1
The contents of local user bbb:
State:                               Active
ServiceType:                          ftp
Access-limit:                          Enable           Current AccessNum: 0
Max AccessNum:                         300
User-group:                             system
Bind attributes:
  IP address:                           1.2.3.4
  Bind location:                         0/4/1 (SLOT/SUBSLOT/PORT)
  MAC address:                           0001-0002-0003
  Vlan ID:                               100
Authorization attributes:
  Idle TimeOut:                          10(min)
  Work Directory:                         flash:/
  User Privilege:                         3
  Acl ID:                                 2000
  Vlan ID:                               100
  User Profile:                           prof1
```

Expiration date: 12:12:12-2018/09/16  
Total 1 local user(s) matched.

**Table 1-3 display local-user command output description**

Field	Description
Slot	Slot number of the card
State	Status of the local user, Active or Block
ServiceType	Service types that the local user can use, including FTP, LAN, Portal, SSH, Telnet, and terminal.
Access-limit	Limit on the number of user connections using the current username
Current AccessNum	Current number of user connections using the current username, either for all cards or for a specified card.
Max AccessNum	Maximum number of user connections using the current username
VLAN ID	VLAN to which the user is bound
Calling Number	Calling number of the ISDN user
Authorization attributes	Authorization attributes of the local user
Idle TimeOut	Idle threshold of the user, in minutes.
Callback-number	Authorized PPP callback number of the local user
Work Directory	Directory accessible to the FTP user
VLAN ID	Authorized VLAN of the local user
Expiration date	Expiration time of the local user

## display user-group

### Syntax

```
display user-group [ group-name ]
```

### View

Any view

### Default Level

2: System level

### Parameters

*group-name*: User group name, a case-insensitive string of 1 to 32 characters.

### Description

Use the **display user-group** command to display configuration information about one or all user groups.

Related commands: **user-group**.

## Examples

```
# Display configuration information about user group abc.
```

```
<Sysname> display user-group abc
```

```
The contents of user group abc:
```

```
Authorization attributes:
```

```
Idle-cut: 120(min)
```

```
Work Directory: FLASH:
```

```
Level: 1
```

```
Acl Number: 2000
```

```
Vlan ID: 1
```

```
User-Profile: 1
```

```
Callback-number: 1
```

```
Total 1 user group(s) matched.
```

## domain

### Syntax

```
domain isp-name
```

```
undo domain isp-name
```

### View

System view

### Default Level

3: Manage level

### Parameters

*isp-name*: ISP domain name, a case-insensitive string of 1 to 24 characters that cannot contain any forward slash (/), colon (:), asterisk (\*), question mark (?), less-than sign (<), greater-than sign (>), or @.

### Description

Use the **domain** *isp-name* command to create an ISP domain and/or enter ISP domain view.

Use the **undo domain** command to remove an ISP domain.

Note that:

- If the specified ISP domain does not exist, the system will create a new ISP domain. All the ISP domains are in the active state when they are created.
- There is a default domain in the system, which cannot be deleted and can only be changed. A user providing no ISP domain name is considered in the default domain. For details about the default domain, refer to command **domain default enable**.

Related commands: **state**, **display domain**.

## Examples

```
# Create ISP domain aabbcc.net, and enter ISP domain view.
```

```
<Sysname> system-view
```

```
[Sysname] domain aabbcc.net
```

[Sysname-isp-aabbcc.net]

## domain default enable

### Syntax

```
domain default enable isp-name  
undo domain default enable
```

### View

System view

### Default Level

3: Manage level

### Parameters

*isp-name*: Name of the default ISP domain, a string of 1 to 24 characters.

### Description

Use the **domain default enable** command to configure the system default ISP domain.

Use the **undo domain default enable** command to restore the default.

By default, there is a default ISP domain named **system**.

Note that:

- There must be only one default ISP domain.
- The specified domain must have existed.
- The default ISP domain configured cannot be deleted unless you configure it as a non-default domain again.

Related commands: **state**, **display domain**.

### Examples

```
# Create a new ISP domain named aabbcc.net, and configure it as the default ISP domain.
```

```
<Sysname> system-view  
[Sysname] domain aabbcc.net  
[Sysname-isp-aabbcc.net] quit  
[Sysname] domain default enable aabbcc.net
```

## expiration-date

### Syntax

```
expiration-date time  
undo expiration-date
```

### View

Local user view

### Default Level

3: Manage level

## Parameters

*time*: Expiration time of the local user, in the format HH:MM:SS-MM/DD/YYYY or HH:MM:SS-YYYY/MM/DD. HH:MM:SS indicates the time, where HH ranges from 0 to 23, MM and SS range from 0 to 59. YYYY/MM/DD indicates the date, where YYYY ranges from 2000 to 2035, MM ranges from 1 to 12, and DD depends on the month. Except for the zeros in 00:00:00, leading zeros can be omitted. For example, 2:2:0-2008/2/2 equals to 02:02:00-2008/02/02.

## Description

Use the **expiration-date** command to configure the expiration time of a local user.

Use the **undo expiration-date** command to remove the configuration.

By default, a local user has no expiration time and no time validity checking is performed.

When some users need to access the network temporarily, you can create a guest account and specify an expiration time for the account. When a user uses the guest account for local authentication and passes the authentication, the access device checks whether the current system time is within the expiration time. If so, it permits the user to access the network. Otherwise, it denies the access request of the user.

Note that if you change the system time manually or the system time is changed in any other way, the access device uses the new system time for time validity checking.

## Examples

```
# Configure the expiration time of user abc to be 12:10:20 on May 31, 2008.
```

```
<Sysname> system-view
[Sysname] local-user abc
[Sysname-luser-abc] expiration-date 12:10:20-2008/05/31
```

## group

### Syntax

```
group group-name
undo group
```

### View

Local user view

### Default Level

3: Manage level

## Parameters

*group-name*: User group name, a case-insensitive string of 1 to 32 characters.

## Description

Use the **group** command to specify the user group for the local user to belong to.

Use the **undo group** command to restore the default.

By default, a local user belongs to user group **system**, which is automatically created by the device.

## Examples

```
# Specify that local user 111 belongs to user group abc.
<Sysname> system-view
[Sysname] local-user 111
[Sysname-luser-111] group abc
```

## idle-cut enable

### Syntax

```
idle-cut enable minute
undo idle-cut enable
```

### View

ISP domain view

### Default Level

2: System level

### Parameters

*minute*: Maximum idle duration allowed, in the range 1 to 120 minutes.

### Description

Use the **idle-cut enable** command to enable the idle cut function and set the maximum idle duration allowed. With the idle cut function enabled for a domain, the system will log out any user in the domain who has been idle for a period greater than the maximum idle duration.

Use the **undo idle-cut** command to restore the default.

By default, the function is disabled.

Related commands: **domain**.

## Examples

```
# Enable the idle cut function and set the idle threshold to 50 minutes for ISP domain aabbcc.net.
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] idle-cut enable 50
```

## local-user

### Syntax

```
local-user user-name
undo local-user { user-name | all service-type { ftp | lan-access | portal | ssh | telnet | terminal } }
```

### View

System view

## Default Level

3: Manage level

## Parameters

*user-name*: Name for the local user, a case-sensitive string of 1 to 55 characters that does not contain the domain name. It cannot contain any backward slash (\), forward slash (/), vertical line (|), colon (:), asterisk (\*), question mark (?), less-than sign (<), greater-than sign (>) and the @ sign and cannot be a, al, or all.

**all**: Specifies all users.

**service-type**: Specifies the users of a type.

- **ftp** refers to users using FTP.
- **lan-access** refers to users accessing the network through an Ethernet, such as 802.1X users.
- **portal** refers to users using Portal.
- **ssh** refers to users using SSH.
- **telnet** refers to users using Telnet.
- **terminal** refers to users logging in through the console port or AUX port.

## Description

Use the **local-user** command to add a local user and enter local user view.

Use the **undo local-user** command to remove the specified local users.

By default, no local user is configured.

Related commands: **display local-user**, **service-type**.

## Examples

```
# Add a local user named user1.
```

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1]
```

## local-user password-display-mode

### Syntax

```
local-user password-display-mode { auto | cipher-force }
```

```
undo local-user password-display-mode
```

### View

System view

## Default Level

2: System level

## Parameters

**auto**: Displays the password of a user based on the configuration of the user by using the **password** command.

**cipher-force**: Displays the passwords of all users in cipher text.

## Description

Use the **local-user password-display-mode** command to set the password display mode for all local users.

Use the **undo local-user password-display-mode** command to restore the default.

The default mode is **auto**.

With the **cipher-force** mode configured:

- A local user password is always displayed in cipher text, regardless of the configuration of the **password** command.
- If you use the **save** command to save the configuration, all existing local user passwords will still be displayed in cipher text after the device restarts, even if you restore the display mode to **auto**.

Related commands: **display local-user**, **password**.

## Examples

# Specify to display the passwords of all users in cipher text.

```
<Sysname> system-view
[Sysname] local-user password-display-mode cipher-force
```

## password

### Syntax

**password** { **cipher** | **simple** } *password*

**undo password**

### View

Local user view

### Default Level

2: System level

### Parameters

**cipher**: Specifies to display the password in cipher text.

**simple**: Specifies to display the password in simple text.

*password*: Password for the local user.

- In simple text, it must be a string of 1 to 63 characters that contains no blank space, for example, aabbcc.
- In cipher text, it must be a string of 24 or 88 characters, for example, \_(TT8FJ)\5SQ=^Q`MAF4<1!!.
- With the **simple** keyword, you must specify the password in simple text. With the **cipher** keyword, you can specify the password in either simple or cipher text.

## Description

Use the **password** command to configure a password for a local user.

Use the **undo password** command to delete the password of a local user.

Note that:

- With the **local-user password-display-mode cipher-force** command configured, the password is always displayed in cipher text, regardless of the configuration of the **password** command.
- With the **cipher** keyword specified, a password of up to 16 characters in plain text will be encrypted into a password of 24 characters in cipher text, and a password of 16 to 63 characters in plain text will be encrypted into a password of 88 characters in cipher text. For a password of 24 characters, if the system can decrypt the password, the system treats it as a password in cipher text. Otherwise, the system treats it as a password in plain text.

Related commands: **display local-user**.

## Examples

# Set the password of **user1** to 123456 and specify to display the password in plain text.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] password simple 123456
```

## self-service-url enable

### Syntax

**self-service-url enable** *url-string*

**undo self-service-url enable**

### View

ISP domain view

### Default Level

2: System level

### Parameters

*url-string*: URL of the self-service server for changing user password, a string of 1 to 64 characters. It must start with `http://` and contain no question mark.

### Description

Use the **self-service-url enable** command to enable the self-service server localization function and specify the URL of the self-service server for changing user password.

Use the **undo self-service-url enable** command to restore the default.

By default, the function is disabled.

Note that:

- A self-service RADIUS server, for example, CAMS/iMC, is required for the self-service server localization function. With the self-service function, a user can manage and control his or her accounting information or card number. A server with self-service software is a self-service server.
- After you configure the **self-service-url enable** command, a user can locate the self-service server by selecting [Service/Change Password] from the 802.1X client. The client software automatically launches the default browser, IE or Netscape, and opens the URL page of the self-service server for changing the user password. A user can change his or her password through the page.
- Only authenticated users can select [Service/Change Password] from the 802.1X client. The option is gray and unavailable for unauthenticated users.

## Examples

# Enable the self-service server localization function and specify the URL of the self-service server for changing user password to `http://10.153.89.94/selfservice/modPasswd1x.jsp|userName` for the default ISP domain **system**.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system]                self-service-url                enable
http://10.153.89.94/selfservice/modPasswd1x.jsp|userName
```

## service-type

### Syntax

```
service-type { ftp | lan-access | { ssh | telnet | terminal } * | portal }
undo service-type { ftp | lan-access | { ssh | telnet | terminal } * | portal }
```

### View

Local user view

### Default Level

3: Manage level

### Parameters

**ftp**: Authorizes the user to use the FTP service. The user can use the root directory of the FTP server by default.

**lan-access**: Authorizes the user to use the LAN access service. Such users are mainly Ethernet users, for example, 802.1X users.

**ssh**: Authorizes the user to use the SSH service.

**telnet**: Authorizes the user to use the Telnet service.

**terminal**: Authorizes the user to use the terminal service, allowing the user to login from the console port or AUX port.

**portal**: Authorizes the user to use the Portal service.

### Description

Use the **service-type** command to specify the service types that a user can use.

Use the **undo service-type** command to delete one or all service types configured for a user.

By default, a user is authorized with no service.

## Examples

# Authorize user **user1** to use the Telnet service.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] service-type telnet
```

## state

### Syntax

```
state { active | block }  
undo state
```

### View

ISP domain view, local user view

### Default Level

2: System level

### Parameters

**active:** Places the current ISP domain or local user in the active state, allowing the users in the current ISP domain or the current local user to request network services.

**block:** Places the current ISP domain or local user in the blocked state, preventing users in the current ISP domain or the current local user from requesting network services.

### Description

Use the **state** command to configure the status of the current ISP domain or local user.

Use the **undo state** command to restore the default.

By default, an ISP domain is active when created. So is a local user.

By blocking an ISP domain, you disable users of the domain that are offline from requesting network services. Note that the online users are not affected.

By blocking a user, you disable the user from requesting network services. No other users are affected.

Related commands: **domain**.

### Examples

# Place the current ISP domain **aabbcc.net** to the state of blocked.

```
<Sysname> system-view  
[Sysname] domain aabbcc.net  
[Sysname-isp-aabbcc.net] state block
```

# Place the current user **user1** to the state of blocked.

```
<Sysname> system-view  
[Sysname] local-user user1  
[Sysname-user-user1] state block
```

## user-group

### Syntax

```
user-group group-name  
undo user-group group-name
```

### View

System view

## Default Level

3: Manage level

## Parameters

*group-name*: User group name, a case-insensitive string of 1 to 32 characters.

## Description

Use the **user-group** command to create a user group and enter its view.

Use the **undo user-group** command to remove a user group.

A user group consists of a group of local users and has a set of local user attributes. You can configure local user attributes for a user group to implement centralized management of user attributes for the local users in the group. Currently, you can configure password control attributes and authorization attributes for a user group.

Note that:

- A user group with one or more local users cannot be removed.
- The default system user group **system** cannot be removed but you can change its configurations.

Related commands: **display user-group**.

## Examples

# Create a user group named **abc** and enter its view.

```
<Sysname> system-view
[Sysname] user-group abc
[Sysname-ugroup-abc]
```

# 2 RADIUS Configuration Commands

---

## RADIUS Configuration Commands

### data-flow-format (RADIUS scheme view)

#### Syntax

```
data-flow-format { data { byte | giga-byte | kilo-byte | mega-byte } | packet { giga-packet | kilo-packet | mega-packet | one-packet } } *  
undo data-flow-format { data | packet }
```

#### View

RADIUS scheme view

#### Default Level

2: System level

#### Parameters

**data**: Specifies the unit for data flows, which can be byte, kilobyte, megabyte, or gigabyte.

**packet**: Specifies the unit for data packets, which can be one-packet, kilo-packet, mega-packet, or giga-packet.

#### Description

Use the **data-flow-format** command to specify the unit for data flows or packets to be sent to a RADIUS server.

Use the **undo data-flow-format** command to restore the default.

By default, the unit for data flows is **byte** and that for data packets is **one-packet**.

Note that:

- The specified unit of data flows sent to the RADIUS server must be consistent with the traffic statistics unit of the RADIUS server. Otherwise, accounting cannot be performed correctly.
- You can use the commands to change the settings only when no user is using the RADIUS scheme.

Related commands: **display radius scheme**.

#### Examples

```
# Define RADIUS scheme radius1 to send data flows and packets destined for the RADIUS server in kilobytes and kilo-packets.
```

```
<Sysname> system-view  
[Sysname] radius scheme radius1  
[Sysname-radius-radius1] data-flow-format data kilo-byte packet kilo-packet
```

## display radius scheme

### Syntax

```
display radius scheme [ radius-scheme-name ] [ slot slot-number ]
```

### View

Any view

### Default Level

2: System level

### Parameters

*radius-scheme-name*: RADIUS scheme name.

**slot** *slot-number*: Specifies the specified member device in an IRF stack. The *slot-number* argument indicates the member device ID.

### Description

Use the **display radius scheme** command to display the configuration information of a specified RADIUS scheme or all RADIUS schemes.

Note that:

- If no RADIUS scheme is specified, the command will display the configurations of all RADIUS schemes.
- If no slot number is specified, the command will display the configurations of the RADIUS schemes on only the specified member device.

Related commands: **radius scheme**.

### Examples

```
# Display the configurations of all RADIUS schemes.
```

```
<Sysname> display radius scheme
```

```
-----  
SchemeName   : radius1  
Index        : 0                               Type : extended  
Primary Auth IP : 1.1.1.1                       Port : 1812   State : active  
Primary Acct IP : 1.1.1.1                       Port : 1813   State : active  
Second Auth IP  : 0.0.0.0                       Port : 1812   State : block  
Second Acct IP  : 0.0.0.0                       Port : 1813   State : block  
Auth Server Encryption Key : 123  
Acct Server Encryption Key : Not configured  
Interval for timeout(second) : 3  
Retransmission times for timeout : 3  
Interval for realtime accounting(minute) : 12  
Retransmission times of realtime-accounting packet : 5  
Retransmission times of stop-accounting packet : 500  
Quiet-interval(min) : 5  
Username format : without-domain  
Data flow unit : Byte
```

-----  
 Total 1 RADIUS scheme(s)

**Table 2-1 display radius scheme** command output description

Field	Description
SchemeName	Name of the RADIUS scheme
Index	Index number of the RADIUS scheme
Type	Type of the RADIUS server
Primary Auth IP/ Port/ State	IP address/access port number/current status of the primary authentication server: (active or block) If there is no primary authentication server specified, the IP address is 0.0.0.0 and the port number is the default. This rule is also applicable to the following three fields.
Primary Acct IP/ Port/ State	IP address/access port number/current status of the primary accounting server: (active or block)
Second Auth IP/ Port/ State	IP address/access port number/current status of the secondary authentication server: (active or block)
Second Acct IP/ Port/ State	IP address/access port number/current status of the secondary accounting server: (active or block)
Auth Server Encryption Key	Shared key of the authentication server
Acct Server Encryption Key	Shared key of the accounting server
Accounting-On packet disable	The accounting-on function is disabled
send times	Retransmission times of accounting-on packets
interval	Interval to retransmit accounting-on packets
Interval for timeout(second)	Timeout time in seconds
Retransmission times for timeout	Times of retransmission in case of timeout
Interval for realtime accounting(minute)	Interval for realtime accounting in minutes
Retransmission times of realtime-accounting packet	Retransmission times of realtime-accounting packet
Retransmission times of stop-accounting packet	Retransmission times of stop-accounting packet
Quiet-interval(min)	Quiet interval for the primary server
Username format	Format of the username
Data flow unit	Unit of data flows
Packet unit	Unit of packets
Total 1 RADIUS scheme(s)	1 RADIUS scheme in total

## display radius statistics

### Syntax

```
display radius statistics [ slot slot-number ]
```

### View

Any view

### Default Level

2: System level

### Parameters

**slot slot-number.** Specifies the specified member device in an IRF stack. The *slot-number* argument indicates the member device ID.

### Description

Use the **display radius statistics** command to display statistics about RADIUS packets.

Related commands: **radius scheme.**

### Examples

# Display statistics about RADIUS packets on the interface board in slot 1.

```
<Sysname> display radius statistics slot 1
Slot 1:state statistic(total=4096):
    DEAD = 4096      AuthProc = 0      AuthSucc = 0
AcctStart = 0      RLTSend = 0      RLWait = 0
    AcctStop = 0    OnLine = 0      Stop = 0
    StateErr = 0

Received and Sent packets statistic:
Sent PKT total    = 1547      Received PKT total = 23
Resend Times      Resend total
1                 508
2                 508
Total             1016
RADIUS received packets statistic:
Code = 2  Num = 15      Err = 0
Code = 3  Num = 4       Err = 0
Code = 5  Num = 4       Err = 0
Code = 11 Num = 0       Err = 0

Running statistic:
RADIUS received messages statistic:
Normal auth request    Num = 24      Err = 0      Succ = 24
EAP auth request       Num = 0       Err = 0      Succ = 0
Account request        Num = 4       Err = 0      Succ = 4
Account off request    Num = 503    Err = 0      Succ = 503
PKT auth timeout       Num = 15     Err = 5      Succ = 10
```

```

PKT acct_timeout      Num = 1509      Err = 503      Succ = 1006
Realtime Account timer Num = 0         Err = 0         Succ = 0
PKT response         Num = 23        Err = 0         Succ = 23
Session ctrl pkt     Num = 0         Err = 0         Succ = 0
Normal author request Num = 0         Err = 0         Succ = 0
Set policy result    Num = 0         Err = 0         Succ = 0
RADIUS sent messages statistic:
Auth accept          Num = 10
Auth reject          Num = 14
EAP auth replying   Num = 0
Account success      Num = 4
Account failure      Num = 3
Server ctrl req      Num = 0
RecError_MSG_sum    = 0
SndMSG_Fail_sum     = 0
Timer_Err           = 0
Alloc_Mem_Err       = 0
State Mismatch      = 0
Other_Error         = 0

```

No-response-acct-stop packet = 1

Discarded No-response-acct-stop packet for buffer overflow = 0

**Table 2-2 display radius statistics** command output description

Field	Description
slot	The specified member device in an IRF stack. The <i>slot</i> indicates the member device ID.
state statistic	state statistics
DEAD	Number of idle users
AuthProc	Number of users waiting for authentication
AuthSucc	Number of users who have passed authentication
AcctStart	Number of users for whom accounting has been started
RLTSend	Number of users for whom the system sends real-time accounting packets
RLTWait	Number of users waiting for real-time accounting
AcctStop	Number of users in the state of accounting waiting stopped
OnLine	Number of online users
Stop	Number of users in the state of stop
StateErr	Number of users with unknown errors
Received and Sent packets statistic	Statistics of packets received and sent
Sent PKT total	Number of packets sent
Received PKT total	Number of packets received
Resend Times	Number of retransmission attempts

<b>Field</b>	<b>Description</b>
Resend total	Number of packets retransmitted
RADIUS received packets statistic	Statistics of packets received by RADIUS
Code	Packet type
Num	Total number of packets
Err	Number of error packets
Running statistic	RADIUS operation message statistics
RADIUS received messages statistic	Number of messages received by RADIUS
Normal auth request	Number of normal authentication requests
EAP auth request	Number of EAP authentication requests
Account request	Number of accounting requests
Account off request	Number of stop-accounting requests
PKT auth timeout	Number of authentication timeout messages
PKT acct_timeout	Number of accounting timeout messages
Realtime Account timer	Number of realtime accounting requests
PKT response	Number of responses
Session ctrl pkt	Number of session control messages
Normal author request	Number of normal authorization requests
Succ	Number of acknowledgement messages
Set policy result	Number of responses to the Set policy packets
RADIUS sent messages statistic	Number of messages that have been sent by RADIUS
Auth accept	Number of accepted authentication packets
Auth reject	Number of rejected authentication packets
EAP auth replying	Number of replying packets of EAP authentication
Account success	Number of accounting succeeded packets
Account failure	Number of accounting failed packets
Server ctrl req	Number of server control requests
RecError_MSG_sum	Number of received packets in error
SndMSG_Fail_sum	Number of packets that failed to be sent out
Timer_Err	Number of timer errors
Alloc_Mem_Err	Number of memory errors
State Mismatch	Number of errors for mismatching status
Other_Error	Number of errors of other types
No-response-acct-stop packet	Number of times that no response was received for stop-accounting packets
Discarded No-response-acct-stop packet for buffer overflow	Number of stop-accounting packets that were buffered but then discarded due to full memory

## display stop-accounting-buffer

### Syntax

```
display stop-accounting-buffer { radius-scheme radius-scheme-name | session-id session-id | time-range start-time stop-time | user-name user-name } [ slot slot-number ]
```

### View

Any view

### Default Level

2: System level

### Parameters

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

**session-id** *session-id*: Specifies a session by its ID. The ID is a string of 1 to 50 characters.

**time-range** *start-time stop-time*: Specifies a time range by its start time and end time in the format of hh:mm:ss-mm/dd/yyyy or hh:mm:ss-yyyy/mm/dd.

**user-name** *user-name*: Specifies a user by the user name, which is a case-sensitive string of 1 to 80 characters. Whether the *user-name* argument should include the domain name depends on the setting by the **user-name-format** command for the RADIUS scheme.

**slot** *slot-number*: Specifies the specified member device in an IRF stack. The *slot-number* argument indicates the member device ID.

### Description

Use the **display stop-accounting-buffer** command to display information about the stop-accounting requests buffered in the device by scheme, session ID, time range, user name, or slot.

Note that if receiving no response after sending a stop-accounting request to a RADIUS server, the device buffers the request and retransmits it. You can use the **retry stop-accounting** command to set the number of allowed transmission attempts.

Related commands: **reset stop-accounting-buffer**, **stop-accounting-buffer enable**, **user-name-format**, **retry stop-accounting**.

### Examples

```
# Display information about the buffered stop-accounting requests from 0:0:0 to 23:59:59 on August 31, 2006.
```

```
<Sysname> display stop-accounting-buffer time-range 0:0:0-08/31/2006 23:59:59-08/31/2006  
Total 0 record(s) Matched
```

## key (RADIUS scheme view)

### Syntax

```
key { accounting | authentication } string
```

```
undo key { accounting | authentication }
```

## View

RADIUS scheme view

## Default Level

2: System level

## Parameters

**accounting:** Sets the shared key for RADIUS accounting packets.

**authentication:** Sets the shared key for RADIUS authentication/authorization packets.

*string:* Shared key, a case-sensitive string of 1 to 64 characters.

## Description

Use the **key** command to set the shared key for RADIUS authentication/authorization or accounting packets.

Use the **undo key** command to restore the default.

By default, no shared key is configured.

Note that:

- You must ensure that the same shared key is set on the device and the RADIUS server.
- If authentication/authorization and accounting are performed on two servers with different shared keys, you must set separate shared key for each on the device.
- You can use the commands to change the settings only when no user is using the RADIUS scheme.

Related commands: **display radius scheme**.

## Examples

# Set the shared key for authentication/authorization packets to hello for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] key authentication hello
```

# Set the shared key for accounting packets to ok for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] key accounting ok
```

## nas-ip (RADIUS scheme view)

### Syntax

**nas-ip** *ip-address*

**undo nas-ip**

### View

RADIUS scheme view

## Default Level

2: System level

## Parameters

*ip-address*: IP address in dotted decimal notation. It must be an address of the device and cannot be all 0s address, all 1s address, a class D address, a class E address or a loopback address.

## Description

Use the **nas-ip** command to set the IP address for the device to use as the source address of the RADIUS packets to be sent to the server.

Use the **undo nas-ip** command to remove the configuration.

By default, the source IP address of a packet sent to the server is that configured by the **radius nas-ip** command in system view.

Note that:

- Specifying a source address for the RADIUS packets to be sent to the server can avoid the situation where the packets sent back by the RADIUS server cannot reach the device as the result of a physical interface failure. The address of a loopback interface is recommended.
- The **nas-ip** command in RADIUS scheme view is only for the current RADIUS scheme, while the **radius nas-ip** command in system view is for all RADIUS schemes. However, the **nas-ip** command in RADIUS scheme view overwrites the configuration of the **radius nas-ip** command.
- You can use the commands to change the settings only when no user is using the RADIUS scheme.

Related commands: **radius nas-ip**.

## Examples

```
# Set the IP address for the device to use as the source address of the RADIUS packets to 10.1.1.1.
```

```
<Sysname> system-view
[Sysname] radius scheme test1
[Sysname-radius-test1] nas-ip 10.1.1.1
```

## primary accounting (RADIUS scheme view)

### Syntax

```
primary accounting ip-address [ port-number ]
undo primary accounting
```

### View

RADIUS scheme view

## Default Level

2: System level

## Parameters

*ip-address*: IP address of the primary accounting server.

*port-number*: UDP port number of the primary accounting server, which ranges from 1 to 65535 and defaults to 1813.

## Description

Use the **primary accounting** command to specify the primary RADIUS accounting server.

Use the **undo primary accounting** command to remove the configuration.

By default, no primary RADIUS accounting server is specified.

Note that:

- The IP addresses of the primary and secondary accounting servers cannot be the same. Otherwise, the configuration fails.
- The RADIUS service port configured on the device and that of the RADIUS server must be consistent.
- You can use the commands to change the settings only when no user is using the RADIUS scheme.

Related commands: **key**, **radius scheme**, **state**.

## Examples

```
# Specify the IP address of the primary accounting server for RADIUS scheme radius1 as 10.110.1.2 and the UDP port of the server as 1813.
```

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary accounting 10.110.1.2 1813
```

## primary authentication (RADIUS scheme view)

### Syntax

```
primary authentication ip-address [ port-number ]
```

```
undo primary authentication
```

### View

RADIUS scheme view

### Default Level

2: System level

### Parameters

*ip-address*: IP address of the primary authentication/authorization server.

*port-number*: UDP port number of the primary authentication/authorization server, which ranges from 1 to 65535 and defaults to 1812.

## Description

Use the **primary authentication** command to specify the primary RADIUS authentication/authorization server.

Use the **undo primary authentication** command to remove the configuration.

By default, no primary RADIUS authentication/authorization server is specified.

Note that:

- After creating a RADIUS scheme, you are supposed to configure the IP address and UDP port of each RADIUS server (primary/secondary authentication/authorization or accounting server). Ensure that at least one authentication/authorization server and one accounting server are configured, and that the RADIUS service port settings on the device are consistent with the port settings on the RADIUS servers.
- The IP addresses of the primary and secondary authentication/authorization servers cannot be the same. Otherwise, the configuration fails.
- You can use the commands to change the settings only when no user is using the RADIUS scheme.

Related commands: **key**, **radius scheme**, **state**.

## Examples

# Specify the primary authentication/authorization server for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary authentication 10.110.1.1 1812
```

## radius client

### Syntax

**radius client enable**

**undo radius client**

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **radius client enable** command to enable the listening port of the RADIUS client.

Use the **undo radius client** command to disable the listening port of the RADIUS client.

By default, the listening port is enabled.

Note that when the listening port of the RADIUS client is disabled:

- The RADIUS client can either accept authentication, authorization or accounting requests or process timer messages. However, it fails to transmit and receive packets to and from the RADIUS server.
- The end account packets of online users cannot be sent out and buffered. This may cause a problem that the RADIUS server still has the user record after a user goes offline for a period of time.

- The authentication, authorization and accounting turn to the local scheme after the RADIUS request fails if the RADIUS scheme and the local authentication, authorization and accounting scheme are configured.
- The buffered accounting packets cannot be sent out and will be deleted from the buffer when the configured maximum number of attempts is reached.

## Examples

```
# Enable the listening port of the RADIUS client.
```

```
<Sysname> system-view  
[Sysname] radius client enable
```

## radius nas-ip

### Syntax

```
radius nas-ip ip-address  
undo radius nas-ip
```

### View

System view

### Default Level

2: System level

### Parameters

*ip-address*: IP address in dotted decimal notation. It must be an address of the device and cannot be all 0s address, all 1s address, a class D address, a class E address or a loopback address.

### Description

Use the **radius nas-ip** command to set the IP address for the device to use as the source address of the RADIUS packets to be sent to the server.

Use the **undo radius nas-ip** command to remove the configuration.

By default, the source IP address of a packet sent to the server is the IP address of the outbound port.

Note that:

- Specifying a source address for the RADIUS packets to be sent to the server can avoid the situation where the packets sent back by the RADIUS server cannot reach the device as the result of a physical interface failure.
- If you configure the command for more than one time, the last configuration takes effect.
- The **nas-ip** command in RADIUS scheme view is only for the current RADIUS scheme, while the **radius nas-ip** command in system view is for all RADIUS schemes. However, the **nas-ip** command in RADIUS scheme view overwrites the configuration of the **radius nas-ip** command.

Related commands: **nas-ip**.

## Examples

```
# Set the IP address for the device to use as the source address of the RADIUS packets to 129.10.10.1.
```

```
<Sysname> system-view  
[Sysname] radius nas-ip 129.10.10.1
```

## radius scheme

### Syntax

```
radius scheme radius-scheme-name  
undo radius scheme radius-scheme-name
```

### View

System view

### Default Level

3: Manage level

### Parameters

*radius-scheme-name*: RADIUS scheme name, a case-insensitive string of 1 to 32 characters.

### Description

Use the **radius scheme** command to create a RADIUS scheme and enter RADIUS scheme view.

Use the **undo radius scheme** command to delete a RADIUS scheme.

By default, no RADIUS scheme is defined.

Note that:

- The RADIUS protocol is configured scheme by scheme. Every RADIUS scheme must at least specify the IP addresses and UDP ports of the RADIUS authentication/authorization/accounting servers and the parameters necessary for a RADIUS client to interact with the servers.
- A RADIUS scheme can be referenced by more than one ISP domain at the same time.
- You cannot remove the RADIUS scheme being used by online users with the **undo radius scheme** command.

Related commands: **key**, **retry** **realtime-accounting**, **timer** **realtime-accounting**, **stop-accounting-buffer enable**, **retry stop-accounting**, **server-type**, **state**, **user-name-format**, **retry**, **display radius scheme**, **display radius statistics**.

### Examples

```
# Create a RADIUS scheme named radius1 and enter RADIUS scheme view.
```

```
<Sysname> system-view  
[Sysname] radius scheme radius1  
[Sysname-radius-radius1]
```

## radius trap

### Syntax

```
radius trap { accounting-server-down | authentication-server-down }  
undo radius trap { accounting-server-down | authentication-server-down }
```

### View

System view

## Default Level

2: System level

## Parameters

**accounting-server-down**: RADIUS trap for accounting servers.

**authentication-server-down**: RADIUS trap for authentication servers.

## Description

Use the **radius trap** command to enable the RADIUS trap function.

Use the **undo radius trap** command to disable the function.

By default, the RADIUS trap function is disabled.

Note that:

- If a NAS sends an accounting or authentication request to the RADIUS server but gets no response, the NAS retransmits the request. With the RADIUS trap function enabled, when the NAS transmits the request for half of the specified maximum number of transmission attempts, it sends a trap message; when the NAS transmits the request for the specified maximum number, it sends another trap message.
- If the specified maximum number of transmission attempts is odd, the half of the number refers to the smallest integer greater than the half of the number.

## Examples

```
# Enable the RADIUS trap function for accounting servers.
```

```
<Sysname> system-view
```

```
[Sysname] radius trap accounting-server-down
```

## reset radius statistics

### Syntax

```
reset radius statistics [ slot slot-number ]
```

### View

User view

## Default Level

2: System level

## Parameters

**slot slot-number**: Specifies the specified member device in an IRF stack. The *slot-number* argument indicates the member device ID.

## Description

Use the **reset radius statistics** command to clear RADIUS statistics.

Related commands: **display radius scheme**.

## Examples

```
# Clear RADIUS statistics.  
<Sysname> reset radius statistics
```

## reset stop-accounting-buffer

### Syntax

```
reset stop-accounting-buffer { radius-scheme radius-scheme-name | session-id session-id |  
time-range start-time stop-time | user-name user-name } [ slot slot-number ]
```

### View

User view

### Default Level

2: System level

### Parameters

**radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, a string of 1 to 32 characters.

**session-id** *session-id*: Specifies a session by its ID, a string of 1 to 50 characters.

**time-range** *start-time stop-time*: Specifies a time range by its start time and end time in the format of hh:mm:ss-mm/dd/yyyy or hh:mm:ss-yyyy/mm/dd.

**user-name** *user-name*: Specifies a user name based on which to reset the stop-accounting buffer. The username is a case-sensitive string of 1 to 80 characters. The format of the *user-name* argument (for example, whether the domain name should be included) must comply with that specified for usernames to be sent to the RADIUS server in the RADIUS scheme.

**slot** *slot-number*: Specifies the specified member device in an IRF stack. The *slot-number* argument indicates the member device ID.

### Description

Use the **reset stop-accounting-buffer** command to clear the buffered stop-accounting requests, which get no responses.

Related commands: **stop-accounting-buffer enable**, **retry stop-accounting**, **user-name-format**, **display stop-accounting-buffer**.

### Examples

```
# Clear the buffered stop-accounting requests for user user0001@aabbcc.net.
```

```
<Sysname> reset stop-accounting-buffer user-name user0001@aabbcc.net
```

```
# Clear the buffered stop-accounting requests in the time range from 0:0:0 to 23:59:59 on August 31, 2006.
```

```
<Sysname> reset stop-accounting-buffer time-range 0:0:0-08/31/2006 23:59:59-08/31/2006
```

## retry

### Syntax

```
retry retry-times
```

```
undo retry
```

### View

RADIUS scheme view

### Default Level

2: System level

### Parameters

*retry-times*: Maximum number of transmission attempts, in the range 1 to 20.

### Description

Use the **retry** command to set the maximum number of RADIUS transmission attempts.

Use the **undo retry** command to restore the default.

The default value for the *retry-times* argument is 3.

Note that:

- As RADIUS uses UDP packets to transmit data, the communication is not reliable. If the device does not receive a response to its request from the RADIUS server within the response timeout time, it will retransmit the RADIUS request. If the number of transmission attempts exceeds the limit but the device still receives no response from the RADIUS server, the device regards that the authentication fails.
- The maximum number of transmission attempts defined by this command refers to the sum of all transmission attempts sent by the device to the primary server and the secondary server. For example, assume that the maximum number of transmission attempts is N and both the primary server and secondary RADIUS server are specified and exist, the device will send a request to the other server if the current server does not respond after the sum of transmission attempts reaches N/2 (if N is an even number) or (N+1)/2 (if N is an odd number).
- The maximum number of transmission attempts multiplied by the RADIUS server response timeout period cannot be greater than 75.

Related commands: **radius scheme**, **timer response-timeout**.

### Examples

```
# Set the maximum number of RADIUS request transmission attempts to 5 for RADIUS scheme radius1.
```

```
<Sysname> system-view  
[Sysname] radius scheme radius1  
[Sysname-radius-radius1] retry 5
```

## retry realtime-accounting

### Syntax

```
retry realtime-accounting retry-times
```

## undo retry realtime-accounting

### View

RADIUS scheme view

### Default Level

2: System level

### Parameters

*retry-times*: Maximum number of accounting request transmission attempts. It ranges from 1 to 255 and defaults to 5.

### Description

Use the **retry realtime-accounting** command to set the maximum number of accounting request transmission attempts.

Use the **undo retry realtime-accounting** command to restore the default.

Note that:

- A RADIUS server usually checks whether a user is online by a timeout timer. If it receives from the NAS no real-time accounting packet for a user in the timeout period, it considers that there may be line or device failure and stops accounting for the user. This may happen when some unexpected failure occurs. In this case, the NAS is required to disconnect the user in accordance. This is done by the maximum number of accounting request transmission attempts. Once the limit is reached but the NAS still receives no response, the NAS disconnects the user.
- Suppose that the RADIUS server response timeout period is 3 seconds (set with the **timer response-timeout** command), the timeout retransmission attempts is 3 (set with the **retry** command), and the real-time accounting interval is 12 minutes (set with the **timer realtime-accounting** command), and the maximum number of accounting request transmission attempts is 5 (set with the **retry realtime-accounting** command). In such a case, the device generates an accounting request every 12 minutes, and retransmits the request when receiving no response within 3 seconds. The accounting is deemed unsuccessful if no response is received within 3 requests. Then the device sends a request every 12 minutes, and if for 5 times it still receives no response, the device will cut the user connection.

Related commands: **radius scheme**, **timer realtime-accounting**.

### Examples

```
# Set the maximum number of accounting request transmission attempts to 10 for RADIUS scheme radius1.
```

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry realtime-accounting 10
```

## retry stop-accounting (RADIUS scheme view)

### Syntax

```
retry stop-accounting retry-times
```

```
undo retry stop-accounting
```

## View

RADIUS scheme view

## Default Level

2: System level

## Parameters

*retry-times*: Maximum number of stop-accounting request transmission attempts. It ranges from 10 to 65,535 and defaults to 500.

## Description

Use the **retry stop-accounting** command to set the maximum number of stop-accounting request transmission attempts.

Use the **undo retry stop-accounting** command to restore the default.

- Suppose that the RADIUS server response timeout period is 3 seconds (set with the **timer response-timeout** command), the timeout retransmission attempts is 5 (set with the **retry** command), and the maximum number of stop-accounting request transmission attempts is 20 (set with the **retry stop-accounting** command). This means that for each stop-accounting request, if the device receives no response within 3 seconds, it will initiate a new request. If still no responses are received within 5 renewed requests, the stop-accounting request is deemed unsuccessful. Then the device will temporarily store the request in the device and resend a request and repeat the whole process described above. Only when 20 consecutive attempts fail will the device discard the request.

Related commands: **reset stop-accounting-buffer**, **radius scheme**, **display stop-accounting-buffer**.

## Examples

```
# Set the maximum number of stop-accounting request transmission attempts to 1,000 for RADIUS scheme radius1.
```

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry stop-accounting 1000
```

## secondary accounting (RADIUS scheme view)

### Syntax

```
secondary accounting ip-address [ port-number ]
undo secondary accounting
```

### View

RADIUS scheme view

### Default Level

2: System level

## Parameters

*ip-address*: IP address of the secondary accounting server, in dotted decimal notation. The default is 0.0.0.0.

*port-number*: UDP port number of the secondary accounting server, which ranges from 1 to 65535 and defaults to 1813.

## Description

Use the **secondary accounting** command to specify the secondary RADIUS accounting server.

Use the **undo secondary accounting** command to remove the configuration.

By default, no secondary RADIUS accounting server is specified.

Note that:

- The IP addresses of the primary and secondary accounting servers cannot be the same. Otherwise, the configuration fails.
- The RADIUS service port configured on the device and that of the RADIUS server must be consistent.
- You can use the commands to change the settings only when no user is using the RADIUS scheme.

Related commands: **key**, **radius scheme**, **state**.

## Examples

```
# Specify the secondary accounting server for RADIUS scheme radius1.
```

```
<Sysname> system-view
```

```
[Sysname] radius scheme radius1
```

```
[Sysname-radius-radius1] secondary accounting 10.110.1.1 1813
```

## secondary authentication (RADIUS scheme view)

### Syntax

```
secondary authentication ip-address [ port-number ]
```

```
undo secondary authentication
```

### View

```
RADIUS scheme view
```

### Default Level

```
2: System level
```

## Parameters

*ip-address*: IP address of the secondary authentication/authorization server, in dotted decimal notation. The default is 0.0.0.0.

*port-number*: UDP port number of the secondary authentication/authorization server, which ranges from 1 to 65535 and defaults to 1812.

## Description

Use the **secondary authentication** command to specify the secondary RADIUS authentication/authorization server.

Use the **undo secondary authentication** command to remove the configuration.

By default, no secondary RADIUS authentication/authorization server is specified.

Note that:

- The IP addresses of the primary and secondary authentication/authorization servers cannot be the same. Otherwise, the configuration fails.
- The RADIUS service port configured on the device and that of the RADIUS server must be consistent.
- You can use the commands to change the settings only when no user is using the RADIUS scheme.

Related commands: **key**, **radius scheme**, **state**.

## Examples

```
# Specify the secondary authentication/authorization server for RADIUS scheme radius1.
```

```
<Sysname> system-view  
[Sysname] radius scheme radius1  
[Sysname-radius-radius1] secondary authentication 10.110.1.2 1812
```

## security-policy-server

### Syntax

```
security-policy-server ip-address  
undo security-policy-server { ip-address | all }
```

### View

RADIUS scheme view

### Default Level

2: System level

### Parameters

*ip-address*: IP address of a security policy server.

**all**: All IP addresses

## Description

Use the **security-policy-server** command to specify a security policy server.

Use the **undo security-policy-server** command to remove one or all security policy servers.

By default, no security policy server is specified.

Note that:

- If more than one interface of the device is configured with user access authentication functions, the interfaces may use different security policy servers. You can specify up to eight security policy servers for a RADIUS scheme.

- The specified security policy server must be a security policy server or RADIUS server that is correctly configured and working normally. Otherwise, the device will regard it as an illegal server.
- You can use the commands to change the settings only when no user is using the RADIUS scheme.

Related commands: **radius nas-ip**.

## Examples

# For RADIUS scheme **radius1**, set the IP address of a security policy server to 10.110.1.2.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] security-policy-server 10.110.1.2
```

## server-type

### Syntax

**server-type** { **extended** | **standard** }

**undo server-type**

### View

RADIUS scheme view

### Default Level

2: System level

### Parameters

**extended**: Specifies the extended RADIUS server (generally CAMS/iMC), which requires the RADIUS client and RADIUS server to interact according to the procedures and packet formats provisioned by the private RADIUS protocol.

**standard**: Specifies the standard RADIUS server, which requires the RADIUS client end and RADIUS server to interact according to the regulation and packet format of the standard RADIUS protocol (RFC 2865/2866 or newer).

### Description

Use the **server-type** command to specify the RADIUS server type supported by the device.

Use the **undo server-type** command to restore the default.

By default, the supported RADIUS server type is **standard**.

Note that you can use the commands to change the setting only when no user is using the RADIUS scheme.

Related commands: **radius scheme**.

## Examples

# Set the RADIUS server type of RADIUS scheme **radius1** to **standard**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] server-type standard
```

## state

### Syntax

```
state { primary | secondary } { accounting | authentication } { active | block }
```

### View

RADIUS scheme view

### Default Level

2: System level

### Parameters

**primary:** Sets the status of the primary RADIUS server.

**secondary:** Sets the status of the secondary RADIUS server.

**accounting:** Sets the status of the RADIUS accounting server.

**authentication:** Sets the status of the RADIUS authentication/authorization server.

**active:** Sets the status of the RADIUS server to **active**, namely the normal operation state.

**block:** Sets the status of the RADIUS server to **block**.

### Description

Use the **state** command to set the status of a RADIUS server.

By default, every RADIUS server configured with an IP address in the RADIUS scheme is in the state of active.

Note that:

- When a primary server, authentication/authorization server or accounting server, fails, the device automatically turns to the secondary server.
- Once the primary server fails, the primary server turns into the blocked state, and the device turns to the secondary server. In this case, if the secondary server is available, the device triggers the primary server quiet timer. After the quiet timer times out, the status of the primary server is active again and the status of the secondary server remains the same. If the secondary server fails, the device restores the status of the primary server to active immediately. If the primary server has resumed, the device turns to use the primary server and stops communicating with the secondary server. After accounting starts, the communication between the client and the secondary server remains unchanged.
- When both the primary server and the secondary server are in the state of blocked, you need to set the status of the secondary server to active to use the secondary server for authentication. Otherwise, the switchover will not occur.
- If one server is in the active state while the other is blocked, the switchover will not take place even if the active server is not reachable.
- You can use this command to change the settings only when no user is using the RADIUS scheme.

Related commands: **radius scheme**, **primary authentication**, **secondary authentication**, **primary accounting**, **secondary accounting**.

### Examples

```
# Set the status of the secondary server in RADIUS scheme radius1 to active.
```

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] state secondary authentication active
```

## stop-accounting-buffer enable (RADIUS scheme view)

### Syntax

```
stop-accounting-buffer enable
undo stop-accounting-buffer enable
```

### View

RADIUS scheme view

### Default Level

2: System level

### Parameters

None

### Description

Use the **stop-accounting-buffer enable** command to enable the device to buffer stop-accounting requests getting no responses.

Use the **undo stop-accounting-buffer enable** command to disable the device from buffering stop-accounting requests getting no responses.

By default, the device is enabled to buffer stop-accounting requests getting no responses.

Since stop-accounting requests affect the charge to users, a NAS must make its best effort to send every stop-accounting request to the RADIUS accounting servers. For each stop-accounting request getting no response in the specified period of time, the NAS buffers and resends the packet until it receives a response or the number of transmission retries reaches the configured limit. In the latter case, the NAS discards the packet.

Note that you can use the commands to change the setting only when no user is using the RADIUS scheme.

Related commands: **reset stop-accounting-buffer**, **radius scheme**, **display stop-accounting-buffer**.

### Examples

# In RADIUS scheme **radius1**, enable the device to buffer the stop-accounting requests getting no responses.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] stop-accounting-buffer enable
```

## timer quiet (RADIUS scheme view)

### Syntax

```
timer quiet minutes
```

## undo timer quiet

### View

RADIUS scheme view

### Default Level

2: System level

### Parameters

*minutes*: Primary server quiet period, in minutes. It ranges from 1 to 255 and defaults to 5.

### Description

Use the **timer quiet** command to set the quiet timer for the primary server, that is, the duration that the status of the primary server stays blocked before resuming the active state.

Use the **undo timer quiet** command to restore the default.

Related commands: **display radius scheme**.

### Examples

# Set the quiet timer for the primary server to 10 minutes.

```
<Sysname> system-view
[Sysname] radius scheme test1
[Sysname-radius-test1] timer quiet 10
```

## timer realtime-accounting (RADIUS scheme view)

### Syntax

**timer realtime-accounting** *minutes*

**undo timer realtime-accounting**

### View

RADIUS scheme view

### Default Level

2: System level

### Parameters

*minutes*: Real-time accounting interval in minutes, must be a multiple of 3 and in the range 3 to 60, with the default value being 12.

### Description

Use the **timer realtime-accounting** command to set the real-time accounting interval.

Use the **undo timer realtime-accounting** command to restore the default.

Note that:

- For real-time accounting, a NAS must transmit the accounting information of online users to the RADIUS accounting server periodically. This command is for setting the interval.

- The setting of the real-time accounting interval somewhat depends on the performance of the NAS and the RADIUS server: a shorter interval requires higher performance. You are therefore recommended to adopt a longer interval when there are a large number of users (more than 1000, inclusive). The following table lists the recommended ratios of the interval to the number of users.

**Table 2-3** Recommended ratios of the accounting interval to the number of users

Number of users	Real-time accounting interval (minute)
1 to 99	3
100 to 499	6
500 to 999	12
1000 or more	15 or more

Related commands: **retry realtime-accounting**, **radius scheme**.

### Examples

# Set the real-time accounting interval to 51 minutes for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer realtime-accounting 51
```

### timer response-timeout (RADIUS scheme view)

#### Syntax

```
timer response-timeout seconds
undo timer response-timeout
```

#### View

RADIUS scheme view

#### Default Level

2: System level

#### Parameters

*seconds*: RADIUS server response timeout period in seconds. It ranges from 1 to 10 and defaults to 3.

#### Description

Use the **timer response-timeout** command to set the RADIUS server response timeout timer.

Use the **undo timer** command to restore the default.

Note that:

- If a NAS receives no response from the RADIUS server in a period of time after sending a RADIUS request (authentication/authorization or accounting request), it has to resend the request so that the user has more opportunity to obtain the RADIUS service. The NAS uses the RADIUS server response timeout timer to control the transmission interval.
- A proper value for the RADIUS server response timeout timer can help improve the system performance. Set the timer based on the network conditions.

- The maximum total number of all types of retransmission attempts multiplied by the RADIUS server response timeout period cannot be greater than 75.

Related commands: **radius scheme**, **retry**.

## Examples

```
# Set the RADIUS server response timeout timer to 5 seconds for RADIUS scheme radius1.
```

```
<Sysname> system-view  
[Sysname] radius scheme radius1  
[Sysname-radius-radius1] timer response-timeout 5
```

## user-name-format (RADIUS scheme view)

### Syntax

```
user-name-format { keep-original | with-domain | without-domain }
```

### View

RADIUS scheme view

### Default Level

2: System level

### Parameters

**keep-original**: Sends the username to the RADIUS server as it is input.

**with-domain**: Includes the ISP domain name in the username sent to the RADIUS server.

**without-domain**: Excludes the ISP domain name from the username sent to the RADIUS server.

### Description

Use the **user-name-format** command to specify the format of the username to be sent to a RADIUS server.

By default, the ISP domain name is included in the username.

Note that:

- A username is generally in the format of `userid@isp-name`, of which `isp-name` is used by the device to determine the ISP domain to which a user belongs. Some earlier RADIUS servers, however, cannot recognize a username including an ISP domain name. Before sending a username including a domain name to such a RADIUS server, the device must remove the domain name. This command is thus provided for you to decide whether to include a domain name in a username to be sent to a RADIUS server.
- If a RADIUS scheme defines that the username is sent without the ISP domain name, do not apply the RADIUS scheme to more than one ISP domain, thus avoiding the confused situation where the RADIUS server regards two users in different ISP domains but with the same user ID as one.
- When 802.1X users use EAP authentication, the **user-name-format** command configured for a RADIUS scheme does not take effect and the device does not change the usernames from clients when forwarding them to the RADIUS server.
- If the RADIUS scheme is for wireless users, specify the **keep-original** keyword. Otherwise, authentication of the wireless users may fail.

Related commands: **radius scheme**.

## Examples

# Specify the device to remove the domain name in the username sent to the RADIUS servers for the RADIUS scheme **radius1**.

```
<Sysname> system-view
```

```
[Sysname] radius scheme radius1
```

```
[Sysname-radius-radius1] user-name-format without-domain
```

# 3 HWTACACS Configuration Commands

---

## HWTACACS Configuration Commands

### data-flow-format (HWTACACS scheme view)

#### Syntax

```
data-flow-format { data { byte | giga-byte | kilo-byte | mega-byte } | packet { giga-packet | kilo-packet | mega-packet | one-packet } } *  
undo data-flow-format { data | packet }
```

#### View

HWTACACS scheme view

#### Default Level

2: System level

#### Parameters

**data**: Specifies the unit for data flows, which can be byte, kilobyte, megabyte, or gigabyte.

**packet**: Specifies the unit for data packets, which can be one-packet, kilo-packet, mega-packet, or giga-packet.

#### Description

Use the **data-flow-format** command to specify the unit for data flows or packets to be sent to a HWTACACS server.

Use the **undo data-flow-format** command to restore the default.

By default, the unit for data flows is **byte** and that for data packets is **one-packet**.

Related commands: **display hwtacacs**.

#### Examples

# Define HWTACACS scheme **hwt1** to send data flows and packets destined for the TACACS server in kilobytes and kilo-packets.

```
<Sysname> system-view  
[Sysname] hwtacacs scheme hwt1  
[Sysname-hwtacacs-hwt1] data-flow-format data kilo-byte packet kilo-packet
```

## display hwtacacs

#### Syntax

```
display hwtacacs [ hwtacacs-scheme-name [ statistics ] ] [ slot slot-number ]
```

## View

Any view

## Default Level

2: System level

## Parameters

*hwtacacs-scheme-name*: HWTACACS scheme name.

**statistics**: Displays complete statistics about the HWTACACS server.

**slot** *slot-number*: Specifies the specified member device in an IRF stack. The *slot-number* argument indicates the member device ID.

## Description

Use the **display hwtacacs** command to display configuration information or statistics of the specified or all HWTACACS schemes.

Note that:

- If no HWTACACS scheme is specified, the command will display the configuration information of all HWTACACS schemes.
- If no slot number is specified, the command will display the configuration information of the HWTACACS scheme on the main processing unit.

Related commands: **hwtacacs scheme**.

## Examples

# Display configuration information about HWTACACS scheme **gy**.

```
<Sysname> display hwtacacs gy
```

```
-----  
HWTACACS-server template name      : gy  
Primary-authentication-server      : 172.31.1.11:49  
Primary-authorization-server       : 172.31.1.11:49  
Primary-accounting-server          : 172.31.1.11:49  
Secondary-authentication-server    : 0.0.0.0:0  
Secondary-authorization-server     : 0.0.0.0:0  
Secondary-accounting-server        : 0.0.0.0:0  
Current-authentication-server      : 172.31.1.11:49  
Current-authorization-server       : 172.31.1.11:49  
Current-accounting-server          : 172.31.1.11:49  
NAS-IP-address                     : 0.0.0.0  
key authentication                  : 790131  
key authorization                   : 790131  
key accounting                      : 790131  
Quiet-interval(min)                : 5  
Realtime-accounting-interval(min)  : 12  
Response-timeout-interval(sec)     : 5  
Acct-stop-PKT retransmit times     : 100  
Username format                    : with-domain
```

```
Data traffic-unit          : B
Packet traffic-unit       : one-packet
-----
```

**Table 3-1 display hwtaacs command output description**

Field	Description
HWTACACS-server template name	Name of the HWTACACS scheme
Primary-authentication-server	IP address and port number of the primary authentication server. If there is no primary authentication server specified, the value of this field is 0.0.0.0:0. This rule is also applicable to the following eight fields.
Primary-authorization-server	IP address and port number of the primary authorization server
Primary-accounting-server	IP address and port number of the primary accounting server
Secondary-authentication-server	IP address and port number of the secondary authentication server
Secondary-authorization-server	IP address and port number of the secondary authorization server
Secondary-accounting-server	IP address and port number of the secondary accounting server
Current-authentication-server	IP address and port number of the currently used authentication server
Current-authorization-server	IP address and port number of the currently used authorization server
Current-accounting-server	IP address and port number of the currently used accounting server
NAS-IP-address	IP address of the NAS If no NAS is specified, the value of this field is 0.0.0.0.
key authentication	Key for authentication
key authorization	Key for authorization
key accounting	Key for accounting
Quiet-interval	Quiet interval for the primary server
Realtime-accounting-interval	Real-time accounting interval
Response-timeout-interval	Server response timeout period
Acct-stop-PKT retransmit times	Number of stop-accounting packet transmission retries
Username format	with-domain Whether a user name includes the domain name
Data traffic-unit	Unit for data flows
Packet traffic-unit	Unit for data packets

## display stop-accounting-buffer

### Syntax

```
display stop-accounting-buffer hwtacacs-scheme hwtacacs-scheme-name [ slot slot-number ]
```

### View

Any view

### Default Level

2: System level

### Parameters

**hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies a HWTACACS scheme by its name, a string of 1 to 32 characters.

**slot** *slot-number*: Specifies the specified member device in an IRF stack. The *slot-number* argument indicates the member device ID.

### Description

Use the **display stop-accounting-buffer** command to display information about the stop-accounting requests buffered in the device.

Related commands: **reset stop-accounting-buffer**, **stop-accounting-buffer enable**, **retry stop-accounting**.

### Examples

```
# Display information about the buffered stop-accounting requests for HWTACACS scheme hwt1.
```

```
<Sysname> display stop-accounting-buffer hwtacacs-scheme hwt1  
Total 0 record(s) Matched
```

## hwtacacs nas-ip

### Syntax

```
hwtacacs nas-ip ip-address  
undo hwtacacs nas-ip
```

### View

System view

### Default Level

2: System level

### Parameters

*ip-address*: IP address in dotted decimal notation. It must be an address of the device and cannot be all 0s address, all 1s address, a class D address, a class E address or a loopback address.

## Description

Use the **hwtacacs nas-ip** command to set the IP address for the device to use as the source address of the HWTACACS packets to be sent to the server.

Use the **undo hwtacacs nas-ip** command to remove the configuration.

By default, the source IP address of a packet sent to the server is the IP address of the outbound port.

Note that:

- Specifying a source address for the HWTACACS packets to be sent to the server can avoid the situation where the packets sent back by the HWTACACS server cannot reach the device as the result of a physical interface failure.
- If you configure the command for more than one time, the last configuration takes effect.
- The **nas-ip** command in HWTACACS scheme view is only for the current HWTACACS scheme, while the **hwtacacs nas-ip** command in system view is for all HWTACACS schemes. However, the **nas-ip** command in HWTACACS scheme view overwrites the configuration of the **hwtacacs nas-ip** command.

Related commands: **nas-ip**.

## Examples

```
# Set the IP address for the device to use as the source address of the HWTACACS packets to 129.10.10.1.
```

```
<Sysname> system-view  
[Sysname] hwtacacs nas-ip 129.10.10.1
```

## hwtacacs scheme

### Syntax

```
hwtacacs scheme hwtacacs-scheme-name  
undo hwtacacs scheme hwtacacs-scheme-name
```

### View

System view

### Default Level

3: Manage level

### Parameters

*hwtacacs-scheme-name*: HWTACACS scheme name, a case-insensitive string of 1 to 32 characters.

## Description

Use the **hwtacacs scheme** command to create an HWTACACS scheme and enter HWTACACS scheme view.

Use the **undo hwtacacs scheme** command to delete an HWTACACS scheme.

By default, no HWTACACS scheme exists.

Note that you cannot delete an HWTACACS scheme with online users.

## Examples

```
# Create an HWTACACS scheme named hwt1 and enter HWTACACS scheme view.
```

```
<Sysname> system-view  
[Sysname] hwtacacs scheme hwt1  
[Sysname-hwtacacs-hwt1]
```

## key (HWTACACS scheme view)

### Syntax

```
key { accounting | authentication | authorization } string  
undo key { accounting | authentication | authorization } string
```

### View

HWTACACS scheme view

### Default Level

2: System level

### Parameters

**accounting**: Sets the shared key for HWTACACS accounting packets.

**authentication**: Sets the shared key for HWTACACS authentication packets.

**authorization**: Sets the shared key for HWTACACS authorization packets.

*string*: Shared key, a string of 1 to 16 characters.

### Description

Use the **key** command to set the shared key for HWTACACS authentication, authorization, or accounting packets.

Use the **undo key** command to remove the configuration.

By default, no shared key is configured.

Related commands: **display hwtacacs**.

## Examples

```
# Set the shared key for HWTACACS accounting packets to hello for HWTACACS scheme hwt1.
```

```
<Sysname> system-view  
[Sysname] hwtacacs scheme hwt1  
[Sysname-hwtacacs-hwt1] key accounting hello
```

## nas-ip (HWTACACS scheme view)

### Syntax

```
nas-ip ip-address  
undo nas-ip
```

## View

HWTACACS scheme view

## Default Level

2: System level

## Parameters

*ip-address*: IP address in dotted decimal notation. It must be an address of the device and cannot be all 0s address, all 1s address, a class D address, a class E address or a loopback address.

## Description

Use the **nas-ip** command to set the IP address for the device to use as the source address of the HWTACACS packets to be sent to the server.

Use the **undo nas-ip** command to remove the configuration.

By default, the source IP address of a packet sent to the server is the IP address of the outbound port.

Note that:

- Specifying a source address for the HWTACACS packets to be sent to the server can avoid the situation where the packets sent back by the HWTACACS server cannot reach the device as the result of a physical interface failure.
- If you configure the command for more than one time, the last configuration takes effect.
- The **nas-ip** command in HWTACACS scheme view is only for the current HWTACACS scheme, while the **hwtacacs nas-ip** command in system view is for all HWTACACS schemes. However, the **nas-ip** command in HWTACACS scheme view overwrites the configuration of the **hwtacacs nas-ip** command.

Related commands: **hwtacacs nas-ip**.

## Examples

```
# Set the IP address for the device to use as the source address of the HWTACACS packets to 10.1.1.1.
```

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] nas-ip 10.1.1.1
```

## primary accounting (HWTACACS scheme view)

### Syntax

```
primary accounting ip-address [ port-number ]
```

```
undo primary accounting
```

### View

HWTACACS scheme view

### Default Level

2: System level

## Parameters

*ip-address*: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

*port-number*: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

## Description

Use the **primary accounting** command to specify the primary HWTACACS accounting server.

Use the **undo primary accounting** command to remove the configuration.

By default, no primary HWTACACS accounting server is specified.

Note that:

- The IP addresses of the primary and secondary accounting servers cannot be the same. Otherwise, the configuration fails.
- The HWTACACS service port configured on the device and that of the HWTACACS server must be consistent.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an accounting server only when no active TCP connection for sending accounting packets is using it.

## Examples

```
# Specify the primary accounting server.
```

```
<Sysname> system-view
```

```
[Sysname] hwtacacs scheme test1
```

```
[Sysname-hwtacacs-test1] primary accounting 10.163.155.12 49
```

## primary authentication (HWTACACS scheme view)

### Syntax

```
primary authentication ip-address [ port-number ]
```

```
undo primary authentication
```

### View

```
HWTACACS scheme view
```

### Default Level

```
2: System level
```

## Parameters

*ip-address*: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

*port-number*: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

## Description

Use the **primary authentication** command to specify the primary HWTACACS authentication server.

Use the **undo primary authentication** command to remove the configuration.

By default, no primary HWTACACS authentication server is specified.

Note that:

- The IP addresses of the primary and secondary authentication servers cannot be the same. Otherwise, the configuration fails.
- The HWTACACS service port configured on the device and that of the HWTACACS server must be consistent.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an authentication server only when no active TCP connection for sending authentication packets is using it.

Related commands: **display hwtacacs**.

## Examples

```
# Specify the primary authentication server.
```

```
<Sysname> system-view
```

```
[Sysname] hwtacacs scheme hwt1
```

```
[Sysname-hwtacacs-hwt1] primary authentication 10.163.155.13 49
```

## primary authorization

### Syntax

```
primary authorization ip-address [ port-number ]
```

```
undo primary authorization
```

### View

```
HWTACACS scheme view
```

### Default Level

2: System level

### Parameters

*ip-address*: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

*port-number*: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

### Description

Use the **primary authorization** command to specify the primary HWTACACS authorization server.

Use the **undo primary authorization** command to remove the configuration.

By default, no primary HWTACACS authorization server is specified.

Note that:

- The IP addresses of the primary and secondary authorization servers cannot be the same. Otherwise, the configuration fails.
- The HWTACACS service port configured on the device and that of the HWTACACS server must be consistent.
- If you configure the command for more than one time, the last configuration takes effect.

- You can remove an authorization server only when no active TCP connection for sending authorization packets is using it.

Related commands: **display hwtacacs**.

## Examples

# Configure the primary authorization server.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] primary authorization 10.163.155.13 49
```

## reset hwtacacs statistics

### Syntax

```
reset hwtacacs statistics { accounting | all | authentication | authorization } [ slot slot-number ]
```

### View

User view

### Default Level

1: Monitor level

### Parameters

**accounting**: Clears HWTACACS accounting statistics.

**all**: Clears all HWTACACS statistics.

**authentication**: Clears HWTACACS authentication statistics.

**authorization**: Clears HWTACACS authorization statistics.

**slot** *slot-number*: Clears HWTACACS statistics on the specified member device in an IRF stack. The *slot-number* argument indicates the member device ID.

### Description

Use the **reset hwtacacs statistics** command to clear HWTACACS statistics.

Related commands: **display hwtacacs**.

### Examples

# Clear all HWTACACS statistics.

```
<Sysname> reset hwtacacs statistics all
```

## reset stop-accounting-buffer

### Syntax

```
reset stop-accounting-buffer hwtacacs-scheme hwtacacs-scheme-name [ slot slot-number ]
```

### View

User view

## Default Level

2: System level

## Parameters

**hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies a HWTACACS scheme by its name, a string of 1 to 32 characters.

**slot** *slot-number*: Specifies the specified member device in an IRF stack. The *slot-number* argument indicates the member device ID.

## Description

Use the **reset stop-accounting-buffer** command to clear the buffered stop-accounting requests that get no responses.

Related commands: **stop-accounting-buffer enable**, **retry stop-accounting**, **display stop-accounting-buffer**.

## Examples

```
# Clear the buffered stop-accounting requests for HWTACACS scheme hwt1.
```

```
<Sysname> reset stop-accounting-buffer hwtacacs-scheme hwt1
```

## retry stop-accounting (HWTACACS scheme view)

### Syntax

```
retry stop-accounting retry-times
```

```
undo retry stop-accounting
```

### View

HWTACACS scheme view

## Default Level

2: System level

## Parameters

*retry-times*: Maximum number of stop-accounting request transmission attempts. It ranges from 1 to 300 and defaults to 100.

## Description

Use the **retry stop-accounting** command to set the maximum number of stop-accounting request transmission attempts.

Use the **undo retry stop-accounting** command to restore the default.

Related commands: **reset stop-accounting-buffer**, **hwtacacs scheme**, **display stop-accounting-buffer**.

## Examples

```
# Set the maximum number of stop-accounting request transmission attempts to 50.
```

```
<Sysname> system-view
```

```
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] retry stop-accounting 50
```

## secondary accounting (HWTACACS scheme view)

### Syntax

```
secondary accounting ip-address [ port-number ]
undo secondary accounting
```

### View

HWTACACS scheme view

### Default Level

2: System level

### Parameters

*ip-address*: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

*port-number*: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

### Description

Use the **secondary accounting** command to specify the secondary HWTACACS accounting server.

Use the **undo secondary accounting** command to remove the configuration.

By default, no secondary HWTACACS accounting server is specified.

Note that:

- The IP addresses of the primary and secondary accounting servers cannot be the same. Otherwise, the configuration fails.
- The HWTACACS service port configured on the device and that of the HWTACACS server must be consistent.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an accounting server only when no active TCP connection for sending accounting packets is using it.

### Examples

```
# Specify the secondary accounting server.
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary accounting 10.163.155.12 49
```

## secondary authentication (HWTACACS scheme view)

### Syntax

```
secondary authentication ip-address [ port-number ]
undo secondary authentication
```

## View

HWTACACS scheme view

## Default Level

2: System level

## Parameters

*ip-address*: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

*port-number*: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

## Description

Use the **secondary authentication** command to specify the secondary HWTACACS authentication server.

Use the **undo secondary authentication** command to remove the configuration.

By default, no secondary HWTACACS authentication server is specified.

Note that:

- The IP addresses of the primary and secondary authentication servers cannot be the same. Otherwise, the configuration fails.
- The HWTACACS service port configured on the device and that of the HWTACACS server must be consistent.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an authentication server only when no active TCP connection for sending authentication packets is using it.

Related commands: **display hwtacacs**.

## Examples

# Specify the secondary authentication server.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary authentication 10.163.155.13 49
```

## secondary authorization

### Syntax

**secondary authorization** *ip-address* [ *port-number* ]

**undo secondary authorization**

### View

HWTACACS scheme view

### Default Level

2: System level

## Parameters

*ip-address*: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

*port-number*: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

## Description

Use the **secondary authorization** command to specify the secondary HWTACACS authorization server.

Use the **undo secondary authorization** command to remove the configuration.

By default, no secondary HWTACACS authorization server is specified.

Note that:

- The IP addresses of the primary and secondary authorization servers cannot be the same. Otherwise, the configuration fails.
- The HWTACACS service port configured on the device and that of the HWTACACS server must be consistent.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an authorization server only when no active TCP connection for sending authorization packets is using it.

Related commands: **display hwtacacs**.

## Examples

# Configure the secondary authorization server.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary authorization 10.163.155.13 49
```

## stop-accounting-buffer enable (HWTACACS scheme view)

### Syntax

**stop-accounting-buffer enable**

**undo stop-accounting-buffer enable**

### View

HWTACACS scheme view

### Default Level

2: System level

### Parameters

None

### Description

Use the **stop-accounting-buffer enable** command to enable the device to buffer stop-accounting requests getting no responses.

Use the **undo stop-accounting-buffer enable** command to disable the device from buffering stop-accounting requests getting no responses.

By default, the device is enabled to buffer stop-accounting requests getting no responses.

Since stop-accounting requests affect the charge to users, a NAS must make its best effort to send every stop-accounting request to the HWTACACS accounting servers. For each stop-accounting request getting no response in the specified period of time, the NAS buffers and resends the packet until it receives a response or the number of transmission retries reaches the configured limit. In the latter case, the NAS discards the packet.

Related commands: **reset stop-accounting-buffer**, **hwtacacs scheme**, **display stop-accounting-buffer**.

## Examples

# In HWTACACS scheme **hwt1**, enable the device to buffer the stop-accounting requests getting no responses.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] stop-accounting-buffer enable
```

## timer quiet (HWTACACS scheme view)

### Syntax

**timer quiet** *minutes*

**undo timer quiet**

### View

HWTACACS scheme view

### Default Level

2: System level

### Parameters

*minutes*: Primary server quiet period, in minutes. It ranges from 1 to 255 and defaults to 5.

### Description

Use the **timer quiet** command to set the quiet timer for the primary server, that is, the duration that the status of the primary server stays blocked before resuming the active state.

Use the **undo timer quiet** command to restore the default.

Related commands: **display hwtacacs**.

## Examples

# Set the quiet timer for the primary server to 10 minutes.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer quiet 10
```

## timer realtime-accounting (HWTACACS scheme view)

### Syntax

```
timer realtime-accounting minutes  
undo timer realtime-accounting
```

### View

HWTACACS scheme view

### Default Level

2: System level

### Parameters

*minutes*: Real-time accounting interval in minutes. It is a multiple of 3 in the range 3 to 60 and defaults to 12.

### Description

Use the **timer realtime-accounting** command to set the real-time accounting interval.

Use the **undo timer realtime-accounting** command to restore the default.

Note that:

- For real-time accounting, a NAS must transmit the accounting information of online users to the HWTACACS accounting server periodically. This command is for setting the interval.
- The setting of the real-time accounting interval somewhat depends on the performance of the NAS and the HWTACACS server: a shorter interval requires higher performance. You are therefore recommended to adopt a longer interval when there are a large number of users (more than 1000, inclusive). The following table lists the recommended ratios of the interval to the number of users.

**Table 3-2** Recommended ratios of the accounting interval to the number of users

Number of users	Real-time accounting interval (minute)
1 to 99	3
100 to 499	6
500 to 999	12
1000 or more	15 or more

### Examples

```
# Set the real-time accounting interval to 51 minutes for HWTACACS scheme hwt1.
```

```
<Sysname> system-view  
[Sysname] hwtacacs scheme hwt1  
[Sysname-hwtacacs-hwt1] timer realtime-accounting 51
```

## timer response-timeout (HWTACACS scheme view)

### Syntax

```
timer response-timeout seconds  
undo timer response-timeout
```

### View

HWTACACS scheme view

### Default Level

2: System level

### Parameters

*seconds*: HWTACACS server response timeout period in seconds. It ranges from 1 to 300 and defaults to 5.

### Description

Use the **timer response-timeout** command to set the HWTACACS server response timeout timer.

Use the **undo timer** command to restore the default.

As HWTACACS is based on TCP, the timeout of the server response timeout timer and/or the TCP timeout timer will cause the device to be disconnected from the HWTACACS server.

Related commands: **display hwtacacs**.

### Examples

```
# Set the HWTACACS server response timeout timer to 30 seconds for HWTACACS scheme hwt1.
```

```
<Sysname> system-view  
[Sysname] hwtacacs scheme hwt1  
[Sysname-hwtacacs-hwt1] timer response-timeout 30
```

## user-name-format (HWTACACS scheme view)

### Syntax

```
user-name-format { keep-original | with-domain | without-domain }
```

### View

HWTACACS scheme view

### Default Level

2: System level

### Parameters

**keep-original**: Sends the username to the HWTACACS server as it is input.

**with-domain**: Includes the ISP domain name in the username sent to the HWTACACS server.

**without-domain**: Excludes the ISP domain name from the username sent to the HWTACACS server.

## Description

Use the **user-name-format** command to specify the format of the username to be sent to a HWTACACS server.

By default, the ISP domain name is included in the username.

Note that:

- A username is generally in the format of `userid@isp-name`, of which `isp-name` is used by the device to determine the ISP domain to which a user belongs. Some earlier HWTACACS servers, however, cannot recognize a username including an ISP domain name. Before sending a username including a domain name to such a HWTACACS server, the device must remove the domain name. This command is thus provided for you to decide whether to include a domain name in a username to be sent to a HWTACACS server.
- If a HWTACACS scheme defines that the username is sent without the ISP domain name, do not apply the HWTACACS scheme to more than one ISP domain, thus avoiding the confused situation where the HWTACACS server regards two users in different ISP domains but with the same `userid` as one.
- If the HWTACACS scheme is for wireless users, specify the **keep-original** keyword. Otherwise, authentication of the wireless users may fail.

Related commands: **hwtacacs scheme**.

## Examples

# Specify the device to remove the ISP domain name in the username sent to the HWTACACS servers for the HWTACACS scheme **hwt1**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] user-name-format without-domain
```

# Table of Contents

<b>1 802.1X Configuration Commands</b> .....	<b>1-1</b>
802.1X Configuration Commands .....	1-1
display dot1x .....	1-1
dot1x .....	1-4
dot1x authentication-method .....	1-5
dot1x guest-vlan .....	1-6
dot1x handshake .....	1-7
dot1x mandatory-domain .....	1-8
dot1x max-user .....	1-9
dot1x multicast-trigger .....	1-10
dot1x port-control .....	1-10
dot1x port-method .....	1-11
dot1x quiet-period .....	1-12
dot1x retry .....	1-13
dot1x timer .....	1-14
reset dot1x statistics .....	1-15
<b>2 EAD Fast Deployment Configuration Commands</b> .....	<b>2-1</b>
EAD Fast Deployment Configuration Commands .....	2-1
dot1x free-ip .....	2-1
dot1x timer ead-timeout .....	2-2
dot1x url .....	2-2

# 1 802.1X Configuration Commands

---

## 802.1X Configuration Commands

### display dot1x

#### Syntax

```
display dot1x [ sessions | statistics ] [ interface interface-list ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

**sessions**: Displays 802.1X session information.

**statistics**: Displays 802.1X statistics.

**interface** *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [ **to interface-type interface-number** ] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must be of the same type.

#### Description

Use the **display dot1x** command to display information about 802.1X.

If you specify neither the **sessions** keyword nor the **statistics** keyword, the command displays all information about 802.1X, including session information, statistics, and configurations.

Related commands: reset dot1x statistics, dot1x, dot1x retry, dot1x max-user, dot1x port-control, dot1x port-method, dot1x timer.

#### Examples

```
# Display all information about 802.1X.
```

```
<Sysname> display dot1x
Equipment 802.1X protocol is enabled
CHAP authentication is enabled
EAD quick deploy is enabled
```

```
Configuration: Transmit Period      30 s, Handshake Period      15 s
                  Quiet Period      60 s, Quiet Period Timer is disabled
                  Supp Timeout       30 s, Server Timeout        100 s
```

EAD quick deploy configuration:

```
URL: http://192.168.19.23
Free IP: 192.168.19.0 255.255.255.0
EAD timeout: 30m
```

The maximum 802.1X user resource number is 1024 per slot  
 Total current used 802.1X resource number is 1

```
GigabitEthernet1/0/1 is link-up
802.1X protocol is enabled
Handshake is disabled
The port is an authenticator
Authenticate Mode is Auto
802.1X Multicast-trigger is enabled
Mandatory authentication domain: NOT configured
Port Control Type is Mac-based
Guest VLAN: 4
Max number of on-line users is 256
```

```
EAPOL Packet: Tx 1087, Rx 986
Sent EAP Request/Identity Packets : 943
    EAP Request/Challenge Packets: 60
    EAP Success Packets: 29, Fail Packets: 55
Received EAPOL Start Packets : 60
    EAPOL LogOff Packets: 24
    EAP Response/Identity Packets : 724
    EAP Response/Challenge Packets: 54
    Error Packets: 0
```

1. Authenticated user : MAC address: 0015-e9a6-7cfe

Controlled User(s) amount to 1

**Table 1-1 display dot1x command output description**

Field	Description
Equipment 802.1X protocol is enabled	Indicates whether 802.1X is enabled globally
CHAP authentication is enabled	Indicates whether CHAP authentication is enabled
EAD quick deploy is enabled	Indicates whether EAD quick deployment is enabled
Transmit Period	Setting of the username request timeout timer
Handshake Period	Setting of the handshake timer
Quiet Period	Setting of the quiet timer
Quiet Period Timer is disabled	Indicates whether the quiet timer is enabled
Supp Timeout	Setting of the supplicant timeout timer
Server Timeout	Setting of the server timeout timer

Field	Description
The maximal retransmitting times	Maximum number of attempts for the authenticator to send authentication requests to the supplicant
EAD quick deploy configuration	EAD quick deployment configurations
URL	Redirect URL for IE users
Free IP	Accessible network segment
EAD timeout	EAD rule timeout time
The maximum 802.1X user resource number per slot	Maximum number of supplicants supported per board
Total current used 802.1X resource number	Total number of online users
GigabitEthernet1/0/1 is link-up	Status of port GigabitEthernet 1/0/1
802.1X protocol is disabled	Indicates whether 802.1X is enabled on the port
Handshake is disabled	Indicates whether handshake is enabled on the port
The port is an authenticator	Role of the port
Authenticate Mode is Auto	Access control mode for the port
802.1X Multicast-trigger is enabled	Indicates whether the 802.1X multicast-trigger function is enabled
Mandatory authentication domain	Mandatory authentication domain for users accessing the port
Port Control Type is Mac-based	Access control method for the port
Guest VLAN	Guest VLAN configured for the port. "NOT configured" means that no guest VLAN is configured.
Max number of on-line users	Maximum number of users supported on the port
EAPOL Packet	Counts of EAPOL packets sent (Tx) and received (Rx)
Sent EAP Request/Identity Packets	Number of EAP Request/Identity packets sent
EAP Request/Challenge Packets	Number of EAP Request/Challenge packets sent
EAP Success Packets	Number of EAP Success packets sent
Received EAPOL Start Packets	Number of EAPOL Start packets received
EAPOL LogOff Packets	Number of EAPOL LogOff packets received
EAP Response/Identity Packets	Number of EAP Response/Identity packets received
EAP Response/Challenge Packets	Number of EAP Response/Challenge packets received
Error Packets	Number of erroneous packets received
Authenticated user	User that has passed the authentication
Controlled User(s) amount	Number of controlled users on the port

## dot1x

### Syntax

In system view:

```
dot1x [ interface interface-list ]  
undo dot1x [ interface interface-list ]
```

In Ethernet interface view:

```
dot1x  
undo dot1x
```

### View

System view, interface view

### Default Level

2: System level

### Parameters

**interface** *interface-list*. Specifies a port list, which can contain multiple ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [ **to** *interface-type interface-number* ] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must be of the same type.

### Description

Use the **dot1x** command in system view to enable 802.1X globally.

Use the **undo dot1x** command in system view to disable 802.1X globally.

Use the **dot1x interface** *interface-list* command in system view or the **dot1x** command in interface view to enable 802.1X for specified ports.

Use the **undo dot1x interface** *interface-list* command in system view or the **undo dot1x** command in interface view to disable 802.1X for specified ports.

By default, 802.1X is neither enabled globally nor enabled for any port.

Note that:

- 802.1X must be enabled both globally in system view and for the intended ports in system view or interface view. Otherwise, it does not function.
- You can configure 802.1X parameters either before or after enabling 802.1X.

Related commands: **display dot1x**.

### Examples

```
# Enable 802.1X for ports GigabitEthernet 1/0/1, and GigabitEthernet 1/0/5 to GigabitEthernet 1/0/7.
```

```
<Sysname> system-view
```

```
[Sysname] dot1x interface GigabitEthernet 1/0/1 GigabitEthernet 1/0/5 to GigabitEthernet  
1/0/7
```

Or

```

<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface GigabitEthernet 1/0/5
[Sysname-GigabitEthernet1/0/5] dot1x
[Sysname-GigabitEthernet1/0/5] quit
[Sysname] interface GigabitEthernet 1/0/6
[Sysname-GigabitEthernet1/0/6] dot1x
[Sysname-GigabitEthernet1/0/6] quit
[Sysname] interface GigabitEthernet 1/0/7
[Sysname-GigabitEthernet1/0/7] dot1x

# Enable 802.1X globally.

<Sysname> system-view
[Sysname] dot1x

```

## dot1x authentication-method

### Syntax

```

dot1x authentication-method { chap / eap / pap }
undo dot1x authentication-method

```

### View

System view

### Default Level

2: System level

### Parameters

**chap:** Authenticates supplicants using CHAP.  
**eap:** Authenticates supplicants using EAP.  
**pap:** Authenticates supplicants using PAP.

### Description

Use the **dot1x authentication-method** command to set the 802.1X authentication method.

Use the **undo dot1x authentication-method** command to restore the default.

By default, CHAP is used.

- The password authentication protocol (PAP) transports passwords in clear text.
- The challenge handshake authentication protocol (CHAP) transports only usernames over the network. Compared with PAP, CHAP provides better security.
- With EAP relay authentication, the authenticator encapsulates 802.1X user information in the EAP attributes of RADIUS packets and sends the packets to the RADIUS server for authentication; it does not need to repackage the EAP packets into standard RADIUS packets for authentication. In this case, you can configure the **user-name-format** command but it does not take effect. For information about the **user-name-format** command, refer to *AAA Commands* in the *Security Volume*.

Note that:

- Local authentication supports PAP and CHAP.
- For RADIUS authentication, the RADIUS server must be configured accordingly to support PAP, CHAP, or EAP authentication.

Related commands: **display dot1x**.

## Examples

```
# Set the 802.1X authentication method to PAP.
```

```
<Sysname> system-view
```

```
[Sysname] dot1x authentication-method pap
```

## dot1x guest-vlan

### Syntax

In system view:

```
dot1x guest-vlan guest-vlan-id [ interface interface-list ]
```

```
undo dot1x guest-vlan [ interface interface-list ]
```

In interface view:

```
dot1x guest-vlan guest-vlan-id
```

```
undo dot1x guest-vlan
```

### View

System view, Layer 2 Ethernet interface view

### Default Level

2: System level

### Parameters

*guest-vlan-id*: ID of the VLAN to be specified as the guest VLAN, in the range 1 to 4094. It must already exist.

**interface** *interface-list*: Specifies a port list. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [ **to** *interface-type interface-number* ] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must be of the same type.

### Description

Use the **dot1x guest-vlan** command to configure the guest VLAN for specified or all ports.

Use the **undo dot1x guest-vlan** command to remove the guest VLAN(s) configured for specified or all ports.

By default, a port is configured with no guest VLAN.

Currently, on the S4800G series Ethernet switches, a guest VLAN can be only a port-based guest VLAN (PGV), which is supported on a port that uses the access control method of **portbased**.

Note that:

- In system view, this command configures a guest VLAN for all Layer 2 Ethernet ports if you do not specify the *interface-list* argument, and configures a guest VLAN for specified ports if you specify the *interface-list* argument.
- In interface view, you cannot specify the *interface-list* argument and can only configure guest VLAN for the current port.
- You must enable 802.1X for a guest VLAN to take effect.
- You must enable the 802.1X multicast trigger function for a PGV to take effect.
- After an PGV takes effect, if you change the port access method from **portbased** to **macbased**, the port will leave the guest VLAN.
- You are not allowed to delete a VLAN that is configured as a guest VLAN. To delete such a VLAN, you need to remove the guest VLAN configuration first.
- You cannot configure both the guest VLAN function and the free IP function on a port.

Related commands: **dot1x**; **dot1x port-method**; **dot1x multicast-trigger**; **mac-vlan enable**, and **display mac-vlan** in *VLAN Commands* in the *Access Volume*.

## Examples

# Specify port GigabitEthernet 1/0/1 to use VLAN 999 as its guest VLAN.

```
<Sysname> system-view
[Sysname] dot1x guest-vlan 999 interface GigabitEthernet 1/0/1
```

# Specify ports GigabitEthernet 1/0/2 to GigabitEthernet 1/0/5 to use VLAN 10 as its guest VLAN.

```
<Sysname> system-view
[Sysname] dot1x guest-vlan 10 interface GigabitEthernet 1/0/2 to GigabitEthernet 1/0/5
```

# Specify all ports to use VLAN 7 as their guest VLAN.

```
<Sysname> system-view
[Sysname] dot1x guest-vlan 7
```

# Specify port GigabitEthernet 1/0/7 to use VLAN 3 as its guest VLAN.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/7
[Sysname-GigabitEthernet1/0/7] dot1x guest-vlan 3
```

## dot1x handshake

### Syntax

**dot1x handshake**

**undo dot1x handshake**

### View

Interface view

### Default Level

2: System level

### Parameters

None

## Description

Use the **dot1x handshake** command to enable the online user handshake function so that the device can periodically send handshake messages to the client to check whether a user is online.

Use the **undo dot1x handshake** command to disable the function.

By default, the function is enabled.

Note that: To ensure that the online user handshake function can work normally, you are recommended to use H3C 802.1X client software.

## Examples

```
# Enable online user handshake.

<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/4
[Sysname-GigabitEthernet1/0/4] dot1x handshake
```

## dot1x mandatory-domain

### Syntax

```
dot1x mandatory-domain domain-name
undo dot1x mandatory-domain
```

### View

Interface view

### Default Level

2: System level

### Parameters

*domain-name*: ISP domain name, a case-insensitive string of 1 to 24 characters.

## Description

Use the **dot1x mandatory-domain** command to specify the mandatory authentication domain for users accessing the port.

Use the **undo dot1x mandatory-domain** command to remove the mandatory authentication domain.

By default, no mandatory authentication domain is specified.

Note that:

- When authenticating an 802.1X user trying to access the port, the system selects an authentication domain in the following order: the mandatory domain, the ISP domain specified in the username, and the default ISP domain.
- The specified mandatory authentication domain must exist.
- On a port configured with a mandatory authentication domain, the user domain name displayed by the **display connection** command is the name of the mandatory authentication domain. For detailed information about the **display connection** command, refer to *AAA Commands* in the *Security Volume*.

Related commands: **display dot1x**.

## Examples

```
# Configure the mandatory authentication domain my-domain for 802.1X users on GigabitEthernet 1/0/1.
```

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x mandatory-domain my-domain
```

```
# After 802.1X user usera passes the authentication, display the user connection information on GigabitEthernet 1/0/1.
```

```
[Sysname-GigabitEthernet1/0/1] display connection interface GigabitEthernet 1/0/1
```

```
Index=68 ,Username=usera@my-domain
MAC=0015-e9a6-7cfe ,IP=3.3.3.3
Total 1 connection(s) matched.
```

## dot1x max-user

### Syntax

In system view:

```
dot1x max-user user-number [ interface interface-list ]
undo dot1x max-user [ interface interface-list ]
```

In Ethernet interface view:

```
dot1x max-user user-number
undo dot1x max-user
```

### View

System view, Ethernet interface view

### Default Level

2: System level

### Parameters

*user-number*: Maximum number of users to be supported simultaneously. The valid settings and the default may vary by device.

**interface** *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [ **to** *interface-type interface-number* ] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must be of the same type.

### Description

Use the **dot1x max-user** command to set the maximum number of users to be supported simultaneously for specified or all ports.

Use the **undo dot1x max-user** command to restore the default.

With no interface specified, the command sets the threshold for all ports.

Related commands: **display dot1x**.

## Examples

# Set the maximum number of users for port GigabitEthernet 1/0/1 to support simultaneously as 32.

```
<Sysname> system-view
[Sysname] dot1x max-user 32 interface GigabitEthernet 1/0/1
```

Or

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x max-user 32
```

## dot1x multicast-trigger

### Syntax

```
dot1x multicast-trigger
undo dot1x multicast-trigger
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **dot1x multicast-trigger** command to enable the multicast trigger function of 802.1X to send multicast trigger messages to the clients periodically.

Use the **undo dot1x multicast-trigger** command to disable this function.

By default, the multicast trigger function is enabled.

Related commands: **display dot1x**.

## Examples

# Disable the multicast trigger function for interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo dot1x multicast-trigger
```

## dot1x port-control

### Syntax

In system view:

```
dot1x port-control { authorized-force | auto | unauthorized-force } [ interface interface-list ]
```

```
undo dot1x port-control [ interface interface-list ]
```

In Ethernet interface view:

```
dot1x port-control { authorized-force | auto | unauthorized-force }
```

```
undo dot1x port-control
```

## View

System view, Ethernet interface view

## Default Level

2: System level

## Parameters

**authorized-force**: Places the specified or all ports in the authorized state, allowing users of the ports to access the network without authentication.

**auto**: Places the specified or all ports in the unauthorized state initially to allow only EAPOL frames to pass, and turns the ports into the authorized state to allow access to the network after the users pass authentication. This is the most common choice.

**unauthorized-force**: Places the specified or all ports in the unauthorized state, denying any access requests from users of the ports.

**interface** *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [ **to interface-type interface-number** ] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must be of the same type.

## Description

Use the **dot1x port-control** command to set the access control mode for specified or all ports.

Use the **undo dot1x port-control** command to restore the default.

The default access control mode is **auto**.

Related commands: **display dot1x**.

## Examples

```
# Set the access control mode of port GigabitEthernet 1/0/1 to unauthorized-force.
```

```
<Sysname> system-view
```

```
[Sysname] dot1x port-control unauthorized-force interface GigabitEthernet 1/0/1
```

Or

```
<Sysname> system-view
```

```
[Sysname] interface GigabitEthernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] dot1x port-control unauthorized-force
```

## dot1x port-method

### Syntax

In system view:

```
dot1x port-method { macbased | portbased } [ interface interface-list ]
```

```
undo dot1x port-method [ interface interface-list ]
```

In Ethernet interface view:

```
dot1x port-method { macbased | portbased }
```

```
undo dot1x port-method
```

## View

System view, Ethernet interface view

## Default Level

2: System level

## Parameters

**macbased**: Specifies to use the **macbased** authentication method. With this method, each user of a port must be authenticated separately, and when an authenticated user goes offline, no other users are affected.

**portbased**: Specifies to use the **portbased** authentication method. With this method, after the first user of a port passes authentication, all other users of the port can access the network without authentication, and when the first user goes offline, all other users get offline at the same time.

**interface** *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [ **to interface-type interface-number** ] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must be of the same type.

## Description

Use the **dot1x port-method** command to set the access control method for specified or all ports.

Use the **undo dot1x port-method** command to restore the default.

The default access control method is **macbased**.

Related commands: **display dot1x**.

## Examples

```
# Set the access control method to portbased for port GigabitEthernet 1/0/1.
```

```
<Sysname> system-view
```

```
[Sysname] dot1x port-method portbased interface GigabitEthernet 1/0/1
```

Or

```
<Sysname> system-view
```

```
[Sysname] interface GigabitEthernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] dot1x port-method portbased
```

## dot1x quiet-period

### Syntax

```
dot1x quiet-period
```

**undo dot1x quiet-period**

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **dot1x quiet-period** command to enable the quiet timer function.

Use the **undo dot1x quiet-period** command to disable the function.

By default, the function is disabled.

After a supplicant fails the authentication, the authenticator refuses further authentication requests from the supplicant in the period dictated by the quiet timer.

Related commands: **display dot1x**, **dot1x timer**.

### Examples

# Enable the quiet timer.

```
<Sysname> system-view
```

```
[Sysname] dot1x quiet-period
```

## dot1x retry

### Syntax

**dot1x retry** *max-retry-value*

**undo dot1x retry**

### View

System view

### Default Level

2: System level

### Parameters

*max-retry-value*: Maximum number of attempts to send an authentication request to a supplicant, in the range 1 to 10.

### Description

Use the **dot1x retry** command to set the maximum number of attempts to send an authentication request to a supplicant.

Use the **undo dot1x retry** command to restore the default.

By default, the authenticator can send an authentication request to a supplicant twice at most.

Note that after sending an authentication request to a supplicant, the authenticator may retransmit the request if it does not receive any response at an interval specified by the username request timeout timer or supplicant timeout timer. The number of retransmission attempts is one less than the value set by this command.

Related commands: **display dot1x**.

## Examples

```
# Set the maximum number of attempts to send an authentication request to a supplicant as 9.
```

```
<Sysname> system-view  
[Sysname] dot1x retry 9
```

## dot1x timer

### Syntax

```
dot1x timer { handshake-period handshake-period-value | quiet-period quiet-period-value | server-timeout server-timeout-value | supp-timeout supp-timeout-value | tx-period tx-period-value }  
undo dot1x timer { handshake-period | quiet-period | server-timeout | supp-timeout | tx-period }
```

### View

System view

### Default Level

2: System level

### Parameters

*handshake-period-value*: Setting for the handshake timer in seconds. It ranges from 5 to 1024 and defaults to 15.

*quiet-period-value*: Setting for the quiet timer in seconds. It ranges from 10 to 120 and defaults to 60.

*server-timeout-value*: Setting for the server timeout timer in seconds. It ranges from 100 to 300 and defaults to 100.

*supp-timeout-value*: Setting for the supplicant timeout timer in seconds. It ranges from 1 to 120 and defaults to 30.

*tx-period-value*: Setting for the username request timeout timer in seconds. It ranges from 10 to 120 and defaults to 30.

### Description

Use the **dot1x timer** command to set 802.1X timers.

Use the **undo dot1x timer** command to restore the defaults.

Several timers are used in the 802.1X authentication process to guarantee that the supplicants, the authenticators, and the RADIUS server interact with each other in a reasonable manner. You can use this command to set these timers:

- Handshake timer (*handshake-period*): After a supplicant passes authentication, the authenticator sends to the supplicant handshake requests at this interval to check whether the supplicant is online. If the authenticator receives no response after sending the allowed maximum number of handshake requests, it considers that the supplicant is offline.

- Quiet timer (quiet-period): When a supplicant fails the authentication, the authenticator refuses further authentication requests from the supplicant in this period of time.
- Server timeout timer (server-timeout): Once an authenticator sends a RADIUS Access-Request packet to the authentication server, it starts this timer. If this timer expires but it receives no response from the server, it retransmits the request.
- Supplicant timeout timer (supp-timeout): Once an authenticator sends an EAP-Request/MD5 Challenge frame to a supplicant, it starts this timer. If this timer expires but it receives no response from the supplicant, it retransmits the request.
- Username request timeout timer (tx-period): Once an authenticator sends an EAP-Request/Identity frame to a supplicant, it starts this timer. If this timer expires but it receives no response from the supplicant, it retransmits the request. In addition, to be compatible with clients that do not send EAPOL-Start requests unsolicitedly, the device multicasts EAP-Request/Identity frame periodically to detect the clients, with the multicast interval defined by tx-period.

It is unnecessary to change the timers unless in some special or extreme network environments. The change of a timer takes effect immediately.

Related commands: **display dot1x**.

## Examples

```
# Set the server timeout timer to 150 seconds.
```

```
<Sysname> system-view
[Sysname] dot1x timer server-timeout 150
```

## reset dot1x statistics

### Syntax

```
reset dot1x statistics [ interface interface-list ]
```

### View

User view

### Default Level

2: System level

### Parameters

**interface** *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [ **to** *interface-type interface-number* ] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must be of the same type.

### Description

Use the **reset dot1x statistics** command to clear 802.1X statistics.

With the **interface** *interface-list* argument specified, the command clears 802.1X statistics on the specified ports. With the argument unspecified, the command clears global 802.1X statistics and 802.1X statistics on all ports.

Related commands: **display dot1x**.

### Examples

# Clear 802.1X statistics on port GigabitEthernet 1/0/1.

```
<Sysname> reset dot1x statistics interface GigabitEthernet 1/0/1
```

# 2 EAD Fast Deployment Configuration Commands

---

## EAD Fast Deployment Configuration Commands

### dot1x free-ip

#### Syntax

```
dot1x free-ip ip-address { mask-address | mask-length }  
undo dot1x free-ip { ip-address { mask | mask-length } | all }
```

#### View

System view

#### Default Level

2: System level

#### Parameters

*ip-address*: IP address of the freely accessible network segment, also called a free IP.

*mask*: Mask of the freely accessible network segment.

*mask-length*: Length of the mask of the freely accessible network segment.

**all**: Specifies all the freely accessible network segments.

#### Description

Use the **dot1x free-ip** command to configure a freely accessible network segment, that is, a network segment that users can access before passing 802.1X authentication.

Use the **undo dot1x free-ip** command to remove one or all freely accessible network segments.

By default, no freely accessible network segment is configured.

Note that:

- The free IP function is mutually exclusive with the global MAC authentication function, the port security function, and the guest VLAN function on a port.
- The free IP function is effective only when the port access control mode is **auto**.
- The maximum number of freely accessible network segments is 4.

Related commands: **display dot1x**.

#### Examples

```
# Configure 192.168.0.0 as a freely accessible network segment.
```

```
<Sysname> system-view  
[Sysname] dot1x free-ip 192.168.0.0 24
```

## dot1x timer ead-timeout

### Syntax

```
dot1x timer ead-timeout ead-timeout-value  
undo dot1x timer ead-timeout
```

### View

System view

### Default Level

2: System level

### Parameters

*ead-timeout-value*: EAD rule timeout time, in the range 1 minute to 1440 minutes.

### Description

Use the **dot1x timer ead-timeout** command to set the EAD rule timeout time.

Use the **undo dot1x timer ead-timeout** command to restore the default.

By default, the timeout time is 30 minutes.

Related commands: **display dot1x**.

### Examples

# Set the EAD rule timeout time to 5 minutes.

```
<Sysname> system-view  
[Sysname] dot1x timer ead-timeout 5
```

## dot1x url

### Syntax

```
dot1x url url-string  
undo dot1x [ url-string ]
```

### View

System view

### Default Level

2: System level

### Parameters

*url-string*: Redirect URL, a case-sensitive string of 1 to 64 characters in the format http://string/.

### Description

Use the **dot1x url** command to configure a redirect URL. After a redirect URL is configured, when a user uses a Web browser to access networks other than the free IP, the device will redirect the user to the redirect URL.

Use the **undo dot1x url** command to remove the redirect URL.

By default, no redirect URL is defined.

Note that:

- The redirect URL and the free IP must be in the same network segment; otherwise, the URL may be inaccessible.
- You can configure the **dot1x url** command for more than once but only the last one takes effect.

Related commands: **display dot1x**, **dot1x free-ip**.

## Examples

# Configure the redirect URL as http://192.168.0.1.

```
<Sysname> system-view
```

```
[Sysname] dot1x url http://192.168.0.1
```

# Table of Contents

<b>1 HABP Configuration Commands .....</b>	<b>1-1</b>
HABP Configuration Commands .....	1-1
display habp .....	1-1
display habp table.....	1-1
display habp traffic.....	1-2
habp enable.....	1-3
habp server vlan .....	1-4
habp timer.....	1-4

# 1 HABP Configuration Commands

---

## HABP Configuration Commands

### display habp

#### Syntax

display habp

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

None

#### Description

Use the **display habp** command to display HABP configuration information.

#### Examples

# Display HABP configuration information.

```
<Sysname> display habp
```

```
Global HABP information:
```

```
  HABP Mode: Server
```

```
  Sending HABP request packets every 20 seconds
```

```
  Bypass VLAN: 2
```

**Table 1-1** display habp command output description

Field	Description
HABP Mode	HABP mode of the current device, server or client
Sending HABP request packets every 20 seconds	Interval to send HABP request packets
Bypass VLAN	ID of the VLAN in which HABP packets are transmitted

### display habp table

#### Syntax

display habp table

## View

Any view

## Default Level

1: Monitor level

## Parameters

None

## Description

Use the **display habp table** command to display HABP MAC address table entries.

## Examples

# Display HABP MAC address table entries.

```
<Sysname> display habp table
MAC                Holdtime  Receive Port
001f-3c00-0030    53          Ethernet1/1
```

**Table 1-2 display habp table** command output description

Field	Description
MAC	MAC address
Holdtime	Lifetime of an entry in seconds. The initial value is three times of the interval to send HABP request packets. An entry will age out if it is not updated during the period.
Receive Port	Port that learned the MAC address

## display habp traffic

### Syntax

```
display habp traffic
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display habp traffic** command to display HABP packet statistics.

### Examples

# Display HABP packet statistics.

```

<Sysname> display habp traffic
HABP counters :
    Packets output: 0, Input: 0
    ID error: 0, Type error: 0, Version error: 0
    Sent failed: 0

```

**Table 1-3 display habp traffic command output description**

Field	Description
Packets output	Number of HABP packets sent
Input	Number of HABP packets received
ID error	Number of packets with an incorrect ID
Type error	Number of packets with an incorrect type
Version error	Number of packets with an incorrect version number
Sent failed	Number of packets failed to be sent

## habp enable

### Syntax

```

habp enable
undo habp enable

```

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **habp enable** command to enable HABP.

Use the **undo habp enable** command to disable HABP.

By default, HABP is enabled.

HABP is required when and only when the cluster function and 802.1X (or MAC authentication) are enabled on the device.

### Examples

```

# Enable HABP.
<Sysname> system-view
[Sysname] habp enable

```

## habp server vlan

### Syntax

```
habp server vlan vlan-id  
undo habp server
```

### View

System view

### Default Level

2: System level

### Parameters

**vlan-id**: ID of the VLAN in which HABP packets are to be transmitted, in the range 1 to 4094.

### Description

Use the **habp server vlan** command to configure HABP to work in server mode and specify the VLAN in which HABP packets are to be transmitted.

Use the **undo habp server vlan** command to configure HABP to work in the default mode.

By default, HABP works in client mode.

### Examples

```
# Configure HABP to work in server mode and specify the VLAN for HABP packets as VLAN 2.
```

```
<Sysname> system-view  
[Sysname] habp server vlan 2
```

## habp timer

### Syntax

```
habp timer interval  
undo habp timer
```

### View

System view

### Default Level

2: System level

### Parameters

**interval**: Interval (in seconds) to send HABP request packets, in the range 5 to 600.

### Description

Use the **habp timer** command to set the interval to send HABP request packets.

Use the **undo habp timer** command to restore the default.

The default interval is 20 seconds.

This command is required only on the HABP server.

### Examples

# Set the interval to send HABP request packets to 50 seconds.

```
<Sysname> system-view
```

```
[Sysname] habp timer 50
```

# Table of Contents

<b>1 MAC Authentication Configuration Commands</b> .....	<b>1-1</b>
MAC Authentication Configuration Commands .....	1-1
display mac-authentication .....	1-1
mac-authentication .....	1-3
mac-authentication domain .....	1-4
mac-authentication timer .....	1-4
mac-authentication user-name-format .....	1-5
reset mac-authentication statistics .....	1-6

# 1 MAC Authentication Configuration Commands

---

## MAC Authentication Configuration Commands

### display mac-authentication

#### Syntax

```
display mac-authentication [ interface interface-list ]
```

#### View

Any view

#### Default Level

2: System level

#### Parameters

**interface** *interface-list*: Specifies an Ethernet port list, in the format of { *interface-type interface-number* [ **to** *interface-type interface-number* ] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. A port range defined without the **to** *interface-type interface-number* portion comprises only one port. With an interface range, the end interface number and the start interface number must be of the same type and the former must be greater than the latter.

#### Description

Use the **display mac-authentication** command to display global MAC authentication information or MAC authentication information about specified ports.

#### Examples

# Display global MAC authentication information.

```
<Sysname> display mac-authentication
MAC address authentication is enabled.
User name format is MAC address, like xxxxxxxxxxxxxx
Fixed username:mac
Fixed password:not configured
    Offline detect period is 300s
    Quiet period is 60s.
    Server response timeout value is 100s
    the max allowed user number is 1024 per slot
    Current user number amounts to 0
    Current domain: not configured, use default domain

Silent Mac User info:
      MAC ADDR           From Port           Port Index
GigabitEthernet1/0/1 is link-up
```

```

MAC address authentication is enabled
Authenticate success: 0, failed: 0
Current online user number is 0
MAC ADDR          Authenticate state          AuthIndex
.....(part of the output omitted)

```

**Table 1-1 display mac-authentication command output description**

Field	Description
MAC address authentication is enabled	Whether MAC authentication is enabled
User name format is MAC address, like xxxxxxxxxxxx	The username is in the format of an MAC address without hyphens, like xxxxxxxxxxxx. If the username format is configured as MCA address with hyphens, "like xx-xx-xx-xx-xx-xx" will be displayed.
Fixed username:	Fixed username
Fixed password:	Password of the fixed username
Offline detect period	Setting of the offline detect timer
Quiet period	Setting of the quiet timer
Server response timeout value	Setting of the server timeout timer
the max allowed user number	Maximum number of users each slot in the device supports
Current user number amounts to	Number of online users
Current domain: not configured, use default domain	Currently used ISP domain
Silent Mac User info	Information about silent MAC addresses
GigabitEthernet1/0/1 is link-up	Status of the link on port GigabitEthernet 1/0/1
MAC address authentication is enabled	Whether MAC authentication is enabled on port GigabitEthernet 1/0/1
Authenticate success: 0, failed: 0	MAC authentication statistics, including the number of successful authentication attempts and that of unsuccessful authentication attempts
Current online user number	Number of online users on the port
MAC ADDR	Online user MAC address
Authenticate state	User status. Possible values are: <ul style="list-style-type: none"> <li>CONNECTING: The user is logging in.</li> <li>SUCCESS: The user has passed the authentication.</li> <li>FAILURE: The user failed the authentication.</li> <li>LOGOFF: The user has logged off.</li> </ul>
AuthIndex	Authenticator Index

## mac-authentication

### Syntax

In system view:

```
mac-authentication [ interface interface-list ]  
undo mac-authentication [ interface interface-list ]
```

In Ethernet interface view:

```
mac-authentication  
undo mac-authentication
```

### View

System view, Ethernet interface view

### Default Level

2: System level

### Parameters

**interface** *interface-list*. Specifies an Ethernet port list, in the format of { *interface-type interface-number* [ **to** *interface-type interface-number* ] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. A port range defined without the **to** *interface-type interface-number* portion comprises only one port.

### Description

Use the **mac-authentication** command to enable MAC authentication globally or for one or more ports.

Use the **undo mac-authentication** command to disable MAC authentication globally or for one or more ports.

By default, MAC authentication is neither enabled globally nor enabled on any port.

Note that:

- In system view, if you provide the *interface-list* argument, the command enables MAC authentication for the specified ports; otherwise, the command enables MAC authentication globally. In Ethernet interface view, the command enables MAC authentication for the port because the *interface-list* argument is not available.
- You can enable MAC authentication for ports before enabling it globally. However, MAC authentication begins to function only after you also enable it globally.
- You can configure MAC authentication parameters globally or for specified ports either before or after enabling MAC authentication. If no MAC authentication parameters are configured when MAC authentication takes effect, the default values are used.

### Examples

```
# Enable MAC authentication globally.
```

```
<Sysname> system-view  
[Sysname] mac-authentication  
Mac-auth is enabled globally.
```

```
# Enable MAC authentication for port GigabitEthernet 1/0/1.
```

```
<Sysname> system-view
[Sysname] mac-authentication interface GigabitEthernet 1/0/1
Mac-auth is enabled on port GigabitEthernet1/0/1.
```

Or

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication
Mac-auth is enabled on port GigabitEthernet1/0/1.
```

## mac-authentication domain

### Syntax

```
mac-authentication domain isp-name
undo mac-authentication domain
```

### View

System view

### Default Level

2: System level

### Parameters

*isp-name*: ISP domain name, a case-insensitive string of 1 to 24 characters that cannot contain any forward slash (/), colon (:), asterisk (\*), question mark (?), less-than sign (<), greater-than sign (>), or @.

### Description

Use the **mac-authentication domain** command to specify the ISP domain for MAC authentication.

Use the **undo mac-authentication domain** command to restore the default.

By default, the default ISP domain is used for MAC authentication users. For information about the default ISP domain, refer to the **domain default enable** command in *AAA Commands of the Security Volume*.

### Examples

```
# Specify the ISP domain for MAC authentication as domain1.
```

```
<Sysname> system-view
[Sysname] mac-authentication domain domain1
```

## mac-authentication timer

### Syntax

```
mac-authentication timer { offline-detect offline-detect-value | quiet quiet-value | server-timeout server-timeout-value }
undo mac-authentication timer { offline-detect | quiet | server-timeout }
```

### View

System view

## Default Level

2: System level

## Parameters

**offline-detect** *offline-detect-value*: Specifies the offline detect interval, in the range 60 to 65,535 seconds.

**quiet** *quiet-value*: Specifies the quiet period, in the range 1 to 3,600 seconds.

**server-timeout** *server-timeout-value*: Specifies the server timeout period, in the range 100 to 300 seconds.

## Description

Use the **mac-authentication timer** command to set the MAC authentication timers.

Use the **undo mac-authentication timer** command to restore the defaults.

By default, the offline detect interval is 300 seconds, the quiet period is 60 seconds, and the server timeout period is 100 seconds.

The following timers function in the process of MAC authentication:

- Offline detect timer: This timer sets the idle timeout interval for users. If no packet is received from a user over two consecutive timeout intervals, the system disconnects the user connection and notifies the RADIUS server.
- Quiet timer: Whenever a user fails MAC authentication, the device does not perform MAC authentication of the user during such a period.
- Server timeout timer: During authentication of a user, if the device receives no response from the RADIUS server in this period, it assumes that its connection to the RADIUS server has timed out and forbids the user from accessing the network.

Related commands: **display mac-authentication**.

## Examples

```
# Set the server timeout timer to 150 seconds.
```

```
<Sysname> system-view  
[Sysname] mac-authentication timer server-timeout 150
```

## mac-authentication user-name-format

### Syntax

```
mac-authentication user-name-format { fixed [ account name ] [ password { cipher | simple } password ] | mac-address [ with-hyphen | without-hyphen ] }
```

```
undo mac-authentication user-name-format
```

### View

System view

## Default Level

2: System level

## Parameters

**fixed:** Uses the MAC authentication username type of fixed username.

**account name:** Specifies the fixed username. The *name* argument is a case-insensitive string of 1 to 55 characters and defaults to mac.

**password { cipher | simple } password:** Specifies the password for the fixed username. Specify the **cipher** keyword to display the password in cipher text or the **simple** keyword to display the password in plain text. In the former case, the password can be either a string of 1 to 63 characters in plain text or a string of 24 or 88 characters in cipher text. In the latter case, the password must be a string of 1 to 63 characters in plain text.

**mac-address:** Uses the source MAC address of a user as the username for authentication.

**with-hyphen:** Indicates that the MAC address must include "-", like xx-xx-xx-xx-xx-xx. The letters in the address must be in lower case.

**without-hyphen:** Indicates that the MAC address must not include "-", like xxxxxxxxxxxx. The letters in the address must be in lower case.

## Description

Use the **mac-authentication user-name-format** command to configure the MAC authentication username type and, if the type of fixed username is used, the username and password for MAC authentication.

Use the **undo mac-authentication user-name-format** command to restore the default.

By default, each user's source MAC address is used as the username and password for MAC authentication, with "-" in the MAC address.

Note that:

- When the type of MAC address is used, each user's source MAC address is used as both the username and password for MAC authentication.
- In cipher display mode, a password in plain text with no more than 16 characters will be encrypted into a password in cipher text with 24 characters, and a password in plain text with 16 to 63 characters will be encrypted into a password in cipher text with 88 characters. For a password with 24 characters, if it can be decrypted by the system, it will be treated as a cipher-text one; otherwise, it will be treated as a plain-text one.

Related commands: **display mac-authentication**.

## Examples

```
# Configure the username for MAC authentication as abc, and the password displayed in plain text as xyz.
```

```
<Sysname> system-view
```

```
[Sysname] mac-authentication user-name-format fixed account abc password simple xyz
```

## reset mac-authentication statistics

### Syntax

```
reset mac-authentication statistics [ interface interface-list ]
```

## View

User view

## Default Level

2: System level

## Parameters

**interface** *interface-list*. Specifies an Ethernet port list, in the format of { *interface-type interface-number* [ **to** *interface-type interface-number* ] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. A port range defined without the **to** *interface-type interface-number* portion comprises only one port.

## Description

Use the **reset mac-authentication statistics** command to clear MAC authentication statistics.

Note that:

- If you do not specify the *interface-list* argument, the command clears the global MAC authentication statistics and the MAC authentication statistics on all ports.
- If you specify the *interface-list* argument, the command clears the MAC authentication statistics on the specified ports.

Related commands: **display mac-authentication**.

## Examples

# Clear MAC authentication statistics on GigabitEthernet 1/0/1.

```
<Sysname> reset mac-authentication statistics interface GigabitEthernet 1/0/1
```

# Table of Contents

<b>1 Portal Configuration Commands</b> .....	<b>1-1</b>
Portal Configuration Commands .....	1-1
display portal acl .....	1-1
display portal connection statistics .....	1-3
display portal free-rule .....	1-6
display portal interface .....	1-7
display portal server .....	1-8
display portal server statistics .....	1-9
display portal tcp-cheat statistics .....	1-11
display portal user .....	1-12
portal auth-network .....	1-13
portal delete-user .....	1-14
portal domain .....	1-14
portal free-rule .....	1-15
portal server .....	1-16
portal server method .....	1-17
reset portal connection statistics .....	1-18
reset portal server statistics .....	1-19
reset portal tcp-cheat statistics .....	1-19

# 1 Portal Configuration Commands

---

## Portal Configuration Commands

### display portal acl

#### Syntax

```
display portal acl { all | dynamic | static } interface interface-type interface-number
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

**all:** Displays all portal access control lists (ACLs), including dynamic ones and static ones.

**dynamic:** Displays dynamic portal ACLs, namely, ACLs generated after a user passes portal authentication.

**static:** Displays static portal ACLs, namely, ACLs generated by related configurations.

**interface *interface-type interface-number*:** Displays the ACLs on the specified interface.

#### Description

Use the **display portal acl** command to display the ACLs on a specified interface.

#### Examples

# Display all ACLs on interface Vlan-interface 100.

```
<Sysname> display portal acl all interface Vlan-interface 100
Vlan-interface 100 portal ACL rule:
Rule 0
Inbound interface = Vlan-interface 100
Type              = static
Action            = permit
Source:
  IP               = 0.0.0.0
  Mask             = 0.0.0.0
  MAC              = 0000-0000-0000
  Interface        = any
  VLAN             = 0
  Protocol         = 0
Destination:
  IP               = 192.168.0.111
```

Mask = 255.255.255.255

Rule 1

Inbound interface = Vlan-interface 100

Type = static

Action = redirect

Source:

IP = 0.0.0.0

Mask = 0.0.0.0

MAC = 0000-0000-0000

Interface = any

VLAN = 2

Protocol = 6

Destination:

IP = 0.0.0.0

Mask = 0.0.0.0

Rule 2

Inbound interface = Vlan-interface 100

Type = dynamic

Action = permit

Source:

IP = 2.2.2.2

Mask = 255.255.255.255

MAC = 000d-88f8-0eab

Interface = GigabitEthernet1/0/1

VLAN = 0

Protocol = 0

Destination:

IP = 0.0.0.0

Mask = 0.0.0.0

Author ACL:

Number = 3001

**Table 1-1 display portal acl command output description**

Field	Description
Rule	Sequence number of the generated ACL, which is numbered from 0 in ascending order
Inbound interface	Interface to which portal ACLs are bound
Type	Type of the portal ACL
Action	Match action in the portal ACL
Source	Source information in the portal ACL
IP	Source IP address in the portal ACL
Mask	Subnet mask of the source IP address in the portal ACL
MAC	Source MAC address in the portal ACL

Field	Description
Interface	Source interface in the portal ACL
VLAN	Source VLAN in the portal ACL
Protocol	Protocol type in the portal ACL
Destination	Destination information in the portal ACL
IP	Destination IP address in the portal ACL
Mask	Subnet mask of the destination IP address in the portal ACL
Author ACL	Authorization ACL of portal ACL. It is displayed only when the Type field has a value of dynamic.
Number	Authorization ACL number assigned by the server. None indicates that the server did not assign any ACL.

## display portal connection statistics

### Syntax

```
display portal connection statistics { all | interface interface-type interface-number }
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**all**: Specifies all interfaces.

**interface** *interface-type interface-number*: Specifies an interface by its type and number.

### Description

Use the **display portal connection statistics** command to display portal connection statistics on a specified interface or all interfaces.

### Examples

# Display portal connection statistics on interface Vlan-interface 100.

```
<Sysname> display portal connection statistics interface Vlan-interface 100
-----Interface: Vlan-interface 100-----
User state statistics:
State-Name          User-Num
VOID                0
DISCOVERED          0
WAIT_AUTHEN_ACK     0
WAIT_AUTHOR_ACK     0
WAIT_LOGIN_ACK      0
WAIT_ACL_ACK        0
WAIT_NEW_IP         0
```

```

WAIT_USERIPCHANGE_ACK 0
ONLINE 1
WAIT_LOGOUT_ACK 0
WAIT_LEAVING_ACK 0

```

Message statistics:

Msg-Name	Total	Err	Discard
MSG_AUTHEN_ACK	3	0	0
MSG_AUTHOR_ACK	3	0	0
MSG_LOGIN_ACK	3	0	0
MSG_LOGOUT_ACK	2	0	0
MSG_LEAVING_ACK	0	0	0
MSG_CUT_REQ	0	0	0
MSG_AUTH_REQ	3	0	0
MSG_LOGIN_REQ	3	0	0
MSG_LOGOUT_REQ	2	0	0
MSG_LEAVING_REQ	0	0	0
MSG_ARPPKT	0	0	0
MSG_TMR_REQAUTH	1	0	0
MSG_TMR_AUTHEN	0	0	0
MSG_TMR_AUTHOR	0	0	0
MSG_TMR_LOGIN	0	0	0
MSG_TMR_LOGOUT	0	0	0
MSG_TMR_LEAVING	0	0	0
MSG_TMR_NEWIP	0	0	0
MSG_TMR_USERIPCHANGE	0	0	0
MSG_PORT_REMOVE	0	0	0
MSG_VLAN_REMOVE	0	0	0
MSG_IF_REMOVE	6	0	0
MSG_L3IF_SHUT	0	0	0
MSG_IP_REMOVE	0	0	0
MSG_ALL_REMOVE	1	0	0
MSG_IFIPADDR_CHANGE	0	0	0
MSG_SOCKET_CHANGE	8	0	0
MSG_NOTIFY	0	0	0
MSG_SETPOLICY	0	0	0
MSG_SETPOLICY_RESULT	0	0	0

**Table 1-2** display portal connection statistics command output description

Field	Description
User state statistics	Statistics on portal users
State-Name	Name of a user state
User-Num	Number of users
VOID	Number of users in void state
DISCOVERED	Number of users in discovered state
WAIT_AUTHEN_ACK	Number of users in wait_authen_ack state

<b>Field</b>	<b>Description</b>
WAIT_AUTHOR_ACK	Number of users in wait_author_ack state
WAIT_LOGIN_ACK	Number of users in wait_login_ack state
WAIT_ACL_ACK	Number of users in wait_acl_ack state
WAIT_NEW_IP	Number of users in wait_new_ip state
WAIT_USERIPCHANGE_ACK	Number of users wait_useripchange_ack state
ONLINE	Number of users in online state
WAIT_LOGOUT_ACK	Number of users in wait_logout_ack state
WAIT_LEAVING_ACK	Number of users in wait_leaving_ack state
Message statistics	Statistics on messages
Msg-Name	Message type
Total	Total number of messages
Err	Number of erroneous messages
Discard	Number of discarded messages
MSG_AUTHEN_ACK	Authentication acknowledgment message
MSG_AUTHOR_ACK	Authorization acknowledgment message
MSG_LOGIN_ACK	Accounting acknowledgment message
MSG_LOGOUT_ACK	Accounting-stop acknowledgment message
MSG_LEAVING_ACK	Leaving acknowledgment message
MSG_CUT_REQ	Cut request message
MSG_AUTH_REQ	Authentication request message
MSG_LOGIN_REQ	Accounting request message
MSG_LOGOUT_REQ	Accounting-stop request message
MSG_LEAVING_REQ	Leaving request message
MSG_ARPPKT	ARP message
MSG_TMR_REQAUTH	Authentication request timeout message
MSG_TMR_AUTHEN	Authentication timeout message
MSG_TMR_AUTHOR	Authorization timeout message
MSG_TMR_LOGIN	Accounting-start timeout message
MSG_TMR_LOGOUT	Accounting-stop timeout message
MSG_TMR_LEAVING	Leaving timeout message
MSG_TMR_NEWIP	Public IP update timeout message
MSG_TMR_USERIPCHANGE	User IP change timeout message
MSG_PORT_REMOVE	Users-of-a-Layer-2-port-removed message
MSG_VLAN_REMOVE	VLAN user removed message
MSG_IF_REMOVE	Users-of-a-Layer-3-interface-removed message
MSG_L3IF_SHUT	Layer 3 interface shutdown message

Field	Description
MSG_IP_REMOVE	User-with-an-IP-removed message
MSG_ALL_REMOVE	All-users-removed message
MSG_IFIPADDR_CHANGE	Interface IP address change message
MSG_SOCKET_CHANGE	Socket change message
MSG_NOTIFY	Notification message
MSG_SETPOLICY	Set policy message for assigning security ACL
MSG_SETPOLICY_RESULT	Set policy response message

## display portal free-rule

### Syntax

```
display portal free-rule [ rule-number ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*rule-number*: Number of a portal-free rule. The value range from 0 to 31.

### Description

Use the **display portal free-rule** command to display information about a specified portal-free rule or all portal-free rules.

Related commands: **portal free-rule**.

### Examples

```
# Display information about portal-free rule 1.
```

```
<Sysname> display portal free-rule 1
Rule-Number 1:
Source:
  IP      = 2.2.2.0
  Mask    = 255.255.255.0
  MAC     = 0000-0000-0000
  Interface = any
  Vlan    = 0
Destination:
  IP      = 0.0.0.0
  Mask    = 0.0.0.0
```

**Table 1-3 display portal free-rule** command output description

Field	Description
Rule-Number	Number of the portal-free rule
Source	Source information in the portal-free rule
IP	Source IP address in the portal-free rule
Mask	Subnet mask of the source IP address in the portal-free rule
MAC	Source MAC address in the portal-free rule
Interface	Source interface in the portal-free rule
Vlan	Source VLAN in the portal-free rule
Destination	Destination information in the portal-free rule
IP	Destination IP address in the portal-free rule
Mask	Subnet mask of the destination IP address in the portal-free rule

## display portal interface

### Syntax

**display portal interface** *interface-type interface-number*

### View

Any view

### Default Level

1: Monitor level

### Parameters

*interface-type interface-number*. Specifies an interface by its type and number.

### Description

Use the **display portal interface** command to display the portal configuration of an interface.

### Examples

# Display the portal configuration of interface Vlan-interface 100.

```
<Sysname> display portal interface Vlan-interface 100
Interface portal configuration:
Vlan-interface 100: Portal running
Portal server: servername
Authentication type: Direct
Authentication domain: my-domain
Authentication network:
address = 0.0.0.0 mask = 0.0.0.0
```

**Table 1-4 display portal interface** command output description

Field	Description
Interface portal configuration	Portal configuration on the interface
Vlan-interface 100	Status of the portal feature on the interface, disable, enable, or running.
Portal server	Portal server referenced by the interface
Authentication type	Authentication mode enabled on the interface
Authentication domain	Mandatory authentication domain of the interface
Authentication network	Information of the portal authentication subnet
address	IP address of the portal authentication subnet
mask	Subnet mask of the IP address of the portal authentication subnet

## display portal server

### Syntax

```
display portal server [ server-name ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*server-name*: Name of a portal server, a case-sensitive string of 1 to 32 characters.

### Description

Use the **display portal server** command to display information about a specified portal server or all portal servers.

Related commands: **portal server**.

### Examples

```
# Display information about portal server aaa.
```

```
<Sysname> display portal server aaa
```

```
Portal server:
```

```
1)aaa:
```

```
IP   = 192.168.0.111
```

```
Key  = portal
```

```
Port = 50100
```

```
URL  = http://192.168.0.111
```

**Table 1-5 display portal server** command output description

Field	Description
1)	Number of the portal server
aaa	Name of the portal server
IP	IP address of the portal server
Key	Key for portal authentication <b>Not configured</b> will be displayed if no key is configured.
Port	Listening port on the portal server
URL	Address the packets are to be redirected to <b>Not configured</b> will be displayed if no address is configured.

## display portal server statistics

### Syntax

**display portal server statistics** { **all** | **interface** *interface-type interface-number* }

### View

Any view

### Default Level

1: Monitor level

### Parameters

**all**: Specifies all interfaces.

**interface** *interface-type interface-number*: Specifies an interface by its type and name.

### Description

Use the **display portal server statistics** command to display portal server statistics on a specified interface or all interfaces.

Note that with the **all** keyword specified, the command displays portal server statistics by interface and therefore statistics about a portal server referenced by more than one interface may be displayed repeatedly.

### Examples

# Display portal server statistics on Vlan-interface 100.

```
<Sysname> display portal server statistics interface Vlan-interface 100
-----Interface: Vlan-interface 100-----
Server name: st
Invalid packets: 0
Pkt-Name                Total   Discard  Checkerr
REQ_CHALLENGE           3       0       0
ACK_CHALLENGE           3       0       0
REQ_AUTH                 3       0       0
```

ACK_AUTH	3	0	0
REQ_LOGOUT	1	0	0
ACK_LOGOUT	1	0	0
AFF_ACK_AUTH	3	0	0
NTF_LOGOUT	1	0	0
REQ_INFO	6	0	0
ACK_INFO	6	0	0
NTF_USERDISCOVER	0	0	0
NTF_USERIPCHANGE	0	0	0
AFF_NTF_USERIPCHANGE	0	0	0
ACK_NTF_LOGOUT	1	0	0

**Table 1-6** display portal server statistics command output description

Field	Description
Interface	Interface referencing the portal server
Server name	Name of the portal server
Invalid packets	Number of invalid packets
Pkt-Name	Packet type
Total	Total number of packets
Discard	Number of discarded packets
Checkerr	Number of erroneous packets
REQ_CHALLENGE	Challenge request message the portal server sends to the access device
ACK_CHALLENGE	Challenge acknowledgment message the access device sends to the portal server
REQ_AUTH	Authentication request message the portal server sends to the access device
ACK_AUTH	Authentication acknowledgment message the access device sends to the portal server
REQ_LOGOUT	Logout request message the portal server sends to the access device
ACK_LOGOUT	Logout acknowledgment message the access device sends to the portal server
AFF_ACK_AUTH	Affirmation message the portal server sends to the access device after receiving an authentication acknowledgement message
NTF_LOGOUT	Forced logout notification message the access device sends to the portal server
REQ_INFO	Information request message
ACK_INFO	Information acknowledgment message
NTF_USERDISCOVER	User discovery notification message the portal server sends to the access device
NTF_USERIPCHANGE	User IP change notification message the access device sends to the portal server
AFF_NTF_USERIPCHANGE	User IP change success notification message the portal server sends to the access device

Field	Description
ACK_NTF_LOGOUT	Forced logout acknowledgment message from the portal server

## display portal tcp-cheat statistics

### Syntax

**display portal tcp-cheat statistics**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display portal tcp-cheat statistics** command to display TCP spoofing statistics.

### Examples

```
# Display TCP spoofing statistics.
<Sysname> display portal tcp-cheat statistics
TCP Cheat Statistic:
Total Opens: 0
Resets Connections: 0
Current Opens: 0
Packets Received: 0
Packets Sent: 0
Packets Retransmitted: 0
Packets Dropped: 0
HTTP Packets Sent: 0
Connection State:
    SYN_RECVD: 0
    ESTABLISHED: 0
    CLOSE_WAIT: 0
    LAST_ACK: 0
    FIN_WAIT_1: 0
    FIN_WAIT_2: 0
    CLOSING: 0
```

**Table 1-7** display portal tcp-cheat statistics command output description

Field	Description
TCP Cheat Statistic	TCP spoofing statistics
Total Opens	Total number of opened connections

Field	Description
Resets Connections	Number of connections reset through RST packets
Current Opens	Number of connections currently being setting up
Packets Received	Number of received packets
Packets Sent	Number of sent packets
Packets Retransmitted	Number of retransmitted packets
Packets Dropped	Number of dropped packets
HTTP Packets Sent	Number of HTTP packets sent
Connection State	Statistics of connections in various state
ESTABLISHED	Number of connections in ESTABLISHED state
CLOSE_WAIT	Number of connections in CLOSE_WAIT state
LAST_ACK	Number of connections in LAST-ACK state
FIN_WAIT_1	Number of connections in FIN_WAIT_1 state
FIN_WAIT_2	Number of connections in FIN_WAIT_2 state
CLOSING	Number of connections in CLOSING state

## display portal user

### Syntax

```
display portal user { all | interface interface-type interface-number }
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**all**: Specifies all interfaces.

**interface** *interface-type interface-number*: Specifies an interface by its type and name.

### Description

Use the **display portal user** command to display information about portal users on a specified interface or all interfaces.

### Examples

```
# Display information about portal users on all interfaces.
```

```
<Sysname> display portal user all
```

```
Index: 2
```

```
State: ONLINE
```

```
SubState: INVALID
```

```
ACL: NONE
```

```

MAC                IP                Vlan  Interface
-----
000d-88f8-0eab    2.2.2.2          0     Vlan-interface 100
Index: 3
State: ONLINE
SubState: INVALID
ACL: 3000
MAC                IP                Vlan  Interface
-----
000d-88f8-0eac    2.2.2.3          0     Vlan-interface 100
Total 2 user(s) matched, 2 listed.

```

**Table 1-8 display portal user command output description**

Field	Description
Index	Index of the portal user
State	Current status of the portal user
SubState	Current sub-status of the portal user
ACL	Authorization ACL of the portal user
MAC	MAC address of the portal user
IP	IP address of the portal user
Vlan	VLAN to which the portal user belongs
Interface	Interface to which the portal user is attached
Total 2 user(s) matched, 2 listed	Total number of portal users

## portal auth-network

### Syntax

```

portal auth-network network-address { mask-length | mask }
undo portal auth-network { network-address | all }

```

### View

Interface view

### Default Level

2: System level

### Parameters

*network-address*: IP address of the authentication subnet.

*mask-length*: Length of the subnet mask, in the range of 0 to 32.

*mask*: Subnet mask, in dotted decimal notation.

**all**: Specifies all authentication subnets.

## Description

Use the **portal auth-network** command to configure a portal authentication subnet.

Use the **undo portal auth-network** command to remove a specified portal authentication subnet or all portal authentication subnets.

Note that this command is only applicable for Layer 3 authentication. The portal authentication subnet for direct authentication is any source IP address, and the portal authentication subnet for re-DHCP authentication is the one determined by the private IP address of the interface.

By default, the portal authentication subnet is 0.0.0.0/0, meaning that users in all subnets are to be authenticated.

## Examples

```
# Configure a portal authentication subnet of 10.10.10.0/24.
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] portal auth-network 10.10.10.0 24
```

## portal delete-user

### Syntax

```
portal delete-user { ip-address | all | interface interface-type interface-number }
```

### View

System view

### Default Level

2: System level

### Parameters

*ip-address*: IP address of a user.

**all**: Logs out all users.

**interface** *interface-type interface-number*: Logs out all users on the specified interface.

## Description

Use the **portal delete-user** command to log out users.

Related commands: **display portal user**.

## Examples

```
# Log out user 1.1.1.1.
<Sysname> system-view
[Sysname] portal delete-user 1.1.1.1
```

## portal domain

### Syntax

```
portal domain domain-name
```

## undo portal domain

### View

Interface view

### Default Level

2: System level

### Parameters

*domain-name*: ISP domain name, a case-insensitive string of 1 to 24 characters. The domain specified by this argument must already exist.

### Description

Use the **portal domain** command to specify a mandatory authentication domain for an interface. After you specify a mandatory authentication domain for an interface, the device will use the mandatory authentication domain for authentication, authorization and accounting (AAA) of the portal users on the interface.

Use the **undo portal domain** command to restore the default.

By default, no mandatory authentication domain is specified for an interface.

Related commands: **display portal interface**.

### Examples

# On VLAN-interface 100, configure the mandatory authentication domain as **my-domain**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal domain my-domain
```

## portal free-rule

### Syntax

```
portal free-rule rule-number { destination { any | ip { ip-address mask { mask-length | netmask } | any } } | source { any | [ interface interface-type interface-number | ip { ip-address mask { mask-length | netmask } | any } | mac mac-address | vlan vlan-id ] * } } *
```

```
undo portal free-rule { rule-number | all }
```

### View

System view

### Default Level

2: System level

### Parameters

*rule-number*: Number for the portal-free rule. The value range from 0 to 31.

**any**: Imposes no limitation on the previous keyword.

**ip** *ip-address*: Specifies an IP address.

**mask** { *mask-length* | *netmask* }: Specifies the mask of the IP address, which can be in dotted decimal notation or an integer in the range 0 to 32.

**interface** *interface-type interface-number*: Specifies a source interface.

**mac** *mac-address*: Specifies a source MAC address in the format of H-H-H.

**vlan** *vlan-id*: Specifies a source VLAN ID.

**all**: Specifies all portal-free rules.

## Description

Use the **portal free-rule** command to configure a portal-free rule and specify the source filtering condition and/or destination filtering condition.

Use the **undo portal free-rule** command to remove a specified portal-free rule or all portal-free rules.

Note that:

- If you specify both the source IP address and source MAC address, the IP address must be a host address under a 32-bit mask. Otherwise, the specified MAC address does not take effect.
- If you specify both a VLAN and interface in a portal-free rule, the interface must belong to the VLAN.
- You cannot configure a portal-free rule to have the same filtering criteria as that of an existing one. Otherwise, the system prompts that the rule already exists.
- No matter whether portal authentication is enabled, you can only add or remove a portal-free rule, rather than modifying it.

Related commands: **display portal free-rule**.



### Note

- If you specify both the source IP and source MAC address information in a portal-free rule, the IP address must be a host address with a mask of 32 bits; otherwise, the specified MAC address will be neglected.
  - You cannot configure two portal-free rules with the same filtering conditions. Otherwise, the device will prompt that the portal-free rule already exists.
- 

## Examples

# Configure a portal-free rule, allowing any packet whose source IP address is 10.10.10.1/24 and source interface is Vlan-interface 100 to bypass portal authentication.

```
<Sysname> system-view
[Sysname] portal free-rule 15 source ip 10.10.10.1 mask 24 interface Vlan-interface 100
destination ip any
```

## portal server

### Syntax

```
portal server server-name ip ip-address [ key key-string | port port-id | url url-string ] *
undo portal server server-name [ key | port | url ]
```

## View

System view

## Default Level

2: System level

## Parameters

*server-name*: Name of the portal server, a case-sensitive string of 1 to 32 characters.

*ip-address*: IP address of the portal server.

*key-string*: Shared key for communication with the portal server, a case-sensitive string of 1 to 16 characters.

*port-id*: Destination port number used when the device sends a message to the portal server unsolicitedly, in the range 1 to 65534. The default is 50100.

*url-string*: Uniform resource locator (URL) to which HTTP packets are to be redirected. The default URL is in the *http://ip-address* format, where *ip-address* is the IP address of the portal server. You can also specify the name of the portal server, in which case you need to use the **portal free-rule** command to configure the IP address of the DNS server as a portal authentication-free IP address.

## Description

Use the **portal server** command to configure a portal server.

Use the **undo portal server** command to remove a portal server, restore the default destination port number or URL, or delete the shared key.

By default, no portal server is configured.

Note that:

- Using the **undo portal server** *server-name* command, you remove the specified portal server if the specified portal server exists and there is no user on the interfaces referencing the portal server.
- The configured portal server and its parameters can be removed or modified only when the portal server is not referenced by an interface. To remove or modify the settings of a portal server that has been referenced by an interface, you must remove the portal configuration on the interface using the **undo portal** command.

Related commands: **display portal server**.

## Examples

```
# Configure portal server pts, setting the IP address to 192.168.0.111, the key to portal, and the redirection URL to http://192.168.0.111/portal.
```

```
<Sysname> system-view
```

```
[Sysname] portal server pts ip 192.168.0.111 key portal url http://192.168.0.111/portal
```

## portal server method

### Syntax

```
portal server server-name method { direct | layer3 | redhcp }
```

```
undo portal
```

## View

Interface view

## Default Level

2: System level

## Parameters

**server-name**: Name of the portal server, a case-sensitive string of 1 to 32 characters.

**method**: Specifies the authentication mode to be used.

**direct**: Direct authentication.

**layer3**: Layer 3 authentication.

**redhcp**: Re-DHCP authentication.

## Description

Use the **portal server** command to enable portal authentication on an interface, and specify the portal server to be referenced and the authentication mode.

Use the **undo portal** command to disable portal authentication on an interface.

By default, portal authentication is disabled on an interface.

Note that: The portal server to be referenced must exist.

Related commands: **display portal server**.

## Examples

# Enable portal authentication on interface VLAN-interface 100, setting the portal server to **pts**, and the authentication mode to **direct**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal server pts method direct
```

## reset portal connection statistics

### Syntax

```
reset portal connection statistics { all | interface interface-type interface-number }
```

## View

User view

## Default Level

1: Monitor level

## Parameters

**all**: Specifies all interfaces.

**interface** *interface-type interface-number*: Specifies an interface by its type and number.

## Description

Use the **reset portal connection statistics** command to clear portal connection statistics on a specified interface or all interfaces.

## Examples

```
# Clear portal connection statistics on interface Vlan-interface 100.
```

```
<Sysname> reset portal connection statistics interface Vlan-interface 100
```

## reset portal server statistics

### Syntax

```
reset portal server statistics { all | interface interface-type interface-number }
```

### View

User view

### Default Level

1: Monitor level

### Parameters

**all**: Specifies all interfaces.

**interface** *interface-type interface-number*: Specifies an interface by its type and number.

## Description

Use the **reset portal server statistics** command to clear portal server statistics on a specified interface or all interfaces.

## Examples

```
# Clear portal server statistics on interface Vlan-interface 100.
```

```
<Sysname> reset portal server statistics interface Vlan-interface 100
```

## reset portal tcp-cheat statistics

### Syntax

```
reset portal tcp-cheat statistics
```

### View

User view

### Default Level

1: Monitor level

### Parameters

None

## Description

Use the **reset portal tcp-cheat statistics** command to clear TCP spoofing statistics.

## Examples

# Clear TCP spoofing statistics.

```
<Sysname> reset portal tcp-cheat statistics
```

# Table of Contents

<b>1 Port Security Configuration Commands</b> .....	<b>1-1</b>
Port Security Configuration Commands.....	1-1
display port-security.....	1-1
display port-security mac-address block .....	1-3
display port-security mac-address security .....	1-4
port-security authorization ignore .....	1-6
port-security enable .....	1-7
port-security intrusion-mode .....	1-8
port-security mac-address security .....	1-9
port-security max-mac-count.....	1-10
port-security ntk-mode.....	1-11
port-security oui .....	1-12
port-security port-mode .....	1-13
port-security timer disableport .....	1-14
port-security trap.....	1-15

# 1 Port Security Configuration Commands

---

## Port Security Configuration Commands

### display port-security

#### Syntax

```
display port-security [ interface interface-list ]
```

#### View

Any view

#### Default Level

2: System level

#### Parameters

*interface-list*: Ethernet port list, in the format of { *interface-type interface-number* [ **to** *interface-type interface-number* ] }&<1-10>, where &<1-10> means that you can specify up to 10 port or port ranges. The starting port and ending port of a port range must be of the same type and the ending port number must be greater than the starting port number.

#### Description

Use the **display port-security** command to display port security configuration information, operation information, and statistics about one or more specified ports or all ports.

Related commands: **port-security enable**, **port-security port-mode**, **port-security ntk-mode**, **port-security intrusion-mode**, **port-security max-mac-count**, **port-security mac-address security**, **port-security authorization ignore**, **port-security oui**, **port-security trap**.

#### Examples

# Display port security configuration information, operation information, and statistics about all ports.

```
<Sysname> display port-security
Equipment port-security is enabled
AddressLearn trap is enabled
Intrusion trap is enabled
Dot1x logon trap is enabled
Dot1x logoff trap is enabled
Dot1x logfailure trap is enabled
```

```

RALM logon trap is enabled
RALM logoff trap is enabled
RALM logfailure trap is enabled
Disableport Timeout: 20s
OUI value:
  Index is 1, OUI value is 000d1a
  Index is 2, OUI value is 003c12

GigabitEthernet1/0/1 is link-down
  Port mode is UserloginWithOUI
  NeedtoKnow mode is needtoknowonly
  Intrusion mode is disableport
  Max MAC address number is 50
  Stored MAC address number is 0
  Authorization is ignored
GigabitEthernet1/0/2 is link-down
  Port mode is noRestriction
  NeedtoKnow mode is disabled
  Intrusion mode is no action
  Max MAC address number is not configured
  Stored MAC address number is 0
  Authorization is permitted

```

**Table 1-1 display port-security command output description**

Field	Description
Equipment port-security is enabled	Port security is enabled.
AddressLearn trap is enabled	Address learning trap is enabled.
Intrusion trap is enabled	Intrusion protection trap is enabled.
Dot1x logon trap is enabled	802.1X logon trap is enabled.
Dot1x logoff trap is enabled	802.1X logoff trap is enabled.
Dot1x logfailure is enabled	802.1X authentication failure trap is enabled.
RALM logon trap is enabled	MAC authentication success trap is enabled.
RALM logoff trap is enabled	MAC authenticated user logoff trap is enabled.
RALM logfailure trap is enabled	MAC authentication failure trap is enabled.
Disableport Timeout	Silence timeout of the port, in seconds.
OUI value	24-bit OUI value
Index	OUI index
Port mode is UserloginWithOUI	The port security mode is UserloginWithOUI.
NeedtoKnow mode is needtoknowonly	The NTK mode is needtoknowonly.
Intrusion mode is disableport	Intrusion protection action is set to <b>disableport</b> .
Max MAC address number	Maximum number of secure MAC addresses allowed on the port
Stored MAC address number	Number of MAC addresses stored

Field	Description
Authorization is ignored	Authorization information from the server is ignored. By default, the information takes effect and this field is displayed as "Authorization is permitted."

## display port-security mac-address block

### Syntax

```
display port-security mac-address block [ interface interface-type interface-number ] [ vlan vlan-id ] [ count ]
```

### View

Any view

### Default Level

2: System level

### Parameters

**interface** *interface-type interface-number*: Specifies a port by its type and number.

**vlan** *vlan-id*: Specifies a VLAN by its number, which is in the range 1 to 4094.

**count**: Displays only the count of the blocked MAC addresses.

### Description

Use the **display port-security mac-address block** command to display information about blocked MAC addresses.

With no keyword or argument specified, the command displays information about all blocked MAC addresses.

Related commands: **port-security intrusion-mode**.

### Examples

# Display information about all blocked MAC addresses.

```
<Sysname> display port-security mac-address block
MAC ADDR          From Port          VLAN ID
0002-0002-0002    GigabitEthernet1/0/1    1
000d-88f8-0577    GigabitEthernet1/0/1    1
```

```
--- On slot 2, 2 mac address(es) found ---
--- 2 mac address(es) found ---
```

# Display the count of all blocked MAC addresses.

```
<Sysname> display port-security mac-address block count
--- On slot 2, 2 mac address(es) found ---
--- 2 mac address(es) found ---
```

**# Display information about all blocked MAC addresses in VLAN 1.**

```
<Sysname> display port-security mac-address block vlan 1
MAC ADDR          From Port          VLAN ID
0002-0002-0002    GigabitEthernet1/0/1    1
000d-88f8-0577    GigabitEthernet1/0/1    1

--- On slot 2,2 mac address(es) found ---
--- 2 mac address(es) found ---
```

**# Display information about all blocked MAC addresses of port GigabitEthernet 1/0/1.**

```
<Sysname> display port-security mac-address block interface GigabitEthernet1/0/1
MAC ADDR          From Port          VLAN ID
000d-88f8-0577    GigabitEthernet1/0/1    1

--- On slot 2, 1 mac address(es) found ---
--- 1 mac address(es) found ---
```

**# Display information about all blocked MAC addresses of port GigabitEthernet 1/0/1 in VLAN 1.**

```
<Sysname> display port-security mac-address block interface GigabitEthernet 1/0/1 vlan 1
MAC ADDR          From Port          VLAN ID
000d-88f8-0577    GigabitEthernet1/0/1    1

--- On slot 2, 1 mac address(es) found ---
--- 1 mac address(es) found ---
```

**Table 1-2** display port-security mac-address block command output description

Field	Description
MAC ADDR	Blocked MAC address
From Port	Port having received frames with the blocked MAC address being the source address
VLAN ID	ID of the VLAN to which the port belongs
2 mac address(es) found	Number of blocked MAC addresses

## display port-security mac-address security

### Syntax

```
display port-security mac-address security [ interface interface-type interface-number ] [ vlan vlan-id ] [ count ]
```

### View

Any view

## Default Level

2: System level

## Parameters

**interface** *interface-type interface-number*: Specifies a port by its type and number.

**vlan** *vlan-id*: Specifies a VLAN by its number, which is in the range 1 to 4094.

**count**: Displays only the count of the secure MAC addresses.

## Description

Use the **display port-security mac-address security** command to display information about secure MAC addresses.

With no keyword or argument specified, the command displays information about all secure MAC addresses.

Related commands: **port-security mac-address security**.

## Examples

# Display information about all secure MAC addresses.

```
<Sysname> display port-security mac-address security
MAC ADDR          VLAN ID  STATE          PORT INDEX          AGING TIME(s)
0002-0002-0002    1        Security       GigabitEthernet1/0/1  NOAGED
000d-88f8-0577    1        Security       GigabitEthernet1/0/1  NOAGED

--- 2 mac address(es) found ---
```

# Display only the count of the secure MAC addresses.

```
<Sysname> display port-security mac-address count
2 mac address(es) found
```

# Display information about secure MAC addresses in a specified VLAN.

```
<Sysname> display port-security mac-address security vlan 1
MAC ADDR          VLAN ID  STATE          PORT INDEX          AGING TIME(s)
0002-0002-0002    1        Security       GigabitEthernet1/0/1  NOAGED
000d-88f8-0577    1        Security       GigabitEthernet1/0/1  NOAGED

--- 2 mac address(es) found ---
```

# Display information about secure MAC addresses on the specified port.

```
<Sysname> display port-security mac-address security interface GigabitEthernet1/0/1
MAC ADDR          VLAN ID  STATE          PORT INDEX          AGING TIME(s)
000d-88f8-0577    1        Security       GigabitEthernet1/0/1  NOAGED

--- 1 mac address(es) found ---
```

# Display information about secure MAC addresses that are on the specified port and in the specified VLAN.

```

<Sysname> display port-security mac-address security interface GigabitEthernet 1/0/1 vlan
1
MAC ADDR          VLAN ID  STATE          PORT INDEX          AGING TIME(s)
000d-88f8-0577  1       Security      GigabitEthernet1/0/1  NOAGED

--- 1 mac address(es) found ---

```

**Table 1-3** display port-security mac-address command output description

Field	Description
MAC ADDR	Secure MAC address
VLAN ID	VLAN to which the port belongs
STATE	Type of the MAC address added
PORT INDEX	Port to which the secure MAC address belongs
AGING TIME(s)	Period of time before the secure MAC address ages out
xxx mac address(es) found	Number of secure MAC addresses stored

## port-security authorization ignore

### Syntax

```

port-security authorization ignore
undo port-security authorization ignore

```

### View

Layer 2 Ethernet interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **port-security authorization ignore** command to configure a port to ignore the authorization information from the RADIUS server.

Use the **undo port-security port-mode ignore** command to restore the default.

By default, a port uses the authorization information from the RADIUS server.

After a user passes RADIUS authentication, the RADIUS server performs authorization based on the authorization attributes configured for the user's account. For example, it may assign a VLAN.

Related commands: **display port-security**.

## Examples

# Configure port GigabitEthernet 1/0/1 to ignore the authorization information from the RADIUS server.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security authorization ignore
```

## port-security enable

### Syntax

**port-security enable**

**undo port-security enable**

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **port-security enable** command to enable port security.

Use the **undo port-security enable** command to disable port security.

By default, port security is disabled.

Note that:

- 1) Port security cannot be enabled when 802.1X or MAC authentication is enabled globally.
- 2) Enabling port security resets the following configurations on a port to the defaults bracketed, making them dependent completely on the port security mode:
  - 802.1X (disabled), port access control method (**macbased**), and port access control mode (**auto**)
  - MAC authentication (disabled)
- 3) Disabling port security resets the following configurations on a port to the defaults bracketed:
  - Port security mode (noRestrictions)
  - 802.1X (disabled), port access control method (**macbased**), and port access control mode (**auto**)
  - MAC authentication (disabled)
- 4) Port security cannot be disabled if there is any user present on a port.

Related commands: **display port-security**, **dot1x**, **dot1x port-method**, **dot1x port-control** in *802.1X Commands* of the *Security Volume*, **mac-authentication** in *MAC Authentication Commands* of the *Security Volume*.

## Examples

```
# Enable port security.
<Sysname> system-view
[Sysname] port-security enable
```

## port-security intrusion-mode

### Syntax

```
port-security intrusion-mode { blockmac | disableport | disableport-temporarily }
undo port-security intrusion-mode
```

### View

Layer 2 Ethernet interface view

### Default Level

2: System level

### Parameters

**blockmac**: Adds the source MAC addresses of illegal frames to the blocked MAC address list and discards frames with blocked source MAC addresses. A blocked MAC address is restored to normal after being blocked for three minutes, which is fixed and cannot be changed. You can use the **display port-security mac-address block** command to view the blocked MAC address list.

**disableport**: Disables the port permanently upon detecting an illegal frame received on the port.

**disableport-temporarily**: Disables the port for a specified period of time whenever it receives an illegal frame. Use the **port-security timer disableport** command to set the period.

### Description

Use the **port-security intrusion-mode** command to configure the intrusion protection feature, so that the interface performs configured security policies in response to received illegal packets.

Use the **undo port-security intrusion-mode** command to restore the default.

By default, intrusion protection is disabled.

You can use the **undo shutdown** command to restore the connection of the port.

Related commands: **display port-security**, **display port-security mac-address block**, **port-security timer disableport**.

## Examples

```
# Configure port GigabitEthernet 1/0/1 to block the source MAC addresses of illegal frames after intrusion protection is triggered.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] port-security intrusion-mode blockmac
```

## port-security mac-address security

### Syntax

In Layer 2 Ethernet interface view:

```
port-security mac-address security mac-address vlan vlan-id
```

In system view:

```
port-security mac-address security mac-address interface interface-type interface-number vlan  
vlan-id
```

```
undo port-security mac-address security [ [ mac-address [ interface interface-type  
interface-number ] ] vlan vlan-id ]
```

### View

Layer 2 Ethernet Interface view, system view

### Default Level

2: System level

### Parameters

*mac-address*: Secure MAC address, in the H-H-H format.

**interface** *interface-type* *interface-number*: Specifies a Layer 2 Ethernet port by its type and number.

*vlan-id*: ID of the VLAN to which the secure MAC address belongs, in the range 1 to 4094.

### Description

Use the **port-security mac-address security** command to add a secure MAC address.

Use the **undo port-security mac-address security** command to remove specified secure MAC addresses.

By default, no secure MAC address is configured.

Note that:

- The port must belong to the specified VLAN.
- You can configure a secure MAC address only if port security is enabled and the specified port operates in autoLearn mode.
- The **undo port-security mac-address security** command can be used in system view only.

Related commands: **display port-security**.

### Examples

```
# Enable port security, set the port security mode of port GigabitEthernet 1/0/1 to autoLearn, and add  
a secure MAC address of 0001-0001-0002 (belonging to VLAN 10) for port GigabitEthernet 1/0/1 in
```

system view.

```
<Sysname> system-view
[Sysname] port-security enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security max-mac-count 100
[Sysname-GigabitEthernet1/0/1] port-security port-mode autolearn
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] port-security mac-address security 0001-0001-0002 interface gigabitethernet 1/0/1
vlan 10
```

# Enable port security, set the port security mode of port GigabitEthernet 1/0/1 to autoLearn, and add a secure MAC address of 0001-0002-0003 (belonging to VLAN 4) for port GigabitEthernet 1/0/1 in interface view.

```
<Sysname> system-view
[Sysname] port-security enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security max-mac-count 100
[Sysname-GigabitEthernet1/0/1] port-security port-mode autolearn
[Sysname-GigabitEthernet1/0/1] port-security mac-address security 0001-0002-0003 vlan 4
```

## port-security max-mac-count

### Syntax

**port-security max-mac-count** *count-value*

**undo port-security max-mac-count**

### View

Ethernet interface view

### Default Level

2: System level

### Parameters

*count-value*: Maximum number of secure MAC addresses allowed on the port, ranging 1 to 1,024.

### Description

Use the **port-security max-mac-count** command to set the maximum number of secure MAC addresses allowed on the port.

Use the **undo port-security max-mac-count** command to restore the default setting.

By default, the maximum number of secure MAC addresses is not limited.

Note that:

- You cannot change the maximum number of secure MAC addresses for a port working in the **autoLearn** mode.

- The maximum number of secure MAC addresses allowed on a port does not include or limit that of the static MAC addresses manually configured.
- The maximum number of secure MAC addresses allowed on a port must not be less than the number of MAC addresses stored on the port.

Related commands: **display port-security**.

## Examples

# Set the maximum number of secure MAC addresses allowed on port GigabitEthernet 1/0/1 to 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security max-mac-count 100
```

## port-security ntk-mode

### Syntax

**port-security ntk-mode { ntk-withbroadcasts | ntk-withmulticasts | ntkonly }**

**undo port-security ntk-mode**

### View

Ethernet interface view

### Default Level

2: System level

### Parameters

**ntk-withbroadcasts:** Sends only frames destined for authenticated MAC addresses or the broadcast address.

**ntk-withmulticasts:** Sends only frames destined for authenticated MAC addresses, multicast addresses, or the broadcast address.

**ntkonly:** Sends only frames destined for authenticated MAC addresses.

### Description

Use the **port-security ntk-mode** command to configure the NTK feature.

Use the **undo port-security ntk-mode** command to restore the default.

By default, NTK is disabled on a port and all frames are allowed to be sent.

The need to know (NTK) feature checks the destination MAC addresses in outbound frames to allow frames to be sent to only devices passing authentication, thus preventing illegal devices from intercepting network traffic.

Related commands: **display port-security**.

## Examples

# Set the NTK mode of port GigabitEthernet 1/0/1 to **ntkonly**, allowing the port to forward received packets to only devices passing authentication.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
```

## port-security oui

### Syntax

**port-security oui** *oui-value* **index** *index-value*

**undo port-security oui index** *index-value*

### View

System view

### Default Level

2: System level

### Parameters

*oui-value*: Organizationally unique identifier (OUI) string, a 48-bit MAC address in the H-H-H format. The system automatically uses only the 24 high-order bits as the OUI value.

*index-value*: OUI index, in the range 1 to 16.

### Description

Use the **port-security oui** command to configure an OUI value for user authentication. This value is used when the port security mode is UserLoginWithOUI.

Use the **undo port-security oui** command to delete an OUI value with the specified OUI index.

By default, no OUI value is configured.

Note that an OUI value configured by using the **port-security oui** command takes effect only when the security mode is userLoginWithOUI.

Related commands: **display port-security**.

## Examples

# Configure an OUI value of 000d2a, setting the index to 4.

```
<Sysname> system-view
[Sysname] port-security oui 000d-2a10-0033 index 4
```

## port-security port-mode

### Syntax

```
port-security port-mode { autolearn | mac-authentication | mac-else-userlogin-secure |  
mac-else-userlogin-secure-ext | secure | userlogin | userlogin-secure | userlogin-secure-ext |  
userlogin-secure-or-mac | userlogin-secure-or-mac-ext | userlogin-withoui }
```

```
undo port-security port-mode
```

### View

Interface view

### Default Level

2: System level

### Parameters

**autolearn:** Operates in autoLearn mode.

**mac-authentication:** Operates in macAddressWithRadius mode.

**mac-else-userlogin-secure:** Operates in macAddressElseUserLoginSecure mode.

**mac-else-userlogin-secure-ext:** Operates in macAddressElseUserLoginSecureExt mode.

**secure:** Operates in secure mode.

**userlogin:** Operates in userLogin mode.

**userlogin-secure:** Operates in userLoginSecure mode.

**userlogin-secure-ext:** Operates in userLoginSecureExt mode.

**userlogin-secure-or-mac:** Operates in macAddressOrUserLoginSecure mode.

**userlogin-secure-or-mac-ext:** Operates in macAddressOrUserLoginSecureExt mode.

**userlogin-withoui:** Operates in userLoginWithOUI mode.

### Description

Use the **port-security port-mode** command to set the port security mode of a port.

Use the **undo port-security port-mode** command to restore the default.

By default, a port operates in noRestrictions mode, where port security does not take effect.

Note that:

- Configuration of port security mode on a port is mutually exclusive with the configuration of 802.1X authentication, port access control method, port access control mode, and MAC authentication on the port.

- With port security enabled, you can change the port security mode of a port only when the port is operating in noRestrictions mode, the default mode. You can use the **undo port-security port-mode** command to restore the default port security mode.
- Before configuring the port security mode to autoLearn, be sure to configure the maximum number of secure MAC addresses allowed on the port by using the **port-security max-mac-count** command.
- You cannot change the port security mode of a port with users online.

Related commands: **display port-security**.

## Examples

# Enable port security and configure the port security mode of port GigabitEthernet 1/0/1 as secure.

```
<Sysname> system-view
[Sysname] port-security enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security port-mode secure
```

# Change the port security mode of port GigabitEthernet 1/0/1 to userLogin.

```
[Sysname-GigabitEthernet1/0/1] undo port-security port-mode
[Sysname-GigabitEthernet1/0/1] port-security port-mode userlogin
```

## port-security timer disableport

### Syntax

**port-security timer disableport** *time-value*

**undo port-security timer disableport**

### View

System view

### Default Level

2: System level

### Parameters

*time-value*: Silence timeout during which the port remains disabled, in seconds. It ranges from 20 to 300.

### Description

Use the **port-security timer disableport** command to set the silence timeout during which the port remains disabled.

Use the **undo port-security timer disableport** command to restore the default.

By default, the silence timeout is 20 seconds.

If you configure the intrusion protection policy as disabling the port temporarily whenever it receives an illegal frame, you can use this command to set the silence period.

Related commands: **display port-security**.

## Examples

# Configure the intrusion protection policy as disabling the port temporarily whenever it receives an illegal frame and set the silence timeout to 30 seconds.

```
<Sysname> system-view
[Sysname] port-security timer disableport 30
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
```

## port-security trap

### Syntax

```
port-security trap { addresslearned | dot1xlogfailure | dot1xlogoff | dot1xlogon | intrusion |
ralmlogfailure | ralmlogoff | ralmlogon }
```

```
undo port-security trap { addresslearned | dot1xlogfailure | dot1xlogoff | dot1xlogon | intrusion
| ralmlogfailure | ralmlogoff | ralmlogon }
```

### View

System view

### Default Level

2: System level

### Parameters

**addresslearned**: Address learning trap. When enabled, this function allows the system to send a trap message when a port learns a new MAC address.

**dot1xlogfailure**: Trap for 802.1X authentication failure.

**dot1xlogon**: Trap for successful 802.1X authentication.

**dot1xlogoff**: Trap for 802.1X user logoff events.

**intrusion**: Trap for illegal frames.

**ralmlogfailure**: Trap for MAC authentication failure.

**ralmlogoff**: Trap for MAC authentication user logoff events.

**ralmlogon**: Trap for successful MAC authentication.



## Note

RALM (RADIUS Authenticated Login using MAC-address) means RADIUS authentication based on MAC address.

---

## Description

Use the **port-security trap** command to enable port security traps.

Use the **undo port-security trap** command to disable port security traps.

By default, no port security trap is enabled.

This command involves the trap feature. With the trap feature, a device can send trap information upon receiving packets that result from, for example, intrusion, abnormal login, or logout operations, allowing you to monitor operations of interest.

Related commands: **display port-security**.

## Examples

# Enable address learning trap.

```
<Sysname> system-view
```

```
[Sysname] port-security trap addresslearned
```

# Table of Contents

<b>1 IP Source Guard Configuration Commands</b> .....	<b>1-1</b>
IP Source Guard Configuration Commands .....	1-1
display ip check source .....	1-1
display user-bind .....	1-2
ip check source.....	1-3
user-bind.....	1-4

# 1 IP Source Guard Configuration Commands

---

## IP Source Guard Configuration Commands

### display ip check source

#### Syntax

```
display ip check source [ interface interface-type interface-number | ip-address ip-address |  
mac-address mac-address ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

**interface** *interface-type interface-number*: Displays the dynamic bindings of the interface specified by its type and number.

**ip-address** *ip-address*: Displays the dynamic bindings of an IP address.

**mac-address** *mac-address*: Displays the dynamic bindings of an MAC address (in the format of H-H-H).

#### Description

Use the **display ip check source** command to display dynamic bindings.

With no options specified, the command displays the dynamic bindings of all interfaces.

Related commands: **ip check source**.

#### Examples

# Display all dynamic bindings.

```
<Sysname> display ip check source
```

```
Total entries found: 5
```

MAC	IP	Vlan	Port	Status
040a-0000-4000	10.1.0.9	2	GigabitEthernet1/0/1	DHCP-SNP
N/A	10.1.0.8	2	GigabitEthernet1/0/1	DHCP-SNP
040a-0000-2000	10.1.0.7	2	GigabitEthernet1/0/1	DHCP-SNP

**Table 1-1 display ip check source** command output description

Field	Description
Total entries found	Total number of found entries
MAC	MAC address of the dynamic binding. N/A means that no MAC address is bound in the entry.
IP	IP address of the dynamic binding. N/A means that no IP address is bound in the entry.
Vlan	VLAN to which the obtained binding entry belongs. N/A means that no VLAN is bound in the entry.
Port	Port to which the dynamic binding entry is applied
Status	Type of dynamically obtaining the binding entry

## display user-bind

### Syntax

```
display user-bind [ interface interface-type interface-number | ip-address ip-address | mac-address mac-address ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**interface** *interface-type interface-number*: Displays the static bindings of the interface specified by its type and number.

**ip-address** *ip-address*: Displays the static bindings of an IP address.

**mac-address** *mac-address*: Displays the static bindings of an MAC address (in the format of H-H-H).

### Description

Use the **display user-bind** command to display static bindings.

With no options specified, the command displays static bindings of all interfaces.

Related commands: **user-bind**.

### Examples

```
# Display all static bindings.
```

```
<Sysname> display user-bind
```

```
Total entries found: 4
```

MAC	IP	Vlan	Port	Status
N/A	1.1.1.1	N/A	GigabitEthernet1/0/1	Static
0001-0001-0001	2.2.2.2	200	GigabitEthernet1/0/1	Static
0003-0003-0003	N/A	N/A	GigabitEthernet1/0/2	Static
0004-0004-0004	4.4.4.4	N/A	GigabitEthernet1/0/2	Static

**Table 1-2 display user-bind command output description**

Field	Description
Total entries found	Total number of found entries
MAC	MAC address of the binding. N/A means that no MAC address is bound in the entry.
IP	IP address of the binding. N/A means that no IP address is bound in the entry.
Vlan	VLAN of the binding. N/A means that no VLAN is bound in the entry.
Port	Port of the binding
Status	Type of the binding. Static means that the binding is manually configured.

## ip check source

### Syntax

```
ip check source { ip-address | ip-address mac-address | mac-address }  
undo ip check source
```

### View

Ethernet interface view, VLAN interface view

### Default Level

2: System level

### Parameters

**ip-address:** Specifies to bind source IP address to the port.

**ip-address mac-address:** Specifies to bind source IP address and MAC address to the port.

**mac-address:** Specifies to bind source MAC address to the port.

### Description

Use the **ip check source** command to configure the dynamic binding function on a port.

Use the **undo ip check source** command to restore the default.

By default, the dynamic binding function is disabled.

Note that: You cannot configure the dynamic binding function on a port that is in an aggregation group.

Related commands: **display ip check source**.

### Examples

```
# Configure dynamic binding function on port GigabitEthernet1/0/1 to filter packets based on both  
source IP address and MAC address.
```

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ip check source ip-address mac-address
```

## user-bind

### Syntax

```
user-bind { ip-address ip-address | ip-address ip-address mac-address mac-address |  
mac-address mac-address } [ vlan vlan-id ]
```

```
undo user-bind { ip-address ip-address | ip-address ip-address mac-address mac-address |  
mac-address mac-address } [ vlan vlan-id ]
```

### View

Layer-2 Ethernet interface view

### Default Level

2: System level

### Parameters

**ip-address** *ip-address*: Specifies the IP address for the static binding. The IP address can only be a Class A, Class B, or Class C address and can be neither 127.x.x.x nor 0.0.0.0.

**mac-address** *mac-address*: Specifies the MAC address for the static binding in the format of H-H-H. The MAC address cannot be all 0s, all Fs (a broadcast address), or a multicast address.

**vlan** *vlan-id*: Specifies the VLAN for the static binding. *vlan-id* is the ID of the VLAN to be bound, in the range 1 to 4094.

### Description

Use the **user-bind** command to configure a static binding.

Use the **undo user-bind** command to delete a static binding.

By default, no static binding exists on a port.

Note that:

- The system does not support repeatedly configuring a binding entry to one port.
- For products supporting multi-port binding, a binding entry can be configured to multiple ports; for products that do not support multi-port binding, a binding entry can be configured to only one port.
- You cannot configure a static binding on a port that is in an aggregation group.

Related commands: **display user-bind**.

### Examples

```
# Configure a static binding on port GigabitEthernet1/0/1.
```

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] user-bind ip-address 192.168.0.1 mac-address 0001-0001-0001
```

# Table of Contents

<b>1 SSH2.0 Configuration Commands</b> .....	<b>1-1</b>
SSH2.0 Server Configuration Commands .....	1-1
display ssh server.....	1-1
display ssh user-information.....	1-2
ssh server authentication-retries .....	1-3
ssh server authentication-timeout .....	1-4
ssh server compatible-ssh1x enable.....	1-5
ssh server enable .....	1-5
ssh server rekey-interval .....	1-6
ssh user .....	1-7
SSH2.0 Client Configuration Commands.....	1-8
display ssh client source.....	1-8
display ssh server-info.....	1-9
ssh client authentication server .....	1-10
ssh client first-time enable.....	1-10
ssh client ipv6 source .....	1-11
ssh client source.....	1-12
ssh2 .....	1-12
ssh2 ipv6 .....	1-14
SFTP Server Configuration Commands .....	1-15
sftp server enable.....	1-15
sftp server idle-timeout .....	1-15
SFTP Client Configuration Commands.....	1-16
bye.....	1-16
cd.....	1-16
cdup.....	1-17
delete.....	1-18
dir.....	1-18
display sftp client source .....	1-19
exit .....	1-20
get.....	1-20
help.....	1-21
ls.....	1-21
mkdir.....	1-22
put.....	1-22
pwd .....	1-23
quit.....	1-24
remove.....	1-24
rename .....	1-25
rmdir.....	1-25
sftp.....	1-26
sftp client ipv6 source .....	1-27
sftp client source.....	1-27



# 1 SSH2.0 Configuration Commands

---

## SSH2.0 Server Configuration Commands

### display ssh server

#### Syntax

```
display ssh server { session | status }
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

**session:** Displays the session information of the SSH server.

**status:** Displays the status information of the SSH server.

#### Description

Use the **display ssh server** command on an SSH server to display SSH server status information or session information.

Related commands: **ssh server authentication-retries**, **ssh server rekey-interval**, **ssh server authentication-timeout**, **ssh server enable**, **ssh server compatible-ssh1x enable**.



#### Note

This command is also available on an SFTP server.

---

#### Examples

```
# Display the SSH server status information.
<Sysname> display ssh server status
SSH Server: Disable
SSH version : 1.99
SSH authentication-timeout : 60 second(s)
SSH server key generating interval : 0 hour(s)
SSH authentication retries : 3 time(s)
SFTP server: Disable
```

SFTP server Idle-Timeout: 10 minute(s)

**Table 1-1 display ssh server status** command output description

Field	Description
SSH Server	Whether the SSH server function is enabled
SSH version	SSH protocol version When the SSH supports SSH1, the protocol version is 1.99. Otherwise, the protocol version is 2.0.
SSH authentication-timeout	Authentication timeout period
SSH server key generating interval	SSH server key pair update interval
SSH authentication retries	Maximum number of SSH authentication attempts
SFTP server	Whether the SFTP server function is enabled
SFTP server Idle-Timeout	SFTP connection idle timeout period

# Display the SSH server session information.

```
<Sysname> display ssh server session
```

```
Conn  Ver  Encry  State          Retry  SerType  Username
VTY 0  2.0  DES    Established    0     SFTP    client001
```

**Table 1-2 display ssh server session** command output description

Field	Description
Conn	Connected VTY channel
Ver	SSH server protocol version
Encry	Encryption algorithm
State	Status of the session, including: Init, Ver-exchange, Keys-exchange, Auth-request, Serv-request, Established, Disconnected
Retry	Number of authentication attempts
SerType	Service type (SFTP, Stelnet)
Username	Name of a user during login

## display ssh user-information

### Syntax

```
display ssh user-information [ username ]
```

### View

Any view

### Default Level

1: Monitor level

## Parameters

*username*: SSH username, a string of 1 to 80 characters.

## Description

Use the **display ssh user-information** command on an SSH server to display information about one or all SSH users.

With the *username* argument not specified, the command displays information about all SSH users.

Related commands: **ssh user**.



### Note

This command is also available on an SFTP server.

---

## Examples

# Display information about all SSH users.

```
<Sysname> display ssh user-information
```

```
Total ssh users : 2
```

Username	Authentication-type	User-public-key-name	Service-type
yemx	password	null	stelnet   sftp
test	publickey	pubkey	sftp

**Table 1-3** display ssh user-information command output description

Field	Description
Username	Name of the user
Authentication-type	Authentication method. If this field has a value of <b>password</b> , the next field will have a value of <b>null</b> .
User-public-key-name	Public key of the user
Service-type	Service type

## ssh server authentication-retries

### Syntax

```
ssh server authentication-retries times
```

```
undo ssh server authentication-retries
```

### View

System view

### Default Level

2: System level

## Parameters

*times*: Maximum number of authentication attempts, in the range 1 to 5.

## Description

Use the **ssh server authentication-retries** command to set the maximum number of SSH connection authentication attempts, which takes effect at next login.

Use the **undo ssh server authentication-retries** command to restore the default.

By default, the maximum number of SSH connection authentication attempts is 3.

Note that:

- Authentication will fail if the number of authentication attempts (including both publickey and password authentication) exceeds that specified in the **ssh server authentication-retries** command.
- If the authentication method of SSH users is **password-publickey**, the maximum number of SSH connection authentication attempts must be at least 2. This is because SSH2.0 users must pass both password and publickey authentication.

Related commands: **display ssh server**.

## Examples

```
# Set the maximum number of SSH connection authentication attempts to 4.
```

```
<Sysname> system-view  
[Sysname] ssh server authentication-retries 4
```

## ssh server authentication-timeout

### Syntax

```
ssh server authentication-timeout time-out-value
```

```
undo ssh server authentication-timeout
```

### View

System view

### Default Level

2: System level

## Parameters

*time-out-value*: Authentication timeout period in seconds, in the range 1 to 120.

## Description

Use the **ssh server authentication-timeout** command to set the SSH user authentication timeout period on the SSH server.

Use the **undo ssh server authentication-timeout** command to restore the default.

By default, the authentication timeout period is 60 seconds.

Related commands: **display ssh server**.

## Examples

```
# Set the SSH user authentication timeout period to 10 seconds.
<Sysname> system-view
[Sysname] ssh server authentication-timeout 10
```

## ssh server compatible-ssh1x enable

### Syntax

```
ssh server compatible-ssh1x enable
undo ssh server compatible-ssh1x
```

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **ssh server compatible-ssh1x** command to enable the SSH server to work with SSH1 clients.

Use the **undo ssh server compatible-ssh1x** command to disable the SSH server from working with SSH1 clients.

By default, the SSH server can work with SSH1 clients.

This configuration takes effect only for users logging in after the configuration.

Related commands: **display ssh server**.

## Examples

```
# Enable the SSH server to work with SSH1 clients.
<Sysname> system-view
[Sysname] ssh server compatible-ssh1x enable
```

## ssh server enable

### Syntax

```
ssh server enable
undo ssh server enable
```

### View

System view

### Default Level

2: System level

## Parameters

None

## Description

Use the **ssh server enable** command to enable SSH server.

Use the **undo ssh server enable** command to disable SSH server.

By default, SSH server is disabled.

## Examples

```
# Enable SSH server.
<Sysname> system-view
[Sysname] ssh server enable
```

## ssh server rekey-interval

### Syntax

```
ssh server rekey-interval hours
undo ssh server rekey-interval
```

### View

System view

### Default Level

2: System level

## Parameters

*hours*: Server key pair update interval in hours, in the range 1 to 24.

## Description

Use the **ssh server rekey-interval** command to set the interval for updating the RSA server key.

Use the **undo ssh server rekey-interval** command to remove the configuration.

By default, the update interval of the RSA server key is 0, that is, the RSA server key is not updated.

Related commands: **display ssh server**.



### Caution

- This command is only available to SSH users using SSH1 client software.
  - The system does not update any DSA key pair periodically.
- 

## Examples

```
# Set the RSA server key pair update interval to 3 hours.
<Sysname> system-view
```

```
[Sysname] ssh server rekey-interval 3
```

## ssh user

### Syntax

```
ssh user username service-type stelnet authentication-type { password | { any | password-publickey | publickey } assign publickey keyname }
```

```
ssh user username service-type { all | sftp } authentication-type { password | { any | password-publickey | publickey } assign publickey keyname work-directory directory-name }
```

```
undo ssh user username
```

### View

System view

### Default Level

2: System level

### Parameters

**username**: SSH username, a case-sensitive string of 1 to 80 characters.

**service-type**: Specifies the service type of an SSH user, which can be one of the following:

- **all**: Specifies both secure Telnet and secure FTP.
- **sftp**: Specifies the service type as secure FTP.
- **stelnet**: Specifies the service type of secure Telnet.

**authentication-type**: Specifies the authentication method of an SSH user, which can be one of the following:

- **password**: Performs password authentication.
- **any**: Performs either password authentication or publickey authentication.
- **password-publickey**: Specifies that SSH2 clients perform both password authentication and publickey authentication and that SSH1 clients perform either type of authentication.
- **publickey**: Performs publickey authentication.

**assign publickey** *keyname*: Assigns an existing public key to an SSH user. *keyname* indicates the name of the client public key and is a string of 1 to 64 characters.

**work-directory** *directory-name*: Specifies the working folder for an SFTP user. *directory-name* indicates the name of the working folder and is a string of 1 to 135 characters.

### Description

Use the **ssh user** command to create an SSH user and specify the service type and authentication method.

Use the **undo ssh user** command to delete an SSH user.

Note that:

- For a publickey authentication user, you must configure the username and the public key on the device. For a password authentication user, you can configure the account information on either the device or the remote authentication server such as a RADIUS server.
- If you use the **ssh user** command to configure a public key for a user who has already had a public key, the new one overwrites the old one.

- Authentication method and public key configuration takes effect only for users logging in after the configuration.
- If an SFTP user has been assigned a public key, it is necessary to set a working folder for the user.
- The working folder of an SFTP user is subject to the user authentication method. For a user using only password authentication, the working folder is the AAA authorized one. For a user using only publickey authentication or using both the publickey and password authentication methods, the working folder is the one set by using the **ssh user** command.

Related commands: **display ssh user-information**.

## Examples

# Create an SSH user named **user1**, setting the service type as **sftp**, the authentication method as **publickey**, the work folder of the SFTP server as **flash**, and assigning a public key named **key1** to the user.

```
<Sysname> system-view
[Sysname] ssh user user1 service-type sftp authentication-type publickey assign publickey
key1 work-directory flash:
```

## SSH2.0 Client Configuration Commands

### display ssh client source

#### Syntax

```
display ssh client source
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

None

#### Description

Use the **display ssh client source** command to display the source IP address or source interface currently set for the SSH client.

If neither source IP address nor source interface is specified for the SSH client, the system will prompt you to specify the source information.

Related commands: **ssh client source**.

## Examples

# Display the source IP address of the SSH client.

```
<Sysname> display ssh client source
The source IP address you specified is 192.168.0.1
```

## display ssh server-info

### Syntax

```
display ssh server-info
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display ssh server-info** command on a client to display mappings between SSH servers and their host public keys saved on the client.

When an SSH client needs to authenticate the SSH server, it uses the locally saved public key of the server for the authentication. If the authentication fails, you can use this command to check the public key of the server saved on the client.

Related commands: **ssh client authentication server**.



#### Note

This command is also available on an SFTP client.

---

### Examples

# Display the mappings between host public keys and SSH servers saved on the client.

```
<Sysname> display ssh server-info
```

```
Server Name(IP)                Server public key name
```

---

```
192.168.0.1                    abc_key01
```

```
192.168.0.2                    abc_key02
```

**Table 1-4 display ssh server-info** command output description

Field	Description
Server Name(IP)	Name or IP address of the server
Server public key name	Name of the host public key of the server

## ssh client authentication server

### Syntax

```
ssh client authentication server server assign publickey keyname  
undo ssh client authentication server server assign publickey
```

### View

System view

### Default Level

2: System level

### Parameters

*server*: IP address or name of the server, a string of 1 to 80 characters.

*keyname*: Name of the host public key of the server, a string of 1 to 64 characters.

### Description

Use the **ssh client authentication server** command on a client to configure the host public key of the server so that the client can determine whether the server is trustworthy.

Use the **undo ssh authentication server** command to remove the configuration.

By default, the host public key of the server is not configured, and when logging into the server, the client uses the IP address or host name used for login as the public key name.

If the client does not support first authentication, it will reject unauthenticated servers. In this case, you need to configure the public keys of the servers and specify the mappings between public keys and servers on the client, so that the client uses the correct public key of a server to authenticate the server.

Note that the specified host public key of the server must already exist.

Related commands: **ssh client first-time enable**.

### Examples

```
# Configure the public key of the server with the IP address of 192.168.0.1 to be key1.
```

```
<Sysname> system-view
```

```
[Sysname] ssh client authentication server 192.168.0.1 assign publickey key1
```

## ssh client first-time enable

### Syntax

```
ssh client first-time enable  
undo ssh client first-time
```

### View

System view

### Default Level

2: System level

## Parameters

None

## Description

Use the **ssh client first-time enable** command to enable the first authentication function.

Use the **undo ssh client first-time** command to disable the function.

By default, the function is enabled.

With first-time authentication, when an SSH client not configured with the server host public key accesses the server for the first time, the user can continue accessing the server, and save the host public key on the client. When accessing the server again, the client will use the saved server host public key to authenticate the server.

Without first-time authentication, a client not configured with the server host public key will deny to access the server. To access the server, a user must configure in advance the server host public key locally and specify the public key name for authentication.

Note that as the server may update its key pairs periodically, clients must obtain the most recent public keys of the server for successful authentication of the server.

## Examples

```
# Enable the first authentication function.
```

```
<Sysname> system-view  
[Sysname] ssh client first-time enable
```

## ssh client ipv6 source

### Syntax

```
ssh client ipv6 source { ipv6 ipv6-address | interface interface-type interface-number }  
undo ssh client ipv6 source
```

### View

System view

### Default Level

3: Manage level

## Parameters

**ipv6** *ipv6-address*: Specifies a source IPv6 address.

**interface** *interface-type interface-number*: Specifies a source interface by its type and number.

## Description

Use the **ssh client ipv6 source** command to specify the source IPv6 address or source interface for the SSH client.

Use the **undo ssh client ipv6 source** command to remove the configuration.

By default, the client uses the source address specified by the route of the device to access the SSH server.

Related commands: **display ssh client source**.

## Examples

# Specify the source IPv6 address as 2:2::2:2 for the SSH client.

```
<Sysname> system-view
[Sysname] ssh client ipv6 source ipv6 2:2::2:2
```

## ssh client source

### Syntax

```
ssh client source { ip ip-address | interface interface-type interface-number }
undo ssh client source
```

### View

System view

### Default Level

3: Manage level

### Parameters

**ip** *ip-address*: Specifies a source IPv4 address.

**interface** *interface-type interface-number*: Specifies a source interface by its type and number.

### Description

Use the **ssh client source** command to specify the source IPv4 address or source interface of the SSH client.

Use the **undo ssh client source** command to remove the configuration.

By default, an SSH client uses the IP address of the interface specified by the route to access the SSH server.

Related commands: **display ssh client source**.

## Examples

# Specify the source IPv4 address of the SSH client as 192.168.0.1.

```
<Sysname> system-view
[Sysname] ssh client source ip 192.168.0.1
```

## ssh2

### Syntax

```
ssh2 server [ port-number ] [ identity-key { dsa | rsa } | prefer-ctos-cipher { aes128 | des } | prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 } | prefer-kex { dh-group-exchange | dh-group1 | dh-group14 } | prefer-stoc-cipher { aes128 | des } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 } ] *
```

### View

User view

## Default Level

0: Visit level

## Parameters

*server*: IPv4 address or host name of the server, a case-insensitive string of 1 to 20 characters.

*port-number*: Port number of the server, in the range 0 to 65535. The default is 22.

**identity-key**: Specifies the algorithm for publickey authentication, either **dsa** or **rsa**. The default is **dsa**.

**prefer-ctos-cipher**: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **aes128**: Encryption algorithm aes128-cbc
- **des**: Encryption algorithm des-cbc.

**prefer-ctos-hmac**: Preferred HMAC algorithm from client to server, defaulted to **sha1**.

- **md5**: HMAC algorithm hmac-md5.
- **md5-96**: HMAC algorithm hmac-md5-96.
- **sha1**: HMAC algorithm hmac-sha1.
- **sha1-96**: HMAC algorithm hmac-sha1-96.

**prefer-kex**: Preferred key exchange algorithm, defaulted to **dh-group-exchange**.

- **dh-group-exchange**: Key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1**: Key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14**: Key exchange algorithm diffie-hellman-group14-sha1.

**prefer-stoc-cipher**: Preferred encryption algorithm from server to client, defaulted to **aes128**.

**prefer-stoc-hmac**: Preferred HMAC algorithm from server to client, defaulted to **sha1**.

## Description

Use the **ssh2** command to establish a connection to an IPv4 SSH server and specify the public key algorithm, the preferred key exchange algorithm, and the preferred encryption algorithms and preferred HMAC algorithms between the client and server.

Note that when the client's authentication method is publickey, the client needs to get the local private key for validation. As the publickey authentication includes RSA and DSA algorithms, you must specify an algorithm (by using the **identity-key** keyword) in order to get the correct data for the local private key. By default, the encryption algorithm is DSA.

## Examples

# Log in to remote SSH2.0 server 10.214.50.51, using the following algorithms:

- Preferred key exchange algorithm: DH-group1
- Preferred encryption algorithm from server to client: AES128
- Preferred HMAC algorithm from client to server: MD5
- Preferred HMAC algorithm from server to client: SHA1-96.

```
<Sysname> ssh2 10.214.50.51 prefer-kex dh-group1 prefer-stoc-cipher aes128 prefer-ctos-hmac  
md5 prefer-stoc-hmac sha1-96
```

## ssh2 ipv6

### Syntax

```
ssh2 ipv6 server [ port-number ] [ identity-key { dsa | rsa } | prefer-ctos-cipher { aes128 | des } |  
prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 } | prefer-kex { dh-group-exchange | dh-group1  
| dh-group14 } | prefer-stoc-cipher { aes128 | des } | prefer-stoc-hmac { md5 | md5-96 | sha1 |  
sha1-96 } ] *
```

### View

User view

### Default Level

0: Visit level

### Parameters

*server*: IPv6 address or host name of the server, a case-insensitive string of 1 to 46 characters.

*port-number*: Port number of the server, in the range 0 to 65535. The default is 22.

**identity-key**: Specifies the algorithm for publickey authentication, either **dsa** or **rsa**. The default is **dsa**.

**prefer-ctos-cipher**: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **aes128**: Encryption algorithm aes128-cbc.
- **des**: Encryption algorithm des-cbc.

**prefer-ctos-hmac**: Preferred HMAC algorithm from client to server, defaulted to **sha1**.

- **md5**: HMAC algorithm hmac-md5.
- **md5-96**: HMAC algorithm hmac-md5-96.
- **sha1**: HMAC algorithm hmac-sha1.
- **sha1-96**: HMAC algorithm hmac-sha1-96.

**prefer-kex**: Preferred key exchange algorithm, default to **dh-group-exchange**.

- **dh-group-exchange**: Key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1**: Key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14**: Key exchange algorithm diffie-hellman-group14-sha1

**prefer-stoc-cipher**: Preferred encryption algorithm from server to client, defaulted to **aes128**.

**prefer-stoc-hmac**: Preferred HMAC algorithm from server to client, defaulted to **sha1**.

### Description

Use the **ssh2 ipv6** command to establish a connection to an IPv6 SSH server and specify public key algorithm, the preferred key exchange algorithm, and the preferred encryption algorithms and preferred HMAC algorithms between the client and server.

Note that when the client's authentication method is publickey, the client needs to get the local private key for validation. As the publickey authentication includes RSA and DSA algorithms, you must specify an algorithm (by using the **identity-key** keyword) in order to get the correct data for the local private key. By default, the encryption algorithm is DSA.

### Examples

```
# Login to remote SSH2.0 server 2000::1, setting the algorithms as follows:
```

- Preferred key exchange algorithm: DH-group1

- Preferred encryption algorithm from server to client: AES128
- Preferred HMAC algorithm from client to server: MD5
- Preferred HMAC algorithm from server to client: SHA1-96.

```
<Sysname> ssh2 ipv6 2000::1 prefer-kex dh-group1 prefer-stoc-cipher aes128 prefer-ctos-hmac
md5 prefer-stoc-hmac sha1-96
```

## SFTP Server Configuration Commands

### sftp server enable

#### Syntax

```
sftp server enable
undo sftp server enable
```

#### View

System view

#### Default Level

2: System level

#### Parameters

None

#### Description

Use the **sftp server enable** command to enable SFTP server.

Use the **undo sftp server enable** command to disable SFTP server.

By default, SFTP server is disabled.

Related commands: **display ssh server**.

#### Examples

```
# Enable SFTP server.
```

```
<Sysname> system-view
[Sysname] sftp server enable
```

### sftp server idle-timeout

#### Syntax

```
sftp server idle-timeout time-out-value
undo sftp server idle-timeout
```

#### View

System view

#### Default Level

2: System level

## Parameters

*time-out-value*: Timeout period in minutes. It ranges from 1 to 35,791.

## Description

Use the **sftp server idle-timeout** command to set the idle timeout period for SFTP user connections.

Use the **undo sftp server idle-timeout** command to restore the default.

By default, the idle timeout period is 10 minutes.

Related commands: **display ssh server**.

## Examples

# Set the idle timeout period for SFTP user connections to 500 minutes.

```
<Sysname> system-view  
[Sysname] sftp server idle-timeout 500
```

# SFTP Client Configuration Commands

## bye

### Syntax

**bye**

### View

SFTP client view

### Default Level

3: Manage level

### Parameters

None

### Description

Use the **bye** command to terminate the connection with a remote SFTP server and return to user view.

This command functions as the **exit** and **quit** commands.

### Examples

# Terminate the connection with the remote SFTP server.

```
sftp-client> bye  
Bye  
<Sysname>
```

## cd

### Syntax

**cd** [ *remote-path* ]

## View

SFTP client view

## Default Level

3: Manage level

## Parameters

*remote-path*: Name of a path on the server.

## Description

Use the **cd** command to change the working path on a remote SFTP server. With the argument not specified, the command displays the current working path.



### Note

- You can use the **cd ..** command to return to the upper-level directory.
  - You can use the **cd /** command to return to the root directory of the system.
- 

## Examples

```
# Change the working path to new1.
```

```
sftp-client> cd new1  
Current Directory is:  
/new1
```

## cdup

### Syntax

**cdup**

### View

SFTP client view

### Default Level

3: Manage level

### Parameters

None

### Description

Use the **cdup** command to return to the upper-level directory.

### Examples

```
# From the current working directory /new1, return to the upper-level directory.
```

```
sftp-client> cdup
```

Current Directory is:

/

## delete

### Syntax

**delete** *remote-file*&<1-10>

### View

SFTP client view

### Default Level

3: Manage level

### Parameters

*remote-file*&<1-10>: Name of a file on the server. &<1-10> means that you can provide up to 10 filenames, which are separated by space.

### Description

Use the **delete** command to delete the specified file(s) from a server.

This command functions as the **remove** command.

### Examples

# Delete file temp.c from the server.

```
sftp-client> delete temp.c
```

The following files will be deleted:

```
/temp.c
```

Are you sure to delete it? [Y/N]:y

This operation may take a long time. Please wait...

```
File successfully Removed
```

## dir

### Syntax

**dir** [ **-a** | **-l** ] [ *remote-path* ]

### View

SFTP client view

### Default Level

3: Manage level

### Parameters

**-a**: Displays the filenames or the folder names of the specified directory.

**-l**: Displays in a list form detailed information of the files and folders of the specified directory.

*remote-path*: Name of the directory to be queried.

## Description

Use the **dir** command to display file and folder information under a specified directory.

With the **-a** and **-l** keyword not specified, the command displays detailed information of files and folders under the specified directory in a list form.

With the *remote-path* not specified, the command displays the file and folder information of the current working directory.

This command functions as the **ls** command.

## Examples

# Display in a list form detailed file and folder information under the current working directory.

```
sftp-client> dir
-rwxrwxrwx  1 noone  nogroup  1759 Aug 23 06:52 config.cfg
-rwxrwxrwx  1 noone  nogroup   225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone  nogroup   283 Aug 24 07:39 pubkey1
-rwxrwxrwx  1 noone  nogroup   225 Sep 28 08:28 publ
drwxrwxrwx  1 noone  nogroup    0 Sep 28 08:24 new1
drwxrwxrwx  1 noone  nogroup    0 Sep 28 08:18 new2
-rwxrwxrwx  1 noone  nogroup   225 Sep 28 08:30 pub2
```

## display sftp client source

### Syntax

**display sftp client source**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display sftp client source** command to display the source IP address or source interface currently set for the SFTP client.

If neither source IP address nor source interface is specified for the SFTP client, the system will prompt you to specify the source information.

Related commands: **sftp client source**.

## Examples

# Display the source IP address of the SFTP client.

```
<Sysname> display sftp client source
The source IP address you specified is 192.168.0.1
```

## exit

### Syntax

**exit**

### View

SFTP client view

### Default Level

3: Manage level

### Parameters

None

### Description

Use the **exit** command to terminate the connection with a remote SFTP server and return to user view. This command functions as the **bye** and **quit** commands.

### Examples

```
# Terminate the connection with the remote SFTP server.
sftp-client> exit
Bye
<Sysname>
```

## get

### Syntax

**get** *remote-file* [ *local-file* ]

### View

SFTP client view

### Default Level

3: Manage level

### Parameters

*remote-file*: Name of a file on the remote SFTP server.

*local-file*: Name for the local file.

### Description

Use the **get** command to download a file from a remote SFTP server and save it locally. If you do not specify the *local-file* argument, the file will be saved locally with the same name as that on the remote SFTP server.

### Examples

```
# Download file temp1.c and save it as temp.c locally.
```

```
sftp-client> get templ.c temp.c
Remote file:/templ.c ---> Local file: temp.c
Downloading file successfully ended
```

## help

### Syntax

```
help [ all | command-name ]
```

### View

SFTP client view

### Default Level

3: Manage level

### Parameters

**all**: Displays a list of all commands.

*command-name*: Name of a command.

### Description

Use the **help** command to display a list of all commands or the help information of an SFTP client command.

With neither the argument nor the keyword specified, the command displays a list of all commands.

### Examples

# Display the help information of the **get** command.

```
sftp-client> help get
get remote-path [local-path] Download file.Default local-path is the same
as remote-path
```

## ls

### Syntax

```
ls [ -a | -l ] [ remote-path ]
```

### View

SFTP client view

### Default Level

3: Manage level

### Parameters

**-a**: Displays the filenames or the folder names of the specified directory.

**-l**: Displays in a list form detailed information of the files and folders of the specified directory

*remote-path*: Name of the directory to be queried.

## Description

Use the **ls** command to display file and folder information under a specified directory.

With the **-a** and **-l** keyword not specified, the command displays detailed information of files and folders under the specified directory in a list form.

With the *remote-path* not specified, the command displays the file and folder information of the current working directory.

This command functions as the **dir** command.

## Examples

# Display in a list form detailed file and folder information under the current working directory.

```
sftp-client> ls
-rwxrwxrwx  1 noone  nogroup  1759 Aug 23 06:52 config.cfg
-rwxrwxrwx  1 noone  nogroup   225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone  nogroup   283 Aug 24 07:39 pubkey1
-rwxrwxrwx  1 noone  nogroup   225 Sep 28 08:28 publ
drwxrwxrwx  1 noone  nogroup    0 Sep 28 08:24 new1
drwxrwxrwx  1 noone  nogroup    0 Sep 28 08:18 new2
-rwxrwxrwx  1 noone  nogroup   225 Sep 28 08:30 pub2
```

## mkdir

### Syntax

```
mkdir remote-path
```

### View

SFTP client view

### Default Level

3: Manage level

### Parameters

*remote-path*: Name for the directory on a remote SFTP server.

## Description

Use the **mkdir** command to create a directory on a remote SFTP server.

## Examples

# Create a directory named **test** on the remote SFTP server.

```
sftp-client> mkdir test
New directory created
```

## put

### Syntax

```
put local-file [ remote-file ]
```

## View

SFTP client view

## Default Level

3: Manage level

## Parameters

*local-file*: Name of a local file.

*remote-file*: Name for the file on a remote SFTP server.

## Description

Use the **put** command to upload a local file to a remote SFTP server.

If you do not specify the *remote-file* argument, the file will be saved remotely with the same name as the local one.

## Examples

```
# Upload local file temp.c to the remote SFTP server and save it as temp1.c.
```

```
sftp-client> put temp.c templ.c
Local file:temp.c ---> Remote file: /templ.c
Uploading file successfully ended
```

## pwd

### Syntax

```
pwd
```

## View

SFTP client view

## Default Level

3: Manage level

## Parameters

None

## Description

Use the **pwd** command to display the current working directory of a remote SFTP server.

## Examples

```
# Display the current working directory of the remote SFTP server.
```

```
sftp-client> pwd
/
```

## quit

### Syntax

quit

### View

SFTP client view

### Default Level

3: Manage level

### Parameters

None

### Description

Use the **quit** command to terminate the connection with a remote SFTP server and return to user view.

This command functions as the **bye** and **exit** commands.

### Examples

# Terminate the connection with the remote SFTP server.

```
sftp-client> quit  
Bye  
<Sysname>
```

## remove

### Syntax

**remove** *remote-file*&<1-10>

### View

SFTP client view

### Default Level

3: Manage level

### Parameters

*remote-file*&<1-10>: Name of a file on an SFTP server. &<1-10> means that you can provide up to 10 filenames, which are separated by space.

### Description

Use the **remove** command to delete the specified file(s) from a remote server.

This command functions as the **delete** command.

### Examples

# Delete file temp.c from the server.

```
sftp-client> remove temp.c  
The following files will be deleted:
```

```
/temp.c
Are you sure to delete it? [Y/N]:y
This operation may take a long time.Please wait...

File successfully Removed
```

## rename

### Syntax

```
rename oldname newname
```

### View

SFTP client view

### Default Level

3: Manage level

### Parameters

*oldname*: Original file name or directory name.

*newname*: New file name or directory name.

### Description

Use the **rename** command to change the name of a specified file or directory on an SFTP server.

### Examples

```
# Change the name of a file on the SFTP server from temp1.c to temp2.c.
sftp-client> rename temp1.c temp2.c
File successfully renamed
```

## rmdir

### Syntax

```
rmdir remote-path&<1-10>
```

### View

SFTP client view

### Default Level

3: Manage level

### Parameters

*remote-path*&<1-10>: Name of the directory on the remote SFTP server. &<1-10> means that you can provide up to 10 directory names that are separated by space.

### Description

Use the **rmdir** command to delete the specified directories from an SFTP server.

## Examples

```
# On the SFTP server, delete directory temp1 in the current directory.  
sftp-client> rmdir temp1  
Directory successfully removed
```

## sftp

### Syntax

```
sftp server [ port-number ] [ identity-key { dsa | rsa } | prefer-ctos-cipher { aes128 | des } |  
prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 } | prefer-kex { dh-group-exchange | dh-group1  
| dh-group14 } | prefer-stoc-cipher { aes128 | des } | prefer-stoc-hmac { md5 | md5-96 | sha1 |  
sha1-96 } ] *
```

### View

User view

### Default Level

3: Manage level

### Parameters

**server**: IPv4 address or host name of the server, a case-insensitive string of 1 to 20 characters.

**port-number**: Port number of the server, in the range 0 to 65535. The default is 22.

**identity-key**: Specifies the algorithm for publickey authentication, either **dsa** or **rsa**. The default is **dsa**.

**prefer-ctos-cipher**: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **aes128**: Encryption algorithm aes128-cbc.
- **des**: Encryption algorithm des-cbc.

**prefer-ctos-hmac**: Preferred HMAC algorithm from client to server, defaulted to **sha1**.

- **md5**: HMAC algorithm hmac-md5.
- **md5-96**: HMAC algorithm hmac-md5-96.
- **sha1**: HMAC algorithm hmac-sha1.
- **sha1-96**: HMAC algorithm hmac-sha1-96.

**prefer-kex**: Preferred key exchange algorithm, defaulted to **dh-group-exchange**.

- **dh-group-exchange**: Key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1**: Key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14**: Key exchange algorithm diffie-hellman-group14-sha1.

**prefer-stoc-cipher**: Preferred encryption algorithm from server to client, defaulted to **aes128**.

**prefer-stoc-hmac**: Preferred HMAC algorithm from server to client, defaulted to **sha1**.

### Description

Use the **sftp** command to establish a connection to a remote IPv4 SFTP server and enter SFTP client view.

Note that when the client's authentication method is publickey, the client needs to get the local private key for validation. As the publickey authentication includes RSA and DSA algorithms, you must specify

an algorithm (by using the **identity-key** keyword) in order to get the correct data for the local private key. By default, the encryption algorithm is DSA.

## Examples

# Connect to SFTP server 10.1.1.2, using the following algorithms:

- Preferred key exchange algorithm: **dh-group1**.
- Preferred encryption algorithm from server to client: **aes128**.
- Preferred HMAC algorithm from client to server: **md5**.
- Preferred HMAC algorithm from server to client: **sha1-96**.

```
<Sysname> sftp 10.1.1.2 prefer-kex dh-group1 prefer-stoc-cipher aes128 prefer-ctos-hmac md5
prefer-stoc-hmac sha1-96
Input Username:
```

## sftp client ipv6 source

### Syntax

```
sftp client ipv6 source { ipv6 ipv6-address | interface interface-type interface-number }
undo sftp client ipv6 source
```

### View

System view

### Default Level

3: Manage level

### Parameters

**ipv6** *ipv6-address*: Specifies a source IPv6 address.

**interface** *interface-type interface-number*: Specifies a source interface by its type and number.

### Description

Use the **sftp client ipv6 source** command to specify the source IPv6 address or source interface for an SFTP client.

Use the **undo sftp client ipv6 source** command to remove the configuration.

By default, the client uses the interface address specified by the route of the device to access the SFTP server.

Related commands: **display sftp client source**.

## Examples

# Specify the source IPv6 address of the SFTP client as 2:2::2:2.

```
<Sysname> system-view
[Sysname] sftp client ipv6 source ipv6 2:2::2:2
```

## sftp client source

### Syntax

```
sftp client source { ip ip-address | interface interface-type interface-number }
```

## undo sftp client source

### View

System view

### Default Level

3: Manage level

### Parameters

**ip** *ip-address*: Specifies a source IPv4 address.

**interface** *interface-type interface-number*: Specifies a source interface by its type and number.

### Description

Use the **sftp client source** command to specify the source IPv4 address or interface of an SFTP client.

Use the **undo sftp source-interface** command to remove the configuration.

By default, a client uses the IP address of the interface specified by the route to access the SFTP server.

Related commands: **display sftp client source**.

### Examples

```
# Specify the source IP address of the SFTP client as 192.168.0.1.
```

```
<Sysname> system-view  
[Sysname] sftp client source ip 192.168.0.1
```

## sftp ipv6

### Syntax

```
sftp ipv6 server [ port-number ] [ identity-key { dsa | rsa } | prefer-ctos-cipher { aes128 | des } |  
prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 } | prefer-kex { dh-group-exchange | dh-group1  
| dh-group14 } | prefer-stoc-cipher { aes128 | des } | prefer-stoc-hmac { md5 | md5-96 | sha1 |  
sha1-96 } ] *
```

### View

User view

### Default Level

3: Manage level

### Parameters

*server*: IPv6 address or host name of the server, a case-insensitive string of 1 to 46 characters.

*port-number*: Port number of the server, in the range 0 to 65535. The default is 22.

**identity-key**: Specifies the algorithm for publickey authentication, either **dsa** or **rsa**. The default is **dsa**.

**prefer-ctos-cipher**: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **aes128**: Encryption algorithm aes128-cbc.
- **des**: Encryption algorithm des-cbc.

**prefer-ctos-hmac:** Preferred HMAC algorithm from client to server, defaulted to **sha1**.

- **md5:** HMAC algorithm hmac-md5.
- **md5-96:** HMAC algorithm hmac-md5-96.
- **sha1:** HMAC algorithm hmac-sha1.
- **sha1-96:** HMAC algorithm hmac-sha1-96.

**prefer-kex:** Preferred key exchange algorithm, defaulted to **dh-group-exchange**.

- **dh-group-exchange:** Key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1:** Key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14:** Key exchange algorithm diffie-hellman-group14-sha1.

**prefer-stoc-cipher:** Preferred encryption algorithm from server to client, defaulted to **aes128**.

**prefer-stoc-hmac:** Preferred HMAC algorithm from server to client, defaulted to **sha1**.

## Description

Use the **sftp ipv6** command to establish a connection to a remote IPv6 SFTP server and enter SFTP client view.

Note that when the client's authentication method is publickey, the client needs to get the local private key for validation. As the publickey authentication includes RSA and DSA algorithms, you must specify an algorithm (by using the **identity-key** keyword) in order to get the correct data for the local private key. By default, the encryption algorithm is DSA.

## Examples

# Connect to server 2:5::8:9, using the following algorithms:

- Preferred key exchange algorithm: **dh-group1**.
- Preferred encryption algorithm from server to client: **aes128**.
- Preferred HMAC algorithm from client to server: **md5**.
- Preferred HMAC algorithm from server to client: **sha1-96**.

```
<Sysname> sftp ipv6 2:5::8:9 prefer-kex dh-group1 prefer-stoc-cipher aes128 prefer-ctos-hmac
md5 prefer-stoc-hmac sha1-96
Input Username:
```

# Table of Contents

<b>1 PKI Configuration Commands</b> .....	<b>1-1</b>
PKI Configuration Commands .....	1-1
attribute .....	1-1
ca identifier .....	1-2
certificate request entity .....	1-3
certificate request from .....	1-3
certificate request mode .....	1-4
certificate request polling .....	1-5
certificate request url .....	1-5
common-name .....	1-6
country .....	1-7
crl check .....	1-7
crl update-period .....	1-8
crl url .....	1-8
display pki certificate .....	1-9
display pki certificate access-control-policy .....	1-11
display pki certificate attribute-group .....	1-11
display pki crl domain .....	1-12
fqdn .....	1-14
ip (PKI entity view) .....	1-14
ldap-server .....	1-15
locality .....	1-16
organization .....	1-16
organization-unit .....	1-17
pki certificate access-control-policy .....	1-17
pki certificate attribute-group .....	1-18
pki delete-certificate .....	1-19
pki domain .....	1-19
pki entity .....	1-20
pki import-certificate .....	1-21
pki request-certificate domain .....	1-21
pki retrieval-certificate .....	1-22
pki retrieval-crl domain .....	1-23
pki validate-certificate .....	1-23
root-certificate fingerprint .....	1-24
rule (access control policy view) .....	1-25
state .....	1-25

# 1 PKI Configuration Commands

---

## PKI Configuration Commands

### attribute

#### Syntax

```
attribute id { alt-subject-name { fqdn | ip } | { issuer-name | subject-name } { dn | fqdn | ip } } { ctn | equ | nctn | nequ } attribute-value  
undo attribute { id | all }
```

#### View

Certificate attribute group view

#### Default Level

2: System level

#### Parameters

*id*: Sequence number of the certificate attribute rule, in the range 1 to 16.

**alt-subject-name**: Specifies the name of the alternative certificate subject.

**fqdn**: Specifies the FQDN of the entity.

**ip**: Specifies the IP address of the entity.

**issuer-name**: Specifies the name of the certificate issuer.

**subject-name**: Specifies the name of the certificate subject.

**dn**: Specifies the distinguished name of the entity.

**ctn**: Specifies the contain operation.

**equ**: Specifies the equal operation.

**nctn**: Specifies the not-contain operation.

**nequ**: Specifies the not-equal operation.

*attribute-value*: Value of the certificate attribute, a case-insensitive string of 1 to 128 characters.

**all**: Specifies all certificate attributes.

#### Description

Use the **attribute** command to configure the attribute rules of the certificate issuer name, certificate subject name and alternative certificate subject name.

Use the **undo attribute** command to delete the attribute rules of one or all certificates.

By default, there is no restriction on the issuer name, subject name, and alternative subject name of a certificate.

Note that the attribute of the alternative certificate subject name does not appear as a distinguished name, and therefore the **dn** keyword is not available for the attribute.

## Examples

# Create a certificate attribute rule, specifying that the DN in the subject name includes the string of abc.

```
<Sysname> system-view
[Sysname] pki certificate attribute-group mygroup
[Sysname-pki-cert-attribute-group-mygroup] attribute 1 subject-name dn ctn abc
```

# Create a certificate attribute rule, specifying that the FQDN in the issuer name cannot be the string of abc.

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 2 issuer-name fqdn nequ abc
```

# Create a certificate attribute rule, specifying that the IP address in the alternative subject name cannot be 10.0.0.1.

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 3 alt-subject-name ip nequ 10.0.0.1
```

## ca identifier

### Syntax

**ca identifier** *name*

**undo ca identifier**

### View

PKI domain view

### Default Level

2: System level

### Parameters

*name*: Identifier of the trusted CA, a case-insensitive string of 1 to 63 characters.

### Description

Use the **ca identifier** command to specify the trusted CA and bind the device with the CA.

Use the **undo ca identifier** command to remove the configuration.

By default, no trusted CA is specified for a PKI domain.

Certificate request, retrieval, revocation, and query all depend on the trusted CA.

## Examples

# Specify the trusted CA as **new-ca**.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] ca identifier new-ca
```

## certificate request entity

### Syntax

```
certificate request entity entity-name  
undo certificate request entity
```

### View

PKI domain view

### Default Level

2: System level

### Parameters

*entity-name*: Name of the entity for certificate request, a case-insensitive string of 1 to 15 characters.

### Description

Use the **certificate request entity** command to specify the entity for certificate request.

Use the **undo certificate request entity** command to remove the configuration.

By default, no entity is specified for a PKI domain.

Related commands: **pki entity**.

### Examples

```
# Specify the entity for certificate request as entity1.
```

```
<Sysname> system-view  
[Sysname] pki domain 1  
[Sysname-pki-domain-1] certificate request entity entity1
```

## certificate request from

### Syntax

```
certificate request from { ca | ra }  
undo certificate request from
```

### View

PKI domain view

### Default Level

2: System level

### Parameters

**ca**: Indicates that the entity requests a certificate from a CA.

**ra**: Indicates that the entity requests a certificate from an RA.

### Description

Use the **certificate request from** command to specify the authority for certificate request.

Use the **undo certificate request from** command to remove the configuration.

By default, no authority is specified for a PKI domain view.

## Examples

```
# Specify that the entity requests a certificate from the CA.
```

```
<Sysname> system-view
```

```
[Sysname] pki domain 1
```

```
[Sysname-pki-domain-1] certificate request from ca
```

## certificate request mode

### Syntax

```
certificate request mode { auto [ key-length key-length | password { cipher | simple } password ]* | manual }
```

```
undo certificate request mode
```

### View

PKI domain view

### Default Level

2: System level

### Parameters

**auto**: Specifies to request a certificate in auto mode.

*key-length*: Length of the RSA keys, in the range 512 to 2,048 bits. It is 1,024 bits by default.

*password*: Password for certificate revocation, a case-sensitive string of 1 to 31 characters.

**cipher**: Specifies to display the password in cipher text.

**simple**: Specifies to display the password in clear text.

**manual**: Specifies to request a certificate in manual mode.

### Description

Use the **certificate request mode** command to set the certificate request mode.

Use the **undo certificate request mode** command to restore the default.

By default, manual mode is used.

In auto mode, an entity automatically requests a certificate from an RA or CA when it has no certificate or when the existing certificate is about to expire. In manual mode, all operations associated with certificate request are carried out manually.

Related commands: **pki request-certificate**.

## Examples

```
# Specify to request a certificate in auto mode.
```

```
<Sysname> system-view
```

```
[Sysname] pki domain 1
```

```
[Sysname-pki-domain-1] certificate request mode auto
```

## certificate request polling

### Syntax

```
certificate request polling { count count | interval minutes }  
undo certificate request polling { count | interval }
```

### View

PKI domain view

### Default Level

2: System level

### Parameters

*count*: Maximum number of attempts to poll the status of the certificate request, in the range 1 to 100.  
*minutes*: Polling interval, in the range 5 to 168 minutes.

### Description

Use the **certificate request polling** command to specify the certificate request polling interval and attempt limit.

Use the **undo certificate request polling** command to restore the defaults.

By default, the polling is executed every 20 minutes for up to 50 times.

After an applicant makes a certificate request, the CA may need a long period of time if it verifies the certificate request manually. During this period, the applicant needs to query the status of the request periodically to get the certificate as soon as possible after the certificate is signed.

Related commands: **display pki certificate**.

### Examples

```
# Specify the polling interval as 15 minutes and the maximum number of attempts as 40.
```

```
<Sysname> system-view  
[Sysname] pki domain 1  
[Sysname-pki-domain-1] certificate request polling interval 15  
[Sysname-pki-domain-1] certificate request polling count 40
```

## certificate request url

### Syntax

```
certificate request url url-string  
undo certificate request url
```

### View

PKI domain view

### Default Level

2: System level

## Parameters

*url-string*: URL of the server for certificate request, a case-insensitive string of 1 to 127 characters. It comprises the location of the server and the location of CGI command interface script in the format of *http://server\_location/ca\_script\_location*, where *server\_location* must be an IP address and does not support domain name resolution currently.

## Description

Use the **certificate request url** command to specify the URL of the server for certificate request through SCEP.

Use the **undo certificate request url** command to remove the configuration.

By default, no URL is specified for a PKI domain.

## Examples

# Specify the URL of the server for certificate request.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request url
http://169.254.0.100/certsrv/mscep/mscep.dll
```

## common-name

### Syntax

**common-name** *name*

**undo common-name**

### View

PKI entity view

### Default Level

2: System level

## Parameters

*name*: Common name of an entity, a case-insensitive string of 1 to 31 characters. No comma can be included.

## Description

Use the **common-name** command to configure the common name of an entity, which can be, for example, the user name.

Use the **undo common-name** command to remove the configuration.

By default, no common name is specified.

## Examples

# Configure the common name of an entity as **test**.

```
<Sysname> system-view
[Sysname] pki entity 1
```

```
[Sysname-pki-entity-1] common-name test
```

## country

### Syntax

```
country country-code-str  
undo country
```

### View

PKI entity view

### Default Level

2: System level

### Parameters

*country-code-str*: Country code for the entity, a 2-character case-insensitive string.

### Description

Use the **country** command to specify the code of the country to which an entity belongs. It is a standard 2-character code, for example, CN for China.

Use the **undo country** command to remove the configuration.

By default, no country code is specified.

### Examples

# Set the country code of an entity to **CN**.

```
<Sysname> system-view  
[Sysname] pki entity 1  
[Sysname-pki-entity-1] country CN
```

## crl check

### Syntax

```
crl check { disable | enable }
```

### View

PKI domain view

### Default Level

2: System level

### Parameters

**disable**: Disables CRL checking.

**enable**: Enables CRL checking.

### Description

Use the **crl check** command to enable or disable CRL checking.

By default, CRL checking is enabled.

CRLs are files issued by the CA to publish all certificates that have been revoked. Revocation of a certificate may occur before the certificate expires. CRL checking is intended for checking whether a certificate has been revoked. A revoked certificate is no longer trusted.

## Examples

```
# Disable CRL checking.  
<Sysname> system-view  
[Sysname] pki domain 1  
[Sysname-pki-domain-1] crl check disable
```

## crl update-period

### Syntax

```
crl update-period hours  
undo crl update-period
```

### View

PKI domain view

### Default Level

2: System level

### Parameters

*hours*: CRL update period, in the range 1 to 720 hours.

### Description

Use the **crl update-period** command to set the CRL update period, that is, the interval at which the PKI entity downloads the latest CRLs.

Use the **undo crl update-period** command to restore the default.

By default, the CRL update period depends on the next update field in the CRL file.

The CRL update period is the interval at which a PKI entity with a certificate downloads a CRL from LDAP server.

## Examples

```
# Set the CRL update period to 20 hours.  
<Sysname> system-view  
[Sysname] pki domain 1  
[Sysname-pki-domain-1] crl update-period 20
```

## crl url

### Syntax

```
crl url url-string  
undo crl url
```

## View

PKI domain view

## Default Level

2: System level

## Parameters

*url-string*: URL of the CRL distribution point, a case-insensitive string of 1 to 127 characters in the format of *ldap://server\_location* or *http://server\_location*, where *server\_location* must be an IP address and does not support domain name resolution currently.

## Description

Use the **cr1 url** command to specify the URL of the CRL distribution point.

Use the **undo cr1 url** command to remove the configuration.

By default, no CRL distribution point URL is specified.

Note that when the URL of the CRL distribution point is not set, you should acquire the CA certificate and a local certificate, and then acquire a CRL through SCEP.

## Examples

```
# Specify the URL of the CRL distribution point.  
<Sysname> system-view  
[Sysname] pki domain 1  
[Sysname-pki-domain-1] cr1 url ldap://169.254.0.30
```

## display pki certificate

### Syntax

```
display pki certificate { { ca | local } domain domain-name | request-status }
```

### View

Any view

### Default Level

2: System level

### Parameters

**ca**: Displays the CA certificate.

**local**: Displays the local certificate.

*domain-name*: Name of the PKI domain, a string of 1 to 15 characters.

**request-status**: Displays the status of a certificate request.

### Description

Use the **display pki certificate** command to display the contents or request status of a certificate.

Related commands: **pki retrieval-certificate**, **pki domain** and **certificate request polling**.

## Examples

# Display the local certificate.

```
<Sysname> display pki certificate local domain 1
```

Certificate:

```
Data:
  Version: 3 (0x2)
  Serial Number:
    10B7D4E3 00010000 0086
  Signature Algorithm: md5WithRSAEncryption
  Issuer:
    emailAddress=myca@aabbcc.net
    C=CN
    ST=Country A
    L=City X
    O=abc
    OU=bjs
    CN=new-ca
  Validity
    Not Before: Jan 13 08:57:21 2004 GMT
    Not After : Jan 20 09:07:21 2005 GMT
  Subject:
    C=CN
    ST=Country B
    L=City Y
    CN=pki test
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (512 bit)
      Modulus (512 bit):
        00D41D1F ...
      Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Subject Alternative Name:
      DNS: hyf.xxyyzz.net
    X509v3 CRL Distribution Points:
      URI:http://1.1.1.1:447/myca.crl
      ...
  Signature Algorithm: md5WithRSAEncryption
    A3A5A447 4D08387D ...
```

**Table 1-1 display pki certificate** command output description

Field	Description
Version	Version of the certificate
Serial Number	Serial number of the certificate
Signature Algorithm	Signature algorithm
Issuer	Issuer of the certificate

Field	Description
Validity	Validity period of the certificate
Subject	Entity holding the certificate
Subject Public Key Info	Public key information of the entity
X509v3 extensions	Extensions of the X.509 (version 3) certificate
X509v3 CRL Distribution Points	Distribution points of X.509 (version 3) CRLs

## display pki certificate access-control-policy

### Syntax

```
display pki certificate access-control-policy { policy-name | all }
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*policy-name*: Name of the certificate attribute-based access control policy, a string of 1 to 16 characters.

**all**: Specifies all certificate attribute-based access control policies.

### Description

Use the **display pki certificate access-control-policy** command to display information about a specified or all certificate attribute-based access control policies.

### Examples

# Display information about the certificate attribute-based access control policy named mypolicy.

```
<Sysname> display pki certificate access-control-policy mypolicy
access-control-policy name: mypolicy
rule 1 deny mygroup1
rule 2 permit mygroup2
```

**Table 1-2** display pki certificate access-control-policy command output description

Field	Description
access-control-policy	Name of the certificate attribute-based access control policy
rule number	Number of the access control rule

## display pki certificate attribute-group

### Syntax

```
display pki certificate attribute-group { group-name | all }
```

## View

Any view

## Default Level

1: Monitor level

## Parameters

*group-name*: Name of a certificate attribute group, a string of 1 to 16 characters.

**all**: Specifies all certificate attribute groups.

## Description

Use the **display pki certificate attribute-group** command to display information about a specified or all certificate attribute groups.

## Examples

# Display information about certificate attribute group mygroup.

```
<Sysname> display pki certificate attribute-group mygroup
attribute group name: mygroup
  attribute 1 subject-name      dn      ctn      abc
  attribute 2 issuer-name      fqdn    nctn    app
```

**Table 1-3** display pki certificate attribute-group command output description

Field	Description
attribute group name	Name of the certificate attribute group
attribute <i>number</i>	Number of the attribute rule
subject-name	Name of the certificate subject
dn	DN of the entity
ctn	Indicates the contain operations
abc	Value of attribute 1
issuer-name	Name of the certificate issuer
fqdn	FQDN of the entity
nctn	Indicates the not-contain operations
app	Value of attribute 2

## display pki crl domain

### Syntax

```
display pki crl domain domain-name
```

### View

Any view

## Default Level

2: System level

## Parameters

*domain-name*: Name of the PKI domain, a string of 1 to 15 characters.

## Description

Use the **display pki crl domain** command to display the locally saved CRLs.

Related commands: **pki retrieval-crl**, **pki domain**.

## Examples

# Display the locally saved CRLs.

```
<Sysname> display pki crl domain 1
Certificate Revocation List (CRL):
  Version 2 (0x1)
  Signature Algorithm: sha1WithRSAEncryption
  Issuer:
    C=CN
    O=abc
    OU=soft
    CN=A Test Root
  Last Update: Jan  5 08:44:19 2004 GMT
  Next Update: Jan  5 21:42:13 2004 GMT
  CRL extensions:
    X509v3 Authority Key Identifier:
      keyid:0F71448E E075CAB8 ADDB3A12 0B747387 45D612EC
    Revoked Certificates:
      Serial Number: 05a234448E...
      Revocation Date: Sep  6 12:33:22 2004 GMT
      CRL entry extensions:...
      Serial Number: 05a278445E...
      Revocation Date: Sep  7 12:33:22 2004 GMT
      CRL entry extensions:...
```

**Table 1-4 display pki crl domain** command output description

Field	Description
Version	Version of the CRLs
Signature Algorithm	Signature algorithm used by the CRLs
Issuer	CA issuing the CRLs
Last Update	Last update time
Next Update	Next update time
CRL extensions	Extensions of CRL
X509v3 Authority Key Identifier	CA issuing the CRLs. The certificate version is X.509v3.

Field	Description
keyid	ID of the public key A CA may have multiple key pairs. This field indicates the key pair used by the CRL's signature.
Revoked Certificates	Revoked certificates
Serial Number	Serial number of the revoked certificate
Revocation Date	Revocation date of the certificate

## fqdn

### Syntax

**fqdn** *name-str*

**undo fqdn**

### View

PKI entity view

### Default Level

2: System level

### Parameters

*name-str*: Fully qualified domain name (FQDN) of an entity, a case-insensitive string of 1 to 127 characters.

### Description

Use the **fqdn** command to configure the FQDN of an entity.

Use the **undo fqdn** command to remove the configuration.

By default, no FQDN is specified for an entity.

An FQDN is the unique identifier of an entity on a network. It consists of a host name and a domain name and can be resolved into an IP address.

### Examples

# Configure the FQDN of an entity as **pki.domain-name.com**.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] fqdn pki.domain-name.com
```

## ip (PKI entity view)

### Syntax

**ip** *ip-address*

**undo ip**

## View

PKI entity view

## Default Level

2: System level

## Parameters

*ip-address*: IP address for an entity.

## Description

Use the **ip** command to configure the IP address of an entity.

Use the **undo ip** command to remove the configuration.

By default, no IP address is specified for an entity.

## Examples

```
# Configure the IP address of an entity as 11.0.0.1.
```

```
<Sysname> system-view  
[Sysname] pki entity 1  
[Sysname-pki-entity-1] ip 11.0.0.1
```

## ldap-server

### Syntax

```
ldap-server ip ip-address [ port port-number ] [ version version-number ]  
undo ldap-server
```

### View

PKI domain view

### Default Level

2: System level

### Parameters

*ip-address*: IP address of the LDAP server, in dotted decimal format.

*port-number*: Port number of the LDAP server, in the range 1 to 65535. The default is 389.

*version-number*: LDAP version number, either 2 or 3. By default, it is 2.

### Description

Use the **ldap-server** command to specify an LDAP server for a PKI domain.

Use the **undo ldap-server** command to remove the configuration.

By default, no LDAP server is specified for a PKI domain.

### Examples

```
# Specify an LDAP server for PKI domain 1.
```

```
<Sysname> system-view
```

```
[Sysname] pki domain 1
[Sysname-pki-domain-1] ldap-server ip 169.254.0.30
```

## locality

### Syntax

**locality** *locality-name*

**undo locality**

### View

PKI entity view

### Default Level

2: System level

### Parameters

*locality-name*: Name for the geographical locality, a case-insensitive string of 1 to 31 characters. No comma can be included.

### Description

Use the **locality** command to configure the geographical locality of an entity, which can be, for example, a city name.

Use the **undo locality** command to remove the configuration.

By default, no geographical locality is specified for an entity.

### Examples

# Configure the locality of an entity as **city**.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] locality city
```

## organization

### Syntax

**organization** *org-name*

**undo organization**

### View

PKI entity view

### Default Level

2: System level

### Parameters

*org-name*: Organization name, a case-insensitive string of 1 to 31 characters. No comma can be included.

## Description

Use the **organization** command to configure the name of the organization to which the entity belongs.

Use the **undo organization** command to remove the configuration.

By default, no organization name is specified for an entity.

## Examples

# Configure the name of the organization to which an entity belongs as **org-name**.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] organization org-name
```

## organization-unit

### Syntax

**organization-unit** *org-unit-name*

**undo organization-unit**

### View

PKI entity view

### Default Level

2: System level

### Parameters

*org-unit-name*: Organization unit name for distinguishing different units in an organization, a case-insensitive string of 1 to 31 characters. No comma can be included.

## Description

Use the **organization-unit** command to specify the name of the organization unit to which this entity belongs.

Use the **undo organization-unit** command to remove the configuration.

By default, no organization unit name is specified for an entity.

## Examples

# Configure the name of the organization unit to which an entity belongs as **unit-name**.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] organization-unit unit-name
```

## pki certificate access-control-policy

### Syntax

**pki certificate access-control-policy** *policy-name*

**undo pki certificate access-control-policy** { *policy-name* | **all** }

## View

System view

## Default Level

2: System level

## Parameters

*policy-name*: Name of the certificate attribute-based access control policy, a case-insensitive string of 1 to 16 characters. It cannot be "a", "al" or "all".

**all**: Specifies all certificate attribute-based access control policies.

## Description

Use the **pki certificate access-control-policy** command to create a certificate attribute-based access control policy and enter its view.

Use the **undo pki certificate access-control-policy** command to remove a specified or all certificate attribute-based access control policies.

No access control policy exists by default.

## Examples

# Configure an access control policy named **mypolicy** and enter its view.

```
<Sysname> system-view
[Sysname] pki certificate access-control-policy mypolicy
[Sysname-pki-cert-acp-mypolicy]
```

## pki certificate attribute-group

### Syntax

```
pki certificate attribute-group group-name
undo pki certificate attribute-group { group-name | all }
```

### View

System view

### Default Level

2: System level

### Parameters

*group-name*: Name for the certificate attribute group, a case-insensitive string of 1 to 16 characters. It cannot be "a", "al" or "all".

**all**: Specifies all certificate attribute groups.

### Description

Use the **pki certificate attribute-group** command to create a certificate attribute group and enter its view.

Use the **undo pki certificate attribute-group** command to delete one or all certificate attribute groups.

By default, no certificate attribute group exists.

## Examples

```
# Create a certificate attribute group named mygroup and enter its view.
```

```
<Sysname> system-view  
[Sysname] pki certificate attribute-group mygroup  
[Sysname-pki-cert-attribute-group-mygroup]
```

## pki delete-certificate

### Syntax

```
pki delete-certificate { ca | local } domain domain-name
```

### View

System view

### Default Level

2: System level

### Parameters

**ca**: Deletes the locally stored CA certificate.

**local**: Deletes the locally stored local certificate.

*domain-name*: Name of the PKI domain whose certificates are to be deleted, a string of 1 to 15 characters.

### Description

Use the **pki delete-certificate** command to delete the certificate locally stored for a PKI domain.

## Examples

```
# Delete the local certificate for PKI domain cer.
```

```
<Sysname> system-view  
[Sysname] pki delete-certificate local domain cer
```

## pki domain

### Syntax

```
pki domain domain-name  
undo pki domain domain-name
```

### View

System view

### Default Level

2: System level

## Parameters

*domain-name*: PKI domain name, a case-insensitive string of 1 to 15 characters.

## Description

Use the **pki domain** command to create a PKI domain and enter PKI domain view or enter the view of an existing PKI domain.

Use the **undo pki domain** command to remove a PKI domain.

By default, no PKI domain exists.

## Examples

# Create a PKI domain and enter its view.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1]
```

## pki entity

### Syntax

```
pki entity entity-name
undo pki entity entity-name
```

### View

System view

### Default Level

2: System level

## Parameters

*entity-name*: Name for the entity, a case-insensitive string of 1 to 15 characters.

## Description

Use the **pki entity** command to create a PKI entity and enter PKI entity view.

Use the **undo pki entity** command to remove a PKI entity.

By default, no entity exists.

You can configure a variety of attributes for an entity in PKI entity view. An entity is intended only for convenience of reference by other commands.

## Examples

# Create a PKI entity named **en** and enter its view.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en]
```

## pki import-certificate

### Syntax

```
pki import-certificate { ca | local } domain domain-name { der | p12 | pem } [ filename filename ]
```

### View

System view

### Default Level

2: System level

### Parameters

**ca**: Specifies the CA certificate.

**local**: Specifies the local certificate.

*domain-name*: Name of the PKI domain, a string of 1 to 15 characters.

**der**: Specifies the certificate format of DER.

**p12**: Specifies the certificate format of P12.

**pem**: Specifies the certificate format of PEM.

*filename*: Name of the certificate file, a case-insensitive string of 1 to 127 characters. It defaults to *domain-name\_ca.cer*, *domain-name\_local.cer*, or *domain-name\_peerentity\_entity-name.cer*, the name for the file to be created to save the imported certificate.

### Description

Use the **pki import-certificate** command to import a CA certificate or local certificate from a file and save it locally.

Related commands: **pki domain**.

### Examples

```
# Import the CA certificate for PKI domain cer in the format of PEM.
```

```
<Sysname> system-view
```

```
[Sysname] pki import-certificate ca domain cer pem
```

## pki request-certificate domain

### Syntax

```
pki request-certificate domain domain-name [ password ] [ pkcs10 [ filename filename ] ]
```

### View

System view

### Default Level

2: System level

### Parameters

*domain-name*: Name of the PKI domain name, a string of 1 to 15 characters.

*password*: Password for certificate revocation, a case-sensitive string of 1 to 31 characters.

**pkcs10**: Displays the BASE64-encoded PKCS#10 certificate request.

*filename*: Name of the file for saving the PKCS#10 certificate request, a case-insensitive string of 1 to 127 characters.

## Description

Use the **pki request-certificate domain** command to request a local certificate from a CA through SCEP. If SCEP fails, you can use the **pkcs10** keyword to save the local certificate request in BASE64 format and send it to the CA by an out-of-band means like phone, disk or e-mail.

This operation will not be saved in the configuration file.

Related commands: **pki domain**.

## Examples

# Display the PKCS#10 certificate request information.

```
<Sysname> system-view
[Sysname] pki request-certificate domain 1 pkcs10
[Sysname] pki request-certificate domain 1 pkcs10
-----BEGIN CERTIFICATE REQUEST-----
MIIBTDCBtgIBADANMQswCQYDVQQDEwJqaJCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEAw5Drj8ofs9THA4ezkDcQPBy8pvH1kumampPsJmx8sGG52NftbrDTnTT5
ALx3LJijB3d/ndKpcHT/DfbJVDCn5gdw32tBZyCkEwMHZN3ol2z7Nvdu5TED6iN8
4m+hfp1QWoV6lty3o9pxAXuQl8peUDcfN6WV3LBXYy1lWCtkLkECAwEAAaAAMA0G
CSqGSIB3DQEBBAUAA4GBAA8E7BaIdmT6NVCZgv/I/1tqZH3TS4e4H9Qo5NiCKiEw
R8owVmA0XVtGMbyqBNcDTG0f5NbHrXZQT5+MbFJOnm5K/mn1ro5TJKMTKV46PlCZ
JUjsugaY02GBY0BVcylpC9iIXLuXNIqjh1MBIqVsallQOHS7YMvno6hXAQlkm4c
-----END CERTIFICATE REQUEST-----
```

## pki retrieval-certificate

### Syntax

```
pki retrieval-certificate { ca | local } domain domain-name
```

### View

System view

### Default Level

2: System level

### Parameters

**ca**: Retrieves the CA certificate.

**local**: Retrieves the local certificate.

*domain-name*: Name of the PKI domain used for certificate request.

### Description

Use the **pki retrieval-certificate** command to retrieve a certificate from the server for certificate distribution.

Related commands: **pki domain**.

## Examples

```
# Retrieve the CA certificate from the certificate issuing server.
```

```
<Sysname> system-view
```

```
[Sysname] pki retrieval-certificate ca domain 1
```

## pki retrieval-crl domain

### Syntax

```
pki retrieval-crl domain domain-name
```

### View

System view

### Default Level

2: System level

### Parameters

*domain-name*: Name of the PKI domain, a string of 1 to 15 characters.

### Description

Use the **pki retrieval-crl domain** command to retrieve the latest CRLs from the server for CRL distribution.

CRLs are used to verify the validity of certificates.

Related commands: **pki domain**.

## Examples

```
# Retrieve CRLs.
```

```
<Sysname> system-view
```

```
[Sysname] pki retrieval-crl domain 1
```

## pki validate-certificate

### Syntax

```
pki validate-certificate { ca | local } domain domain-name
```

### View

System view

### Default Level

2: System level

### Parameters

**ca**: Verifies the CA certificate.

**local**: Verifies the local certificate.

*domain-name*: Name of the PKI domain to which the certificate to be verified belongs, a string of 1 to 15 characters.

## Description

Use the **pki validate-certificate** command to verify the validity of a certificate.

The focus of certificate validity verification is to check that the certificate is signed by the CA and that the certificate has neither expired nor been revoked.

Related commands: **pki domain**.

## Examples

```
# Verify the validity of the local certificate.
```

```
<Sysname> system-view
```

```
[Sysname] pki validate-certificate local domain 1
```

## root-certificate fingerprint

### Syntax

```
root-certificate fingerprint { md5 | sha1 } string
```

```
undo root-certificate fingerprint
```

### View

PKI domain view

### Default Level

2: System level

### Parameters

**md5**: Uses an MD5 fingerprint.

**sha1**: Uses a SHA1 fingerprint.

*string*: Fingerprint to be used. An MD5 fingerprint must be a string of 32 characters in hexadecimal. A SHA1 fingerprint must be a string of 40 characters in hexadecimal.

## Description

Use the **root-certificate fingerprint** command to configure the fingerprint to be used for verifying the validity of the CA root certificate.

Use the **undo root-certificate fingerprint** command to remove the configuration.

By default, no fingerprint is configured for verifying the validity of the CA root certificate.

## Examples

```
# Configure an MD5 fingerprint for verifying the validity of the CA root certificate.
```

```
<Sysname> system-view
```

```
[Sysname] pki domain 1
```

```
[Sysname-pki-domain-1] root-certificate fingerprint md5 12EF53FA355CD23E12EF53FA355CD23E
```

```
# Configure a SHA1 fingerprint for verifying the validity of the CA root certificate.
```

```
[Sysname-pki-domain-1] root-certificate fingerprint sha1
D1526110AAD7527FB093ED7FC037B0B3CDDAD93
```

## rule (access control policy view)

### Syntax

```
rule [ id ] { deny | permit } group-name
undo rule { id | all }
```

### View

Access control policy view

### Default Level

2: System level

### Parameters

**id**: Number of the certificate attribute access control rule, in the range 1 to 16. The default is the smallest unused number in this range.

**deny**: Indicates that a certificate whose attributes match an attribute rule in the specified attribute group is considered invalid and denied.

**permit**: Indicates that a certificate whose attributes match an attribute rule in the specified attribute group is considered valid and permitted.

**group-name**: Name of the certificate attribute group to be associated with the rule, a case-insensitive string of 1 to 16 characters. It cannot be “a”, “al” or “all”.

**all**: Specifies all access control rules.

### Description

Use the **rule** command to create a certificate attribute access control rule.

Use the **undo rule** command to delete a specified or all access control rules.

By default, no access control rule exists.

Note that a certificate attribute group must exist to be associated with a rule.

### Examples

```
# Create an access control rule, specifying that a certificate is considered valid when it matches an
attribute rule in certificate attribute group mygroup.
```

```
<Sysname> system-view
[Sysname] pki certificate access-control-policy mypolicy
[Sysname-pki-cert-acp-mypolicy] rule 1 permit mygroup
```

## state

### Syntax

```
state state-name
undo state
```

## View

PKI entity view

## Default Level

2: System level

## Parameters

*state-name*: State or province name, a case-insensitive string of 1 to 31 characters. No comma can be included.

## Description

Use the **state** command to specify the name of the state or province where an entity resides.

Use the **undo state** command to remove the configuration.

By default, no state or province is specified.

## Examples

# Specify the state where an entity resides.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] state country
```

# Table of Contents

<b>1 SSL Configuration Commands</b> .....	<b>1-1</b>
SSL Configuration Commands .....	1-1
ciphersuite .....	1-1
client-verify enable.....	1-2
close-mode wait.....	1-2
display ssl client-policy .....	1-3
display ssl server-policy.....	1-4
handshake timeout .....	1-5
pki-domain .....	1-6
prefer-cipher .....	1-6
session .....	1-7
ssl client-policy .....	1-8
ssl server-policy.....	1-9
version .....	1-9

# 1 SSL Configuration Commands

---

## SSL Configuration Commands

### ciphersuite

#### Syntax

```
ciphersuite [ rsa_aes_128_cbc_sha | rsa_des_cbc_sha | rsa_rc4_128_md5 | rsa_rc4_128_sha ] *
```

#### View

SSL server policy view

#### Default Level

2: System level

#### Parameters

**rsa\_aes\_128\_cbc\_sha**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit AES\_CBC, and the MAC algorithm of SHA.

**rsa\_des\_cbc\_sha**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of DES\_CBC, and the MAC algorithm of SHA.

**rsa\_rc4\_128\_md5**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of MD5.

**rsa\_rc4\_128\_sha**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of SHA.

#### Description

Use the **ciphersuite** command to specify the cipher suite(s) for an SSL server policy to support.

By default, an SSL server policy supports all cipher suites.

With no keyword specified, the command configures an SSL server policy to support all cipher suites.

Related commands: **display ssl server-policy**.

#### Examples

```
# Specify the cipher suites for SSL server policy policy1 to support as rsa_rc4_128_md5 and rsa_rc4_128_sha.
```

```
<Sysname> system-view
```

```
[Sysname] ssl server-policy policy1
```

```
[Sysname-ssl-server-policy-policy1] ciphersuite rsa_rc4_128_md5 rsa_rc4_128_sha
```

## client-verify enable

### Syntax

```
client-verify enable
undo client-verify enable
```

### View

SSL server policy view

### Default Level

2: System level

### Parameters

None

### Description

Use the **client-verify enable** command to enable certificate-based SSL client authentication, that is, to enable the SSL server to perform certificate-based authentication of the client during the SSL handshake process.

Use the **undo client-verify enable** command to restore the default.

By default, certificate-based SSL client authentication is disabled.

### Examples

```
# Enable certificate-based client authentication.
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] client-verify enable
```

## close-mode wait

### Syntax

```
close-mode wait
undo close-mode wait
```

### View

SSL server policy view

### Default Level

2: System level

### Parameters

None

## Description

Use the **close-mode wait** command to set the SSL connection close mode to wait. In this mode, after sending a close-notify message to a client, the server does not close the connection until it receives a close-notify message from the client.

Use the **undo close-mode wait** command to restore the default.

By default, an SSL server sends a close-notify alert message to the client and close the connection without waiting for the close-notify alert message from the client.

Related commands: **display ssl server-policy**.

## Examples

```
# Set the SSL connection close mode to wait mode.
```

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] close-mode wait
```

## display ssl client-policy

### Syntax

```
display ssl client-policy { policy-name | all }
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*policy-name*: SSL client policy name, a case-insensitive string of 1 to 16 characters.

**all**: Displays information about all SSL client policies.

## Description

Use the **display ssl client-policy** command to view information about a specified or all SSL client policies.

## Examples

```
# Display information about SSL client policy policy1.
```

```
<Sysname> display ssl client-policy policy1
SSL Client Policy: policy1
  SSL Version: SSL 3.0
  PKI Domain: 1
  Prefer Ciphersuite:
    RSA_RC4_128_SHA
```

**Table 1-1 display ssl client-policy command output description**

Field	Description
SSL Client Policy	SSL client policy name
SSL Version	Version of the protocol used by the SSL client policy, SSL 3.0 or TLS 1.0.
PKI Domain	PKI domain of the SSL client policy
Prefer Ciphersuite	Preferred cipher suite of the SSL client policy

## display ssl server-policy

### Syntax

```
display ssl server-policy { policy-name | all }
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*policy-name*: SSL server policy name, a case-insensitive string of 1 to 16 characters.

**all**: Displays information about all SSL server policies.

### Description

Use the **display ssl server-policy** command to view information about a specified or all SSL server policies.

### Examples

```
# Display information about SSL server policy policy1.
```

```
<Sysname> display ssl server-policy policy1
SSL Server Policy: policy1
  PKI Domain: domain1
  Ciphersuite:
    RSA_RC4_128_MD5
    RSA_RC4_128_SHA
    RSA_DES_CBC_SHA
    RSA_AES_128_CBC_SHA
  Handshake Timeout: 3600
  Close-mode: wait disabled
  Session Timeout: 3600
  Session Cachesize: 500
  Client-verify: disabled
```

**Table 1-2 display ssl server-policy** command output description

Field	Description
SSL Server Policy	SSL server policy name
PKI Domain	PKI domain used by the SSL server policy
Ciphersuite	Cipher suite supported by the SSL server policy
Handshake Timeout	Handshake timeout time of the SSL server policy, in seconds
Close-mode	Close mode of the SSL server policy, which can be: <ul style="list-style-type: none"><li>• wait disabled: In this mode, the server sends a close-notify message to the client and then closes the connection immediately without waiting for the close-notify message of the client.</li><li>• wait enabled: In this mode, the server sends a close-notify message to the client and then waits for the close-notify message of the client. Only after receiving the expected message, does the server close the connection.</li></ul>
Session Timeout	Session timeout time of the SSL server policy, in seconds
Session Cachesize	Maximum number of buffered sessions of the SSL server policy
Client-verify	Whether client authentication is enabled

## handshake timeout

### Syntax

```
handshake timeout time  
undo handshake timeout
```

### View

SSL server policy view

### Default Level

2: System level

### Parameters

*time*: Handshake timeout time in seconds, in the range 180 to 7,200.

### Description

Use the **handshake timeout** command to set the handshake timeout time for an SSL server policy.

Use the **undo handshake timeout** command to restore the default.

By default, the handshake timeout time is 3,600 seconds.

If the SSL server does not receive any packet from the SSL client before the handshake timeout time expires, the SSL server will terminate the handshake process.

Related commands: **display ssl server-policy**.

### Examples

```
# Set the handshake timeout time of SSL server policy policy1 to 3,000 seconds.
```

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] handshake timeout 3000
```

## pki-domain

### Syntax

```
pki-domain domain-name
undo pki-domain
```

### View

SSL server policy view, SSL client policy view

### Default Level

2: System level

### Parameters

*domain-name*: Name of a PKI domain, a case-insensitive string of 1 to 15 characters.

### Description

Use the **pki-domain** command to specify a PKI domain for an SSL server policy or SSL client policy.

Use the **undo pki-domain** command to restore the default.

By default, no PKI domain is configured for an SSL server policy or SSL client policy.

Related commands: **display ssl server-policy** and **display ssl client-policy**.

### Examples

# Configure SSL server policy policy1 to use the PKI domain named server-domain.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] pki-domain server-domain
```

# Configure SSL client policy policy1 to use the PKI domain named client-domain.

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] pki-domain client-domain
```

## prefer-cipher

### Syntax

```
prefer-cipher { rsa_aes_128_cbc_sha | rsa_des_cbc_sha | rsa_rc4_128_md5 | rsa_rc4_128_sha }
undo prefer-cipher
```

### View

SSL client policy view

### Default Level

2: System level

## Parameters

**rsa\_aes\_128\_cbc\_sha**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit AES\_CBC, and the MAC algorithm of SHA.

**rsa\_des\_cbc\_sha**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of DES\_CBC, and the MAC algorithm of SHA.

**rsa\_rc4\_128\_md5**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of MD5.

**rsa\_rc4\_128\_sha**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of SHA.

## Description

Use the **prefer-cipher** command to specify the preferred cipher suite for an SSL client policy.

Use the **undo prefer-cipher** command to restore the default.

By default, the preferred cipher suite for an SSL client policy is **rsa\_rc4\_128\_md5**.

Related commands: **display ssl client-policy**.

## Examples

```
# Set the preferred cipher suite for SSL client policy policy1 to rsa_aes_128_cbc_sha.
```

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] prefer-cipher rsa_aes_128_cbc_sha
```

## session

### Syntax

```
session { cache-size size | timeout time } *
```

```
undo session { cache-size | timeout } *
```

### View

SSL server policy view

### Default Level

2: System level

## Parameters

*size*: Maximum number of cached sessions, in the range 100 to 1,000.

*time*: Caching timeout time in seconds, in the range 1,800 to 72,000.

## Description

Use the **session** command to set the maximum number of cached sessions and the caching timeout time.

Use the **undo session** command to restore the default.

By default, the maximum number of cached sessions is 500 and the caching timeout time is 3,600 seconds.

The process of the session parameters negotiation and session establishment by using the SSL handshake protocol is quite complicated. SSL allows reusing the negotiated session parameters to establish sessions. Therefore, the SSL server needs to maintain information about existing sessions. Note that the number of sessions and the time that the session information will be maintained are limited:

- If the number of sessions in the cache reaches the maximum, SSL rejects to cache new sessions.
- If a session exists in the cache for a period equal to the caching timeout time, SSL will remove the information of the session.

Related commands: **display ssl server-policy**.

## Examples

```
# Set the caching timeout time to 4,000 seconds and the maximum number of cached sessions to 600.
```

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] session timeout 4000 cachesize 600
```

## ssl client-policy

### Syntax

```
ssl client-policy policy-name
undo ssl client-policy { policy-name | all }
```

### View

System view

### Default Level

2: System level

### Parameters

*policy-name*: SSL client policy name, a case-insensitive string of 1 to 16 characters, which cannot be “a”, “al” and “all”.

**all**: Specifies all SSL client policies.

### Description

Use the **ssl client-policy** command to create an SSL policy and enter its view.

Use the **undo ssl client-policy** command to remove a specified or all SSL client policies.

Related commands: **display ssl client-policy**.

## Examples

```
# Create an SSL client policy named policy1 and enter its view.
```

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1]
```

## ssl server-policy

### Syntax

```
ssl server-policy policy-name  
undo ssl server-policy { policy-name | all }
```

### View

System view

### Default Level

2: System level

### Parameters

*policy-name*: SSL server policy name, a case-insensitive string of 1 to 16 characters, which cannot be "a", "al" and "all".

**all**: Specifies all SSL server policies.

### Description

Use the **ssl server-policy** command to create an SSL server policy and enter its view.

Use the **undo ssl server-policy** command to remove a specified or all SSL server policies.

Note that you cannot delete an SSL server policy that has been associated with one or more application layer protocols.

### Examples

# Create an SSL server policy named **policy1** and enter its view.

```
<Sysname> system-view  
[Sysname] ssl server-policy policy1  
[Sysname-ssl-server-policy-policy1]
```

## version

### Syntax

```
version { ssl3.0 | tls1.0 }  
undo version
```

### View

SSL client policy view

### Default Level

2: System level

### Parameters

**ssl3.0**: Specifies SSL 3.0.

**tls1.0**: Specifies TLS 1.0.

## Description

Use the **version** command to specify the SSL protocol version for an SSL client policy.

Use the **undo version** command to restore the default.

By default, the SSL protocol version for an SSL client policy is TLS 1.0.

Related commands: **display ssl client-policy**.

## Examples

# Specify the SSL protocol version for SSL client policy policy1 as SSL 3.0.

```
<Sysname> system-view
```

```
[Sysname] ssl client-policy policy1
```

```
[Sysname-ssl-client-policy-policy1] version ssl3.0
```

# Table of Contents

<b>1 Public Key Configuration Commands</b> .....	<b>1-1</b>
Public Key Configuration Commands .....	1-1
display public-key local public .....	1-1
display public-key peer .....	1-2
peer-public-key end .....	1-3
public-key-code begin .....	1-4
public-key-code end .....	1-4
public-key local create .....	1-5
public-key local destroy .....	1-6
public-key local export dsa .....	1-7
public-key local export rsa .....	1-8
public-key peer .....	1-9
public-key peer import sshkey .....	1-10

# 1 Public Key Configuration Commands

---

## Public Key Configuration Commands

### display public-key local public

#### Syntax

```
display public-key local { dsa | rsa } public
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

**dsa**: DSA key pair.

**rsa**: RSA key pair.

#### Description

Use the **display public-key local public** command to display the public key information of the local key pair(s).

Related commands: **public-key local create**.

#### Examples

# Display the public key information of the local RSA key pairs.

```
<Sysname> display public-key local rsa public
```

```
=====
Time of Key pair created: 19:59:16 2007/10/25
Key name: HOST_KEY
Key type: RSA Encryption Key
=====
Key code:
30819F300D06092A864886F70D010101050003818D0030818902818100BC4C392A97734A633BA0F1DB01F84E
B51228EC86ADE1DBA597E0D9066FDC4F04776CEA3610D2578341F5D049143656F1287502C06D39D39F28F0F5
CBA630DA8CD1C16ECE8A7A65282F2407E8757E7937DCCDB5DB620CD1F471401B7117139702348444A2D89004
97A87B8D5F13D61C4DEFA3D14A7DC07624791FC1D226F62DF3020301
0001
=====
Time of Key pair created: 19:59:17 2007/10/25
Key name: SERVER_KEY
```

```

Key type: RSA Encryption Key
=====
Key code:
307C300D06092A864886F70D0101010500036B003068026100C51AF7CA926962284A4654B2AACC7B2AE12B2B
1EABFAC1CDA97E42C3C10D7A70D1012BF23ADE5AC4E7AAB132CFB6453B27E054BF0A0A85E113FBDE751EE0EC
EF659529E857CF8C211E2A03FD8F10C5BEC162B2989ABB5D299D1E4E27A13C7DD10203010001

# Display the public key information of the local DSA key pair.
<Sysname> display public-key local dsa public

=====
Time of Key pair created: 20:00:16 2007/10/25
Key name: HOST_KEY
Key type: DSA Encryption Key
=====
Key code:
308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD96E5F061C4F0A4
23F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1EDBD13EC8B274DA9F75BA26CCB987
723602787E922BA84421F22C3C89CB9B06FD06FE01941DDD77FE6B12893DA76EEBC1D128D97F0678D7722B53
41C8506F358214B16A2FAC4B368950387811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F
0281810082269009E14EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B
20CD35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B612391C76C1FB2
E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1585DA7F42519718CC9B09EEF
0381850002818100CCF1F78E0860BE937FD3CA07D2F2A1B66E74E5D1E16693EB374D677A7A6124EBABD59FE4
8796C56F3FF919F999AEB97D1F2B83D9B98AC09BC1F72E80DBE337CB29989A23378EB21C38EE083F11ED6DC8
D4DBE001BA85450CEA071C2A471C83761E4CF32C174B418612CDD597B441F0CAA05DC01CB93A0ABB247C06FB
A4C79054

```

## display public-key peer

### Syntax

```
display public-key peer [ brief | name publickey-name ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**brief:** Displays brief information about all the public keys of peers.

**name *publickey-name*:** Specifies a peer's host public key by its name, which is a case-sensitive string of 1 to 64 characters.

### Description

Use the **display public-key peer** command to display information about the specified or all locally saved public keys of peers.

With neither the **brief** keyword nor the **name** *publickey-name* combination specified, the command displays detailed information about all locally saved public keys of peers.

You can use the **public-key peer** command or the **public-key peer import sshkey** command to get a local copy of the public keys of a peer.

Related commands: **public-key peer**, **public-key peer import sshkey**.

## Examples

```
# Display detailed information about the peer host public key named idrsa.
```

```
<Sysname> display public-key peer name idrsa
```

```
=====
```

```
Key name   : idrsa
```

```
Key type   : RSA
```

```
Key module: 1024
```

```
=====
```

```
Key Code:
```

```
30819D300D06092A864886F70D010101050003818B00308187028181009C46A8710216CEC0C01C7CE136BA76  
C79AA6040E79F9E305E453998C7ADE8276069410803D5974F708496947AB39B3F39C5CE56C95B6AB7442D563  
93BF241F99A639DD02D9E29B1F5C1FD05CC1C44FBD6CFFB58BE6F035FAA2C596B27D1231D159846B7CB9A775  
7C5800FADA9FD72F65672F4A549EE99F63095E11BD37789955020123
```

```
# Display brief information about all locally saved public keys of the peers.
```

```
<Sysname> display public-key peer brief
```

```
Type  Module  Name
```

```
-----
```

```
RSA   1024    idrsa
```

```
DSA   1024    10.1.1.1
```

## peer-public-key end

### Syntax

```
peer-public-key end
```

### View

Public key view

### Default Level

2: System level

### Parameters

None

### Description

Use the **peer-public-key end** command to return from public key view to system view.

Related commands: **public-key peer**.

## Examples

```
# Exit public key view.
```

```
<Sysname> system-view
[Sysname] public-key peer key1
[Sysname-pkey-public-key] peer-public-key end
[Sysname]
```

## public-key-code begin

### Syntax

```
public-key-code begin
```

### View

Public key view

### Default Level

2: System level

### Parameters

None

### Description

Use the **public-key-code begin** command to enter public key code view.

After entering public key code view, you can input the key. The key must be a hexadecimal string that has not been converted and in the distinguished encoding rules (DER) encoding format. Spaces and carriage returns are allowed between characters.

Related commands: **public-key peer**, **public-key-code end**.

### Examples

# Enter public key code view and input the key.

```
<Sysname> system-view
[Sysname] public-key peer key1
[Sysname-pkey-public-key] public-key-code begin
[Sysname-pkey-key-code]30819F300D06092A864886F70D010101050003818D0030818902818100C0EC801
4F82515F6335A0A
[Sysname-pkey-key-code]EF8F999C01EC94E5760A079BD73E4F4D97F3500EDB308C29481B77E719D164313
5877E13B1C531B4
[Sysname-pkey-key-code]FF1877A5E2E7B1FA4710DB0744F66F6600EEFE166F1B854E2371D5B952ADF6B80
EB5F52698FCF3D6
[Sysname-pkey-key-code]1F0C2EAD9813ECB16C5C7DC09812D4EE3E9A0B074276FFD4AF2050BD4A9B1DDE
675AC30CB020301
[Sysname-pkey-key-code]0001
```

## public-key-code end

### Syntax

```
public-key-code end
```

## View

Public key code view

## Default Level

2: System level

## Parameters

None

## Description

Use the **public-key-code end** command to return from public key code view to public key view and to save the configured public key.

The system verifies the key before saving it. If the key contains invalid characters, the system displays an error message and discards the key. Otherwise, the system saves the key.

Related commands: **public-key peer**, **public-key-code begin**.

## Examples

# Exit public key code view and save the configured public key.

```
<Sysname> system-view
[Sysname] public-key peer key1
[Sysname-pkey-public-key] public-key-code begin
[Sysname-pkey-key-code] 30819F300D06092A864886F70D010101050003818D0030818902818100C0EC801
4F82515F6335A0A
[Sysname-pkey-key-code] EF8F999C01EC94E5760A079BD73E4F4D97F3500EDB308C29481B77E719D164313
5877E13B1C531B4
[Sysname-pkey-key-code] FF1877A5E2E7B1FA4710DB0744F66F6600EAFE166F1B854E2371D5B952ADF6B80
EB5F52698FCF3D6
[Sysname-pkey-key-code] 1F0C2EAAD9813ECB16C5C7DC09812D4EE3E9A0B074276FFD4AF2050BD4A9B1DDE
675AC30CB020301
[Sysname-pkey-key-code] 0001
[Sysname-pkey-key-code] public-key-code end
[Sysname-pkey-public-key]
```

## public-key local create

### Syntax

```
public-key local create { dsa | rsa }
```

### View

System view

### Default Level

2: System level

### Parameters

**dsa**: DSA key pair.

**rsa:** RSA key pair.

## Description

Use the **public-key local create** command to create local key pair(s).

Note that:

- When using this command to create DSA or RSA key pairs, you will be prompted to provide the length of the key modulus. The modulus length is in the range 512 to 2048 bits, and defaults to 1024 bits. If the type of key pair already exists, the system will ask you whether you want to overwrite it.
- The configuration of this command can survive a reboot.

Related commands: **public-key local destroy**, **display public-key local**.

## Examples

# Create local RSA key pairs.

```
<Sysname> system-view
[Sysname] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++
++++++
+++++++
+++++++
```

# Create a local DSA key pair.

```
<Sysname> system-view
[Sysname] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
*
*
```

## public-key local destroy

### Syntax

```
public-key local destroy { dsa | rsa }
```

### View

System view

## Default Level

2: System level

## Parameters

**dsa**: DSA key pair.

**rsa**: RSA key pair.

## Description

Use the **public-key local destroy** command to destroy the local key pair(s).

Related commands: **public-key local create**.

## Examples

```
# Destroy the local RSA key pairs.
<Sysname> system-view
[Sysname] public-key local destroy rsa
Warning: Confirm to destroy these keys? [Y/N]:y

# Destroy the local DSA key pair.
<Sysname> system-view
[Sysname] public-key local destroy dsa
Warning: Confirm to destroy these keys? [Y/N] :y
```

## public-key local export dsa

### Syntax

```
public-key local export dsa { openssh | ssh2 } [ filename ]
```

### View

System view

### Default Level

1: Monitor level

### Parameters

**openssh**: Uses the format of OpenSSH.

**ssh2**: Uses the format of SSH2.0.

*filename*: Name of the file for storing public key. For detailed information about file name, refer to *File System Management* in the *System Volume*.

### Description

Use the **public-key local export dsa** command to display the local DSA public key on the screen or export it to a specified file.

If you do not specify the *filename* argument, the command displays the local DSA public key on the screen; otherwise, the command exports the local DSA public key to the specified file and saves the file.

SSH2.0 and OpenSSH are two different public key formats for different requirements.

Related commands: **public-key local create**, **public-key local destroy**.

## Examples

# Export the local DSA public key in OpenSSH format to a file named **key.pub**.

```
<Sysname> system-view
[Sysname] public-key local export dsa openssh key.pub
```

# Display the local DSA public key in SSH2.0 format.

```
<Sysname> system-view
[Sysname] public-key local export dsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "dsa-key-20070625"
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3B7b
0T7IsnTan3W6Jsy5h3I2Anh+kiuORChyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKN1/BnjXcitTQchQbzWCFLFq
L6xLNolQOHgRx9ozAAAAFQDHcyGmc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN
/OrpbsTV75MTPoS0cJPFKyDNNdAkkroVnsZJliW8T6UILLiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2B
cdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRLxjMmwnu8AAACBANvcLNEKdDt6xcatpRjxsSrhXFVIdRjx
w59qZnKh187GsbGP4ccUp3KmcRzuqz1qNtfgoZOLzHnG1YGxPp7Q2k/uRuuHN0bJfBkOLO2/RyGqDJlqB4FQwmr
kwJuauYGqQy+mgE6dmHn0VG4gAkx9MQxDIBjzbZRX0bvXmDNKR22
---- END SSH2 PUBLIC KEY ----
```

# Display the local DSA public key in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export dsa openssh
ssh-dss
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3B7b
0T7IsnTan3W6Jsy5h3I2Anh+kiuORChyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKN1/BnjXcitTQchQbzWCFLFq
L6xLNolQOHgRx9ozAAAAFQDHcyGmc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN
/OrpbsTV75MTPoS0cJPFKyDNNdAkkroVnsZJliW8T6UILLiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2B
cdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRLxjMmwnu8AAACBANvcLNEKdDt6xcatpRjxsSrhXFVIdRjx
w59qZnKh187GsbGP4ccUp3KmcRzuqz1qNtfgoZOLzHnG1YGxPp7Q2k/uRuuHN0bJfBkOLO2/RyGqDJlqB4FQwmr
kwJuauYGqQy+mgE6dmHn0VG4gAkx9MQxDIBjzbZRX0bvXmDNKR22 dsa-key
```

## public-key local export rsa

### Syntax

```
public-key local export rsa { openssh | ssh1 | ssh2 } [ filename ]
```

### View

System view

### Default Level

1: Monitor level

### Parameters

**openssh**: Uses the format of OpenSSH.

**ssh1**: Uses the format of SSH1.5.

**ssh2**: Uses the format of SSH2.0.

*filename*: Name of the file for storing the public key. For detailed information about file name, refer to *File System Management* in the *System Volume*.

## Description

Use the **public-key local export rsa** command to display the local RSA public key on the screen or export them to a specified file.

If you do not specify the *filename* argument, the command displays the local RSA public key on the screen; otherwise, the command exports the local RSA public key to the specified file and saves the file.

SSH1, SSH2.0 and OpenSSH are three different public key formats for different requirements.

Related commands: **public-key local create**, **public-key local destroy**.

## Examples

# Export the local RSA public key in OpenSSH format to a file named **key.pub**.

```
<Sysname> system-view
[Sysname] public-key local export rsa openssh key.pub
```

# Display the local RSA public key in SSH2.0 format.

```
<Sysname> system-view
[Sysname] public-key local export rsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20070625"
AAAAB3NzaC1yc2EAAAADAQABAAQgQDAo0dVYR1S5f30eLKGnKucb5HU3M0TTSaG1ER2GmcRI2sgSegbo1x6ut5N
Ic5+jJxuRCU4+gMc76iS8d+2d50FqIweEkHHkSG/ddgXt/iAZ6cY81bdu/CKxGiQ1kUpbw4vSv+X5KeE7j+o0MpO
pzh3W768/+ulriz+1LcwVTs51Q==
---- END SSH2 PUBLIC KEY ----
```

# Display the local RSA public key in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export rsa openssh
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQgQDAo0dVYR1S5f30eLKGnKucb5HU3M0TTSaG1ER2GmcRI2sgSegbo1x6ut5N
Ic5+jJxuRCU4+gMc76iS8d+2d50FqIweEkHHkSG/ddgXt/iAZ6cY81bdu/CKxGiQ1kUpbw4vSv+X5KeE7j+o0MpO
pzh3W768/+ulriz+1LcwVTs51Q== rsa-key
```

## public-key peer

### Syntax

**public-key peer** *keyname*

**undo public-key peer** *keyname*

### View

System view

### Default Level

2: System level

## Parameters

*keyname*: Public key name, a case-sensitive string of 1 to 64 characters.

## Description

Use the **public-key peer** command to configure the public key name and enter public key view.

Use the **undo public-key peer** command to remove a configured peer public key.

After entering public key view, you can configure the public key of the peer with the **public-key-code begin** and **public-key-code end** commands. This requires that you obtain the hexadecimal public key from the peer beforehand.

Related commands: **public-key-code begin**, **public-key-code end**, **display public-key peer**.

## Examples

```
# Enter public key view, specifying a public key name of key1.
```

```
<Sysname> system-view  
[Sysname] public-key peer key1  
[Sysname-pkey-public-key]
```

## public-key peer import sshkey

### Syntax

```
public-key peer keyname import sshkey filename
```

```
undo public-key peer keyname
```

### View

System view

### Default Level

2: System level

## Parameters

*keyname*: Public key name, a case-sensitive string of 1 to 64 characters.

*filename*: Public key file name. For detailed information about file name, refer to *File System Management* in the *System Volume*.

## Description

Use the **public-key peer import sshkey** command to import the public key of a peer from the public key file.

Use the **undo public-key peer** command to remove a configured peer public key.

After execution of this command, the system automatically transforms the public key in SSH1, SSH2.0 or OpenSSH format to PKCS format, and imports the peer public key. This requires that you get a copy of the public key file from the peer through FTP or TFTP in advance.

Related commands: **display public-key peer**.

## Examples

```
# Import the peer host public key named key2 from the public key file key.pub.
```

```
<Sysname> system-view
```

```
[Sysname] public-key peer key2 import sshkey key.pub
```

# Table of Contents

<b>1 ACL Configuration Commands</b> .....	<b>1-1</b>
Common Configuration Commands .....	1-1
display acl resource .....	1-1
display time-range .....	1-2
time-range .....	1-3
IPv4 ACL Configuration Commands .....	1-5
acl .....	1-5
acl copy .....	1-6
acl name .....	1-7
description (for IPv4) .....	1-8
display acl .....	1-9
reset acl counter .....	1-10
rule (basic IPv4 ACL view) .....	1-10
rule (advanced IPv4 ACL view) .....	1-12
rule (Ethernet frame header ACL view) .....	1-16
rule comment (for IPv4) .....	1-18
step (for IPv4) .....	1-19
IPv6 ACL Configuration Commands .....	1-20
acl ipv6 .....	1-20
acl ipv6 copy .....	1-21
acl ipv6 name .....	1-22
description (for IPv6) .....	1-22
display acl ipv6 .....	1-23
reset acl ipv6 counter .....	1-24
rule (basic IPv6 ACL view) .....	1-25
rule (advanced IPv6 ACL view) .....	1-26
rule comment (for IPv6) .....	1-30
step (for IPv6) .....	1-31

# 1 ACL Configuration Commands

---

## Common Configuration Commands

### display acl resource

#### Syntax

```
display acl resource [ slot slot number ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

**slot slot-number**: Displays the usage of ACL resources on the specified device in the IRF stack. If the *slot-number* argument is not specified, the usage on all devices in the IRF stack is displayed. If no IRF stack is formed, the usage on the current device is displayed. The range for the *slot-number* argument depends on the number of devices and the numbering of the devices in the IRF stack.

#### Description

Use the **display acl resource** command to display the usage of ACL resources on a switch.

#### Examples

# Display the ACL uses on the switch.

```
<Sysname> display acl resource
Interface:
  GE1/0/1 to GE1/0/28
```

Type	Total	Reserved	Configured	Remaining
VFP ACL	1024	0	0	1024
IFP ACL	4096	0	60	4036
IFP Meter	2048	0	46	2002
IFP Counter	2048	0	0	2048
EFP ACL	512	0	0	512
EFP Meter	256	0	0	256
EFP Counter	512	0	0	512

# Display the ACL uses on all devices in the IRF stack.

```
<Sysname> display acl resource
Interface:
```

GE1/0/1 to GE1/0/28, XGE1/2/1

Type	Total	Reserved	Configured	Remaining
VFP ACL	1024	0	0	1024
IFP ACL	4096	0	86	4010
IFP Meter	2048	0	35	2013
IFP Counter	2048	0	35	2013
EFP ACL	512	0	0	512
EFP Meter	256	0	0	256
EFP Counter	512	0	0	512

Interface:

GE2/0/1 to GE2/0/32, GE2/0/1

Type	Total	Reserved	Configured	Remaining
VFP ACL	1024	0	0	1024
IFP ACL	4096	0	86	4010
IFP Meter	2048	0	35	2013
IFP Counter	2048	0	35	2013
EFP ACL	512	0	0	512

**Table 1-1 display acl resource command output description**

Field	Description
Interface	Interface indicated by its type and number
Type	Resource type: <ul style="list-style-type: none"> <li>• ACL indicates ACL rule resources,</li> <li>• Meter indicates traffic policing resources,</li> <li>• Counter indicates traffic statistics resources,</li> <li>• VFP indicates the count of resources that are before Layer 2 forwarding and applied in QinQ,</li> <li>• IFP indicates the count of resources in the inbound direction,</li> <li>• EFP indicates the count of resources in the outbound direction.</li> </ul>
Total	Total number of ACLs supported
Reserved	Number of reserved ACLs
Configured	Number of configured ACLs
Remaining	Number of remaining ACLs

## display time-range

### Syntax

**display time-range** { *time-range-name* | all }

## View

Any view

## Default Level

1: Monitor level

## Parameters

*time-range-name*: Time range name, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

**all**: Specifies all existing time ranges.

## Description

Use the **display time-range** command to display the configuration and status of a specified time range or all time ranges.

A time range is active if the system time falls into its range.

## Examples

# Display the configuration and status of time range **trname**.

```
<Sysname> display time-range trname
Current time is 22:20:18 1/5/2006 Thursday
Time-range : trname ( Inactive )
  from 15:00 1/28/2006 to 15:00 1/28/2008
```

**Table 1-2 display time-range** command output description

Field	Description
Current time	Current system time
Time-range	Configuration and status of the time range, including the name of the time range, its status (active or inactive), and its start time and end time.

## time-range

### Syntax

```
time-range time-range-name { start-time to end-time days [ from time1 date1 ] [ to time2 date2 ] | from time1 date1 [ to time2 date2 ] | to time2 date2 }
```

```
undo time-range time-range-name [ start-time to end-time days [ from time1 date1 ] [ to time2 date2 ] | from time1 date1 [ to time2 date2 ] | to time2 date2 ]
```

### View

System view

### Default Level

2: System level

## Parameters

*time-range-name*: Time range name, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

*start-time*: Start time of a periodic time range, in *hh:mm* format (24-hour clock), where *hh* is hours and *mm* is minutes. Its value ranges from 00:00 to 23:59.

*end-time*: End time of the periodic time range, in *hh:mm* format (24-hour clock), where *hh* is hours and *mm* is minutes. Its value ranges from 00:00 to 24:00. The end time must be greater than the start time.

*days*: Indicates on which day or days of the week the periodic time range is valid. You may specify multiple values, in words or in digits, separated by spaces, but make sure that they do not overlap. These values can take one of the following forms:

- A digit in the range 0 to 6, respectively for Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday.
- Week in words, that is, Mon, Tue, Wed, Thu, Fri, Sat, or Sun.
- working-day for Monday through Friday.
- off-day for Saturday and Sunday.
- daily for seven days of a week.

**from** *time1 date1*: Indicates the start time and date of an absolute time range. The *time1* argument specifies the time of the day in *hh:mm* format (24-hour clock), where *hh* is hours and *mm* is minutes. Its value ranges from 00:00 to 23:59. The *date1* argument specifies a date in *MM/DD/YYYY* or *YYYYMM/DD* format, where *MM* is the month of the year in the range 1 to 12, *DD* is the day of the month in the range 1 to 31, and *YYYY* is the year in the usual Gregorian calendar in the range 1970 to 2100. If not specified, the start time is the earliest time available in the system, namely, 01/01/1970 00:00:00 AM.

**to** *time2 date2*: Indicates the end time and date of the absolute time range. The format of the *time2* argument is the same as that of the *time1* argument, but its value ranges from 00:00 to 24:00. The end time must be greater than the start time. If not specified, the end time is the maximum time available in the system, namely, 12/31/2100 24:00:00 PM. The format and value range of the *date2* argument are the same as those of the *date1* argument.

## Description

Use the **time-range** command to create a time range.

Use the **undo time-range** command to remove a time range.

You may create a maximum of 256 time ranges.

A time range can be one of the following:

- Periodic time range created using the **time-range** *time-range-name start-time to end-time days* command. A time range thus created recurs periodically on the day or days of the week.
- Absolute time range created using the **time-range** *time-range-name { from time1 date1 [ to time2 date2 ] | to time2 date2 }* command. Unlike a periodic time range, a time range thus created does not recur. For example, to create an absolute time range that is active between January 1, 2004 00:00 and December 31, 2004 23:59, you may use the **time-range test from 00:00 01/01/2004 to 23:59 12/31/2004** command.
- Compound time range created using the **time-range** *time-range-name start-time to end-time days { from time1 date1 [ to time2 date2 ] | to time2 date2 }* command. A time range thus created recurs on the day or days of the week only within the specified period. For example, to create a time range that is active from 12:00 to 14:00 on Wednesdays between January 1, 2004 00:00 and December

31, 2004 23:59, you may use the **time-range test 12:00 to 14:00 wednesday from 00:00 01/01/2004 to 23:59 12/31/2004** command.

You may create individual time ranges identified with the same name. They are regarded as one time range whose active period is the result of ORing periodic ones, ORing absolute ones, and ANDing periodic and absolute ones.

## Examples

# Create an absolute time range named **test**, setting it to become active from 00:00 on January 1, 2008.

```
<Sysname> system-view
[Sysname] time-range test from 0:0 2008/1/1
```

# Create a periodic time range named **test**, setting it to be active between 8:00 to 18:00 during working days.

```
<Sysname> system-view
[Sysname] time-range test 8:00 to 18:00 working-day
```

# Create a periodic time range named **test**, setting it to be active between 14:00 and 18:00 on Saturday and Sunday.

```
<Sysname> system-view
[Sysname] time-range test 14:00 to 18:00 off-day
```

## IPv4 ACL Configuration Commands

### acl

#### Syntax

```
acl number acl-number [ name acl-name ] [ match-order { auto | config } ]
undo acl { all | name acl-name | number acl-number }
```

#### View

System view

#### Default Level

2: System level

#### Parameters

**number** *acl-number*: Specifies the number of the IPv4 ACL, which must be in the following ranges:

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Ethernet frame header ACLs

**name** *acl-name*: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

**match-order**: Specifies the order in which ACL rules are matched.

- **auto**: Performs depth-first match.
- **config**: Performs matching against rules in the order in which they are configured.

**all**: Specifies all IPv4 ACLs.

## Description

Use the **acl** command to enter IPv4 ACL view. If the ACL does not exist, it is created first.

Use the **undo acl** command to remove a specified IPv4 ACL or all IPv4 ACLs.

By default, the match order is **config**.

Note that:

- You can specify a name for an IPv4 ACL only when you create the ACL. After creating an ACL, you cannot specify a name for it, nor can you change or remove its name.
- The name of an IPv4 ACL must be unique among IPv4 ACLs. However, an IPv4 ACL and an IPv6 ACL can share the same name.
- If you specify both an ACL number and an ACL name in one command to enter the view of an existing ACL, be sure that the ACL number and ACL name identify the same ACL.
- You can also use this command to modify the match order of an existing ACL but only when the ACL does not contain any rules.

## Examples

# Create IPv4 ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000]
```

# Create IPv4 ACL 2002, naming it **flow**.

```
<Sysname> system-view
[Sysname] acl number 2002 name flow
[Sysname-acl-basic-2002-flow]
```

# Enter the view of an unnamed IPv4 ACL by specifying its number.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000]
```

# Enter the view of a named IPv4 ACL by specifying its number.

```
<Sysname> system-view
[Sysname] acl number 2002
[Sysname-acl-basic-2002-flow]
```

# Delete the IPv4 ACL numbered 2000.

```
<Sysname> system-view
[Sysname] undo acl number 2000
```

# Delete the IPv4 ACL named **flow**.

```
<Sysname> system-view
[Sysname] undo acl name flow
```

## acl copy

### Syntax

```
acl copy { source-acl-number | name source-acl-name } to { dest-acl-number | name dest-acl-name }
```

## View

System view

## Default Level

2: System level

## Parameters

*source-acl-number*: Number of an existing IPv4 ACL, which must be in the following ranges:

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Ethernet frame header ACLs

**name** *source-acl-name*: Name of an existing IPv4 ACL, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

*dest-acl-number*: Number of a non-existent IPv4 ACL, which must be of the same ACL type as the source ACL and in the following ranges:

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Ethernet frame header ACLs

**name** *dest-acl-name*: Name of a non-existent IPv4 ACL, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion. The system will automatically assign the new ACL a number which is the smallest among the available numbers of the same ACL type.

## Description

Use the **acl copy** command to create an IPv4 ACL by copying an existing IPv4 ACL. The new ACL is of the same ACL type and has the same match order, rules, rule numbering step and descriptions.

Note that:

- The source IPv4 ACL and the destination IPv4 ACL must be of the same type.
- The new ACL does not take the name of the source IPv4 ACL.

## Examples

```
# Copy ACL 2008 to generate ACL 2009.
```

```
<Sysname> system-view  
[Sysname] acl copy 2008 to 2009
```

## acl name

### Syntax

```
acl name acl-name
```

### View

System view

### Default Level

2: System level

## Parameters

*acl-name*: Name of the IPv4 ACL, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

## Description

Use the **acl name** command to enter the view of an existing IPv4 ACL by specifying its name.

## Examples

# Enter the view of the IPv4 ACL named **flow**.

```
<Sysname> system-view
[Sysname] acl name flow
[Sysname-acl-basic-2002-flow]
```

## description (for IPv4)

### Syntax

```
description text
undo description
```

### View

Basic IPv4 ACL view, advanced IPv4 ACL view, Ethernet frame header ACL view

### Default Level

2: System level

## Parameters

*text*: ACL description, a case-sensitive string of 1 to 127 characters.

## Description

Use the **description** command to configure a description for an IPv4 ACL to, for example, describe the purpose of the ACL.

Use the **undo description** command to remove the ACL description.

By default, an IPv4 ACL has no ACL description.

## Examples

# Configure a description for IPv4 ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] description This acl is used in geth 1/0/1
```

# Configure a description for IPv4 ACL 3000.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] description This acl is used in geth 1/0/1
```

# Configure a description for ACL 4000.

```
<Sysname> system-view
```

```
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] description This acl is used in geth 1/0/1
```

## display acl

### Syntax

```
display acl { acl-number | all | name acl-name }
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*acl-number*: IPv4 ACL number, which must be in the following ranges:

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Ethernet frame header ACLs

**all**: Specifies all IPv4 ACLs.

**name *acl-name***: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

### Description

Use the **display acl** command to display information about a specified IPv4 ACL or all IPv4 ACLs.

Note that this command displays ACL rules in the match order.

### Examples

```
# Display information about IPv4 ACL 2001.
<Sysname> display acl 2001
Basic ACL 2001, named flow, 1 rule,
ACL's step is 5
rule 5 permit source 1.1.1.1 0 (5 times matched)
rule 5 comment This rule is used in geth 1/0/1
```

**Table 1-3 display acl** command output description

Field	Description
Basic ACL 2001	The displayed information is about basic IPv4 ACL 2001.
named flow	The name of the ACL is flow.
1 rule	The ACL contains one rule.
ACL's step is 5	The rule numbering step is 5.
5 times matched	There have been five matches for the rule. Only ACL matches performed by software are counted. This field is not displayed when no match is found.

Field	Description
rule 5 comment This rule is used in geth 1/0/1	The description of ACL rule 5 is "This rule is used in geth 1/0/1."

## reset acl counter

### Syntax

```
reset acl counter { acl-number | all | name acl-name }
```

### View

User view

### Default Level

2: System level

### Parameters

*acl-number*: IPv4 ACL number, which must be in the following ranges:

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Ethernet frame header ACLs

**all**: Specifies all IPv4 ACLs except for user-defined ACLs.

**name** *acl-name*: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

### Description

Use the **reset acl counter** command to clear statistics on a specified IPv4 ACL or all IPv4 ACLs that are referenced by upper layer software.

### Examples

```
# Clear statistics on IPv4 ACL 2001.
```

```
<Sysname> reset acl counter 2001
```

```
# Clear statistics on IPv4 ACL flow.
```

```
<Sysname> reset acl counter name flow
```

## rule (basic IPv4 ACL view)

### Syntax

```
rule [ rule-id ] { deny | permit } [ fragment | logging | source { sour-addr sour-wildcard | any } |
time-range time-range-name | vpn-instance vpn-instance-name ] *
undo rule rule-id [ fragment | logging | source | time-range | vpn-instance ] *
```

### View

Basic IPv4 ACL view

## Default Level

2: System level

## Parameters

*rule-id*: Basic IPv4 ACL rule number, in the range 0 to 65534.

**deny**: Drops matched packets.

**permit**: Allows matched packets to pass.

**fragment**: Indicates that the rule applies to only non-first fragments. A rule without this keyword applies to all fragments and non-fragments.

**logging**: Generates log entries for matched packets. This function requires that the module using the ACL support logging.

**source** { *sour-addr sour-wildcard* | **any** }: Specifies a source address. The *sour-addr sour-wildcard* argument combination specifies a source IP address in dotted decimal notation. A wildcard of zero indicates a host address. The **any** keyword indicates any source IP address.

**time-range** *time-range-name*: Specifies the time range in which the rule takes effect. The *time-range-name* argument is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

**vpn-instance** *vpn-instance-name*: Specifies a VPN instance. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Without this combination, the rule applies to only non-VPN packets.

## Description

Use the **rule** command to create a basic IPv4 ACL rule or modify an existing basic IPv4 ACL rule.

Use the **undo rule** command to remove a basic IPv4 ACL rule or remove some criteria from the rule.

If you specify no optional keywords, the **undo rule** command removes the entire ACL rule; otherwise, the command removes only the specified criteria. Before performing the **undo rule** command, you may use the **display acl** command to view the ID of the rule.

When defining ACL rules, you do not need to assign them IDs; the system can automatically assign rule IDs starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is the smallest multiple of the step that is bigger than the current biggest number. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the next rule will be numbered 30.

You cannot create a rule with, or modify a rule to have, the same permit/deny statement as an existing rule in the ACL.

You can only modify the existing rules of an ACL that uses the match order of **config**. When modifying a rule of such an ACL, you may choose to change just some of the settings, in which case the other settings remain the same.

When the ACL match order is **auto**, a newly created rule will be inserted among the existing rules in the depth-first match order. Note that the IDs of the rules still remain the same.



## Note

For a basic IPv4 ACL rule to be referenced by a QoS policy for traffic classification, the **logging** keyword is not supported.

---

Related commands: **display acl**.

## Examples

```
# Create a rule to deny packets with the source IP address 1.1.1.1.
```

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule deny source 1.1.1.1 0
```

## rule (advanced IPv4 ACL view)

### Syntax

```
rule [ rule-id ] { deny | permit } protocol [ { ack ack-value | fin fin-value | psh psh-value | rst rst-value |
syn syn-value | urg urg-value } * | destination { dest-addr dest-wildcard | any } | destination-port
operator port1 [ port2 ] | dscp dscp | fragment | icmp-type { icmp-type icmp-code | icmp-message } |
logging | precedence precedence | reflective | source { sour-addr sour-wildcard | any } | source-port
operator port1 [ port2 ] | time-range time-range-name | tos tos | vpn-instance vpn-instance-name ] *
undo rule rule-id [ { ack | fin | psh | rst | syn | urg } * | destination | destination-port | dscp |
fragment | icmp-type | logging | precedence | reflective | source | source-port | time-range | tos |
vpn-instance ] *
```

### View

Advanced IPv4 ACL view

### Default Level

2: System level

### Parameters

*rule-id*: Advanced IPv4 ACL rule number, in the range 0 to 65534.

**deny**: Drops matched packets.

**permit**: Allows matched packets to pass.

*protocol*: Protocol carried by IP. It can be a number in the range 0 to 255, or in words, **gre** (47), **icmp** (1), **igmp** (2), **ip**, **ipinip** (4), **ospf** (89), **tcp** (6), or **udp** (17). [Table 1-4](#) shows the parameters that can be specified after the *protocol* argument.

**Table 1-4** Match criteria and other rule information for advanced IPv4 ACL rules

Parameters	Function	Description
<b>source</b> { <i>sour-addr</i> <i>sour-wildcard</i>   <b>any</b> }	Specifies a source address.	The <i>sour-addr sour-wildcard</i> argument combination specifies a source IP address in dotted decimal notation. A wildcard of zero indicates a host address. The <b>any</b> keyword indicates any source IP address.
<b>destination</b> { <i>dest-addr</i> <i>dest-wildcard</i>   <b>any</b> }	Specifies a destination address.	The <i>dest-addr dest-wildcard</i> argument combination specifies a destination IP address in dotted decimal notation. A wildcard of zero indicates a host address. The <b>any</b> keyword indicates any destination IP address.
<b>precedence</b> <i>precedence</i>	Specifies an IP precedence value.	The <i>precedence</i> argument can be a number in the range 0 to 7, or in words, <b>routine</b> (0), <b>priority</b> (1), <b>immediate</b> (2), <b>flash</b> (3), <b>flash-override</b> (4), <b>critical</b> (5), <b>internet</b> (6), or <b>network</b> (7).
<b>tos</b> <i>tos</i>	Specifies a ToS preference.	The <i>tos</i> argument can be a number in the range 0 to 15, or in words, <b>max-reliability</b> (2), <b>max-throughput</b> (4), <b>min-delay</b> (8), <b>min-monetary-cost</b> (1), or <b>normal</b> (0).
<b>dscp</b> <i>dscp</i>	Specifies a DSCP priority.	The <i>dscp</i> argument can be a number in the range 0 to 63, or in words, <b>af11</b> (10), <b>af12</b> (12), <b>af13</b> (14), <b>af21</b> (18), <b>af22</b> (20), <b>af23</b> (22), <b>af31</b> (26), <b>af32</b> (28), <b>af33</b> (30), <b>af41</b> (34), <b>af42</b> (36), <b>af43</b> (38), <b>cs1</b> (8), <b>cs2</b> (16), <b>cs3</b> (24), <b>cs4</b> (32), <b>cs5</b> (40), <b>cs6</b> (48), <b>cs7</b> (56), <b>default</b> (0), or <b>ef</b> (46).
<b>logging</b>	Specifies to log matched packets.	This function requires that the module using the ACL support logging.
<b>reflective</b>	Specifies that the rule be reflective.	A rule with the <b>reflective</b> keyword can be defined only for TCP, UDP, or ICMP packets and can only be a permit statement.
<b>vpn-instance</b> <i>vpn-instance-name</i>	Specifies a VPN instance.	The <i>vpn-instance-name</i> argument is a case-sensitive string of 1 to 31 characters. Without this combination, the rule applies to only non-VPN packets.
<b>fragment</b>	Indicates that the rule applies to only non-first fragments.	Without this keyword, the rule applies to all fragments and non-fragments.
<b>time-range</b> <i>time-range-name</i>	Specifies the time range in which the rule takes effect.	The <i>time-range-name</i> argument is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

Setting the *protocol* argument to **tcp** or **udp**, you may define the parameters shown in [Table 1-5](#).

**Table 1-5** TCP/UDP-specific parameters for advanced IPv4 ACL rules

Parameters	Function	Description
<b>source-port</b> <i>operator port1 [ port2 ]</i>	Specifies one or more UDP or TCP source ports.	<p>The <i>operator</i> argument can be <b>lt</b> (lower than), <b>gt</b> (greater than), <b>eq</b> (equal to), <b>neq</b> (not equal to), or <b>range</b> (inclusive range).</p> <p>The <i>port1</i> and <i>port2</i> arguments are TCP or UDP port numbers in the range 0 to 65535. <i>port2</i> is needed only when the <i>operator</i> argument is <b>range</b>.</p> <p>TCP port numbers can be represented in these words: <b>chargen</b> (19), <b>bgp</b> (179), <b>cmd</b> (514), <b>daytime</b> (13), <b>discard</b> (9), <b>domain</b> (53), <b>echo</b> (7), <b>exec</b> (512), <b>finger</b> (79), <b>ftp</b> (21), <b>ftp-data</b> (20), <b>gopher</b> (70), <b>hostname</b> (101), <b>irc</b> (194), <b>klogin</b> (543), <b>kshell</b> (544), <b>login</b> (513), <b>lpd</b> (515), <b>nntp</b> (119), <b>pop2</b> (109), <b>pop3</b> (110), <b>smtp</b> (25), <b>sunrpc</b> (111), <b>tacacs</b> (49), <b>talk</b> (517), <b>telnet</b> (23), <b>time</b> (37), <b>uucp</b> (540), <b>whois</b> (43), and <b>www</b> (80).</p> <p>UDP port numbers can be represented in these words: <b>biff</b> (512), <b>bootpc</b> (68), <b>bootps</b> (67), <b>discard</b> (9), <b>dns</b> (53), <b>dnsix</b> (90), <b>echo</b> (7), <b>mobilip-ag</b> (434), <b>mobilip-mn</b> (435), <b>nameserver</b> (42), <b>netbios-dgm</b> (138), <b>netbios-ns</b> (137), <b>netbios-ssn</b> (139), <b>ntp</b> (123), <b>rip</b> (520), <b>snmp</b> (161), <b>snmptrap</b> (162), <b>sunrpc</b> (111), <b>syslog</b> (514), <b>tacacs-ds</b> (65), <b>talk</b> (517), <b>tftp</b> (69), <b>time</b> (37), <b>who</b> (513), and <b>xdmcp</b> (177).</p> <p>With the <b>range</b> operator, the value of <i>port2</i> does not need to be greater than that of <i>port1</i> because the switch can automatically judge the value range. If the two values are the same, the switch will convert the operator <b>range</b> to <b>eq</b>.</p> <p>Note that if you specify a combination of <b>lt 1</b> or <b>gt 65534</b>, the switch will convert it to <b>eq 0</b> or <b>eq 65535</b>.</p>
<b>destination-port</b> <i>operator port1 [ port2 ]</i>	Specifies one or more UDP or TCP destination ports.	
{ <b>ack</b> <i>ack-value</i>   <b>fin</b> <i>fin-value</i>   <b>psh</b> <i>psh-value</i>   <b>rst</b> <i>rst-value</i>   <b>syn</b> <i>syn-value</i>   <b>urg</b> <i>urg-value</i> } *	Specifies one or more TCP flags	<p>Parameters specific to TCP.</p> <p>The value for each argument can be 0 or 1.</p>

Setting the *protocol* argument to **icmp**, you may define the parameters shown in [Table 1-6](#).

**Table 1-6** ICMP-specific parameters for advanced IPv4 ACL rules

Parameters	Function	Description
<b>icmp-type</b> { <i>icmp-type</i> <i>icmp-code</i>   <i>icmp-message</i> }	Specifies the ICMP message type and code.	The <i>icmp-type</i> argument ranges from 0 to 255. The <i>icmp-code</i> argument ranges from 0 to 255. The <i>icmp-message</i> argument specifies a message name. Supported ICMP message names and their corresponding type and code values are listed in <a href="#">Table 1-7</a> .

**Table 1-7** ICMP message names supported in advanced IPv4 ACL rules

ICMP message name	Type	Code
echo	8	0
echo-reply	0	0
fragmentneed-DFset	3	4
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1
information-reply	16	0
information-request	15	0
net-redirect	5	0
net-tos-redirect	5	2
net-unreachable	3	0
parameter-problem	12	0
port-unreachable	3	3
protocol-unreachable	3	2
reassembly-timeout	11	1
source-quench	4	0
source-route-failed	3	5
timestamp-reply	14	0
timestamp-request	13	0
ttl-exceeded	11	0

**Description**

Use the **rule** command to create an advanced IPv4 ACL rule or modify an existing advanced IPv4 ACL rule.

Use the **undo rule** command to remove an advanced IPv4 ACL rule or remove some criteria from the rule.

If you specify no optional keywords, the **undo rule** command removes the entire ACL rule; otherwise, the command removes only the specified criteria. Before performing the **undo rule** command, you may use the **display acl** command to view the ID of the rule.

When defining ACL rules, you do not need to assign them IDs; the system can automatically assign rule IDs starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is the smallest multiple of the step that is bigger than the current biggest number. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the next rule will be numbered 30.

You cannot create a rule with, or modify a rule to have, the same permit/deny statement as an existing rule in the ACL.

You can only modify the existing rules of an ACL that uses the match order of **config**. When modifying a rule of such an ACL, you may choose to change just some of the settings, in which case the other settings remain the same.

When the ACL match order is **auto**, a newly created rule will be inserted among the existing rules in the depth-first match order. Note that the IDs of the rules still remain the same.

If the ACL match order is **auto**, rules are displayed in the depth-first match order rather than by rule number.



#### Note

For an advanced IPv4 ACL to be referenced by a QoS policy for traffic classification:

- The **logging** and **reflective** keywords are not supported.
- The operator cannot be **neq** if the ACL is for the inbound traffic.
- The operator cannot be **gt**, **lt**, **neq**, or **range** if the ACL is for the outbound traffic.

---

Related commands: **display acl**.

## Examples

```
# Define a rule to permit TCP packets with the destination port of 80 from 129.9.0.0 to 202.38.160.0.
<Sysname> system-view
[Sysname] acl number 3101
[Sysname-acl-adv-3101] rule permit tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0
0.0.0.255 destination-port eq 80
```

## rule (Ethernet frame header ACL view)

### Syntax

```
rule [ rule-id ] { deny | permit } [ cos vlan-pri | dest-mac dest-addr dest-mask | isap isap-code
isap-wildcard | source-mac sour-addr source-mask | time-range time-range-name | type type-code
type-wildcard ] *
```

```
undo rule rule-id
```

### View

Ethernet frame header ACL view

## Default Level

2: System level

## Parameters

*rule-id*: Ethernet frame header ACL rule number, in the range 0 to 65534.

**deny**: Drops matched packets.

**permit**: Allows matched packets to pass.

**cos** *vlan-pri*: Defines an 802.1p priority. The *vlan-pri* argument can be a number in the range 0 to 7 or in words, **best-effort** (0), **background** (1), **spare** (2), **excellent-effort** (3), **controlled-load** (4), **video** (5), **voice** (6), or **network-management** (7).

**dest-mac** *dest-addr dest-mask*: Specifies a destination MAC address range. The *dest-addr* and *dest-mask* arguments indicate a destination MAC address and mask in xxxx-xxxx-xxxx format.

**isap** *isap-code isap-wildcard*: Defines the DSAP and SSAP fields in the LLC encapsulation. The *isap-code* argument is a 16-bit hexadecimal number indicating the frame encapsulation. The *isap-wildcard* argument is a 16-bit hexadecimal number indicating the wildcard of the LSAP code. Support for this keyword and argument combination depends on the device model.

**source-mac** *sour-addr source-mask*: Specifies a source MAC address range. The *sour-addr* and *sour-mask* arguments indicate a source MAC address and mask in xxxx-xxxx-xxxx format.

**time-range** *time-range-name*: Specifies the time range in which the rule takes effect. The *time-range-name* argument is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

**type** *type-code type-wildcard*: Defines a link layer protocol. The *type-code* argument is a 16-bit hexadecimal number indicating the frame type. It corresponds to the *type-code* field in Ethernet\_II and Ethernet\_SNAP frames. The *type-wildcard* argument is a 16-bit hexadecimal number indicating the wildcard. Support for this keyword and argument combination depends on the device model.

## Description

Use the **rule** command to create an Ethernet frame header ACL rule or modify an existing Ethernet frame header ACL rule.

Use the **undo rule** command to remove an Ethernet frame header ACL rule.

When defining ACL rules, you do not need to assign them IDs; the system can automatically assign rule IDs starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is the smallest multiple of the step that is bigger than the current biggest number. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the next rule will be numbered 30.

Before performing the **undo rule** command to remove an Ethernet frame header ACL rule, you may use the **display acl** command to view the ID of the rule.

You cannot create a rule with, or modify a rule to have, the same permit/deny statement as an existing rule in the ACL.

You can only modify the existing rules of an ACL that uses the match order of **config**. When modifying a rule of such an ACL, you may choose to change just some of the settings, in which case the other settings remain the same.

When the ACL match order is **auto**, a newly created rule will be inserted among the existing rules in the depth-first match order. Note that the IDs of the rules still remain the same.

If the ACL match order is **auto**, rules are displayed in the depth-first match order rather than by rule number.



#### Note

For an Ethernet frame header ACL to be referenced by a QoS policy for traffic classification, the **Isap** keyword is not supported.

---

Related commands: **display acl**.

### Examples

# Create a rule to deny packets with the 802.1p priority of 3.

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] rule deny cos 3
```

### rule comment (for IPv4)

#### Syntax

```
rule rule-id comment text
undo rule rule-id comment
```

#### View

Basic IPv4 ACL view, advanced IPv4 ACL view, Ethernet frame header ACL view

#### Default Level

2: System level

#### Parameters

*rule-id*: IPv4 ACL rule number, in the range 0 to 65534.

*text*: IPv4 ACL rule description, a case-sensitive string of 1 to 127 characters.

#### Description

Use the **rule comment** command to configure a description for an existing IPv4 ACL rule or modify the description of an IPv4 ACL rule. You may use the rule description to, for example, describe the purpose of the ACL rule or the parameters it contains.

Use the **undo rule comment** command to remove the ACL rule description.

By default, an IPv4 ACL rule has no rule description.

### Examples

# Create a rule in ACL 2000 and define the rule description.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule 0 deny source 1.1.1.1 0
```

```

[Sysname-acl-basic-2000] rule 0 comment This rule is used in geth 1/0/1

# Create a rule in ACL 3000 and define the rule description.

<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule 0 permit ip source 1.1.1.1 0
[Sysname-acl-adv-3000] rule 0 comment This rule is used in geth 1/0/1

# Create a rule in ACL 4000 and define the rule description.

<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] rule 0 deny cos 3
[Sysname-acl-ethernetframe-4000] rule 0 comment This rule is used in geth 1/0/1

```

## step (for IPv4)

### Syntax

```

step step-value
undo step

```

### View

Basic IPv4 ACL view, advanced IPv4 ACL view, Ethernet frame header ACL view

### Default Level

2: System level

### Parameters

*step-value*: IPv4 ACL rule numbering step, in the range 1 to 20.

### Description

Use the **step** command to set a rule numbering step for an ACL.

Use the **undo step** command to restore the default.

By default, the rule numbering step is five.

### Examples

# Set the rule numbering step to 2 for ACL 2000.

```

<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] step 2

```

# Set the rule numbering step to 2 for ACL 3000.

```

<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] step 2

```

# Set the rule numbering step to 2 for ACL 4000.

```

<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] step 2

```

# IPv6 ACL Configuration Commands

## acl ipv6

### Syntax

```
acl ipv6 number acl6-number [ name acl6-name ] [ match-order { auto | config } ]  
undo acl ipv6 { all | name acl6-name | number acl6-number }
```

### View

System view

### Default Level

2: System level

### Parameters

**number** *acl6-number*: Specifies the number of the IPv6 ACL, which must be in the following ranges:

- 2000 to 2999 for basic IPv6 ACLs
- 3000 to 3999 for advanced IPv6 ACLs

**name** *acl6-name*: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

**match-order**: Specifies the order in which ACL rules are matched.

**auto**: Performs depth-first match.

**config**: Performs matching against rules in the order in which they are configured.

**all**: Specifies all IPv6 ACLs.

### Description

Use the **acl ipv6** command to enter IPv6 ACL view. If the ACL does not exist, it is created first.

Use the **undo acl ipv6** command to remove a specified IPv6 ACL or all IPv6 ACLs.

By default, the match order is **config**.

Note that:

- You can specify a name for an IPv6 ACL only when you create the ACL. After creating an ACL, you cannot specify a name for it, nor can you change or remove its name.
- The name of an IPv6 ACL must be unique among IPv6 ACLs. However, an IPv4 ACL and an IPv6 ACL can share the same name.
- If you specify both an ACL number and an ACL name in one command to enter the view of an existing ACL, be sure that the ACL number and ACL name identify the same ACL.
- You can also use this command to modify the match order of an existing IPv6 ACL, but only when the ACL does not contain any rules.

### Examples

```
# Create IPv6 ACL 2000.  
<Sysname> system-view  
[Sysname] acl ipv6 number 2000  
[Sysname-acl6-basic-2000]
```

# Create IPv6 ACL 2002, giving the ACL a name of flow.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2002 name flow
[Sysname-acl6-basic-2002-flow]
```

# Enter the view of an IPv6 ACL that has no name by specifying its number.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000]
```

# Enter the view of an IPv6 ACL that has a name by specifying its number.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2002
[Sysname-acl6-basic-2002-flow]
```

# Delete the IPv6 ACL with the number of 2000.

```
<Sysname> system-view
[Sysname] undo acl ipv6 number 2000
```

# Delete the IPv6 ACL named flow.

```
<Sysname> system-view
[Sysname] undo acl ipv6 name flow
```

## acl ipv6 copy

### Syntax

```
acl ipv6 copy { source-acl6-number | name source-acl6-name } to { dest-acl6-number | name dest-acl6-name }
```

### View

System view

### Default Level

2: System level

### Parameters

*source-acl6-number*: Number of an existing IPv6 ACL, which must be in the following ranges:

- 2000 to 2999 for basic IPv6 ACLs,
- 3000 to 3999 for advanced IPv6 ACLs.

**name** *source-acl6-name*: Name of an existing IPv6 ACL, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

*dest-acl6-number*: Number of a non-existent IPv6 ACL, which must be in the following ranges:

- 2000 to 2999 for basic IPv6 ACLs
- 3000 to 3999 for advanced IPv6 ACLs

**name** *dest-acl6-name*: Name for the new IPv6 ACL, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion. The system will automatically assign the new ACL a number which is the smallest one among the available numbers of the same ACL type.

## Description

Use the **acl ipv6 copy** command to create an IPv6 ACL by copying an existing IPv6 ACL. The new ACL is of the same ACL type and has the same match order, rules, rule numbering step and descriptions.

Note that:

- The source IPv6 ACL and the destination IPv6 ACL must be of the same type.
- The new ACL does not take the name of the source IPv6 ACL.

## Examples

```
# Copy ACL 2008 to generate ACL 2009.
<Sysname> system-view
[Sysname] acl ipv6 copy 2008 to 2009
```

## acl ipv6 name

### Syntax

```
acl ipv6 name acl6-name
```

### View

System view

### Default Level

2: System level

### Parameters

*acl6-name*: Name of the IPv6 ACL, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

## Description

Use the **acl ipv6 name** command to enter the view of an existing IPv6 ACL by specifying its name.

## Examples

```
# Enter the view of the IPv6 ACL named flow.
<Sysname> system-view
[Sysname] acl ipv6 name flow
[Sysname-acl6-basic-2002-flow]
```

## description (for IPv6)

### Syntax

```
description text
undo description
```

### View

Basic IPv6 ACL view, advanced IPv6 ACL view

## Default Level

2: System level

## Parameters

*text*: ACL description, a case-sensitive string of 1 to 127 characters.

## Description

Use the **description** command to configure a description for an IPv6 ACL to, for example, describe the purpose of the ACL.

Use the **undo description** command to remove the IPv6 ACL description.

By default, an IPv6 ACL has no ACL description.

## Examples

# Configure a description for IPv6 ACL 2000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] description This acl is used in geth 1/0/1
```

# Configure a description for IPv6 ACL 3000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] description This acl is used in geth 1/0/1
```

## display acl ipv6

### Syntax

```
display acl ipv6 { acl6-number | all | name acl6-name }
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*acl6-number*: IPv6 ACL number, which must be in the following ranges:

- 2000 to 2999 for basic IPv6 ACLs
- 3000 to 3999 for advanced IPv6 ACLs

**all**: Specifies all IPv6 ACLs.

**name** *acl6-name*: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

### Description

Use the **display acl ipv6** command to display information about a specified IPv6 ACL or all IPv6 ACLs.

Note that this command displays ACL rules in the match order.

## Examples

```
# Display information about IPv6 ACL 2001.
<Sysname> display acl ipv6 2001
Basic IPv6 ACL 2001, named flow, 1 rule,
ACL's step is 5
rule 0 permit source 1::2/128 (5 times matched)
rule 0 comment This rule is used in geth 1/0/1
```

**Table 1-8 display acl ipv6 command output description**

Field	Description
Basic IPv6 ACL 2001	The displayed information is about basic IPv6 ACL 2001.
named flow	The name of the ACL is flow.
1 rule	The ACL contains one rule.
ACL's step is 5	The rules in this ACL are numbered in steps of 5.
5 times matched	There have been five matches for the rule. Only ACL matches performed by software are counted. This field is not displayed when no match is found.
rule 0 comment This rule is used in geth 1/0/1	The description of ACL rule 0 is "This rule is used in geth 1/0/1."

## reset acl ipv6 counter

### Syntax

```
reset acl ipv6 counter { acl6-number | all | name acl6-name }
```

### View

User view

### Default Level

2: System level

### Parameters

*acl6-number*: IPv6 ACL number, which must be in the following ranges:

- 2000 to 2999 for basic IPv6 ACLs,
- 3000 to 3999 for advanced IPv6 ACLs.

**all**: Specifies all basic and advanced IPv6 ACLs.

**name** *acl6-name*: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

### Description

Use the **reset acl ipv6 counter** command to clear statistics on a specified IPv6 ACL or all basic and advanced IPv6 ACLs.

## Examples

# Clear the statistics on IPv6 ACL 2001, which is referenced by upper layer software.

```
<Sysname> reset acl ipv6 counter 2001
```

# Clear the statistics on IPv6 ACL flow, which is referenced by upper layer software.

```
<Sysname> reset acl ipv6 counter name flow
```

## rule (basic IPv6 ACL view)

### Syntax

```
rule [ rule-id ] { deny | permit } [ fragment | logging | source { ipv6-address prefix-length |  
ipv6-address/prefix-length | any } | time-range time-range-name ] *
```

```
undo rule rule-id [ fragment | logging | source | time-range ] *
```

### View

Basic IPv6 ACL view

### Default Level

2: System level

### Parameters

*rule-id*: IPv6 ACL rule number, in the range 0 to 65534.

**deny**: Drops matched packets.

**permit**: Allows matched packets to pass.

**fragment**: Indicates that the rule applies to only non-first fragments. A rule without this keyword applies to all fragments and non-fragments.

**logging**: Logs matched packets. This function requires that the module using the ACL support logging.

**source** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* | **any** }: Specifies a source address. The *ipv6-address* and *prefix-length* arguments specify a source IPv6 address and its address prefix length in the range 1 to 128. The **any** keyword indicates any IPv6 source address.

**time-range** *time-range-name*: Specifies the time range in which the rule takes effect. The *time-range-name* argument is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

### Description

Use the **rule** command to create a basic IPv6 ACL rule or modify an existing basic IPv6 ACL rule.

Use the **undo rule** command to remove a basic IPv6 ACL rule or remove some criteria from the rule.

If you specify no optional keywords, the **undo rule** command removes the entire ACL rule; otherwise, the command removes only the specified criteria. Before performing the **undo rule** command, you may need to use the **display acl ipv6** command to view the ID of the rule.

When defining ACL rules, you do not need to assign them IDs; the system can automatically assign rule IDs starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is the smallest multiple of the step that is bigger than the current biggest number. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the next rule will be numbered 30.

You cannot create a rule with, or modify a rule to have, the same permit/deny statement as an existing rule in the ACL.

You can only modify the existing rules of an ACL that uses the match order of **config**. When modifying a rule of such an ACL, you may choose to change just some of the settings, in which case the other settings remain the same.

When the ACL match order is **auto**, a newly created rule will be inserted among the existing rules in the depth-first match order. Note that the IDs of the rules still remain the same.



#### Note

For a basic IPv6 ACL to be referenced by a QoS policy for traffic classification, the **logging** and **fragment** keywords are not supported.

---

Related commands: **display acl ipv6**.

### Examples

# Create IPv6 ACL 2000 and add two rules.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source 2030:5060::9050/64
[Sysname-acl6-basic-2000] rule 8 deny source fe80:5060::8050/96
```

### rule (advanced IPv6 ACL view)

#### Syntax

```
rule [ rule-id ] { deny | permit } protocol [ { ack ack-value | fin fin-value | psh psh-value | rst rst-value |
syn syn-value | urg urg-value } * | destination { dest dest-prefix | dest/dest-prefix | any } |
destination-port operator port1 [ port2 ] | dscp dscp | fragment | icmpv6-type { icmpv6-type
icmpv6-code | icmpv6-message } | logging | source { source source-prefix | source/source-prefix | any }
| source-port operator port1 [ port2 ] | time-range time-range-name ] *
undo rule rule-id [ { ack | fin | psh | rst | syn | urg } * | destination | destination-port | dscp |
fragment | icmpv6-type | logging | source | source-port | time-range ] *
```

#### View

Advanced IPv6 ACL view

#### Default Level

2: System level

#### Parameters

**rule-id**: IPv6 ACL rule number, in the range 0 to 65534.

**deny**: Drops matched packets.

**permit**: Allows matched packets to pass.

*protocol*: Protocol carried over IPv6. It can be a number in the range 0 to 255, or in words, **gre** (47), **icmpv6** (58), **ipv6**, **ipv6-ah** (51), **ipv6-esp** (50), **ospf** (89), **tcp** (6), or **udp** (17). [Table 1-9](#) shows the parameters that can be specified after the *protocol* argument.

**Table 1-9** Match criteria and other rule information for advanced IPv6 ACL rules

Parameters	Function	Description
<b>source</b> { <i>source</i> <i>source-prefix</i>   <i>source/source-prefix</i>   <b>any</b> }	Specifies a source IPv6 address.	The <i>source</i> and <i>source-prefix</i> arguments specify an IPv6 source address and its prefix length in the range 1 to 128. The <b>any</b> keyword indicates any IPv6 source address.
<b>destination</b> { <i>dest</i> <i>dest-prefix</i>   <i>dest/dest-prefix</i>   <b>any</b> }	Specifies a destination IPv6 address.	The <i>dest</i> and <i>dest-prefix</i> arguments specify a destination IPv6 address, and its prefix length in the range 1 to 128. The <b>any</b> keyword indicates any IPv6 destination address.
<b>dscp</b> <i>dscp</i>	Specifies a DSCP preference	The <i>dscp</i> argument can be a number in the range 0 to 63, or in words, <b>af11</b> (10), <b>af12</b> (12), <b>af13</b> (14), <b>af21</b> (18), <b>af22</b> (20), <b>af23</b> (22), <b>af31</b> (26), <b>af32</b> (28), <b>af33</b> (30), <b>af41</b> (34), <b>af42</b> (36), <b>af43</b> (38), <b>cs1</b> (8), <b>cs2</b> (16), <b>cs3</b> (24), <b>cs4</b> (32), <b>cs5</b> (40), <b>cs6</b> (48), <b>cs7</b> (56), <b>default</b> (0), or <b>ef</b> (46).
<b>logging</b>	Specifies to log matched packets	This function requires that the module using the ACL support logging.
<b>fragment</b>	Indicates that the rule applies to only non-first fragments.	Without this keyword, the rule applies to all fragments and non-fragments.
<b>time-range</b> <i>time-range-name</i>	Specifies the time range in which the rule takes effect.	The <i>time-range-name</i> argument is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

Setting the *protocol* argument to **tcp** or **udp**, you may define the parameters shown in [Table 1-10](#).

**Table 1-10** TCP/UDP-specific parameters for advanced IPv6 ACL rules

Parameters	Function	Description
<b>source-port</b> <i>operator port1 [ port2 ]</i>	Specifies one or more UDP or TCP source ports.	<p>The <i>operator</i> argument can be <b>lt</b> (lower than), <b>gt</b> (greater than), <b>eq</b> (equal to), <b>neq</b> (not equal to), or <b>range</b> (inclusive range).</p> <p>The <i>port1</i> and <i>port2</i> arguments are TCP or UDP port numbers in the range 0 to 65535. <i>port2</i> is needed only when the <i>operator</i> argument is <b>range</b>.</p> <p>TCP port numbers can be represented in these words: <b>chargen</b> (19), <b>bgp</b> (179), <b>cmd</b> (514), <b>daytime</b> (13), <b>discard</b> (9), <b>domain</b> (53), <b>echo</b> (7), <b>exec</b> (512), <b>finger</b> (79), <b>ftp</b> (21), <b>ftp-data</b> (20), <b>gopher</b> (70), <b>hostname</b> (101), <b>irc</b> (194), <b>klogin</b> (543), <b>kshell</b> (544), <b>login</b> (513), <b>lpd</b> (515), <b>nntp</b> (119), <b>pop2</b> (109), <b>pop3</b> (110), <b>smtp</b> (25), <b>sunrpc</b> (111), <b>tacacs</b> (49), <b>talk</b> (517), <b>telnet</b> (23), <b>time</b> (37), <b>uucp</b> (540), <b>whois</b> (43), and <b>www</b> (80).</p> <p>UDP port numbers can be represented in these words: <b>biff</b> (512), <b>bootpc</b> (68), <b>bootps</b> (67), <b>discard</b> (9), <b>dns</b> (53), <b>dnsix</b> (90), <b>echo</b> (7), <b>mobilip-ag</b> (434), <b>mobilip-mn</b> (435), <b>nameserver</b> (42), <b>netbios-dgm</b> (138), <b>netbios-ns</b> (137), <b>netbios-ssn</b> (139), <b>ntp</b> (123), <b>rip</b> (520), <b>snmp</b> (161), <b>snmptrap</b> (162), <b>sunrpc</b> (111), <b>syslog</b> (514), <b>tacacs-ds</b> (65), <b>talk</b> (517), <b>tftp</b> (69), <b>time</b> (37), <b>who</b> (513), and <b>xdmcp</b> (177).</p> <p>With the <b>range</b> operator, the value of <i>port2</i> does not need to be greater than that of <i>port1</i> because the switch can automatically judge the value range. If the two values are the same, the switch will convert the operator <b>range</b> to <b>eq</b>.</p> <p>Note that if you specify a combination of <b>lt</b> 1 or <b>gt</b> 65534, the switch will convert it to <b>eq</b> 0 or <b>eq</b> 65535.</p>
<b>destination-port</b> <i>operator port1 [ port2 ]</i>	Specifies one or more UDP or TCP destination ports.	
{ <b>ack</b> <i>ack-value</i>   <b>fin</b> <i>fin-value</i>   <b>psh</b> <i>psh-value</i>   <b>rst</b> <i>rst-value</i>   <b>syn</b> <i>syn-value</i>   <b>urg</b> <i>urg-value</i> } *	Specifies one or more TCP flags.	<p>Parameters specific to TCP.</p> <p>The value for each argument can be 0 or 1.</p>

Setting the *protocol* argument to **icmpv6**, you may define the parameters shown in [Table 1-11](#).

**Table 1-11** ICMPv6-specific parameters for advanced IPv6 ACL rules

Parameters	Function	Description
<b>icmpv6-type</b> { <i>icmpv6-type</i> <i>icmpv6-code</i>   <i>icmpv6-message</i> }	Specifies the ICMPv6 message type and code.	The <i>icmpv6-type</i> argument ranges from 0 to 255. The <i>icmpv6-code</i> argument ranges from 0 to 255. The <i>icmpv6-message</i> argument specifies a message name. Supported ICMP message names and their corresponding type and code values are listed in <a href="#">Table 1-12</a> .

**Table 1-12** ICMPv6 message names supported in advanced IPv6 ACL rules

ICMPv6 message name	Type	Code
redirect	137	0
echo-request	128	0
echo-reply	129	0
err-Header-field	4	0
frag-time-exceeded	3	1
hop-limit-exceeded	3	0
host-admin-prohib	1	1
host-unreachable	1	3
neighbor-advertisement	136	0
neighbor-solicitation	135	0
network-unreachable	1	0
packet-too-big	2	0
port-unreachable	1	4
router-advertisement	134	0
router-solicitation	133	0
unknown-ipv6-opt	4	2
unknown-next-hdr	4	1

**Description**

Use the **rule** command to create an advanced IPv6 ACL rule or modify an existing advanced IPv6 ACL rule.

Use the **undo rule** command to remove an advanced IPv6 ACL rule or remove some criteria from the rule.

If you specify no optional keywords, the **undo rule** command removes the entire ACL rule; otherwise, the command removes only the specified criteria. Before performing the **undo rule** command, you may need to use the **display acl ipv6** command to view the ID of the rule.

When defining ACL rules, you do not need to assign them IDs; the system can automatically assign rule IDs starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is the smallest multiple of the step that is bigger than the current biggest number. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the next rule will be numbered 30.

You cannot create a rule with, or modify a rule to have, the same permit/deny statement as an existing rule in the ACL.

You can only modify the existing rules of an ACL that uses the match order of **config**. When modifying a rule of such an ACL, you may choose to change just some of the settings, in which case the other settings remain the same.

When the ACL match order is **auto**, a newly created rule will be inserted among the existing rules in the depth-first match order. Note that the IDs of the rules still remain the same.



#### Note

For an advanced IPv6 ACL to be referenced by a QoS policy for traffic classification,

- The **logging** and **fragment** keywords are not supported.
- The operator cannot be **neq** if the ACL is for the inbound traffic.
- The operator cannot be **gt**, **lt**, **neq**, or **range** if the ACL is for the outbound traffic.

---

Related commands: **display acl ipv6**.

## Examples

```
# Configure IPv6 ACL 3000 to permit TCP packets with the source address of 2030:5060::9050/64.
```

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule permit tcp source 2030:5060::9050/64
```

## rule comment (for IPv6)

### Syntax

```
rule rule-id comment text
```

```
undo rule rule-id comment
```

### View

Basic IPv6 ACL view, advanced IPv6 ACL view

### Default Level

2: System level

### Parameters

*rule-id*: IPv6 ACL rule number, in the range 0 to 65534.

*text*: IPv6 ACL rule description, a case-sensitive string of 1 to 127 characters.

## Description

Use the **rule comment** command to configure a description for an existing IPv6 ACL rule or modify the description of an IPv6 ACL rule. You may use the rule description to, for example, describe the purpose of the ACL rule.

Use the **undo rule comment** command to remove the IPv6 ACL rule description.

By default, an IPv6 ACL rule has no rule description.

## Examples

# Define a rule in IPv6 ACL 2000 and create a description for the rule.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule 0 permit source 2030:5060::9050/64
[Sysname-acl6-basic-2000] rule 0 comment This rule is used in geth 1/0/1
```

# Define a rule in IPv6 ACL 3000 and create a description for the rule.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule 0 permit tcp source 2030:5060::9050/64
[Sysname-acl6-adv-3000] rule 0 comment This rule is used in geth 1/0/1
```

## step (for IPv6)

### Syntax

**step** *step-value*

**undo step**

### View

Basic IPv6 ACL view, advanced IPv6 ACL view

### Default Level

2: System level

### Parameters

*step-value*: IPv6 ACL rule numbering step, in the range 1 to 20.

## Description

Use the **step** command to set a rule numbering step for an IPv6 ACL.

Use the **undo step** command to restore the default.

By default, the rule numbering step is five.

## Examples

# Set the rule numbering step to 2 for IPv6 ACL 2000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] step 2
```

# Set the rule numbering step to 2 for IPv6 ACL 3000.

```
<Sysname> system-view  
[Sysname] acl ipv6 number 3000  
[Sysname-acl6-adv-3000] step 2
```

# System Volume Organization

---

## Manual Version

6W100-20090120

## Product Version

Release 2202

## Organization

The System Volume is organized as follows:

Features	Description
Login	<p>Upon logging into a device, you can configure user interface properties and manage the system conveniently. This document introduces the commands for:</p> <ul style="list-style-type: none"><li>• The user interface and common configurations</li><li>• Console Port Login Configuration</li><li>• Telnet Login Configuration</li><li>• Logging in Through Web-based Network Management System Configuration</li><li>• Specifying Source for Telnet Packets</li><li>• Controlling Login Users</li></ul>
Basic System Configuration	<p>Basic system configuration involves the configuration of device name, system clock, welcome message, and user privilege levels. This document introduces the commands for:</p> <ul style="list-style-type: none"><li>• Configuring the device name, the system clock and a Banner</li><li>• Configuring CLI Hotkeys</li><li>• Configuring User Privilege Levels and Command Levels</li><li>• Multiple-screen output configuring</li></ul>

Features	Description
Device Management	<p>Through the device management function, you can view the current condition of your device and configure running parameters. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• Rebooting a device</li> <li>• Configuring the scheduled automatic execution function</li> <li>• Specifying a file for the next device boot</li> <li>• Upgrading Boot ROM</li> <li>• Configuring a detection interval</li> <li>• Configuring temperature alarm thresholds for a board</li> <li>• Clearing the 16-bit interface indexes not used in the current system</li> <li>• Configuring the system load sharing function</li> <li>• Configuring the traffic forwarding mode of SRPUs</li> <li>• Configuring the working mode of EA LPUs</li> <li>• Enabling the port down function globally</li> <li>• Enabling expansion memory data recovery function on a board</li> <li>• Identifying and diagnosing pluggable transceivers</li> </ul>
File System Management	<p>A major function of the file system is to manage storage devices, mainly including creating the file system, creating, deleting, modifying and renaming a file or a directory and opening a file. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• File system management</li> <li>• Configuration File Management</li> <li>• FTP configuration</li> <li>• TFTP configuration</li> </ul>
HTTP	<p>Hypertext Transfer Protocol (HTTP) is used for transferring web page information across the Internet. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• HTTP Configuration</li> <li>• HTTPS Configuration</li> </ul>
SNMP	<p>Simple network management protocol (SNMP) offers a framework to monitor network devices through TCP/IP protocol suite. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• Basic SNMP function configuration</li> <li>• SNMP log configuration</li> <li>• Trap configuration</li> <li>• MIB style configuration</li> </ul>
RMON	<p>RMON provides an efficient means of monitoring subnets and allows SNMP to monitor remote network devices in a more proactive and effective way. This document introduces the commands for RMON configuration (event group, history group, alarm group, private alarm group)</p>
MAC Address Table Management	<p>A switch maintains a MAC address table for fast forwarding packets. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• Configuring MAC Address Entries</li> <li>• Disabling Global MAC Address Learning</li> <li>• Disabling MAC Address Learning on a VLAN</li> <li>• Configuring MAC Address Aging Timer</li> <li>• Configuring the Maximum Number of MAC Addresses an Ethernet Port or a Port Group Can Learn</li> </ul>

Features	Description
System Maintenance and Debugging	For the majority of protocols and features supported, the system provides corresponding debugging information to help users diagnose errors. This document introduces the commands for maintenance and debugging configuration
Information Center	<p>As the system information hub, Information Center classifies and manages all types of system information. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• Setting to Output System Information to the Console</li> <li>• Setting to Output System Information to a Monitor Terminal</li> <li>• Setting to Output System Information to a Log Host</li> <li>• Setting to Output System Information to the Trap Buffer</li> <li>• Setting to Output System Information to the Log Buffer</li> <li>• Setting to Output System Information to the SNMP Module</li> <li>• Configuring Synchronous Information Output</li> <li>• Disabling a Port from Generating Link Up/Down Logging Information</li> </ul>
PoE	<p>The Power over Ethernet (PoE) feature enables the power sourcing equipment (PSE) to feed powered devices (PDs) from Ethernet ports through twisted pair cables. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• Configuring the PSE</li> <li>• Configuring the PoE interface</li> <li>• Configuring PoE power management</li> <li>• Configuring the PoE monitoring function</li> <li>• Online upgrading the PSE processing software</li> <li>• Configuring a PD Disconnection Detection Mode</li> <li>• Enabling the PSE to detect nonstandard PDs</li> </ul>
Track	<p>The track module is used to implement collaboration between different modules through established collaboration objects. The detection modules trigger the application modules to perform certain operations through the track module. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• Configuring Collaboration Between the Track Module and the Detection Modules</li> <li>• Configuring Collaboration Between the Track Module and the Application Modules</li> </ul>
NQA	<p>NQA analyzes network performance, services and service quality by sending test packets to provide you with network performance and service quality parameters. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• Configuring the NQA Server</li> <li>• Enabling the NQA Client</li> <li>• Creating an NQA Test Group</li> <li>• Configuring an NQA Test Group</li> <li>• Configuring the Collaboration Function</li> <li>• Configuring Trap Delivery</li> <li>• Configuring the NQA Statistics Function</li> <li>• Configuring Optional Parameters Common to an NQA Test Group</li> <li>• Scheduling an NQA Test Group</li> </ul>

Features	Description
NTP	<p>Network Time Protocol (NTP) is the TCP/IP that advertises the accurate time throughout the network. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• Configuring the Operation Modes of NTP</li> <li>• Configuring Optional Parameters of NTP</li> <li>• Configuring Access-Control Rights</li> <li>• Configuring NTP Authentication</li> </ul>
VRRP	<p>Virtual Router Redundancy Protocol (VRRP) combines a group of switches (including a master and multiple backups) on a LAN into a virtual router called VRRP group. VRRP streamlines host configuration while providing high reliability. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• IPv4-Based VRRP configuration</li> <li>• IPv6-Based VRRP configuration</li> </ul>
Hotfix	<p>Hotfix is a fast, cost-effective method to fix software defects of the device without interrupting the running services. This document introduces the commands for hotfix operations</p>
Cluster Management	<p>A cluster is a group of network devices. Cluster management is to implement management of large numbers of distributed network devices. This document introduces the commands for:</p> <ul style="list-style-type: none"> <li>• Configuring the Management Device</li> <li>• Configuring the Member Devices</li> <li>• Configuring Access Between the Management Device and Its Member Devices</li> <li>• Adding a Candidate Device to a Cluster</li> <li>• Configuring Advanced Cluster Functions</li> </ul>
IRF Stack	<p>Intelligent Resilient Framework (IRF) allows you to build an IRF stack, namely a united device, by interconnecting multiple devices through stack ports. You can manage all the devices in the IRF stack by managing the united device. This document introduces the commands for IRF stack operations.</p>
IPC	<p>Inter-Process Communication (IPC) is a reliable communication mechanism among different nodes. This document introduces the commands for Enabling IPC Performance Statistics.</p>

# Table of Contents

<b>1 Commands for Logging into an Ethernet Switch</b> .....	<b>1-1</b>
Commands for Logging into an Ethernet Switch .....	1-1
activation-key.....	1-1
authentication-mode.....	1-2
auto-execute command.....	1-3
databits .....	1-4
display telnet client configuration .....	1-5
display user-interface .....	1-5
display users.....	1-7
display web users.....	1-8
escape-key .....	1-9
flow-control .....	1-10
free user-interface .....	1-11
history-command max-size .....	1-11
idle-timeout.....	1-12
ip http enable.....	1-13
lock .....	1-13
parity.....	1-14
protocol inbound.....	1-15
screen-length.....	1-16
send.....	1-16
set authentication password.....	1-17
shell .....	1-18
speed.....	1-19
stopbits .....	1-20
sysname .....	1-21
telnet.....	1-21
telnet ipv6 .....	1-22
telnet client source.....	1-23
telnet server enable .....	1-24
terminal type .....	1-24
user-interface.....	1-25
user privilege level.....	1-26
<b>2 Commands for Controlling Login Users</b> .....	<b>2-1</b>
Commands for Controlling Login Users.....	2-1
acl .....	2-1
free web-users .....	2-2
ip http acl .....	2-2

# 1 Commands for Logging into an Ethernet Switch

---

## Commands for Logging into an Ethernet Switch

### activation-key

#### Syntax

**activation-key** *character*

**undo activation-key**

#### View

AUX interface view

#### Default Level

3: Manage level

#### Parameters

*character*: Shortcut key for starting terminal sessions, a character or its ASCII decimal equivalent in the range 0 to 127; or a string of 1 to 3 characters.

#### Description

Use the **activation-key** command to define a shortcut key for starting a terminal session.

Use the **undo activation-key** command to restore the default shortcut key.

You can use a single character (or its corresponding ASCII code value in the range 0 to 127) or a string of 1 to 3 characters to define a shortcut key. In the latter case, the system takes only the first character to define the shortcut key. For example, if you input an ASCII code value 97, the system will set the shortcut key to <a>; if you input the string **b@c**, the system will set the shortcut key to <b>.

You may use the **display current-configuration** command to verify the shortcut key you have defined.

By default, pressing **Enter** key will start a terminal session.

#### Examples

# Set the shortcut key for starting terminal sessions to <s>.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] activation-key s
```

To verify the configuration, do the following:

# Exit the terminal session on the aux port, and enter <s> at the prompt of "Please press ENTER". You will see the terminal session being started.

```
[Sysname-ui-aux0] return
<Sysname> quit
```

```
*****
* Copyright (c) 2004-2008 3Com Corp. and its licensors. All rights reserved. *
* This software is protected by copyright law and international treaties.      *
* Without the prior written permission of 3Com Corporation and its licensors,*
* any reproduction republication, redistribution, decompiling, reverse      *
* engineering is strictly prohibited. Any unauthorized use of this software  *
* or any portion of it may result in severe civil and criminal penalties, and*
* will be prosecuted to the maximum extent possible under the applicable law.*
*****
User interface aux0 is available.
```

Please press ENTER.

<Sysname>

%Apr 28 04:33:11:611 2005 Sysname SHELL/5/LOGIN: Console login from aux0

## authentication-mode

### Syntax

```
authentication-mode { none | password | scheme [ command-authorization ] }
```

### View

User interface view

### Default Level

3: Manage level

### Parameters

**none:** Does not authenticate users.

**password:** Authenticates users using the local password.

**scheme:** Authenticates users locally or remotely using usernames and passwords.

**command-authorization:** Performs command authorization on TACACS authentication server.

### Description

Use the **authentication-mode** command to specify the authentication mode.

- If you specify the **password** keyword to authenticate users using the local password, remember to set the local password using the **set authentication password { cipher | simple } password** command.
- If you specify the **scheme** keyword to authenticate users locally or remotely using usernames and passwords, the actual authentication mode depends on other related configuration. Refer to the AAA-RADIUS-HWTACACS module of this manual for more.
- If this command is executed with the **command-authorization** keywords specified, authorization is performed on the TACACS server whenever you attempt to execute a command, and the command can be executed only when you pass the authorization. Normally, a TACACS server contains a list of the commands available to different users.

After you specify to perform local password authentication, when a user logs in through the Console port, a user can log into the switch even if the password is not configured on the switch. But for a VTY user interface, a password is needed for a user to log into the switch through it under the same condition.

By default, users logging in through the Console port and Telnet are scheme authenticated.

---

 **Caution**

For VTY user interface, if you want to set the login authentication mode to **none** or **password**, you must first verify that the SSH protocol is not supported by the user interface. Otherwise, your configuration will fail. Refer to [protocol inbound](#).

---

## Examples

# Configure to authenticate users using the local password.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] authentication-mode password
```

## auto-execute command

### Syntax

```
auto-execute command text
undo auto-execute command
```

### View

User interface view

### Default Level

3: Manage level

### Parameters

*text*: Command to be executed automatically.

### Description

Use the **auto-execute command** command to set the command that is executed automatically after a user logs in.

Use the **undo auto-execute command** command to disable the specified command from being automatically executed.

Use these two commands in the VTY user interface only.

Normally, the **telnet** command is specified to be executed automatically to enable the user to Telnet to a specific network device automatically.

By default, no command is automatically executed.



### Caution

- The **auto-execute command** command may cause you unable to perform common configuration in the user interface, so use it with caution.
  - Before executing the **auto-execute command** command and save your configuration, make sure you can log into the switch in other modes and cancel the configuration.
- 

### Examples

# Configure the **telnet 10.110.100.1** command to be executed automatically after users log into VTY 0.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0
[Sysname-ui-vty0] auto-execute command telnet 10.110.100.1
% This action will lead to configuration failure through ui-vty0. Are you sure?[Y/N]y
```

After the above configuration, when a user logs onto the device through VTY 0, the device automatically executes the configured command and logs off the current user.

### databits

#### Syntax

```
databits { 5 | 6 | 7 | 8 }
undo databits
```

#### View

AUX interface view

#### Default Level

2: System level

#### Parameters

- 5:** Five data bits.
- 6:** Six data bits.
- 7:** Seven data bits.
- 8:** Eight data bits.

#### Description

Use the **databits** command to set the databits for the user interface.

Use the **undo databits** command to revert to the default data bits.

The default data bits is 8.



## Note

3Com Switch 4800G only support data bits 7 and 8. To establish the connection again, you need to modify the configuration of the termination emulation utility running on your PC accordingly.

---

## Examples

```
# Set the data bits to 7.
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] databits 7
```

## display telnet client configuration

### Syntax

```
display telnet client configuration
```

### View

Any view

### Default Level

1: Monitor level

### Parameter

None

### Description

Use the **display telnet client configuration** command to display the source IP address or source interface configured for the current device.

### Example

```
# Display the source IP address or source interface configured for the current device.
<Sysname> display telnet client configuration
The source IP address is 1.1.1.1.
```

## display user-interface

### Syntax

```
display user-interface [ type number | number ] [ summary ]
```

### View

Any view

## Default Level

1: Monitor level

## Parameters

*type*: User interface type.

*number*: Absolute or relative index of the user interface. This argument can be an absolute user interface index (if you do not provide the *type* argument) or a relative user interface index (if you provide the *type* argument).

**summary**: Displays the summary information about a user interface.

## Description

Use the **display user-interface** command to view information about the specified or all user interfaces.

When the **summary** keyword is absent, the command will display the type of the user interface, the absolute or relative number, the speed, the user privilege level, the authentication mode and the physical location.

When the **summary** keyword is present, the command will display all the number and type of user interfaces under use and without use.

## Examples

# Display the information about user interface 0.

```
<Sysname> display user-interface 0
```

```
  Idx  Type    Tx/Rx      Modem Privi Auth  Int
F 0    AUX 0    9600      -      3    N    -
```

+ : Current user-interface is active.

F : Current user-interface is active and work in async mode.

Idx : Absolute index of user-interface.

Type : Type and relative index of user-interface.

Privi: The privilege of user-interface.

Auth : The authentication mode of user-interface.

Int : The physical location of UIs.

A : Authenticate use AAA.

L : Authentication use local database.

N : Current UI need not authentication.

P : Authenticate use current UI's password.

**Table 1-1** Descriptions on the fields of the **display user-interface** command

Filed	Description
+	The information displayed is about the current user interface.
F	The information displayed is about the current user interface. And the current user interface operates in asynchronous mode.
Idx	The absolute index of the user interface
Type	User interface type and the relative index
Tx/Rx	Transmission speed of the user interface

Filed	Description
Modem	Indicates whether or not a modem is used.
Privi	The available command level
Auth	The authentication mode
Int	The physical position of the user interface

## display users

### Syntax

**display users [ all ]**

### View

Any view

### Default Level

1: Monitor level

### Parameters

**all**: Displays the information about all user interfaces.

### Description

Use the **display users** command to display the information about user interfaces. If you do not specify the **all** keyword, only the information about the current user interface is displayed.

### Examples

# Display the information about the current user interface.

```
<Sysname> display users
```

```
The user application information of the user interface(s):
```

```
  Idx  UI      Delay  Type Userlevel
  ---  --      -
  1    VTY 0    00:11:45 TEL 3
  2    VTY 1    00:16:35 TEL 3
  3    VTY 2    00:16:54 TEL 3
+ 4    VTY 3    00:00:00 TEL 3
```

```
Following are more details.
```

```
VTY 0  :
        Location: 192.168.0.123
VTY 1  :
        Location: 192.168.0.43
VTY 2  :
        Location: 192.168.0.2
VTY 3  :
        User name: user
        Location: 192.168.0.33
+      : Current operation user.
```

F : Current operation user work in async mode.

**Table 1-2** Descriptions on the fields of the **display users** command

Field	Description
+	The information displayed is about the current user interface.
F	The information is about the current user interface, and the current user interface operates in asynchronous mode.
UI	The numbers in the left sub-column are the absolute user interface indexes, and those in the right sub-column are the relative user interface indexes.
Delay	The period in seconds the user interface idles for.
Type	User type
Userlevel	The level of the commands available to the users logging into the user interface
Location	The IP address form which the user logs in.
User name	The login name of the user that logs into the user interface.

## display web users

### Syntax

**display web users**

### View

Any view

### Parameter

None

### Description

Use the **display web users** command to display information about web users.

### Example

# Display information about the current web users.

```
<Sysname> display web users
```

```
UserIDName    Language  Level      State    LinkCount LoginTime  LastTime
ab820000    admin    Chinese    Management Enable    0          08:41:50  08:45:59
```

**Table 1-3** Description on the fields of the **display web users** command

Field	Description
UserID	ID of a web user
Name	Name of the web user
Language	Login language used by the web user
Level	Level of the web user
State	State of the web user

Field	Description
LinkCount	Number of tasks that the web user runs
LoginTime	Time when the web user logged in
LastTime	Last time when the web user accessed the switch

## escape-key

### Syntax

```
escape-key { default | character }
undo escape-key
```

### View

User interface view

### Default Level

3: Manage level

### Parameters

**default:** Restores the default escape key combination <Ctrl + C>.

*character:* Specifies the shortcut key for aborting a task, a single character (or its corresponding ASCII code value in the range 0 to 127) or a string of 1 to 3 characters.

### Description

Use the **escape-key** command to define a shortcut key for aborting tasks.

Use the **undo escape-key** command to restore the default shortcut key.

You can use a single character (or its corresponding ASCII code value in the range 0 to 127) or a string of 1 to 3 characters to define a shortcut key. But in fact, only the first character functions as the shortcut key. For example, if you enter an ASCII value 113, the system will use its corresponding character <q> as the shortcut key; if you input the string **q@c**, the system will use the first letter <q> as the shortcut key.

By default, you can use <Ctrl + C> to terminate a task. You can use the **display current-configuration** command to verify the shortcut key you have defined.

### Examples

```
# Define <Q> as the escape key.
```

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] escape-key Q
```

To verify the configuration, do the following:

```
# Run the ping command to test the connection.
```

```
<Sysname> ping -c 20 125.241.23.46
PING 125.241.23.46: 56 data bytes, press Q to break
```

```
Request time out
```

```
--- 125.241.23.46 ping statistics ---  
 2 packet(s) transmitted  
 0 packet(s) received  
100.00% packet loss
```

Enter <Q>, if the ping task is terminated and return to the current view, the configuration is correct.

<Sysname>

## flow-control

### Syntax

```
flow-control { hardware | none | software }  
undo flow-control
```

### View

AUX interface view

### Default Level

2: System level

### Parameters

**hardware**: Configures to perform hardware flow control.

**none**: Configures no flow control.

**software**: Configures to perform software flow control.

### Description

Using **flow-control** command, you can configure the flow control mode on AUX port. Using **undo flow-control** command, you can restore the default flow control mode.

By default, the value is **none**. That is, no flow control will be performed.



#### Note

3Com Switch 4800G only support **none** keyword.

---

### Examples

```
# Configure software flow control on AUX port.
```

```
<Sysname> system-view  
System View: return to User View with Ctrl+Z.  
[Sysname] user-interface aux 0  
[Sysname-ui-aux0] flow-control none
```

## free user-interface

### Syntax

**free user-interface** [ *type* ] *number*

### View

User view

### Default Level

3: Manage level

### Parameters

*type*: User interface type.

*number*: Absolute user interface index or relative user interface index.

- Relative user interface index: If you provide the *type* argument, *number* indicates the user interface index of the type. When the type is AUX, the *number* is 0; when the type is VTY, the *number* ranges from 0 to 4.
- Absolute user interface index: If you do not provide the *type* argument, *number* indicates absolute user interface index, which ranges from 0 to 5.

### Description

Use the **free user-interface** command to clear a specified user interface. If you execute this command, the corresponding user interface will be disconnected.

Note that the current user interface can not be cleared.

### Examples

# Log into user interface 0 and clear user interface 1.

```
<Sysname> free user-interface 1
Are you sure to free user-interface vty0
[Y/N]y
[OK]
```

After you execute this command, user interface 1 will be disconnected. The user in it must log in again to connect to the switch.

## history-command max-size

### Syntax

**history-command max-size** *value*

**undo history-command max-size**

### View

User interface view

### Default Level

2: System level

## Parameters

*value*: Size of the history command buffer. This argument ranges from 0 to 256 and defaults to 10. That is, the history command buffer can store 10 commands by default.

## Description

Use the **history-command max-size** command to set the size of the history command buffer.

Use the **undo history-command max-size** command to revert to the default history command buffer size.

## Examples

```
# Set the size of the history command buffer to 20 to enable it to store up to 20 commands.
```

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] history-command max-size 20
```

## idle-timeout

### Syntax

**idle-timeout** *minutes* [ *seconds* ]

**undo idle-timeout**

### View

User interface view

### Default Level

2: System level

## Parameters

*minutes*: Number of minutes. This argument ranges from 0 to 35,791.

*seconds*: Number of seconds. This argument ranges from 0 to 59.

## Description

Use the **idle-timeout** command to set the timeout time. The connection to a user interface is terminated if no operation is performed in the user interface within the specified period.

Use the **undo idle-timeout** command to revert to the default timeout time.

You can use the **idle-timeout 0** command to disable the timeout function.

The default timeout time is 10 minutes.

## Examples

```
# Set the timeout time of AUX 0 to 1 minute.
```

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] idle-timeout 1 0
```

## ip http enable

### Syntax

```
ip http enable
undo ip http enable
```

### View

System view

### Parameter

None

### Description

Use the **ip http enable** command to launch the Web server.

Use the **undo ip http enable** command to shut down the Web server.

By default, the Web server is launched.

### Example

```
# Shut down the Web server.
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] undo ip http enable

# Launch the Web server.
[Sysname] ip http enable
```

## lock

### Syntax

```
lock
```

### View

User view

### Default Level

3: Manage level

### Parameters

None

### Description

Use the **lock** command to lock the current user interface to prevent unauthorized users from operating the user interface.

With the execution of this command, the system prompts to enter and confirm the password (up to 16 characters), and then locks the user interface.

To cancel the lock, press the **Enter** key and enter the correct password.

By default, the system will not lock the current user interface automatically.

## Examples

```
# Lock the current user interface.
```

```
<Sysname> lock
```

```
Please input password<1 to 16> to lock current user terminal interface:
```

```
Password:
```

```
Again:
```

```
locked !
```

```
# Cancel the lock.
```

```
Password:
```

```
Again:
```

```
<Sysname>
```

## parity

### Syntax

```
parity { even | mark | none | odd | space }
```

```
undo parity
```

### View

AUX interface view

### Default Level

2: System level

### Parameters

**even**: Performs even checks.

**mark**: Performs mark checks.

**none**: Does not check.

**odd**: Performs odd checks.

**space**: Performs space checks.

### Description

Use the **parity** command to set the check mode of the user interface.

Use the **undo parity** command to revert to the default check mode.

No check is performed by default.



## Note

3Com Switch 4800G support the **even**, **none**, and **odd** check modes only. To establish the connection again, you need to modify the configuration of the termination emulation utility running on your PC accordingly.

---

## Examples

```
# Set to perform mark checks.
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] parity mark
```

## protocol inbound

### Syntax

```
protocol inbound { all | ssh | telnet }
```

### View

VTY interface view

### Default Level

3: Manage level

### Parameters

**all**: Supports both Telnet protocol and SSH protocol.

**ssh**: Supports SSH protocol.

**telnet**: Supports Telnet protocol.

### Description

Use the **protocol inbound** command to configure the user interface to support specified protocols.

Both Telnet and SSH protocols are supported by default.

Related command: **user-interface vty**.



## Caution

If you want to configure the user interface to support SSH, to ensure a successful login, you must first configure the authentication mode to **scheme** on the user interface. If you set the authentication mode to **password** or **none**, the **protocol inbound ssh** command will fail. Refer to [authentication-mode](#).

---

## Examples

```
# Configure VTY 0 to support only SSH protocol.
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0
[Sysname-ui-vty0] protocol inbound ssh
```

## screen-length

### Syntax

```
screen-length screen-length
undo screen-length
```

### View

User interface view

### Default Level

2: System level

### Parameters

*screen-length*: Number of lines the screen can contain. This argument ranges from 0 to 512 and defaults to 24.

### Description

Use the **screen-length** command to set the number of lines the terminal screen can contain.

Use the **undo screen-length** command to revert to the default number of lines.

You can use the **screen-length 0** command to disable the function to display information in pages.

## Examples

```
# Set the number of lines the terminal screen can contain to 20.
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] screen-length 20
```

## send

### Syntax

```
send { all | number | type number }
```

### View

User view

### Default Level

1: Monitor level

## Parameters

**all:** Specifies to send messages to all user interfaces.

**type:** User interface type.

**number:** Absolute user interface index or relative user interface index.

- Relative user interface index: If you provide the *type* argument, the *number* argument indicates the user interface index of the type. When the type is AUX, *number* is 0; when the type is VTY, *number* ranges from 0 to 4.
- Absolute user interface index: If you do not provide the *type* argument, the *number* argument indicates the absolute user interface index, and ranges from 0 to 5.

## Description

Use the **send** command to send messages to a specified user interface or all user interfaces.

## Examples

```
# Send messages to all user interfaces.
<Sysname> send all
Enter message, end with CTRL+Z or Enter; abort with CTRL+C:
hello^Z
Send message? [Y/N]y
<Sysname>

***
***
***Message from vty0 to vty0
***
hello

<Sysname>
```

## set authentication password

### Syntax

```
set authentication password { cipher | simple } password
```

```
undo set authentication password
```

### View

User interface view

### Default Level

3: Manage level

## Parameters

**cipher:** Specifies to display the local password in encrypted text when you display the current configuration.

**simple:** Specifies to display the local password in plain text when you display the current configuration.

*password*: Password. The password must be in plain text if you specify the **simple** keyword in the **set authentication password** command. If you specify the **cipher** keyword, the password can be in either encrypted text or plain text. Whether the password is in encrypted text or plain text depends on the password string entered. Strings containing up to 16 characters (such as 123) are regarded as plain text passwords and are converted to the corresponding 24-character encrypted password (such as !TP<\\*EMUHL,408`W7TH!Q!!). A encrypted password must contain 24 characters and must be in ciphered text (such as !TP<\\*EMUHL,408`W7TH!Q!!).

## Description

Use the **set authentication password** command to set the local password.

Use the **undo set authentication password** command to remove the local password.

Note that only plain text passwords are expected when users are authenticated.



By default, Telnet users need to provide their passwords to log in. If no password is set, the “Login password has not been set !” message appears on the terminal when users log in.

---

## Examples

# Set the local password of VTY 0 to “123”.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0
[Sysname-ui-vty0] set authentication password simple 123
```

## shell

### Syntax

**shell**

**undo shell**

### View

User interface view

### Default Level

3: Manage level

### Parameters

None

### Description

Use the **shell** command to make terminal services available for the user interface.

Use the **undo shell** command to make terminal services unavailable to the user interface.

By default, terminal services are available in all user interfaces.

Note the following when using the **undo shell** command:

- This command is available in all user interfaces except the AUX user interface, because the AUX port (also the Console) is exclusively used for configuring the switch.
- This command is unavailable in the current user interface.
- This command prompts for confirmation when being executed in any valid user interface.

## Examples

```
# Log into user interface 0 and make terminal services unavailable in VTY 0 through VTY 4.
```

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] undo shell
% Disable ui-vty0-4 , are you sure ? [Y/N]y
```

## speed

### Syntax

```
speed speed-value
```

```
undo speed
```

### View

AUX interface view

### Default Level

2: System level

### Parameters

*speed-value*: Transmission speed (in bps). This argument can be 300, 600, 1200, 2400, 4800, 9600, 19,200, 38,400, 57,600, 115,200 and defaults to 19,200.

### Description

Use the **speed** command to set the transmission speed of the user interface.

Use the **undo speed** command to revert to the default transmission speed.



#### Note

After you use the **speed** command to configure the transmission speed of the AUX user interface, you must change the corresponding configuration of the terminal emulation program running on the PC, to keep the configuration consistent with that on the switch.

---

## Examples

```
# Set the transmission speed of the AUX user interface to 19,200 bps.
```

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] speed 19200
```

## stopbits

### Syntax

```
stopbits { 1 | 1.5 | 2 }
```

```
undo stopbits
```

### View

AUX interface view

### Default Level

2: System level

### Parameters

**1**: Sets the stop bits to 1.

**1.5**: Sets the stop bits to 1.5.

**2**: Sets the stop bits to 2.

### Description

Use the **stopbits** command to set the stop bits of the user interface.

Use the **undo stopbits** command to revert to the default stop bits.

By default, the stop bits is 1.



#### Note

- 3Com Switch 4800G do not support communication with a terminal emulation program with stopbits set to 1.5.
  - Changing the stop bits value of the switch to a value different from that of the terminal emulation utility does not affect the communication between them.
- 

### Examples

# Set the stop bits to 2.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] stopbits 2
```

## sysname

### Syntax

```
sysname string  
undo sysname
```

### View

System view

### Default Level

2: System level

### Parameters

*string*: System name of the switch. This argument can contain 1 to 30 characters and defaults to **3Com**.

### Description

Use the **sysname** command to set a system name for the switch.

Use the **undo sysname** command to revert to the default system name.

The CLI prompt reflects the system name of a switch. For example, if the system name of a switch is "3Com", then the prompt of user view is <4800G>.

### Examples

```
# Set the system name of the switch to ABC.  
<Sysname> system-view  
System View: return to User View with Ctrl+Z.  
[Sysname] sysname ABC  
[ABC]
```

## telnet

### Syntax

```
telnet remote-system [ port-number ] [ source { ip ip-address | interface interface-type  
interface-number } ]
```

### View

User view

### Default Level

0: Visit level

### Parameters

*remote-system*: IP address or host name of the remote system. The host name is a string of 1 to 20 characters, which can be specified using the **ip host** command.

*port-number*: TCP port number assigned to Telnet service on the remote system, in the range 0 to 65535.

*ip-address*: Source IP address of the packets sent by the Telnet client.

*interface-type interface-number*: Type and number of the interface through which the Telnet client sends packets.

## Description

Use the **telnet** command to Telnet to another switch from the current switch to manage the former remotely. You can terminate a Telnet connection by pressing <Ctrl + K>.

Related commands: **display tcp status**, **ip host**.

## Examples

# Telnet to the switch with the host name of **Sysname2** and IP address of 129.102.0.1 from the current switch (with the host name of **Sysname1**).

```
<Sysname1> telnet 129.102.0.1
Trying 129.102.0.1 ...
Press CTRL+K to abort
Connected to 129.102.0.1 ...
*****
* Copyright (c) 2004-2008 3Com Corp. and its licensors. All rights reserved. *
* This software is protected by copyright law and international treaties.    *
* Without the prior written permission of 3Com Corporation and its licensors,*
* any reproduction republication, redistribution, decompiling, reverse      *
* engineering is strictly prohibited. Any unauthorized use of this software  *
* or any portion of it may result in severe civil and criminal penalties, and*
* will be prosecuted to the maximum extent possible under the applicable law.*
*****
<Sysname2>
```

## telnet ipv6

### Syntax

```
telnet ipv6 remote-system [ -i interface-type interface-number ] [ port-number ]
```

### View

User view

### Default Level

0: Visit level

### Parameters

*remote-system*: IPv6 address or host name of the remote system. An IPv6 address can be up to 46 characters; a host name is a string of 1 to 20 characters.

**-i** *interface-type interface-number*: Specifies the outbound interface by interface type and interface number. The outbound interface is required when the destination address is a local link address.

*port-number*: TCP port number assigned to Telnet service on the remote system, in the range 0 to 65535 and defaults to 23.

## Description

Use the **telnet ipv6** command to telnet to a remote device for remote management. You can terminate a Telnet connection by pressing <Ctrl + K>.

## Examples

```
# Telnet to the device with IPv6 address 3001::1.
```

```
<Sysname> telnet ipv6 3001::1
Trying 3001::1 ...
Press CTRL+K to abort
Connected to 3001::1 ...
*****
* Copyright (c) 2004-2008 3Com Corp. and its licensors. All rights reserved. *
* This software is protected by copyright law and international treaties.     *
* Without the prior written permission of 3Com Corporation and its licensors,*
* any reproduction republication, redistribution, decompiling, reverse      *
* engineering is strictly prohibited. Any unauthorized use of this software  *
* or any portion of it may result in severe civil and criminal penalties, and*
* will be prosecuted to the maximum extent possible under the applicable law.*
*****
<Sysname>
```

## telnet client source

### Syntax

```
telnet client source { ip ip-address | interface interface-type interface-number }
```

```
undo telnet client source
```

### View

System view

### Default Level

2: System level

### Parameters

None

## Description

Use the **telnet client source** command to specify the source IP address or source interface for the Telnet packets to be sent.

Use the **undo telnet client source** command to remove the source IP address or source interface configured for Telnet packets.

By default, source IP address or source interface of the Telnet packets sent is not configured.

## Examples

```
# Specify the source IP address for Telnet packets.
```

```
<Sysname> system-view
```

```
[Sysname] telnet client source ip 129.102.0.2
# Remove the source IP address configured for Telnet packets.
[Sysname] undo telnet client source
```

## telnet server enable

### Syntax

```
telnet server enable
undo telnet server enable
```

### View

System view

### Default Level

3: Manage level

### Parameters

None

### Description

Use the **telnet server enable** command to make the switch to operate as a Telnet Server.

Use the **undo telnet server enable** command disable the switch from operating as a Telnet server.

By default, a switch does not operate as a Telnet server.

### Examples

# Make the switch to operate as a Telnet Server.

```
<Sysname> system-view
[Sysname] telnet server enable
% Start Telnet server
```

# Disable the switch from operating as a Telnet server.

```
[Sysname] undo telnet server enable
% Close Telnet server
```

## terminal type

### Syntax

```
terminal type { ansi | vt100 }
undo terminal type
```

### View

User interface view

### Default Level

2: System level

## Parameters

**ansi**: Specifies the terminal display type to ANSI.

**vt100**: Specifies the terminal display type to VT100.

## Description

Use the **terminal type** command to configure the type of terminal display .

Use the **undo terminal type** command to restore the default.

Currently, the system support two types of terminal display : ANSI and VT100.

By default, the terminal display type is ANSI. The device must use the same display type as the terminal.

If the terminal uses VT 100, the device should also use VT 100.

## Examples

# Set the terminal display type to VTY 100.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0
[Sysname-ui-vty0] terminal type vt100
```

## user-interface

### Syntax

**user-interface** [ *type* ] *first-number* [ *last-number* ]

### View

System view

### Default Level

2: System level

### Parameters

*type*: User interface type.

*first-number*: User interface index, which identifies the first user interface to be configured.

*last-number*: User interface index, which identifies the last user interface to be configured.

### Description

Use the **user-interface** command to enter one or more user interface views to perform configuration.

### Examples

# Enter VTY 0 user interface view.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0
[Sysname-ui-vty0]
```

## user privilege level

### Syntax

```
user privilege level level  
undo user privilege level
```

### View

User interface view

### Default Level

3: Manage level

### Parameters

*level*: Command level ranging from 0 to 3.

### Description

Use the **user privilege level** command to configure the command level available to the users logging into the user interface.

Use the **undo user privilege level** command to revert to the default command level.

By default, the commands of level 3 are available to the users logging into the AUX user interface. The commands of level 0 are available to the users logging into VTY user interfaces.

Commands fall into four command levels: visit, monitor, system, and manage, which are described as follows:

- Visit level: Commands of this level are used to diagnose network and change the language mode of user interface, such as the **ping**, **tracert**. The **Telnet** command is also of this level. Commands of this level cannot be saved in configuration files.
- Monitor level: Commands of this level are used to maintain the system, to debug service problems, and so on. The **display** and **debugging** command are of monitor level. Commands of this level cannot be saved in configuration files.
- System level: Commands of this level are used to configure services. Commands concerning routing and network layers are of system level. You can utilize network services by using these commands.
- Manage level: Commands of this level are for the operation of the entire system and the system supporting modules. Services are supported by these commands. Commands concerning file system, file transfer protocol (FTP), trivial file transfer protocol (TFTP), downloading using XModem, user management, and level setting are of administration level.

### Examples

# Configure that commands of level 0 are available to the users logging into VTY 0.

```
<Sysname> system-view  
System View: return to User View with Ctrl+Z.  
[Sysname] user-interface vty 0  
[Sysname-ui-vty0] user privilege level 0
```

# You can verify the above configuration by Telnetting to VTY 0 and displaying the available commands, as listed in the following.

<Sysname> ?

User view commands:

ping	Ping function
quit	Exit from current command view
super	Set the current user priority level
telnet	Establish one TELNET connection
tracert	Trace route function
undo	Undo a command or set to its default status

# 2 Commands for Controlling Login Users

---

## Commands for Controlling Login Users

### acl

#### Syntax

```
acl [ ipv6 ] acl-number { inbound | outbound }  
undo acl [ ipv6 ] { inbound | outbound }
```

#### View

User interface view

#### Default Level

2: System level

#### Parameters

*acl-number*: ACL number ranging from 2000 to 4999, where:

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Layer 2 ACLs

**ipv6** *acl-number*: IPv6 ACL number ranging from 2000 to 3999.

**inbound**: Filters the users Telnetting to the current switch.

**outbound**: Filters the users Telnetting to other switches from the current switch.

#### Description

Use the **acl** command to apply an ACL to filter Telnet users.

Use the **undo acl** command to disable the switch from filtering Telnet users using the ACL.

Note that if you use Layer 2 ACL rules, you can only choose the **inbound** keyword in the command here.

#### Examples

```
# Apply ACL 2000 to filter users Telnetting to the current switch (assuming that ACL 2,000 already exists.)
```

```
<Sysname> system-view  
System View: return to User View with Ctrl+Z.  
[Sysname] user-interface vty 0 4  
[Sysname-ui-vty0-4] acl 2000 inbound
```

## free web-users

### Syntax

```
free web-users { all | user-id userid | user-name username }
```

### View

User view

### Parameter

*userid*: Web user ID.

*username*: User name of the Web user. This argument can contain 1 to 80 characters.

**all**: Specifies all Web users.

### Description

Use the **free web-users** command to disconnect a specified Web user or all Web users by force.

### Example

```
# Disconnect all Web users by force.
```

```
<Sysname> free web-users all
```

## ip http acl

### Syntax

```
ip http acl acl-number
```

```
undo ip http acl
```

### View

System view

### Parameter

*acl-number*: ACL number ranging from 2,000 to 2,999.

### Description

Use the **ip http acl** command to apply an ACL to filter Web users.

Use the **undo ip http acl** command to disable the switch from filtering Web users using the ACL.

### Example

```
# Apply ACL 2000 to filter Web users (assuming that ACL 2,000 already exists.)
```

```
<Sysname> system-view
```

```
System View: return to User View with Ctrl+Z.
```

```
[Sysname] ip http acl 2000
```

# Table of Contents

<b>1 Basic Configuration Commands</b> .....	<b>1-1</b>
Basic Configuration Commands .....	1-1
clock datetime.....	1-1
clock summer-time one-off .....	1-1
clock summer-time repeating .....	1-2
clock timezone.....	1-4
command-privilege level.....	1-5
copyright-info enable .....	1-6
display clipboard.....	1-7
display clock .....	1-8
display current-configuration .....	1-8
display default-configuration.....	1-10
display diagnostic-information .....	1-10
display history-command.....	1-11
display hotkey .....	1-12
display this.....	1-13
display version.....	1-14
header .....	1-14
hotkey .....	1-16
quit .....	1-18
return .....	1-18
screen-length disable .....	1-19
super.....	1-19
super password .....	1-20
sysname .....	1-21
system-view.....	1-22

# 1 Basic Configuration Commands

---

## Basic Configuration Commands

### clock datetime

#### Syntax

**clock datetime** *time date*

#### View

User view

#### Default Level

3: Manage level

#### Parameters

*time*: Current time in the format of *HH:MM:SS*, where *HH* is hours in the range 0 to 23, *MM* is minutes in the range 0 to 59, and *SS* is seconds in the range 0 to 59. The zeros in the argument can be omitted except for indicating 0 hours.

*date*: Current date in the format of *MM/DD/YYYY* or *YYYY/MM/DD*. *MM* is the month of the year in the range 1 to 12, *DD* is the day of the month that varies with months, and *YYYY* is a year in the range 2000 to 2035.

#### Description

Use the **clock datetime** command to set the current time and date of the device.

The current time and date of the device must be set in an environment that requires the acquisition of absolute time.

You may choose not to provide seconds when inputting the time parameters.

Related commands: **clock summer-time one-off**, **clock summer-time repeating**, **clock timezone**, **display clock**.

#### Examples

```
# Set the current system time to 14:10:20 08/01/2005.
```

```
<Sysname> clock datetime 14:10:20 8/1/2005
```

```
# Set the current system time to 00:06:00 01/01/2007.
```

```
<Sysname> clock datetime 0:6 2007/1/1
```

### clock summer-time one-off

#### Syntax

**clock summer-time** *zone-name one-off start-time start-date end-time end-date add-time*

## undo clock summer-time

### View

System view

### Default Level

3: Manage level

### Parameters

*zone-name*: Name of the daylight saving time, a string of 1 to 32 characters. It is case sensitive.

*start-time*: Start time, in the format of *HH:MM:SS* (hours/minutes/seconds). The zeros in the argument can be omitted except for indicating 0 hours.

*start-date*: Start date, in the format of *MM/DD/YYYY* (months/days/years) or *YYYY/MM/DD*.

*end-time*: End time, in the format of *HH:MM:SS* (hours/minutes/seconds). The zeros in the argument can be omitted except for indicating 0 hours.

*end-date*: End date, in the format of *MM/DD/YYYY* (months/days/years) or *YYYY/MM/DD*.

*add-time*: Time added to the standard time of the device, in the format of *HH:MM:SS* (hours/minutes/seconds). The zeros in the argument can be omitted except for indicating 0 hours.

### Description

Use the **clock summer-time one-off** command to adopt daylight saving time from the *start-time* of the *start-date* to the *end-time* of the *end-date*. Daylight saving time adds the *add-time* to the current time of the device.

Use the **undo clock summer-time** command to cancel the configuration of the daylight saving time.

After the configuration takes effect, you can use the **display clock** command to view it. Besides, the time of the log or debug information is the local time of which the time zone and daylight saving time have been adjusted.

Note that:

- The time range from *start-time* in *start-date* to *end-time* in *end-date* must be longer than one day and shorter than one year. Otherwise, the argument is considered as invalid and the configuration fails.
- If the current system time is in the time range specified with this command, the system time automatically adds "add-time" after the execution of this command.

Related commands: **clock datetime**, **clock summer-time repeating**, **clock timezone**, **display clock**.

### Examples

# For daylight saving time in **abc1** between 06:00:00 on 08/01/2006 and 06:00:00 on 09/01/2006, set the system clock ahead one hour.

```
<Sysname> system-view
```

```
[Sysname] clock summer-time abc1 one-off 6 08/01/2006 6 09/01/2006 1
```

## clock summer-time repeating

### Syntax

```
clock summer-time zone-name repeating start-time start-date end-time end-date add-time
```

## undo clock summer-time

### View

System view

### Default Level

3: Manage level

### Parameters

*zone-name*: Name of the daylight saving time, a string of 1 to 32 characters.

*start-time*: Start time, in the format of *HH:MM:SS* (hours/minutes/seconds). The zeros in the argument can be omitted except for indicating 0 hours.

*start-date*: Start date which can be set in two ways:

- Enter the year, month and date at one time, in the format of *MM/DD/YYYY* (months/days/years) or *YYYY/MM/DD*.
- Enter the year, month and date one by one, separated by spaces. The year ranges from 2000 to 2035; the month can be **January, February, March, April, May, June, July, August, September, October, November** or **December**; the start week can be the **first, second, third, fourth, fifth** or **last** week of the month; the start date is **Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday**.

*end-time*: End time, in the format of *HH:MM:SS* (hours/minutes/seconds). The zeros in the argument can be omitted except for indicating 0 hours.

*end-date*: End date which can be set in two ways:

- Enter the year, month and date at one time, in the format of *MM/DD/YYYY* (months/days/years) or *YYYY/MM/DD*.
- Enter the year, month and date one by one, separated by spaces. The year ranges from 2000 to 2035; the month can be **January, February, March, April, May, June, July, August, September, October, November** or **December**; the end week can be the **first, second, third, fourth, fifth** or **last** week of the month; the end date is **Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday**.

*add-time*: Time added to the current standard time of the device, in the format of *HH:MM:SS* (hours/minutes/seconds). The zeros in the argument can be omitted except for indicating 0 hours.

### Description

Use the **clock summer-time repeating** command to adopt summer-time repeatedly.

Use the **undo clock summer-time** command to cancel the configuration of the daylight saving time.

For example, when *start-date* and *start-time* are set to 2007/6/6 and 00:00:00, *end-date* and *end-time* to 2007/10/01 and 00:00:00, and *add-time* to 01:00:00, it specifies to adopt daylight saving time from 00:00:00 of June 6 until 00:00:00 of October 1 each year from 2007 (2007 inclusive). The daylight saving time adds one hour to the current device time.

After the configuration takes effect, use the **display clock** command to view the result. The information such as log file and debug adopts the local time modified by time-zone and daylight saving time.

Note that:

- The time range from “start-time” in “start-date” to “end-time” in “end-date” must be longer than one day and shorter than one year. Otherwise, the argument is considered as invalid and the configuration fails.
- If the current system time is in the time range specified with this command, the system time automatically adds “add-time” after the execution of this command.

Related commands: **clock datetime**, **clock summer-time one-off**, **clock timezone**, **display clock**.

## Examples

```
# For the daylight saving time in abc2 between 06:00:00 on 08/01/2007 and 06:00:00 on 09/01/2007
and from 06:00:00 08/01 to 06:00:00 on 09/01 each year after 2007, set the system clock ahead one
hour.
```

```
<Sysname> system-view
```

```
[Sysname] clock summer-time abc2 repeating 06:00:00 08/01/2007 06:00:00 09/01/2007 01:00:00
```

## clock timezone

### Syntax

```
clock timezone zone-name { add | minus } zone-offset
```

```
undo clock timezone
```

### View

System view

### Default Level

3: Manage level

### Parameters

*zone-name*: Time zone name, a string of 1 to 32 characters. It is case sensitive.

**add**: Positive offset to universal time coordinated (UTC) time.

**minus**: Negative offset to UTC time.

*zone-offset*: Offset to UTC time. In the format of *HH/MM/SS* (hours/minutes/seconds), where *HH* is hours in the range 0 to 23, *MM* is minutes in the range 0 to 59, and *SS* is seconds in the range 0 to 59. The zeros in the argument can be omitted except for indicating 0 hours.

### Description

Use the **clock timezone** command to set the local time zone.

Use the **undo clock timezone** command to restore the local time zone to the default UTC time zone.

By default, the local time zone is UTC zone.

After the configuration takes effect, use the **display clock** command to view the result. The information such as log file and debug adopts the local time modified by time-zone and daylight saving time.

Related commands: **clock datetime**, **clock summer-time one-off**, **clock summer-time repeating**, **display clock**.

## Examples

```
# Set the name of the local time zone to Z5, five hours ahead of UTC time.
```

```
<Sysname> system-view
[Sysname] clock timezone z5 add 5
```

## command-privilege level

### Syntax

**command-privilege level** *level* **view** *view command*

**undo command-privilege view** *view command*

### View

System view

### Default Level

3: Manage level

### Parameters

**level** *level*: Command level, in the range 0 to 3.

**view** *view*: Specifies a view. The value **shell** of the argument *view* represents user view. The specified view must be the view to which the command provided by the *command* argument belongs; for the corresponding view, refer to the "View" section of the specified command.

*command*: Command to be set in the specified view.

### Description

Use the **command-privilege** command to assign a level for the specified command in the specified view.

Use the **undo command-privilege view** command to restore the default.

By default, each command in a view has its specified level. For the details, refer to the related part of *Basic System Configuration* in this manual. Command level falls into four levels: visit, monitor, system, and manage, which are identified by 0 through 3. The administrator can assign a privilege level for a user according to his need. When the user logs on a device, the commands available depend on the user's privilege. For example, if a user's privilege is 3 and the command privilege of VTY 0 user interface is 1, and the user logs on the system from VTY 0, he can use all the commands with privilege smaller than three (inclusive).

Note that:

- You are recommended to use the default command level or modify the command level under the guidance of professional staff; otherwise, the change of command level may bring inconvenience to your maintenance and operation, or even potential security problem.
- When you configure the **command-privilege** command, the value of the *command* argument must be a complete form of the specified command, that is, you must enter all needed keywords and arguments of the command. The argument should be in the value range. For example, the default level of the **tftp server-address { get | put | sget } source-filename [ destination-filename ] [ source { interface interface-type interface-number | ip source-ip-address } ]** command is 3; after the **command-privilege level 0 view shell tftp 1.1.1.1 put a.cfg** command is executed, when users with the user privilege level of 0 log in to the device, they can execute the **tftp server-address put source-filename** command (such as the **tftp 192.168.1.26 put syslog.txt** command); users with the

user privilege level of 0 cannot execute the command with the **get**, **sget** or **source** keyword, and cannot specify the *destination-filename* argument.

- When you configure the **undo command-privilege view** command, the value of the *command* argument can be an abbreviated form of the specified command, that is, you only need to enter the keywords at the beginning of the command. For example, after the **undo command-privilege view** system ftp command is executed, all commands starting with the keyword **ftp** (such as **ftp server acl**, **ftp server enable**, and **ftp timeout**) will be restored to the default level; if you have modified the command level of commands **ftp server enable** and **ftp timeout**, and you want to restore only the **ftp server enable** command to its default level, you should use the **undo command-privilege view** system ftp server command.
- If you modify the command level of a command in a specified view from the default command level to a lower level, remember to modify the command levels of the **quit** command and the corresponding command that is used to enter this view. For example, the default command level of commands **interface** and **system-view** is 2 (system level); if you want to make the **interface** command available to the users with the user privilege level of 1, you need to execute the following three commands: **command-privilege level 1 view** shell system-view, **command-privilege level 1 view** system interface gigabitethernet 1/0/1, and **command-privilege level 1 view** system quit, so that the login users with the user privilege level of 1 can enter system view, execute the **interface gigabitethernet** command, and then return to user view.

## Examples

# Set the command level of the **system-view** command in user view to 3. (By default, users with the user privilege level of 2 or 3 can use the **system-view** command after login; after the following configuration, only users with the user privilege level of 3 can use this command to enter system view and configure the device. Therefore, the device security is improved.)

```
<Sysname> system-view  
[Sysname] command-privilege level 3 view shell system-view
```

## copyright-info enable

### Syntax

```
copyright-info enable  
undo copyright-info enable
```

### View

System view

### Default Level

3: Manage level

### Parameters

None

### Description

Use the **copyright-info enable** command to enable the display of copyright information.

Use the **undo copyright-info enable** command to disable the display of copyright information.

By default, the display of copyright information is enabled.

## Examples

# Enable the display of copyright information

```
<Sysname> system-view
```

```
[Sysname] copyright-info enable
```

- If a user logs in to the device through Telnet, the following information is displayed:

```
*****  
* Copyright (c) 2004-2008 3Com Corp. and its licensors. All rights reserved. *  
* This software is protected by copyright law and international treaties. *  
* Without the prior written permission of 3Com Corporation and its licensors,*  
* any reproduction republication, redistribution, decompiling, reverse *  
* engineering is strictly prohibited. Any unauthorized use of this software *  
* or any portion of it may result in severe civil and criminal penalties, and*  
* will be prosecuted to the maximum extent possible under the applicable law.*  
*****
```

```
<Sysname>
```

- If a user has already logged in through the console port, and then quits user view, the following information is displayed:

```
*****  
* Copyright (c) 2004-2008 3Com Corp. and its licensors. All rights reserved. *  
* This software is protected by copyright law and international treaties. *  
* Without the prior written permission of 3Com Corporation and its licensors,*  
* any reproduction republication, redistribution, decompiling, reverse *  
* engineering is strictly prohibited. Any unauthorized use of this software *  
* or any portion of it may result in severe civil and criminal penalties, and*  
* will be prosecuted to the maximum extent possible under the applicable law.*  
*****
```

```
User interface aux is available.
```

```
Please press ENTER.
```

## display clipboard

### Syntax

```
display clipboard
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

## Description

Use the **display clipboard** command to view the contents of the clipboard.

To copy the specified content to the clipboard:

Move the cursor to the starting position of the content and press the <Esc+Shift+,> combination ("," is an English comma).

Move the cursor to the ending position of the content and press the <Esc+Shift+.> combination (". " is an English dot) to copy the specified content to the clipboard.

## Examples

```
# View the content of the clipboard.
```

```
<Sysname> display clipboard
----- CLIPBOARD-----
      display arp all
```

## display clock

### Syntax

```
display clock
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display clock** command to view the current system time and date.

The current system time and date are decided by the **clock datetime**, **clock summer-time one-off** (or **clock summer-time repeating**), **clock timezone**. Refer to *Configuring the system clock* in the operation manual for the detailed rules.

Related commands: **clock datetime**, **clock summer-time one-off**, **clock summer-time repeating**, **clock timezone**.

### Examples

```
# Display the current time and date.
```

```
<Sysname> display clock
09:41:23 UTC Thu 12/15/2005
```

## display current-configuration

### Syntax

```
display current-configuration [ [ configuration [ configuration ] | interface [ interface-type ] [ interface-number ] ] [ by-linenum ] [ [ { begin | exclude | include } regular-expression ] ]
```

## View

Any view

## Default Level

2: System level

## Parameters

**configuration** [ *configuration* ]: Specifies to display non-interface configuration. If no parameter is used, all the non-interface configuration is displayed; if parameters are used, display the specified information. For example:

- **isp**: Displays the ISP configuration.
- **post-system**: Displays the post-system configuration.
- **radius-template**: Displays the Radius template configuration.
- **system**: Displays the system configuration.
- **user-interface**: Displays the user interface configuration.

**interface** [ *interface-type* ] [ *interface-number* ]: Displays the interface configuration, where *interface-type* represents the interface type and *interface-number* represents the interface number.

**by-linenum**: Specifies to display the number of each line.

**|**: Specifies to use regular expression to filter the configuration of display device. For the detailed description of the regular expression, refer to the *CLI Display* part of *Basic System Configuration* in the *System Volume*.

- **begin**: Displays the line that matches the regular expression and all the subsequent lines.
- **exclude**: Displays the lines that do not match the regular expression.
- **include**: Displays only the lines that match the regular expression.

*regular-expression*: Regular expression, a string of 1 to 256 characters. Note that this argument is case-sensitive and can have spaces included.

## Description

Use the **display current-configuration** command to display the current validated configuration of a device.

You can use the **display current-configuration** command to view the currently validated configuration. A parameter is not displayed if it has the default configuration. If the validated parameter is changed, although you have configured it, the validated parameter is displayed. For example, ip address 11.11.11.11 24 has been configured on a Loopback interface. In this case, if you execute the **display current-configuration** command, ip address 11.11.11.11 255.255.255.255 is displayed, meaning the validated subnet mask is 32 bits.

Related commands: **save**, **reset saved-configuration**, **display saved-configuration**.

## Examples

# Display the configuration from the line containing "user-interface" to the last line in the current validated configuration (the output information depends on the current configuration).

```
<Sysname> display current-configuration | begin user-interface
user-interface aux 0
user-interface vty 0 4
authentication-mode none
```

```
user privilege level 3
#
return
```

## display default-configuration

### Syntax

```
display default-configuration
```

### View

Any view

### Default Level

2: System level

### Parameters

None

### Description

Use the **display default-configuration** command to display the factory defaults of a device. The command displays all commands to be executed when the device boots with the factory defaults.

Related commands: **display current-configuration**, **display saved-configuration**.

### Examples

# Display the factory defaults of the device (The factory defaults vary with device models. The detailed displays are omitted here).

```
<Sysname> display default-configuration
```

## display diagnostic-information

### Syntax

```
display diagnostic-information
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display diagnostic-information** command to display or save the statistics of each module's running status in the system.

When the system is out of order, you need to collect a lot of information to locate the problem. At this time you can use the **display diagnostic-information** command to display or save the statistics of

each module's running status in the system. The **display diagnostic-information** command collects prompt information of the commands **display clock**, **display version**, **display device**, and **display current-configuration**.

## Examples

# Save the statistics of each module's running status in the system.

```
<Sysname> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)?[Y/N]y
Please input the file name(*.diag)[flash:/default.diag]:aa.diag
Diagnostic information is outputting to flash:/aa.diag.
Please wait...
Save succeeded.
```

You can view the content of the file aa.diag by executing the **more aa.diag** command in user view, in combination of the **Page Up** and **Page Down** keys.

# Display the statistics of each module's running status in the system.

```
<Sysname> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:n
```

## display history-command

### Syntax

**display history-command**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display history-command** command to display commands saved in the history buffer.

The system will save validated history commands performed last in current user view to the history buffer, which can save up to ten commands by default. You can use the **history-command max-size** command to set the size of the history buffer. Refer to the **history-command max-size** command in *Login Commands* in the *System Volume* for related configuration.

## Examples

# Display validated history commands in current user view (the display information varies with configuration).

```
<Sysname> display history-command
display history-command
system-view
vlan 2
```

quit

## display hotkey

### Syntax

**display hotkey**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display hotkey** command to display hotkey information.

### Examples

# Display hotkey information.

```
<Sysname> display hotkey
----- HOTKEY -----

          =Defined hotkeys=
Hotkeys Command
CTRL_G  display current-configuration
CTRL_L  display ip routing-table
CTRL_O  undo debug all

          =Undefined hotkeys=
Hotkeys Command
CTRL_T  NULL
CTRL_U  NULL

          =System hotkeys=
Hotkeys Function
CTRL_A  Move the cursor to the beginning of the current line.
CTRL_B  Move the cursor one character left.
CTRL_C  Stop current command function.
CTRL_D  Erase current character.
CTRL_E  Move the cursor to the end of the current line.
CTRL_F  Move the cursor one character right.
CTRL_H  Erase the character left of the cursor.
CTRL_K  Kill outgoing connection.
CTRL_N  Display the next command from the history buffer.
CTRL_P  Display the previous command from the history buffer.
CTRL_R  Redisplay the current line.
```

CTRL\_V Paste text from the clipboard.  
CTRL\_W Delete the word left of the cursor.  
CTRL\_X Delete all characters up to the cursor.  
CTRL\_Y Delete all characters after the cursor.  
CTRL\_Z Return to the User View.  
CTRL\_] Kill incoming connection or redirect connection.  
ESC\_B Move the cursor one word back.  
ESC\_D Delete remainder of word.  
ESC\_F Move the cursor forward one word.  
ESC\_N Move the cursor down a line.  
ESC\_P Move the cursor up a line.  
ESC\_< Specify the beginning of clipboard.  
ESC\_> Specify the end of clipboard.

## display this

### Syntax

**display this** [ **by-linenum** ]

### View

Any view

### Default Level

1: Monitor level

### Parameters

**by-linenum**: Specifies to display the number of each line.

### Description

Use the **display this** command to display the validated configuration under the current view.

After finishing a set of configurations under a view, you can use the **display this** command to check whether the configuration takes effect.

Note that:

- A parameter is not displayed if it has the default configuration.
- A parameter is not displayed if the configuration has not taken effect.
- When you use the command in a user interface view, the command displays the valid configuration in all the user interfaces.
- When you use the command in a VLAN view, the command displays configurations of all created VLANs.

### Examples

# Display the valid configuration information of the current view (the output information depends on the current configuration of the device).

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] display this
#
```

```
user-interface aux 0
user-interface vty 0
  history-command max-size 256
user-interface vty 1 4
#
return
```

## display version

### Syntax

```
display version
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display version** command to view system version information.

By viewing system version information, you can learn about the current software version, rack type and the information related to the interface boards.

### Examples

```
# Display system version information (The system version information varies with devices.).
<Sysname> display version
```

## header

### Syntax

```
header { incoming | legal | login | motd | shell } text
undo header { incoming | legal | login | motd | shell }
```

### View

System view

### Default Level

2: System level

### Parameters

**incoming**: Sets the banner displayed when a Modem login user enters user view. If authentication is needed, the incoming banner is displayed after the authentication is passed.

**legal**: Sets the authorization banner before a user logs onto the terminal interface. The legal banner is displayed before the user inputs the username and password.

**login:** Sets the login banner at authentication.

**motd:** Banner displayed before login. If authentication is required, the banner is displayed before authentication.

**shell:** Sets the banner displayed when a non Modem login user enters user view.

**text:** Banner message, which can be input in two formats. Refer to *Basic System Configuration* for the detailed information.

## Description

Use the **header** command to create a banner.

Use the **undo header** command to clear a banner.

## Examples

```
# Configure banners.<Sysname> system-view
[Sysname] header incoming %
Please input banner content, and quit with the character '%'.
Welcome to incoming(header incoming)%
[Sysname] header legal %
Please input banner content, and quit with the character '%'.
Welcome to legal (header legal)%
[Sysname] header login %
Please input banner content, and quit with the character '%'.
Welcome to login(header login)%
[Sysname] header motd %
Please input banner content, and quit with the character '%'.
Welcome to motd(header motd)%
[Sysname] header shell %
Please input banner content, and quit with the character '%'.
Welcome to shell(header shell)%
```



### Note

The character % is the starting/ending character of text in this example. Entering % after the displayed text quits the **header** command.

As the starting and ending character, % is not a part of a banner.

---

```
# Test the configuration remotely using Telnet. (only when login authentication is configured
can the login banner be displayed).
*****
* Copyright (c) 2004-2008 3Com Corp. and its licensors. All rights reserved. *
* This software is protected by copyright law and international treaties.      *
* Without the prior written permission of 3Com Corporation and its licensors,*
* any reproduction republication, redistribution, decompiling, reverse      *
* engineering is strictly prohibited. Any unauthorized use of this software  *
* or any portion of it may result in severe civil and criminal penalties, and*
```

\* will be prosecuted to the maximum extent possible under the applicable law.\*

\*\*\*\*\*

Welcome to legal(header legal)

Press Y or ENTER to continue, N to exit.

Welcome to motd(header motd)

Welcome to login(header login)

Login authentication

Password:

Welcome to shell(header shell)

<Sysname>

## hotkey

### Syntax

**hotkey** { **CTRL\_G** | **CTRL\_L** | **CTRL\_O** | **CTRL\_T** | **CTRL\_U** } *command*

**undo hotkey** { **CTRL\_G** | **CTRL\_L** | **CTRL\_O** | **CTRL\_T** | **CTRL\_U** }

### View

System view

### Default Level

2: System level

### Parameters

**CTRL\_G**: Assigns the hot key **Ctrl+G** to a command.

**CTRL\_L**: Assigns the hot key **Ctrl+L** to a command.

**CTRL\_O**: Assigns the hot key **Ctrl+O** to a command.

**CTRL\_T**: Assigns the hot key **Ctrl+T** to a command.

**CTRL\_U**: Assigns the hot key **Ctrl+U** to a command.

*command*: The command line associated with the hot key.

### Description

Use the **hotkey** command to assign a hot key to a command line.

Use the **undo hotkey** command to restore the default.

By default, the system specifies corresponding commands for **Ctrl+G**, **Ctrl+L** and **Ctrl+O**, while the others are null.

- **Ctrl+G** corresponds to **display current-configuration**

- **Ctrl+L** corresponds to **display ip routing-table**
- **Ctrl+O** corresponds to **undo debugging all**

You can customize this scheme as needed however.

## Examples

# Assign the hot key **Ctrl+T** to the **display tcp status** command.

```
<Sysname> system-view
[Sysname] hotkey ctrl_t display tcp status
```

# Display the configuration of hotkeys.

```
[Sysname] display hotkey
----- HOTKEY -----

                =Defined hotkeys=
Hotkeys Command
CTRL_G  display current-configuration
CTRL_L  display ip routing-table
CTRL_O  undo debug all
CTRL_T  display tcp status
                =Undefined hotkeys=
Hotkeys Command
CTRL_U  NULL

                =System hotkeys=
Hotkeys Function
CTRL_A  Move the cursor to the beginning of the current line.
CTRL_B  Move the cursor one character left.
CTRL_C  Stop current command function.
CTRL_D  Erase current character.
CTRL_E  Move the cursor to the end of the current line.
CTRL_F  Move the cursor one character right.
CTRL_H  Erase the character left of the cursor.
CTRL_K  Kill outgoing connection.
CTRL_N  Display the next command from the history buffer.
CTRL_P  Display the previous command from the history buffer.
CTRL_R  Redisplay the current line.
CTRL_V  Paste text from the clipboard.
CTRL_W  Delete the word left of the cursor.
CTRL_X  Delete all characters up to the cursor.
CTRL_Y  Delete all characters after the cursor.
CTRL_Z  Return to the user view.
CTRL_]  Kill incoming connection or redirect connection.
ESC_B   Move the cursor one word back.
ESC_D   Delete remainder of word.
ESC_F   Move the cursor forward one word.
ESC_N   Move the cursor down a line.
ESC_P   Move the cursor up a line.
ESC_<  Specify the beginning of clipboard.
```

ESC\_> Specify the end of clipboard.

## quit

### Syntax

**quit**

### View

Any view

### Default Level

0: User level (in user view)

2: System level (in other views)

### Parameters

None

### Description

Use the **quit** command to exit to a lower-level view. If the current view is user view, the **quit** command terminates the current connection and quit the system.

### Examples

# Switch from GigabitEthernet1/0/1 interface view to system view, and then to user view.

```
[Sysname-GigabitEthernet1/0/1] quit
```

```
[Sysname] quit
```

```
<Sysname>
```

## return

### Syntax

**return**

### View

Any view except user view

### Default Level

2: System level

### Parameters

None

### Description

Use the **return** command to return to user view from current view (not user view).

You can also use the hot key **Ctrl+Z** to return to user view from current (not user view).

Related commands: **quit**.

## Examples

```
# Return to user view from GigabitEthernet1/0/1 view.  
[Sysname-GigabitEthernet1/0/1] return  
<Sysname>
```

## screen-length disable

### Syntax

```
screen-length disable  
undo screen-length disable
```

### View

User view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **screen-length disable** command to disable the multiple-screen output function of the current user.

Use the **undo screen-length disable** command to enable the multiple-screen output function of the current user.

By default, a login user uses the settings of the **screen-length** command. The default settings of the **screen-length** command are: multiple-screen output is enabled and 24 lines are displayed on the next screen. (For the details of the **screen-length** command, refer to *Login Commands* in the *System Volume*.)

Note that this command is applicable to the current user only and when a user re-logs in, the settings restore to the system default.

## Examples

```
# Disable multiple-screen output of the current user.  
<Sysname> screen-length disable
```

## super

### Syntax

```
super [ /level ]
```

### View

User view

### Default Level

0: Visit level

## Parameters

*level*: User level, in the range 0 to 3, and defaults to 3.

## Description

Use the **super** command to switch from the current user privilege level to a specified user privilege level.

If you do not provide the *level* argument, the current user privilege level will be switched to 3.

Login users are classified into four levels that correspond to the four command levels. After users at different levels log in, they can only use commands at their own, or lower, levels.

Note that:

Users can switch to a lower user privilege level unconditionally. However, no password is needed only for console login user level switching; to switch to a higher user privilege level, and log in from AUX and VTY user interfaces, users need to enter the password needed for the security's sake. If the entered password is incorrect or no password is configured, the switching fails. Therefore, before switching a user to a higher user privilege level, you should configure the password needed.

Related commands: **super password**.

## Examples

# Set the user privilege level to 2 (The current user privilege level is 3.).

```
<Sysname> super 2
```

```
User privilege level is 2, and only those commands can be used  
whose level is equal or less than this.
```

```
Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
```

# Switch the user privilege level back to 3 (Suppose password **123** has been set; otherwise, the user privilege level cannot be switched to 3.).

```
<Sysname> super 3
```

```
Password:
```

```
User privilege level is 3, and only those commands can be used  
whose level is equal or less than this.
```

```
Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
```

## super password

### Syntax

```
super password [ level user-level ] { simple | cipher } password
```

```
undo super password [ level user-level ]
```

### View

System view

### Default Level

2: System level

### Parameters

**level user-level**: User privilege level in the range 1 to 3, with the default as 3.

**simple:** Plain text password.

**cipher:** Cipher text password.

*password:* Password, a string of characters. It is case-sensitive.

- For simple password, it is a string of 1 to 16 characters.
- For cipher password, it is a string of 1 to 16 characters in plain text or 24 characters in cipher text. For example, the simple text “1234567” corresponds to the cipher text “(TT8FJY\5SQ=^Q`MAF4<1!!”.

## Description

Use the **super password** command to set the password needed to switch from a lower user privilege level to a higher one.

Use the **undo super password** command to restore the default.

By default, no password is set to switch from a lower user privilege level to a higher one.

Note that:

- If **simple** is specified, the configuration file saves a simple password.
- If **cipher** is specified, the configuration file saves a cipher password.
- The user must always enter a simple password, no matter **simple** or **cipher** is specified.
- Cipher passwords are recommended, as simple ones are easily getting cracked.

## Examples

# Set the password to **abc** in simple form for switching user-level to 3.

```
<Sysname> system-view
[Sysname] super password level 3 simple abc
```

Display the password for switching user-level.

```
[Sysname] display current-configuration
#
super password level 3 simple abc
```

# Set the password to abc in cipher form for switching user-level to 3.

```
<Sysname> system-view
[Sysname] super password level 3 cipher abc
```

Display the password for switching user-level.

```
[Sysname] display current-configuration
#
super password level 3 cipher =`*Y=F>*.%-a_SW8\MYM2A!!
```

## sysname

### Syntax

**sysname** *sysname*

**undo sysname**

### View

System view

## Default Level

2: System level

## Parameters

*sysname*: Name of the device, a string of 1 to 30 characters.

## Description

Use the **sysname** command to set the name of the device.

Use the **undo sysname** demand to restore the device name to the default.

The default name is “**3Com**” by default.

Modifying device name affects the prompt of the CLI. For example, if the device name is **Sysname**, the prompt of user view is <Sysname>.

## Examples

# Set the name of the device to **Switch**.

```
<Sysname> system-view
[Sysname] sysname Switch
[Switch]
```

## system-view

### Syntax

**system-view**

### View

User view

### Default Level

2: System level

### Parameters

None

### Description

Use the **system-view** command to enter system view from the current user view.

Related commands: **quit**, **return**.

### Examples

# Enter system view from the current user view.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname]
```

# Table of Contents

<b>1 Device Management Commands</b> .....	<b>1-1</b>
Device Management Commands.....	1-1
boot-loader file.....	1-1
bootrom .....	1-2
bootrom-update security-check enable .....	1-4
display boot-loader .....	1-4
display cpu-usage.....	1-5
display cpu-usage history.....	1-7
display device .....	1-10
display device manuinfo .....	1-11
display environment.....	1-12
display fan .....	1-13
display memory .....	1-13
display power.....	1-14
display reboot-type .....	1-15
display rps .....	1-15
display schedule job .....	1-16
display schedule reboot.....	1-17
display system-failure .....	1-17
display transceiver alarm.....	1-18
display transceiver diagnosis .....	1-21
display transceiver.....	1-22
display transceiver manuinfo.....	1-23
reboot.....	1-24
reset unused porttag.....	1-25
schedule job .....	1-26
schedule reboot at.....	1-27
schedule reboot delay .....	1-29
shutdown-interval .....	1-30
startup bootrom-access enable .....	1-31
system-failure .....	1-32

# 1 Device Management Commands

---

## Device Management Commands

### boot-loader file

#### Syntax

```
boot-loader file file-url slot { all | slot-number } { main | backup }
```

#### View

User view

#### Default Level

2: System level

#### Parameters

*file-url*: Specifies a file name, a string of 1 to 63 characters, in the format of [*drive*:/][*path*]/*file-name*, where

- The items in square brackets [ ] are optional.
- *drive* specifies the storage medium of the file. The value is the name of the storage medium. For the 3Com Switch 4800G, the storage medium can only be a flash.
- *path* specifies the folder of the file. If you do not provide this argument, the file must be in the root directory of the specified storage medium. If the file is saved in a subfolder, you can use this argument multi-times, for example, **test/subtest/test.bin**.
- *file-name* specifies the filename, which is usually suffixed by **.bin**. Suffixes vary with devices.
- If you do not provide arguments *drive* and *path*, the file with the name *file-name* under the current path is specified. You can use the **cd** command to switch to another path. For details of the **cd** command, refer to *File System Management Commands* in the *System Volume*.

**slot** *slot-number*: Specifies the member ID of a device.

- **all**: Specifies a file as the boot file at the next boot for all member devices in a stack system.
- *slot-number*: Specifies a file as the boot file at the next boot for a member device. *slot-number* is the member ID of the device. You can use the **display irf** command to view the member IDs of devices in a stack system.

**main**: Specifies a file as a main boot file. A main boot file is used to boot a device.

**backup**: Specifies a file as a backup boot file. A backup boot file is used to boot a device only when a main boot file is unavailable.

#### Description

Use the **boot-loader** command to specify a boot file for a member device for the next device boot.

Note the following:

- To execute the **boot-loader** command successfully, you must save the file for the next device boot under the root directory of the storage media on a member device.
- If the storage medium is on the master, you can specify the storage medium by giving its name, such as **flash**; if the storage medium is on a slave, you can specify the storage medium by giving its name and the member ID of the device, that is, in the format of `slotslot-number#StorageMediumName` (*slot-number* represents the member ID of the slave), such as **slot2#flash**.
- When you specify the boot file of the master, the *file-url* argument cannot contain the member ID of the device, and *slot-number* should be specified as the member ID of the master; when you specify the boot file of the slave, the *file-url* argument must contain the member ID (such as **slot2#flash:/test.bin**), and *slot-number* should be specified as the member ID of the slave.
- If you provide the keyword **all**, the *file-url* argument cannot contain a member ID, otherwise, the execution of this command will fail; you must save the specified boot file on the storage media of all member devices in the same filename, otherwise, member devices without this file will fail to be reconfigured during the reboot.
- The names of the files for the next boot of the master and slaves may be different, but the versions of the files must be the same; otherwise, a slave will reboot by using the master's boot file and join the stack again.

Related commands: **display boot-loader**.

## Examples

# Specify the main boot file for the master (the member ID is 1) for the next device boot as **test.bin** (Make sure that the file **test.bin** is already saved on the storage medium of the master; otherwise, the system prompts error and the execution of the command fails).

```
<Sysname> boot-loader file test.bin slot 1 main
```

```
This command will set the boot file of the specified board. Continue? [Y/N]:y
```

```
The specified file will be used as the main boot file at the next reboot on slot 1!
```

# Specify the main boot file for the slave (the member ID is 2) for the next device boot as **test.bin** (Make sure that the file **test.bin** is already saved on the storage medium of the slave; otherwise, the system prompts error and the execution of the command fails).

```
<Sysname> boot-loader file slot2#flash:/test.bin slot 2 main
```

```
This command will set the boot file of the specified board. Continue? [Y/N]:y
```

```
The specified file will be used as the main boot file at the next reboot on slot 2!
```

# Specify the main boot file for all member devices for the next device boot as **test.bin** (Make sure that the file **test.bin** is already saved on the storage media of all the member devices; otherwise, the system prompts error and the execution of the command fails).

```
<Sysname> boot-loader file test.bin slot all main
```

```
This command will set the boot file of the specified board. Continue? [Y/N]:y
```

```
The specified file will be used as the main boot file at the next reboot on slot 1!
```

```
The specified file will be used as the main boot file at the next reboot on slot 2!
```

```
<Sysname> boot-loader update slot 1
```

## bootrom

### Syntax

**bootrom** | **update file** *file-url* **slot** *slot-number-list*

## View

User view

## Default Level

2: System level

## Parameters

**update file** *file-url*: Upgrades Boot ROM, where *file-url* is a string of 1 to 63 characters and represents name of the file to be upgraded. *file-url* is in the format of [*drive:/*][*path*]/*file-name*, where

- The items in square brackets [ ] are optional.
- *drive* specifies the storage medium of the file. The value is the name of the storage medium. For the 3Com Switch 4800G, the storage medium can only be a flash.
- *path* specifies the folder of the file. If you do not provide this argument, the file must be in the root directory of the specified storage medium. If the file is saved in a subfolder, you can use this argument multi-times, for example, **test/subtest/test.bin**.
- *file-name* specifies the filename.
- If you do not provide arguments *drive* and *path*, the file with the name *file-name* under the current path is specified. You can use the **cd** command to switch to another path. For details of the **cd** command, refer to the *File System Management Commands* in the *System Volume*.

**slot** *slot-number-list*: Specifies a list of IDs of member devices, in the format of { *slot-number* [ **to** *slot-number* ] }&<1-7>. The *slot-number* argument represents the ID of a member device. You can use the **display irf** command to view the member IDs of stack members.

## Description

Use the **bootrom** command to read, restore, back up, or upgrade the Boot ROM program on a specified member device(s).

Note the following:

- To execute the **bootrom** command successfully, you must save the Boot ROM program under the root directory of the storage media on a member device.
- If the storage medium is on the master, you can specify the storage medium by giving its name, such as **flash**; If a storage medium is on a slave, you can specify the storage medium by giving its name and the member ID of the device, that is, in the format of *slotslot-number#StorageMediumName* (*slot-number* represents the member ID of the slave), such as **slot2#flash**.
- When you upgrade the Boot ROM program for the master, the *file-url* argument cannot contain the member ID of the device, and *slot-number* should be specified as the member ID of the master; when you upgrade the Boot ROM program for a slave, the *file-url* argument must contain the member ID (such as **slot2#flash:/test.bin**), *slot-number* should be specified as the member ID of the slave.

## Examples

# Use the **a.btm** file to upgrade the Boot ROM program on the master (the member ID is 1).

```
<Sysname> bootrom update file a.btm slot 1
This command will update bootrom file on the specified board(s), Continue? [Y/N]:y
This command will update bootrom file on the specified board(s), Continue? [Y/N]:y
Now updating bootrom, please wait...
Succeeded to update bootrom of Board 1.
```

# Use the **a.btm** file to upgrade the Boot ROM program on the slave (the member ID is 2).

```
<Sysname> bootrom update file slot2#flash:/a.btm slot 2
This command will update bootrom file on the specified board(s), Continue? [Y/N]:y
Now updating bootrom, please wait...
Succeeded to update bootrom of Board 1
```

## bootrom-update security-check enable

### Syntax

```
bootrom-update security-check enable
undo bootrom-update security-check enable
```

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **bootrom-update security-check enable** command to enable the validity check function.

Use the **undo bootrom-update security-check enable** command to disable the validity check function.

By default, the validity check function is enabled at the time of upgrading Boot ROM.

After the validity check function is enabled, the device will strictly check whether the Boot ROM upgrade files are valid and can match the hardware.

### Examples

```
# Enable the validity check function when upgrading Boot ROM.
```

```
<Sysname> system-view
[Sysname] bootrom-update security-check enable
```

## display boot-loader

### Syntax

```
display boot-loader [ slot slot-number ]
```

### View

Any view

### Default Level

2: System level

## Parameters

**slot** *slot-number*: Displays boot file information of a member device, where *slot-number* represents the member ID of the device. If you do not provide this argument, the information of the boot files of all member devices will be displayed. You can use the **display irf** command to view the member IDs of devices in a stack system.

## Description

Use the **display boot-loader** command to display information of the boot file.

Related commands: **boot-loader**.

## Examples

# Display the file adopted for the current and next boot of the device.

```
<Sysname> display boot-loader
Slot 12
The current boot app is:  flash:/test.bin
The main boot app is:    flash:/test.bin
The backup boot app is:  flash:/test.bin
```

**Table 1-1 display boot-loader** command output description

Field	Description
Slot 1	The member ID of the device is 1
The current boot app is	Boot file used for the device for the current device boot
The main boot app is	Main boot file used for the device for the next device boot
The backup boot app is	Backup boot file used for the device for the next device boot

## display cpu-usage

### Syntax

```
display cpu-usage [ slot slot-number [ cpu cpu-number ] ]
display cpu-usage entry-number [ offset ] [ verbose ] [ slot slot-number [ cpu cpu-number ] ]
[ from-device ]
```

### View

Any view

### Default Level

1: Monitor level

## Parameters

*entry-number*: Number of entries to be displayed once, in the range 1 to 60.

*offset*: Offset between the serial number of the first CPU usage statistics record to be displayed and that of the last CPU usage record to be displayed, in the range 0 to 59. For example, the idx of the latest statistics record is 12, if the *offset* is set to 3, the system will display the statistics records from the one

with the `idx` of 9. `idx` represents the serial number of the period for the statistics, and its value ranges from 0 to 60 cyclically. The system makes CPU usage statistics periodically; after each period, the system records the average CPU usage during this period, and the `idx` value is added by 1 automatically.

**verbose:** Specifies to display detailed information of CPU usage statistics. If this keyword is not provided, the system displays the brief information of the CPU usage statistics; if this keyword is provided, the system displays the average CPU usage statistics for each task in the specified period.

**from-device:** Displays external storage media such as Flash and hard disk. The device currently does not support the **from-device** keyword.

**slot** *slot-number*: Indicates to display the statistics of the CPU usage of the specified member device. *slot-number* specifies the member ID of the device. You can use the **display irf** command to view the member IDs of devices in a stack system.

**cpu** *cpu-number*: Displays the CPU usage statistics of the specified CPU. If the *cpu-number* argument is not provided, the system displays the CPU usage statistics of all CPUs of the specified board or member device.

## Description

Use the **display cpu-usage** command to display the CPU usage statistics.

The system takes statistics of CPU usage at intervals (usually every 60 seconds) and saves the statistical results in the history record area. **display cpu-usage** *entry-number* indicates the system displays *entry-number* records from the newest (last) record. **display cpu-usage** *entry-number* *offset* indicates the system displays *entry-number* records from the last but *offset* record.

Equivalent to the **display cpu-usage 1 0 verbose** command, the **display cpu-usage** command displays detailed information of the last CPU usage statistics record.

## Examples

# Display information of the current CPU usage statistics.

```
<Sysname> display cpu-usage
Slot 1 CPU usage:
    6% in last 5 seconds
    10% in last 1 minute
    5% in last 5 minutes
Slot 2 CPU usage:
    5% in last 5 seconds
    8% in last 1 minute
    5% in last 5 minutes
```

# Display the last fifth and sixth records of the CPU usage statistics history.

```
<Sysname> display cpu-usage 2 4
===== CPU usage info (no: 0 idx: 58) =====
CPU Usage Stat. Cycle: 60 (Second)
CPU Usage           : 3%
CPU Usage Stat. Time : 2006-07-10 10:56:55
CPU Usage Stat. Tick : 0x1d9d(CPU Tick High) 0x3a659a70(CPU Tick Low)
Actual Stat. Cycle   : 0x0(CPU Tick High) 0x95030517(CPU Tick Low)

===== CPU usage info (no: 1 idx: 57) =====
```

```

CPU Usage Stat. Cycle: 60 (Second)
CPU Usage           : 3%
CPU Usage Stat. Time : 2006-07-10 10:55:55
CPU Usage Stat. Tick : 0x1d9c(CPU Tick High) 0xa50e5351(CPU Tick Low)
Actual Stat. Cycle   : 0x0(CPU Tick High) 0x950906af(CPU Tick Low)

```

**Table 1-2 display cpu-usage command output description**

Field	Description
6% in last 5 seconds	After the device boots, the system calculates and records the average CPU usage in every five seconds. This field displays the average CPU usage in the last five seconds.
10% in last 1 minute	After the device boots, the system calculates and records the average CPU usage in every one minute. This field displays the average CPU usage in the last minute.
5% in last 5 minutes	After the device boots, the system calculates and records the average CPU usage in every five minutes. This field displays the average CPU usage in the last five minutes.
Slot 2 CPU usage	The CPU usage of the member device (the member ID is 2).
CPU usage info (no: idx:)	Information of CPU usage records (no: The (no+1)th record is currently displayed. no numbers from 0, a smaller number equals a newer record. idx: index of the current record in the history record table). If only the information of the current record is displayed, no and idx are not displayed.
CPU Usage Stat. Cycle	CPU usage measurement interval, in seconds. For example, if the value is 41, it indicates that the average CPU usage during the last 41 seconds is calculated. The value range of this field is 1 to 60.
CPU Usage	Average CPU usage in a measurement interval, in percentage
CPU Usage Stat. Time	CPU usage statistics time in seconds, that is, the system time when the command is executed
CPU Usage Stat. Tick	System runtime in ticks, represented by a 64-bit hexadecimal. CPU Tick High represents the most significant 32 bits and the CPU Tick Low the least significant 32 bits.
Actual Stat. Cycle	Actual CPU usage measurement interval in ticks, represented by a 64-bit hexadecimal. CPU Tick High represents the most significant 32 bits and the CPU Tick Low the least significant 32 bits. Owing to the precision of less than one second, the actual measurement periods of different CPU usage records may differ slightly.

## display cpu-usage history

### Syntax

```
display cpu-usage history [ task task-id ] [ slot slot-number [ cpu cpu-number ] ]
```

### View

Any view

## Default Level

1: Monitor level

## Parameters

**task** *task-id*: Displays the history statistics of the CPU usage of the specified task, where *task-id* represents the task number. If the *task-id* argument is not provided, the system displays the history statistics of the CPU usage of the entire system (the CPU usage of the entire system is the sum of CPU usages of all tasks).

**slot** *slot-number*: Displays the history statistics of the CPU usage of the specified member device. *slot-number* specifies the member ID of a device. You can use the **display irf** command to view the member IDs of devices in a stack system. If the *slot-number* argument is not provided, the system displays the history statistics of the CPU usage of the master.

**cpu** *cpu-number*: Displays the history statistics of the CPU usage of the specified CPU. If the *cpu-number* argument is not provided, the system displays the history statistics of the CPU usage of the main CPU.

## Description

Use the **display cpu-usage history** command to display the history statistics of the CPU usage in a chart.

If no argument is provided, the system displays the CPU usage of the master.

The system takes statistics of the CPU usage at an interval and saves the statistical results in the history record area. You can use the **display cpu-usage history** command to display the CPU usage statistics records during the last 60 minutes. The statistical results are displayed through geographical coordinates. In the output information:

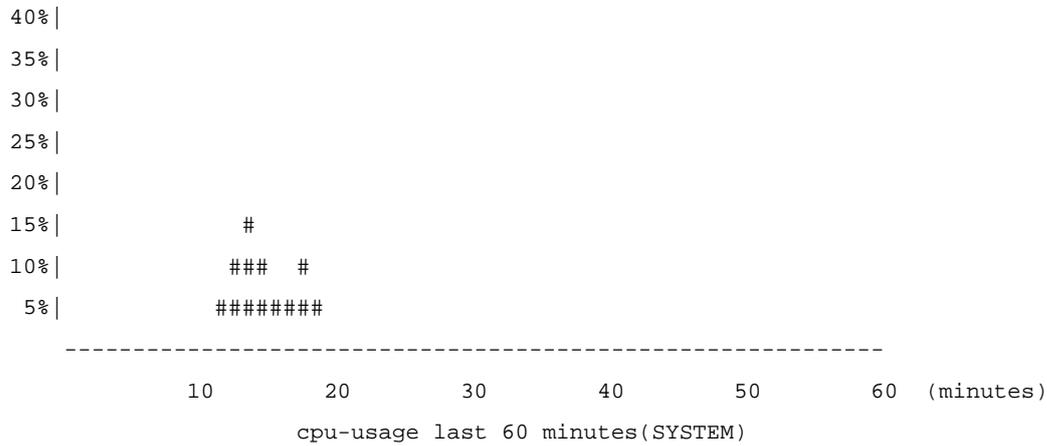
- Latitude indicates the CPU usage, which is displayed based on the step. For example, if the step of the CPU usage is 5%, then the actual statistics value 53% is displayed as 55%, and actual statistics value 52% is displayed as 50%.
- Longitude indicates the time.
- Consecutive pond marks (#) indicate the CPU usage at a certain moment. The value of the latitude corresponding to the # mark on the top of a moment is the CPU usage at this moment.

## Examples

# Display the CPU usage statistics of the whole system.

```
<Sysname> display cpu-usage history
```

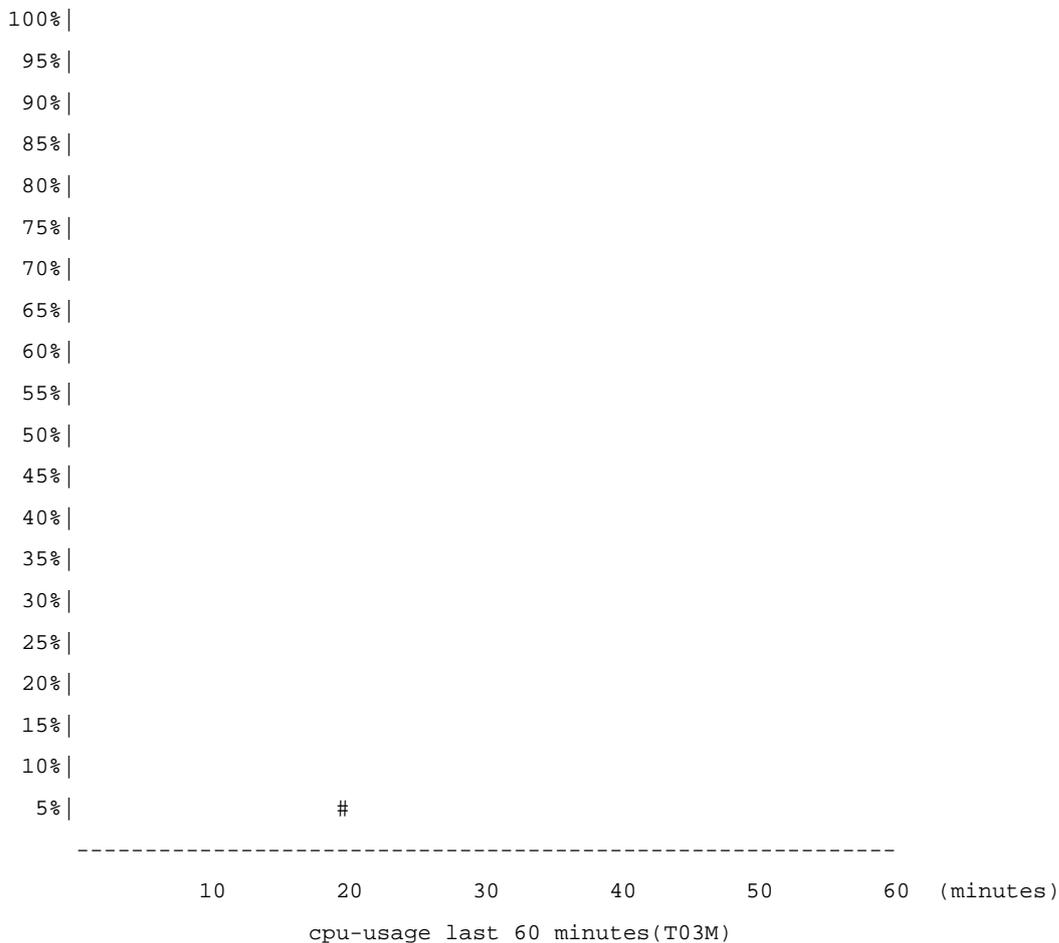
```
100% |
 95% |
 90% |
 85% |
 80% |
 75% |
 70% |
 65% |
 60% |
 55% |
 50% |
 45% |
```



The above output information indicates the CPU usage of the whole system in the last 60 minutes: 5% in the twelfth minute, 10% in the thirteenth minute, 15% in the fourteenth minute, 10% in the fifteenth minute, 5% in the sixteenth and seventeenth minute, 10% in the eighteenth minute, 5% in the nineteenth minute, and 2% or lower than 2% at other times.

# Display the CPU usage statistics of task 6.

```
<Sysname> display cpu-usage history task 6
```



The above output information indicates the CPU usage of task 6 (with the task name **T03M**) in the last 60 minutes: 5% in the twentieth minute, and 2% or lower than 2% at other times.

## display device

### Syntax

```
display device [ [ shelf shelf-number ] [ frame frame-number ] [ slot slot-number [ subslot
subslot-number ] ] | verbose ]
```

### View

Any view

### Default Level

2: System level

### Parameters

**shelf** *shelf-number*: Displays detailed information of the specified shelf or unit. The *shelf-number* argument represents a shelf number or unit number and the value is 0 for the 3Com Switch 4800G.

**frame** *frame-number*: Displays detailed information of the specified frame. The *frame-number* argument represents a frame number and the value is 0 for the 3Com Switch 4800G.

**slot** *slot-number*: Displays information of the specified member device. The *slot-number* argument represents the member ID of the device. You can use the **display irf** command to view the member IDs of devices in a stack system.

**subslot** *subslot-number*: Displays information of the specified subboard. The *subslot-number* represents the subslot of a subboard.

**verbose**: Displays detailed information.

### Description

Use the **display device** command to display information about the device.

### Examples

# Display the information of all stack members.

```
<Sysname> display device
Slot 1
SubSNo PortNum PCBVer FPGAVer CPLDVer BootRomVer AddrLM Type State
0 28 REV.C NULL 002 505 IVL MAIN Normal
1 0 REV.A NULL NULL NULL IVL 2*10GE Normal
Slot 2
SubSNo PortNum PCBVer FPGAVer CPLDVer BootRomVer AddrLM Type State
0 28 REV.C NULL 002 503 IVL MAIN Normal
1 0 REV.B NULL NULL NULL IVL 2*10GE Normal
```

The above information indicates that the stack contains two member devices, each of which has 28 Ethernet interfaces and is configured with two 10 GE physical stack ports.

**Table 1-3 display device** command output description

Field	Description
Slot 1	Information of the device with the member ID of 1
SubSNo	Number of the slot in which the subboard resides

Field	Description
PortNum	Maximum number of ports that a subboard supports
AddrLM	Address learning mode

## display device manuinfo

### Syntax

**display device manuinfo**

### View

Any view

### Default Level

3: Manage level

### Parameters

**None**

### Description

Use the **display device manuinfo** command to display electrical label information about the device.

Electrical label information is also called permanent configuration data or archive information, which is written to the storage medium of the device during debugging or test of device. The information includes name of the board, device serial number, and vendor name. This command displays part of the electrical label information of the device.

### Examples

# Display electrical label information.

```
<Sysname> display device manuinfo
slot 1
DEVICE_NAME          : 3CRS48G-24-91
DEVICE_SERIAL_NUMBER : 210235A2540000000001
MAC_ADDRESS          : 001C-C5BC-3111
MANUFACTURING_DATE   : 2008-05-08
VENDOR_NAME          : 3Com
slot 2
DEVICE_NAME          : 3CRS48G-24-91
DEVICE_SERIAL_NUMBER : 210235A252A079000140
MAC_ADDRESS          : 000F-E269-46D1
MANUFACTURING_DATE   : 2007-09-26
VENDOR_NAME          : 3Com
```

**Table 1-4 display device manuinfo** command output description

Field	Description
DEVICE_NAME	Device name

Field	Description
DEVICE_SERIAL_NUMBER	Device serial number
MAC_ADDRESS	MAC address of the device
MANUFACTURING_DATE	Manufacturing date of the device
VENDOR_NAME	Vendor name

## display environment

### Syntax

**display environment**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display environment** command to display the temperature information, including the current temperature and temperature thresholds of boards.

### Examples

# Display the temperature information of the device.

```
<Sysname> display environment
System Temperature information (degree centigrade):
-----
SlotNo    Temperature    Lower limit    Upper limit
1         34             0              55
2         34             0              55
```

**Table 1-5 display environment** command output description

Field	Description
System Temperature information (degree centigrade)	Temperature information of system boards (degree centigrade)
SlotNO	Member ID of the device
Temperature	Current temperature
Lower limit	Lower limit of temperature
Upper limit	Upper limit of temperature

## display fan

### Syntax

```
display fan [ slot slot-number [ fan-id ] ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*fan-id*: Displays the operating state of the specified fan, where *fan-id* represents the built-in fan number.

**slot** *slot-number*: Displays the operating state of fans of the specified member device, where *slot-number* represents the member ID of the device. Support for **slot** *slot-number* depends on the device model. You can use the **display irf** command to view the member IDs of devices in a stack system. If the *slot-number* argument is not provided, the system displays the operating state of fans of all member devices.

### Description

Use the **display fan** command to display the operating state of built-in fans.

### Examples

# Display the operating state of all fans in a device.

```
<Sysname> display fan
Slot 1
  FAN    1
  State  : Normal
Slot 2
  FAN    1
  State  : Normal
```

## display memory

### Syntax

```
display memory [ slot slot-number [ cpu cpu-number ] ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**slot** *slot-number*: Displays the memory of a CPU of the specified member device, where *slot-number* represents the member ID of the device. You can use the **display irf** command to view the member IDs of devices in a stack system.

**cpu *cpu-number***: Displays the memory of a specified CPU, where *cpu-number* represents the ID of the CPU.

## Description

Use the **display memory** command to display the usage of the memory of a device.

If the keyword **slot** is not provided, the system displays the usage of the memory of the master device; if the keyword **cpu** is not provided, the system displays the memory of the main CPU.

## Examples

# Display the usage of the memory of a device.

```
<Sysname> display memory
System Total Memory(bytes): 431869088
Total Used Memory(bytes): 71963156
Used Rate: 16%
```

**Table 1-6 display memory command output description**

Field	Description
System Total Memory(bytes)	Total size of the system memory (in bytes)
Total Used Memory(bytes)	Size of the memory used (in bytes)
Used Rate	Percentage of the memory used to the total memory

## display power

### Syntax

```
display power [ slot slot-number [ power-id ] ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**slot *slot-number***: Displays the status of the power supply of the specified device in an IRF stack, where *slot-number* represents the member ID of the device. You can use the **display irf** command to view the member IDs of devices in a stack system.

***power-id***: Displays the status of the specified power supply unit (PSU), where *power-id* represents the PSU number. The value varies with devices.

## Description

Use the **display power** command to display the status of the power supply of a device.

## Examples

# Display the status of the power supply of a device.

```
<Sysname> display power
Slot 1
    Power    1
    State    : Normal
    Type     : AC

Slot 2
    Power    1
    State    : Normal
    Type     : AC
```

## display reboot-type

### Syntax

```
display reboot-type [ slot slot-number ]
```

### View

Any view

### Default Level

2: System level

### Parameters

**slot** *slot-number*: Displays reboot mode of the specified member device, where *slot-number* represents the member ID of the device. You can use the **display irf** command to view the member IDs of devices in a stack system.

### Description

Use the **display reboot-type** command to display the reboot mode of the device.

If no keyword is provided, the system displays the reboot mode of the master.

### Examples

# Display the reboot mode of the device.

```
<Sysname> display reboot-type
The rebooting type this time is: Cold
```

The above information indicates that the last reboot mode of the device is Cold boot (cold boot is to restart a device by powering it on). (The display of Warm represents a warm boot, which means to restart a device by using the commands like **reboot**).

## display rps

### Syntax

```
display rps [ slot slot-number [ rps-id ] ]
```

### View

Any view

## Default Level

1: Monitor level

## Parameters

**slot** *slot-number*: Displays the RPS status of the specified member device, where *slot-number* represents the member ID of the device. You can use the **display irf** command to view the member IDs of devices in a stack system. If the *slot-number* argument is not provided, the system displays the RPS status of all stack members.

*rps-id*: Displays the status of the specified RPS, where *rps-id* represents the RPS number. The value varies with devices.

## Description

Use the **display rps** command to display status of the RPS.

## Examples

# Display RPS status of the device.

```
<Sysname> display rps
Slot 1
    Power      2
    State      : Absent

Slot 2
    Power      2
    State      : Absent
```

## display schedule job

### Syntax

```
display schedule job
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display schedule job** command to display the detailed configurations of the scheduled automatic execution function.

### Examples

# Display the detailed configurations of the current scheduled automatic execution function.

```
<Sysname> display schedule job
```

```
Specified command: execute 1.bat
Specified view: system view
Executed time: at 12:00 10/31/2007 (in 0 hours and 16 minutes)
```

If you modify the system time within 16 minutes, the configurations of scheduled automatic execution of the batch file will become invalid, and then when you execute the **display schedule job** command again, the system displays nothing.

## display schedule reboot

### Syntax

```
display schedule reboot
```

### View

Any view

### Default Level

3: Manage level

### Parameters

None

### Description

Use the **display schedule reboot** command to display the device reboot time set by the user.

Related commands: **schedule reboot at** and **schedule reboot delay**.

### Examples

```
# Display the reboot time of a device.
```

```
<Sysname> display schedule reboot
```

```
System will reboot at 16:00:00 03/10/2006 (in 2 hours and 5 minutes).
```

The above information indicates the system will reboot at 16:00:00 on March 10, 2006 (in two hours and five minutes).

## display system-failure

### Syntax

```
display system-failure
```

### View

Any view

### Default Level

3: Manage level

### Parameters

None

## Description

Use the **display system-failure** command to display the exception handling method of all member devices in a stack system.

Related commands: **system-failure**.

## Examples

```
# Display the exception handling method.
<Sysname> display system-failure
System failure handling method: reboot
```

## display transceiver alarm

### Syntax

```
display transceiver alarm interface interface-type interface-number
```

### View

Any view

### Default Level

2: System level

### Parameters

**interface** [ *interface-type interface-number* ]: Displays the current alarm information of the pluggable transceiver plugged in the specified interface. *interface-type interface-number* represents interface type and interface number. If it is not specified, the command displays the current alarm information of the pluggable transceiver in all the interfaces.

## Description

Use the **display transceiver alarm** command to display the current alarm information of a single or all transceivers.

If no error occurs, **None** is displayed.

[Table 1-7](#) shows the alarm information that may occur for the four types of commonly used transceivers.

**Table 1-7 display transceiver alarm** command output description

Field	Remarks
GBIC/SFP	
RX loss of signal	Incoming (RX) signal is lost.
RX power high	Incoming (RX) power level is high.
RX power low	Incoming (RX) power level is low.
TX fault	Transmit (TX) fault
TX bias high	TX bias current is high.
TX bias low	TX bias current is low.
TX power high	TX power is high.

Field	Remarks
TX power low	TX power is low.
Temp high	Temperature is high.
Temp low	Temperature is low.
Voltage high	Voltage is high.
Voltage low	Voltage is low.
Transceiver info I/O error	Transceiver information read and write error
Transceiver info checksum error	Transceiver information checksum error
Transceiver type and port configuration mismatch	Transceiver type does not match port configuration.
Transceiver type not supported by port hardware	Transceiver type is not supported on the port.
XFP	
RX loss of signal	Incoming (RX) signal is lost.
RX not ready	RX is not ready
RX CDR loss of lock	RX clock cannot be recovered.
RX power high	RX power is high.
RX power low	RX power is low.
TX not ready	TX is not ready.
TX fault	TX fault
TX CDR loss of lock	TX clock cannot be recovered.
TX bias high	TX bias current is high.
TX bias low	TX bias current is low.
TX power high	TX power is high.
TX power low	TX power is low.
Module not ready	Module is not ready.
APD supply fault	APD (Avalanche Photo Diode) supply fault
TEC fault	TEC (Thermoelectric Cooler) fault
Wavelength unlocked	Wavelength of optical signal exceeds the manufacturer's tolerance.
Temp high	Temperature is high.
Temp low	Temperature is low.
Voltage high	Voltage is high.
Voltage low	Voltage is low.
Transceiver info I/O error	Transceiver information read and write error
Transceiver info checksum error	Transceiver information checksum error
Transceiver type and port configuration mismatch	Transceiver type does not match port configuration.

Field	Remarks
Transceiver type not supported by port hardware	Transceiver type is not supported on the port.
XENPAK	
WIS local fault	WIS (WAN Interface Sublayer) local fault
Receive optical power fault	Receive optical power fault
PMA/PMD receiver local fault	PMA/PMD (Physical Medium Attachment/Physical Medium Dependent) receiver local fault
PCS receive local fault	PCS (Physical Coding Sublayer) receiver local fault
PHY XS receive local fault	PHY XS (PHY Extended Sublayer) receive local fault
RX power high	RX power is high.
RX power low	RX power is low.
Laser bias current fault	Laser bias current fault
Laser temperature fault	Laser temperature fault
Laser output power fault	Laser output power fault
TX fault	TX fault
PMA/PMD receiver local fault	PMA/PMD receiver local fault
PCS receive local fault	PCS receive local fault
PHY XS receive local fault	PHY XS receive local fault
TX bias high	TX bias current is high.
TX bias low	TX bias current is low.
TX power high	TX power is high.
TX power low	TX power is low.
Temp high	Temperature is high.
Temp low	Temperature is low.
Transceiver info I/O error	Transceiver information read and write error
Transceiver info checksum error	Transceiver information checksum error
Transceiver type and port configuration mismatch	Transceiver type does not match port configuration.
Transceiver type not supported by port hardware	Transceiver type is not supported on the port.

## Examples

# Display the alarm information of the pluggable transceiver plugged in interface GigabitEthernet1/0/1. (The output of this command varies with devices.)

```
<Sysname> display transceiver alarm interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 transceiver current alarm information:
  RX loss of signal
  RX power low
```

**Table 1-8 display transceiver alarm** command output description

Field	Description
transceiver current alarm information	Current alarm information of the transceiver
RX loss of signal	Incoming (RX) signal is lost.
RX power low	Incoming (RX) power level is low.

## display transceiver diagnosis

### Syntax

**display transceiver diagnosis interface** [ *interface-type interface-number* ]

### View

Any view

### Default Level

2: System level

### Parameters

**interface** [ *interface-type interface-number* ]: Displays the currently measured value of digital diagnosis parameters of the 3Com customized anti-spoofing pluggable optical transceiver plugged in the specified interface. *interface-type interface-number* represents interface type and interface number. If it is not specified, the command displays the currently measured value of digital diagnosis parameters of 3Com customized anti-spoofing pluggable optical transceivers in all the interfaces.

### Description

Use the **display transceiver diagnosis** command to display the currently measured value of digital diagnosis parameters of H3C customized anti-spoofing pluggable optical transceivers.

### Examples

# Display the currently measured value of the digital diagnosis parameters of the H3C customized anti-spoofing pluggable optical transceiver plugged in interface GigabitEthernet1/0/2.

```
<Sysname> display transceiver diagnosis interface gigabitethernet1/0/2
GigabitEthernet1/0/2 transceiver diagnostic information:
  Current diagnostic parameters:
    Temp(°C)  Voltage(V)  Bias(mA)  RX power(dBM)  TX power(dBM)
    36        3.31         6.13     -35.64         -5.19
```

**Table 1-9 display transceiver diagnosis** command output description

Field	Description
transceiver diagnostic information	Digital diagnosis information of the transceiver plugged in the interface
Current diagnostic parameters	Current diagnostic parameters
Temp.(°C)	Digital diagnosis parameter-temperature, in °C, with the precision to 1°C.

Field	Description
Voltage(V)	Digital diagnosis parameter-voltage, in V, with the precision to 0.01 V.
Bias(mA)	Digital diagnosis parameter-bias current, in mA, with the precision to 0.01 mA.
RX power(dBM)	Digital diagnosis parameter-RX power, in dBM, with the precision to 0.01 dBM.
TX power(dBM)	Digital diagnosis parameter-TX power, in dBM, with the precision to 0.01 dBM.

## display transceiver

### Syntax

**display transceiver interface** [ *interface-type interface-number* ]

### View

Any view

### Default Level

2: System level

### Parameters

**interface** [ *interface-type interface-number* ]: Displays main parameters of the pluggable transceiver plugged in the specified interface. *interface-type interface-number* represents interface type and interface number. If it is not specified, the command displays main parameters of the pluggable transceiver(s) in all the interfaces.

### Description

Use the **display transceiver** command to display main parameters of a single or all pluggable transceivers.

### Examples

# Display main parameters of the pluggable transceiver plugged in interface GigabitEthernet1/0/3.

```
<Sysname> display transceiver interface gigabitethernet1/0/3
GigabitEthernet1/0/3 transceiver information:
  Transceiver Type           : 1000_BASE_SX_SFP
  Connector Type             : LC
  Wavelength(nm)            : 850
  Transfer Distance(m)       : 550(50um) , 270(62.5um)
  Digital Diagnostic Monitoring : YES
  Vendor Name                 : H3C
  Ordering Name               : None
```

**Table 1-10 display transceiver command output description**

Field	Description
transceiver information	Pluggable transceiver information
Transceiver Type	Pluggable transceiver type
Connector Type	Type of the connectors of the transceiver: <ul style="list-style-type: none"> <li>Optical connectors, including SC (SC connector, developed by NTT) and LC (LC connector, 1.25 mm/RJ-45 optical connector developed by Lucent).</li> <li>Other connectors, including RJ-45 and CX 4.</li> </ul>
Wavelength(nm)	<ul style="list-style-type: none"> <li>Optical transceiver: central wavelength of the laser sent, in nm. If the transceiver supports multiple wavelengths, every two wavelength values are separated by a comma.</li> <li>Electrical transceiver: displayed as N/A.</li> </ul>
Transfer distance(xx)	Transfer distance, with xx representing km for single-mode transceivers and m for other transceivers. If the transceiver supports multiple transfer medium, every two values of the transfer distance are separated by a comma. The corresponding transfer medium is included in the bracket following the transfer distance value. The following are the transfer media: <ul style="list-style-type: none"> <li>9 um: 9/125 um single-mode fiber</li> <li>50 um: 50/125 um multi-mode fiber</li> <li>62.5 um: 62.5/125 um multi-mode fiber</li> <li>TP: Twisted pair</li> <li>CX4: CX4 cable</li> </ul>
Digital Diagnostic Monitoring	Whether the digital diagnosis function is supported, where: <ul style="list-style-type: none"> <li>YES: supported</li> <li>NO: not supported</li> </ul>
Vendor Name	Vendor name or name of the vendor who customizes the transceiver: <ul style="list-style-type: none"> <li>H3C customized anti-spoofing transceiver: H3C is displayed.</li> <li>Other transceivers: The vendor name is displayed.</li> </ul>
Ordering Name	Pluggable transceiver model

## display transceiver manuinfo

### Syntax

```
display transceiver manuinfo interface [ interface-type interface-number ]
```

### View

Any view

### Default Level

2: System level

## Parameters

**interface** [ *interface-type interface-number* ]: Displays part of the electrical label information of the H3C customized anti-spoofing pluggable transceiver plugged in the specified interface. *interface-type interface-number* represents interface type and interface number. If it is not specified, the command displays part of the electrical label information of the H3C customized anti-spoofing pluggable transceiver(s) in all the interfaces.

## Description

Use the **display transceiver manuinfo** command to display part of the electrical label information of a single or all 3Com customized anti-spoofing pluggable transceivers.

## Examples

# Display the electrical label information of the H3C customized anti-spoofing pluggable transceiver plugged in interface GigabitEthernet1/0/4.

```
<Sysname> display transceiver manuinfo interface gigabitethernet1/0/4
GigabitEthernet1/0/4 transceiver manufacture information:
  Manu. Serial Number   : 213410A0000054000251
  Manufacturing Date    : 2006-09-01
  Vendor Name           : H3C
```

**Table 1-11** display transceiver manuinfo command output description

Field	Description
Manu. Serial Number	Serial number generated during debugging and testing of the customized transceivers
Manufacturing Date	Debugging and testing date. The date takes the value of the system clock of the computer that performs debugging and testing.
Vendor Name	Name of the vendor who customizes the transceiver, that is, 3Com.

## reboot

### Syntax

**reboot** [ *slot slot-number* ]

### View

User view

### Default Level

2: System level

### Parameters

**slot slot-number**: Specifies the slot number of a member device. You can use the **display irf** command to view the member IDs of devices in a stack system.

### Description

Use the **reboot** command to reboot a member device, a subboard, or the whole stack system.

You can use the **reboot** [ **slot** *slot-number* ] command on the master to reboot the master or a slave. If the **slot** keyword is not provided, the whole stack system will reboot.

---

 **Caution**

- Device reboot may result in the interruption of the ongoing services. Use these commands with caution.
  - If a main boot file fails or does not exist, the device cannot be rebooted with the **reboot** command. In this case, you can re-specify a main boot file to reboot the device, or you can power off the device, then power it on and the system automatically uses the backup boot file to restart the device.
  - If you are performing file operations when the device is to be rebooted, the system does not execute the command for the sake of security.
- 

## Examples

# If the current configuration does not change, reboot the device.

```
<Sysname> reboot
Start to check configuration with next startup configuration file, please wait.....DONE!
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

# If the current configuration changes, reboot the device.

```
<Sysname> reboot
Start to check configuration with next startup configuration file, please wait.....DONE!
This command will reboot the device. Current configuration will be lost in next startup if
you continue. Continue? [Y/N]:y
Now rebooting, please wait...
```

## reset unused porttag

### Syntax

**reset unused porttag**

### View

User view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **reset unused porttag** command to clear the 16-bit index saved but not used in the current systems of all member devices.

A confirmation is required when you carry out this command. If you fail to make a confirmation within 30 seconds or enter “N” to cancel the operation, the command will not be carried out.

## Examples

# Clear the 16-bit index saved but not used in the current system.

```
<Sysname> reset unused porttag
Current operation will delete all unused port tag(s). Continue? [Y/N]:y
<Sysname>
```

## schedule job

### Syntax

```
schedule job { at time1 [ date ] | delay time2 } view view command
undo schedule job
```

### View

User view

### Default Level

3: Manage level

### Parameters

**at** *time1* [ *date* ]: Specifies the execution time of a specified command.

- *time1*: Execution time of the command, in the format of *hh:mm* (hour/minute). The *hh* value ranges from 0 to 23, and the *mm* value ranges from 0 to 59. The value of *hh:mm* cannot exceed 23:59.
- *date*: Execution date of the command, in the format of *MM/DD/YYYY* (month/day/year) or *YYYY/MM/DD* (year/month/day). The *YYYY* value ranges from 2000 to 2035, the *MM* value ranges from 1 to 12, and the *DD* value range depends on a specific month.

**delay** *time2*: Specifies the execution waiting time of a specified command. *time2* represents the waiting time, which can be in the following format:

- *hh:mm* (hour/minute): The *hh* value ranges from 0 to 720, and the *mm* value ranges from 0 to 59. The value of *hh:mm* cannot exceed 720:00.
- *mm* (minute): It ranges from 0 to 432000, with 0 indicating that a command is executed immediately without any delay.

**view** *view*: Specifies the view in which a command is executed. *view* represents the view name, and it takes the following values at present:

- **shell**, represents user view.
- **system**, represents system view.

*command*: The command string to be automatically executed at the scheduled time.

### Description

Use the **schedule job** command to automatically execute a specified command at the scheduled time.

Use the **undo schedule job** command to remove the configuration.

Note the following:

- If you provide both the *time1* and *date* arguments, the execution time must be a future time.

- If you only provide the *time1* argument, when *time1* is earlier than the current system time, the specified command is executed at *time1* of the next day; when *time1* is later than the current system time, the specified command is executed at *time1* of the current day.
- No matter whether you use the **at** or **delay** keyword, the difference between the execution time of a command and the current system time cannot exceed 720 hours (namely, 30 days).
- At present, you can specify only user view and system view. To automatically execute the specified commands in other views or automatically execute multiple commands at a time, you can configure the system to automatically execute a batch file at a specified time (note that you must provide a complete file path for the system to execute the batch file.).
- The system does not check the *view* and *command* arguments. Therefore, ensure the correctness of the *command* argument (including the correct format of *command* and the correct relationship between the *command* and *view* arguments.).
- After the specified automatic execution time is reached, the system executes the specified commands without displaying any information except system information such as log, trap and debug.
- When the system is executing the specified command, you do not need to input any information. If there is information for you to confirm, the system automatically inputs **Y** or **Yes**; if certain characters need to be input, the system automatically inputs a default character string, and inputs an empty character string when there is no default character string.
- For the commands used to switch user interfaces, such as **telnet**, **ftp**, and **ssh2**, the commands used to switch views, such as **system-view**, **quit** and **interface ethernet**, and the commands used to modify status of the user that is executing commands, such as **super**, the operation interface, command view and status of the current user are not changed after the automatic execution function is performed.
- If you modify the system time after the automatic execution function is configured, the scheduled automatic execution configuration turns invalid automatically.
- Only the latest configuration takes effect if you execute the **schedule job** command repeatedly.

## Examples

# Configure that the device will execute the batch file **1.bat** in system view in 60 minutes (supposing that the current time is 11:43).

```
<Sysname> schedule job delay 60 view system execute 1.bat
```

```
Info: Command execute 1.bat in system view will be executed at 12:43 10/31/2007 (in 1 hours and 0 minutes).
```

# Configure that the device will execute the batch file **1.bat** in system view at 12:00 in the current day (supposing that the current time is 11:43).

```
<Sysname> schedule job at 12:00 view system execute 1.bat
```

```
Info: Command execute 1.bat in system view will be executed at 12:00 10/31/2007 (in 0 hours and 16 minutes).
```

## schedule reboot at

### Syntax

```
schedule reboot at hh:mm [date]
```

```
undo schedule reboot
```

## View

User view

## Default Level

3: Manage level

## Parameters

*hh:mm*: Reboot time of a device, in the format of hh:mm (hours:minutes). The value of the *hh* argument ranges from 0 to 23, and the value of the *mm* argument ranges from 0 to 59.

*date*: Reboot date of a device, in the format mm/dd/yyyy (month/day/year) or in the format yyyy/mm/dd (year/month/day) The yyyy value ranges from 2000 to 2035, the mm value ranges from 1 to 12, and the dd value depends on a specific month.

## Description

Use the **schedule reboot at** command to enable the scheduled reboot function on all member devices and specify a specific reboot time and date.

Use the **undo schedule reboot** command to disable the scheduled reboot function.

By default, the scheduled reboot function is disabled.

There are two cases if no specific reboot date is specified:

- When the specified reboot time is later than the current time, the device will be rebooted at the reboot time of the current day.
- When the specified reboot time is earlier than the current time, the device will be rebooted at the reboot time the next day.
- If you are performing file operations when the device is to be rebooted, the system does not execute the command for the sake of security.

Note that:

- The precision of the device timer is 1 minute. One minute before the reboot time, the device will prompt "REBOOT IN ONE MINUTE" and will be rebooted in one minute.
- The difference between the reboot date and the current date cannot exceed 30 x 24 hours (namely, 30 days).
- After you execute the above command, the device will prompt you to confirm the configuration. You must enter **Y** or **y** to make the configuration take effect. The original configuration will be overwritten at the same time.
- If a date (month/day/year or year/month/day) later than the current date is specified for the **schedule reboot at** command, the device will be rebooted at the reboot time.
- If you use the **clock** command after the **schedule reboot at** command to adjust the system time, the reboot time set by the **schedule reboot at** command will become invalid.



This command reboots the device in a future time, thus resulting in service interruption. Please use it with caution.

---

## Examples

```
# Configure the device to reboot at 12:00 AM (supposing that the current time is 11:43).
```

```
<Sysname> schedule reboot at 12:00
Reboot system at 12:00 06/06/2006(in 0 hour(s) and 16 minute(s))
confirm? [Y/N]:
```

# If you have used the **terminal logging** command to enable the log display function on the terminal before setting a reboot time, the system will automatically display related log information after you enter <y>. By default, the log display function is enabled.

```
<Sysname>
%Jun  6 11:43:11:629 2006 Sysname CMD/4/REBOOT:
vty0(192.168.1.54): Set schedule reboot parameters at 11:43:11 06/06/2006, and system will
reboot at 12:00 06/06/2006.
```

## schedule reboot delay

### Syntax

```
schedule reboot delay { hh:mm | mm }
```

```
undo schedule reboot
```

### View

User view

### Default Level

3: Manage level

### Parameters

*hh:mm*: Device reboot wait time, in the format of hh:mm (hours:minutes). The value of the *hh* argument ranges from 0 to 720, and the value of the *mm* argument ranges from 0 to 59, and the value of the *hh:mm* argument cannot exceed 720:00.

*mm*: Device reboot wait time in minutes, in the range of 0 to 43,200.

### Description

Use the **schedule reboot delay** command to enable the scheduled reboot function of all member devices and set a reboot wait time.

Use the **undo schedule reboot** command to disable the scheduled reboot function.

By default, the scheduled reboot function is disabled.

Note that:

- The reboot wait time can be in the format of hh:mm (hours:minutes) or mm (absolute minutes). The absolute minutes cannot exceed 30 x 24 x 60 minutes, namely, 30 days.
- The precision of the device timer is 1 minute. One minute before the reboot time, the device will prompt "REBOOT IN ONE MINUTE" and will be rebooted in one minute.
- After you execute the above command, the device will prompt you to confirm the configuration. You must enter <Y> or <y> to make the configuration take effect. The original configuration will be overwritten at the same time.

- If you use the **clock** command after the **schedule reboot delay** command to adjust the system time, the reboot wait time set by the **schedule reboot delay** command will become invalid.
- If you are performing file operations when the device is to be rebooted, the system does not execute the command for the sake of security.



### Caution

This command reboots the device after the specified delay time, thus resulting in service interruption. Please use it with caution.

---

## Examples

# Configure the device to reboot in 88 minutes (supposing the current time is 11:48).

```
<Sysname> schedule reboot delay 88
Reboot system at 13:16 06/06/2006(in 1 hour(s) and 28 minute(s)). confirm? [Y/N]:
```

# If you have used the **terminal logging** command to enable the log display function on the terminal before setting a reboot time, the system will automatically display related log information after you enter **y**. By default, the log display function is enabled on the terminal.

```
<Sysname>
%Jun  6 11:48:44:860 2006 Sysname CMD/4/REBOOT:
vty0(192.168.1.54): Set schedule reboot parameters at 11:48:44 06/06/2006, and system will
reboot at 13:16 06/06/2006.
```

## shutdown-interval

### Syntax

```
shutdown-interval time
undo shutdown-interval
```

### View

System view

### Default Level

2: System level

### Parameters

*time*: Detection interval in seconds, in the range of 1 to 300.

### Description

Use the **shutdown-interval** command to set a detection interval.

Use the **undo shutdown-interval** command to restore the default.

By default, the detection interval is 30 seconds.

Note that:

- If a protocol module such as the operation, administration and maintenance (OAM) module detects an exception on a port (for example, signal loss of the link on the peer end), the port will be closed automatically, without execution of the **shutdown** command. You can set the automatic recovery time of the port by using the **shutdown-interval** command.
- The **shutdown-interval** command helps you to dynamically set a detection interval to cooperate with the OAM module.
- If you change the detection interval to T1 during interface detection, the interval from when you change the interval to the time when detection starts is T. If  $T < T1$ , the interface which is down will be brought up after T1-T time; if  $T \geq T1$ , the interface which is down will be brought up immediately.

## Examples

```
# Set the detection interval to 100 seconds.
```

```
<Sysname> system-view
[Sysname] shutdown-interval 100
```

## startup bootrom-access enable

### Syntax

```
startup bootrom-access enable
undo startup bootrom-access enable
```

### View

User view

### Default Level

2: System level

### Parameters

None

### Description

Use the **startup bootrom-access enable** command to enable Boot ROM access during system startup (that is, you can press **Ctrl+B** to enter the Boot ROM menu).

Use the **undo startup bootrom-access enable** command to disable Boot ROM access during system startup (that is, you cannot enter the Boot ROM menu no matter whether you press **Ctrl+B** or not).

By default, Boot ROM access during system startup is enabled.

Refer to the **display startup** command in *File System Management Commands* in the *System Volume* for the related configuration.

## Examples

```
# Disable Boot ROM access during system startup.
```

```
<Sysname> undo startup bootrom-access enable
```

## system-failure

### Syntax

```
system-failure { maintain | reboot }  
undo system-failure { maintain | reboot }
```

### View

System view

### Default Level

3: Manage level

### Parameters

**maintain**: Specifies that when the system detects any software abnormality, it maintains the current situation, and does not take any measure to recover itself.

**reboot**: Specifies that when the system detects any software abnormality, it recovers itself through automatic reboot.

### Description

Use the **system-failure** command to configure the exception handling method on all member devices.

By default, all member devices adopt the **reboot** method to handle exceptions.

The exception handling method is effective to the failed member device only, and does not influence the operations of other stack members

### Examples

# Set the exception handling method to **reboot**.

```
<Sysname> system-view  
[Sysname] system-failure reboot
```

# Table of Contents

<b>1 File System Management Commands</b> .....	<b>1-1</b>
File System Configuration Commands .....	1-1
cd .....	1-1
copy .....	1-2
delete .....	1-3
dir .....	1-4
execute .....	1-5
file prompt .....	1-6
fixdisk .....	1-7
format .....	1-7
mkdir .....	1-8
more .....	1-9
move .....	1-10
pwd .....	1-10
rename .....	1-11
reset recycle-bin .....	1-11
rmdir .....	1-14
undelete .....	1-14
Configuration File Management Commands .....	1-15
backup startup-configuration .....	1-15
display saved-configuration .....	1-16
display startup .....	1-18
reset saved-configuration .....	1-19
restore startup-configuration .....	1-20
save .....	1-21
slave auto-update config .....	1-23
startup saved-configuration .....	1-23
<b>2 FTP Configuration Commands</b> .....	<b>2-1</b>
FTP Server Configuration Commands.....	2-1
display ftp-server .....	2-1
display ftp-user .....	2-2
free ftp user .....	2-3
ftp server acl .....	2-3
ftp server enable .....	2-4
ftp timeout .....	2-4
ftp update .....	2-5
FTP Client Configuration Commands .....	2-6
ascii .....	2-6
binary .....	2-7
bye .....	2-7
cd .....	2-8
cdup .....	2-8
close .....	2-9

debugging .....	2-10
delete .....	2-11
dir .....	2-11
disconnect .....	2-13
display ftp client configuration .....	2-13
ftp .....	2-14
ftp client source .....	2-15
ftp ipv6 .....	2-16
get .....	2-17
lcd .....	2-18
ls .....	2-18
mkdir .....	2-20
open .....	2-20
open ipv6 .....	2-21
passive .....	2-22
put .....	2-22
pwd .....	2-23
quit .....	2-24
remotehelp .....	2-24
rmdir .....	2-26
user .....	2-27
verbose .....	2-28
<b>3 TFTP Configuration Commands .....</b>	<b>3-1</b>
TFTP Client Configuration Commands .....	3-1
display tftp client configuration .....	3-1
tftp-server acl .....	3-1
tftp .....	3-2
tftp client source .....	3-4
tftp ipv6 .....	3-5

# 1 File System Management Commands

---



## Note

- The current working directory is the root directory of the storage medium on the device in the examples in this manual.
  - For the qualified filename formats, refer to *File System Management Configuration* in the *System Volume*.
- 

## File System Configuration Commands

### cd

#### Syntax

```
cd { directory | .. | / }
```

#### View

User view

#### Default Level

3: Manage level

#### Parameters

*directory*: Name of the target directory, in the format of [*drive*:[*/*]*path*. *drive* represents the name of the storage medium, which is flash for the 3Com Switch 4800G. If *drive* is not specified, it indicates the file or subfolder under the current directory.

*..*: Returns to the upper directory. If the current working directory is the root directory, or there is no such an upper directory, the current working directory is not changed after the execution of the **cd** command. No command line help for this keyword.

*/*: Returns to the root directory of the storage medium. No command line help for this keyword.

#### Description

Use the **cd** command to change the current working directory.

#### Examples

# Enter the **test** folder after logging in to the device.

```
<Sysname> cd test
```

# Return to the upper directory (Remember to enter a space after the keyword **cd**).

```
<Sysname> cd ..  
  
# Return to the root directory.  
  
<Sysname> cd /  
  
# Enter the root directory of the flash on a slave with the member ID 2 after logging in to the master.  
  
<Sysname> cd slot2#flash:/  
  
# Change the current directory from the file system of the slave to the test folder under the root directory  
of the master.  
  
<Sysname> cd flash:/test
```

## copy

### Syntax

```
copy fileurl-source fileurl-dest
```

### View

User view

### Default Level

3: Manage level

### Parameters

*fileurl-source*: Name of the source file.

*fileurl-dest*: Name of the target file or folder.

### Description

Use the **copy** command to copy a file.

If you specify a target folder, the system will copy the file to the specified folder and use the name of the source file as the file name.

### Examples

```
# Copy file testcfg.cfg under the current folder and save it as testbackup.cfg.
```

```
<Sysname> copy testcfg.cfg testbackup.cfg  
Copy flash:/test.cfg to flash:/testbackup.cfg?[Y/N]:y  
....  
%Copy file flash:/test.cfg to flash:/testbackup.cfg...Done.
```

```
# After logging in to the master, copy the configuration file of the master to the root directory of a slave  
(with the member ID 2).
```

```
<Sysname> copy vrcfg.cfg slot2#flash:/  
Copy flash:/vrcfg.cfg to slot2#flash:/vrcfg.cfg?[Y/N]:y  
  
%Copy file flash:/vrcfg.cfg to slot2#flash:/vrcfg.cfg...Done.
```

## delete

### Syntax

```
delete [ /unreserved ] file-url
```

### View

User view

### Default Level

3: Manage level

### Parameters

**/unreserved:** Permanently deletes the specified file, and the deleted file can never be restored.

**file-url:** Name of the file to be deleted. Asterisks (\*) are acceptable as wildcards. For example, to remove files with the extension of **.txt** in the current directory, you may use the **delete \*.txt** command.

### Description

Use the **delete** command to move a specified file from a storage medium to the recycle bin, where you can restore the file with the **undelete** command or permanently delete it with the **reset recycle-bin** command.

The **dir /all** command can display the files moved to the recycle bin. These files are enclosed in pairs of brackets.



If you delete two files in different directories but with the same filename, only the last one is retained in the recycle bin.

---

### Examples

# Remove file **tt.cfg** from the root directory of the storage medium on the master after logging in to the device.

```
<Sysname> delete tt.cfg
.
Delete flash:/tt.cfg?[Y/N]:y
.
%Delete file flash:/tt.cfg...Done.
```

# Remove file **tt.cfg** from the root directory of the storage medium on a slave (with the member ID 2) after logging in to the device.

- Method 1

```
<Sysname> delete slot2#flash:/tt.cfg
Delete slot2#flash:/tt.cfg?[Y/N]:y
%Delete file slot2#flash:/tt.cfg...Done.
```

- Method 2

```
<Sysname> cd slot2#flash:/
<Sysname> delete tt.cfg
Delete slot2#flash:/tt.cfg?[Y/N]:y
%Delete file slot2#flash:/tt.cfg...Done.
```

## dir

### Syntax

```
dir [ /all ] [ file-url ]
```

### View

User view

### Default Level

3: Manage level

### Parameters

**/all**: Displays all files (including those in the recycle bin).

**file-url**: Name of the file or directory to be displayed. Asterisks (\*) are acceptable as wildcards. For example, to display files with the **.txt** extension under the current directory, you may use the **dir \*.txt** command.

### Description

Use the **dir** command to display information about all visible files and folders in the current directory.

Use the **dir /all** command to display information about all files and folders in the current directory, including hidden files, hidden sub-folders and the files in the recycle bin that originally belong to the current directory. The names of these deleted files are enclosed in pairs of brackets [ ].

The **dir file-url** command displays information about a file or folder.

### Examples

# Display information about all files and folders in the storage medium of the master after logging in to the device.

```
<Sysname> dir /all
Directory of flash:/
```

```
 0  -rwh          4  Apr 26 2008 12:02:05  snmpboots
 1  -rw- 10187730  Apr 26 2008 16:47:07  startup.bin
 2  -rwh       3144  Apr 26 2008 13:45:35  private-data.txt
 3  -rw-       2161  Apr 26 2008 13:53:25  startup.cfg
 4  -rw- 10058752  Sep 19 2008 17:41:46  startup_b58.bin
 5  -rw- 10139143  Apr 26 2008 13:08:20  startup_wenxiangchong.bin
 6  -rwh        716  Apr 26 2008 12:01:58  hostkey
 7  -rwh        572  Apr 26 2008 12:02:11  serverkey
 8  -rwh        548  Apr 26 2008 12:02:17  dsakey
 9  -rw-       3035  Apr 26 2008 13:45:42  new-config.cfg
10  -rw-       2200  Apr 26 2008 14:58:35  [aa.cfg]
```

31496 KB total (1801 KB free)

# Display information about all files and folders in the storage medium of a slave (with the member ID 2) after logging in to the device.

```
<Sysname> cd slot2#flash:/
```

```
<IRF>dir /all
```

Directory of slot2#flash:/

```
 0  -rwh      3144  Apr 26 2008 13:45:28  private-data.txt
 1  -rw-      2341  Apr 26 2008 16:36:18  startup.cfg
 2  -rw-       124  Apr 26 2008 12:00:22  patchstate
 3  -rwh       716  Apr 26 2008 14:31:36  hostkey
 4  -rwh         4  Apr 26 2008 14:31:41  snmpboots
 5  -rw- 10187730  Apr 26 2008 12:01:10  startup.bin
 6  -rwh       572  Apr 26 2008 14:31:47  serverkey
 7  -rwh       548  Apr 26 2008 14:31:52  dsakey
 8  -rw-      3035  Apr 26 2008 13:45:36  new-config.cfg
 9  drw-         -  Apr 26 2008 12:11:53  oldver
```

31496 KB total (1839 KB free)

**Table 1-1** dir command output description

Field	Description
Directory of	The current working directory
d	Directory. If it is not displayed, it indicates that the displayed item is a file.
r	The directory or file is readable.
w	The directory or file is writeable.
h	The directory or file is hidden.
[ ]	The file is in the recycle bin.

## execute

### Syntax

```
execute filename
```

### View

System view

### Default Level

2: System level

### Parameters

*filename*: Name of a batch file with a .bat extension. You can use the **rename** command to change the suffix of the configuration file to .bat to use it as a batch file.

## Description

Use the **execute** command to execute the specified batch file.

Batch files are command line files. Executing a batch file is to execute a set of command lines in the file.

- You should not include invisible characters in a batch file. If an invisible character is found during the execution, the batch process will abort and the commands that have been executed cannot be cancelled.
- Not every command in a batch file is sure to be executed. For example, if a certain command is not correctly configured, the system omits this command and goes to the next one.
- The configuration generated after a batch file is executed will not be backed up to the standby main board automatically.
- Each configuration command in a batch file must be a standard configuration command, meaning that the valid configuration information can be displayed with the **display current-configuration** command after this command is configured successfully; otherwise, this command may not be executed correctly.

## Examples

```
# Execute the batch file test.bat in the root directory.
```

```
<Sysname> system-view  
[Sysname] execute test.bat
```

## file prompt

### Syntax

```
file prompt { alert | quiet }
```

### View

System view

### Default Level

3: Manage level

### Parameters

**alert**: Enables the system to warn you about operations that may bring undesirable results such as file corruption or data loss.

**quiet**: Disables the system from warning you about any operation.

## Description

Use the **file prompt** command to set a prompt mode for file operations.

By default, the prompt mode is **alert**.

Note that when the prompt mode is set to **quiet**, the system does not warn for any file operation. To avoid undesirable consequences resulting from misoperation, you are recommended to use the **alert** mode.

## Examples

```
# Set the file operation prompt mode to alert.
```

```
<Sysname> system-view
[Sysname] file prompt alert
```

## fixdisk

### Syntax

```
fixdisk device
```

### View

User view

### Default Level

3: Manage level

### Parameters

*device*: Storage medium name.

### Description

Use the **fixdisk** command to restore the space of a storage medium when it becomes unavailable because of some abnormal operation.

Note that you can execute the **fixdisk** command for the storage medium on the master, but you cannot execute the command for the storage medium on the slaves.

### Examples

```
# Restore the space of the flash.
<Sysname> fixdisk flash:
Fixdisk flash: may take some time to complete...
%Fixdisk flash: completed.
```

## format

### Syntax

```
format device
```

### View

User view

### Default Level

3: Manage level

### Parameters

*device*: Name of a storage medium.

### Description

Use the **format** command to format a storage medium.



## Caution

Formatting a storage medium results in loss of all the files on the storage medium and these files cannot be restored. In particular, if there is a startup configuration file on a storage medium, formatting the storage medium results in loss of the startup configuration file.

---

## Examples

# Format the flash.

```
<Sysname> format flash:
All data on flash: will be lost, proceed with format? [Y/N]:y
./
%Format flash: completed.
```

## mkdir

### Syntax

**mkdir** *directory*

### View

User view

### Default Level

3: Manage level

### Parameters

*directory*: Name of a folder.

### Description

Use the **mkdir** command to create a folder under a specified directory on the storage medium.

Note that:

- The name of the folder to be created must be unique under the specified directory. Otherwise, you will fail to create the folder under the directory.
- To use this command to create a folder, the specified directory must exist. For instance, to create folder **flash:/test/mytest**, the **test** folder must exist. Otherwise, you will fail to create folder **mytest**.

## Examples

# Create a folder named **test** under the current directory.

```
<Sysname> mkdir test
....
%Created dir flash:/test
```

# Create folder **test/subtest** under the current directory.

```
<Sysname> mkdir test/subtest
....
%Created dir flash:/test/subtest
```

# Create folder **test** on a slave (with the member ID 2) after logging in to the device.

```
<Sysname> mkdir slot2#flash:/test
....
%Created dir slot2#flash:/test.
```

## more

### Syntax

**more** *file-url*

### View

User view

### Default Level

3: Manage level

### Parameters

*file-url*: File name.

### Description

Use the **more** command to display the contents of the specified file.

So far, this command is valid only for text files.

### Examples

# Display the contents of file **test.txt**.

```
<Sysname> more test.txt
Welcome to 3Com.
```

# Display the contents of file **testcfg.cfg**.

```
<Sysname> more testcfg.cfg
```

```
#
version 5.20, ESS 2201
#
sysname Sysname
#
configure-user count 5
#
vlan 2
#
return
<Sysname>
```

# Display the contents of file **testcfg.cfg** on a slave (with the member ID 2).

```
<Sysname> more slot2#flash:/testcfg.cfg
```

```
#
version 5.20, ESS 2201
```

```
#
  sysname Test
#
  ---- More ----
```

## move

### Syntax

```
move fileurl-source fileurl-dest
```

### View

User view

### Default Level

3: Manage level

### Parameters

*fileurl-source*: Name of the source file.

*fileurl-dest*: Name of the target file or folder.

### Description

Use the **move** command to move a file.

If you specify a target folder, the system will move the source file to the specified folder, with the file name unchanged.

### Examples

# Move file **flash:/test/sample.txt** to **flash:/**, and save it as **1.txt**.

```
<Sysname> move test/sample.txt 1.txt
Move flash:/test/sample.txt to flash:/1.txt?[Y/N]:y
...
% Moved file flash:/test/sample.txt to flash:/1.txt
```

# Move file **b.cfg** to the subfolder **test2**.

```
<Sysname> move b.cfg test2
Move flash:/b.cfg to flash:/test2/b.cfg?[Y/N]:y
.
%Moved file flash:/b.cfg to flash:/test2/b.cfg.
```

## pwd

### Syntax

```
pwd
```

### View

User view

### Default Level

3: Manage level

### Parameters

None

### Description

Use the **pwd** command to display the current path.

### Examples

```
# Display the current path.
```

```
<Sysname> pwd
```

```
flash:
```

## rename

### Syntax

```
rename fileurl-source fileurl-dest
```

### View

User view

### Default Level

3: Manage level

### Parameters

*fileurl-source*: Name of the source file or folder.

*fileurl-dest*: Name of the target file or folder.

### Description

Use the **rename** command to rename a file or folder.

The target file name must be unique under the current path.

### Examples

```
# Rename file sample.txt as sample.bat.
```

```
<Sysname> rename sample.txt sample.bat
```

```
Rename flash:/sample.txt to flash:/sample.bat? [Y/N]:y
```

```
% Renamed file flash:/sample.txt to flash:/sample.bat
```

## reset recycle-bin

### Syntax

```
reset recycle-bin [ /force ]
```

## View

User view

## Default Level

3: Manage level

## Parameters

**/force**: Deletes all files in the recycle bin, including files that cannot be deleted by the command without the **/force** keyword.

## Description

Use the **reset recycle-bin** command to permanently delete the files in the recycle bin in the current directory.

If a file is corrupted, you may not be able to delete the file using the **reset recycle-bin** command. In this case, you can use the **reset recycle-bin /force** command, which can delete all the files in the recycle bin forcibly.

Note that:

- Unlike this command, the **delete file-url** command only moves a file to the recycle bin, and the file still occupies the memory space. To delete the file in the recycle bin, you need to execute the **reset recycle-bin** command in the original directory of the file.
- The **reset recycle-bin** command deletes files in the current directory and in the recycle bin. If the original path of the file to be deleted is not the current directory, use the **cd** command to enter the original directory of the file, and then execute the **reset recycle-bin** command.

## Examples

# Delete file **b.cfg** under the current directory and in the recycle bin.

- Display all the files in the recycle bin and under the current directory.

```
<Sysname> dir /all
```

```
Directory of flash:/
```

```
 0  -rw-  10471471  Sep 18 2008 02:45:15  s4800g.bin
 1  -rwh      4  Apr 26 2000 12:03:51  snmpboots
 2  -rwh    1792  Apr 26 2000 12:49:53  private-data.txt
 3  -rw-  9989823  Jul 14 2008 19:30:46  s4800_b57.bin
 4  -rw-      6  Apr 26 2000 12:04:33  patchstate
 5  -rw-    2209  Apr 26 2000 12:07:20  startup.cfg
 6  -rwh    716  Apr 26 2000 12:03:46  hostkey
 7  -rwh    572  Apr 26 2000 12:03:55  serverkey
 8  -rwh    548  Apr 26 2000 12:04:00  dsakey
 9  -rw-  478164  Apr 26 2000 14:52:35  s4800g.btm
10  -rw-    368  Apr 26 2000 12:04:04  patch_xxx.bin
11  -rw-    2195  Apr 26 2000 12:43:08  sfp.cfg
12  -rw-    5501  Apr 26 2000 13:05:57  [a.cfg]
13  -rw-    2159  Apr 26 2000 13:06:04  [b.cfg]
```

31496 KB total (11018 KB free)

//The above information indicates that the current directory is **flash:**, and there are two files **a.cfg** and **b.cfg** in the recycle bin.

- Delete file **b.cfg** under the current directory and in the recycle bin.

```
<Sysname> reset recycle-bin
```

```
Clear flash:~/a.cfg ?[Y/N]:n
```

```
Clear flash:~/b.cfg ?[Y/N]:y
```

```
Clearing files from flash may take a long time. Please wait...
```

```
.....
```

```
%Cleared file flash:~/b.cfg...
```

- In directory **flash:**, check whether the file **b.cfg** in the recycle bin is deleted.

```
<Sysname> dir /all
```

```
Directory of flash:/
```

0	-rw-	10471471	Sep 18 2008 02:45:15	s4800g.bin
1	-rwh	4	Apr 26 2000 12:03:51	snmpboots
2	-rwh	1792	Apr 26 2000 12:49:53	private-data.txt
3	-rw-	9989823	Jul 14 2008 19:30:46	s4800g_b57.bin
4	-rw-	6	Apr 26 2000 12:04:33	patchstate
5	-rw-	2209	Apr 26 2000 12:07:20	startup.cfg
6	-rwh	716	Apr 26 2000 12:03:46	hostkey
7	-rwh	572	Apr 26 2000 12:03:55	serverkey
8	-rwh	548	Apr 26 2000 12:04:00	dsakey
9	-rw-	478164	Apr 26 2000 14:52:35	s4800g_505.btm
10	-rw-	368	Apr 26 2000 12:04:04	patch_xxx.bin
11	-rw-	2195	Apr 26 2000 12:43:08	sfp.cfg
12	-rw-	2195	Apr 26 2000 13:08:47	[a.cfg]

31496 KB total (11015 KB free)

// The above information indicates that file **flash:/b.cfg** is deleted permanently.

# Delete file **aa.cfg** in the subdirectory **test** and in the recycle bin.

- Enter the subdirectory

```
<Sysname> cd test/
```

- Check all the files in the subfolder **test**.

```
<Sysname> dir /all
```

```
Directory of flash:/test
```

0	-rw-	2195	Apr 26 2000 21:22:35	[aa.cfg]
---	------	------	----------------------	----------

31496 KB total (11010 KB free)

// The above information indicates only one file exists in the folder, and the file has been moved to the recycle bin.

- Permanently delete file **test/aa.cfg**.

```
<Sysname> reset recycle-bin
```

```
Clear flash:/test/~/aa.cfg ?[Y/N]:y
```

```
Clearing files from flash may take a long time. Please wait...
```

```
..
```

```
%Cleared file flash:/test/~//aa.cfg...
```

## rmdir

### Syntax

```
rmdir directory
```

### View

User view

### Default Level

3: Manage level

### Parameters

*directory*: Name of the folder.

### Description

Use the **rmdir** command to remove a folder.

- The folder must be an empty one. If not, you need to delete all files and subfolders under it with the **delete** command.
- After you execute the **rmdir** command successfully, the files in the recycle bin under the folder will be automatically deleted.

### Examples

```
# Remove folder mydir.
```

```
<Sysname> rmdir mydir
```

```
Rmdir flash:/mydir?[Y/N]:y
```

```
%Removed directory flash:/mydir.
```

## undelete

### Syntax

```
undelete file-url
```

### View

User view

### Default Level

3: Manage level

### Parameters

*file-url*: Name of the file to be restored.

## Description

Use the **undelete** command to restore a file from the recycle bin.

If another file with the same name exists under the same path, the undelete operation will cause it to be overwritten and the system will prompt you whether to continue.

## Examples

# Restore file **a.cfg** in directory **flash:** from the recycle bin.

```
<Sysname> undelete a.cfg
Undelete flash:/a.cfg?[Y/N]:y
.....
%Undeleted file flash:/a.cfg.
```

# Restore file **b.cfg** in directory **flash:/test** from the recycle bin.

```
<Sysname> undelete flash:/test/b.cfg
Undelete flash:/test/b.cfg?[Y/N]:y
.....
%Undeleted file flash:/test/b.cfg.
```

Or, you can use the following steps to restore file **flash:/test/b.cfg**.

```
<Sysname> cd test
<Sysname> undelete b.cfg
Undelete flash:/test/b.cfg?[Y/N]:y
.....
%Undeleted file flash:/test/b.cfg.
```

# Configuration File Management Commands

## backup startup-configuration

### Syntax

```
backup startup-configuration to dest-addr [dest-filename]
```

### View

User view

### Default Level

2: System level

### Parameters

*dest-addr*: IP address or name of a TFTP server. The address cannot be an IPv6 address.

*dest-filename*: Target filename used to save the startup configuration file for the next system startup on the server.

### Description

Use the **backup startup-configuration** command to back up the startup configuration file (used at the next system startup) to a specified TFTP server. If you do not specify this filename, the original filename is used.

For a device that has main and backup startup configuration files, this command only backs up the main startup configuration file.

Presently, the device uses TFTP to back up configuration files.

## Examples

# Back up the startup configuration file of the device to the TFTP server with IP address 2.2.2.2, using filename **192-168-1-26.cfg**.

```
<Sysname> display startup
  Current startup saved-configuration file: flash:/sfp.cfg
  Next main startup saved-configuration file: flash:/sfp.cfg
  Next backup startup saved-configuration file: NULL
<Sysname> backup startup-configuration to 2.2.2.2 192-168-1-26.cfg
Backup next startup-configuration file to 2.2.2.2, please wait...finished!
<Sysname>
```

After the above operation, the device backs up file **sfp.cfg** to TFTP server 2.2.2.2, where the file is saved as **192-168-1-26.cfg**.

## display saved-configuration

### Syntax

```
display saved-configuration [ by-linenum ]
```

### View

Any view

### Default Level

2: System level

### Parameters

**by-linenum**: Identifies each line of displayed information with a line number.

### Description

Use the **display saved-configuration** command to display the contents of the configuration file saved for the next startup of the device.

During device management and maintenance, you can use this command to check whether important configurations are saved to the configuration file to be used for the next startup of the device.

This command displays the main configuration file to be used for the next system startup.

If the system is not specified with a configuration file for the next startup or the specified configuration file does not exist, no information will be displayed when you execute the **display saved-configuration** command.

Related commands: **save**, **reset saved-configuration**; **display current-configuration** in *Basic System Configuration Commands* in the *System Volume*.

## Examples

# Display the configuration file saved for the next startup of the device.

```
<Sysname> display saved-configuration
```

```

#
version 5.20, ESS 2201
#
sysname Sysname
#
domain default enable system
#
telnet server enable
#
multicast routing-enable
#
vlan 1
#
vlan 999
#
domain system
access-limit disable
state active
idle-cut disable
self-service-url disable
#
interface NULL0
#
---- More ----

```

The configurations are displayed in the order of global, port, and user interface. “ ---- More ----” means that all information on this screen has been displayed, and if you press the Space key, the next screen will be displayed.

# Display the contents of the configuration file saved for the next startup of the device with a number identifying each line.

```

<Sysname> display saved-configuration by-linenum
1: #
2:  version 5.20, ESS 2201
3: #
4:  sysname Sysname
5: #
6:  domain default enable system
7: #
8:  telnet server enable
9: #
10: multicast routing-enable
11: #
12: vlan 1
13: #
14: vlan 999
15: #
16: domain system
17:  access-limit disable

```

```
18: state active
19: idle-cut disable
20: self-service-url disable
21: #
22: interface NULL0
23: #
---- More ----
```

“ ---- More ----” means that all information on this screen has been displayed, and if you press the Space key, the next screen will be displayed.

## display startup

### Syntax

**display startup**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display startup** command to display the configuration files used at the current system startup and the configuration file(s) to be used at the next system startup.

Note that:

- The slaves are started and run based on the current configurations of the master; therefore the current startup configuration files displayed on all the member devices in a stack are always the same.
- After the master is changed, the new master does not restart using the configuration file but runs with the current configuration instead. Therefore, when you execute the **display startup** command, the startup configuration file used for the current startup of the new master is displayed as NULL and those of the slaves are also NULL to keep consistent with the new master.

Related commands: **startup saved-configuration**.

### Examples

# Display the startup configuration file used at the current system startup and the one to be used at the next system startup.

```
<Sysname> display startup
MainBoard:
  Current startup saved-configuration file: NULL
  Next main startup saved-configuration file: flash:/startup.cfg
  Next backup startup saved-configuration file: flash:/startup2.cfg
Slot 2:
```

```

Current startup saved-configuration file: NULL
Next main startup saved-configuration file: flash:/startup.cfg
Next backup startup saved-configuration file: flash:/startup2.cfg

```

**Table 1-2 display startup command output description**

Field	Description
MainBoard	The configuration files used for the current and the next startup of the master
Current Startup saved-configuration file	The configuration file used for the current startup
Next main startup saved-configuration file	The main configuration file used for the next startup
Next backup startup saved-configuration file	The backup configuration file used for the next startup
Slot 2	The configuration files used for the current and the next startup of the slave (with the member ID 2)

## reset saved-configuration

### Syntax

```
reset saved-configuration [ backup | main ]
```

### View

User view

### Default Level

2: System level

### Parameters

**backup**: Deletes the backup startup configuration file.

**main**: Deletes the main startup configuration file.

### Description

Use the **reset saved-configuration** command to delete the startup configuration file saved on the storage medium of the device.

Note that:

- This command will permanently delete the configuration file from all the member devices in a stack. Use it with caution.
- On a device that has the main and backup startup configuration files, you can choose to delete either the main or backup startup configuration file. However, in the case that the main and backup startup configuration files are the same, if you perform the delete operation for once, the system will not delete the configuration file but only set the corresponding startup configuration file (main or backup, according to which one you specified in the command) to NULL.
- The execution of the **reset saved-configuration** command and that of the **reset saved-configuration main** command have the same effect, that is, they will delete the main startup configuration file.

Related commands: **save**, **display saved-configuration**.

## Examples

```
# Delete the startup configuration file for the next startup from the storage medium of the device.
<Sysname> reset saved-configuration backup
The saved configuration file will be erased. Are you sure? [Y/N]:y
Configuration file in flash is being cleared.
Please wait ...
..
MainBoard:
  Configuration file is cleared.
Slot 2:
  Erase next configuration file successfully
```

## restore startup-configuration

### Syntax

```
restore startup-configuration from src-addr src-filename
```

### View

User view

### Default Level

2: System level

### Parameters

*src-addr*: IP address or name of a TFTP server. The address cannot be an IPv6 address.

*src-filename*: Filename of the configuration file to be downloaded from the specified server.

### Description

Use the **restore startup-configuration** command to download a configuration file from the specified TFTP server to the device and specify the configuration file as the startup configuration file to be used at the next startup of the device.

- The file downloaded is set as the main startup configuration file to be used at the next system startup.
- This command downloads the configuration file to the root directory of the storage medium of all the member devices and specifies the file as the startup configuration file to be used at the next startup of all the member devices.

If the file to be downloaded has the same filename as an existing file on a member device, you will be prompted whether you want to overwrite the existing file or not. In addition, both the master and the slaves are assumed to use the storage media of the same type when the device is checking the filename or backing up the configuration file to the slaves. When backing up the configuration file to the slaves, the device saves the file to the same directory on the slaves as on the master, that is, the root directory.

## Examples

```
# Download file config.cfg from the TFTP server whose IP address is 2.2.2.2, and the file is to be used as the main configuration file at the next startup of the device.
```

```
<Sysname> restore startup-configuration from 2.2.2.2 config.cfg
Restore next startup-configuration file from 2.2.2.2. Please wait...finished!
Now restore next startup-configuration file from main to slave board. Please wait...finished!
```

## save

### Syntax

```
save file-url [ all | slot slot-number ]
save [ safely ] [ backup | main ]
```

### View

Any view

### Default Level

2: System level

### Parameters

*file-url*: File path, where the extension of the file name must be .cfg. When used with the keyword **all** or **slot**, this argument cannot include a member ID. If the file path includes a folder name, you must first create the folder on the member device; otherwise, the operation will fail.

**all**: Saves the current configuration in the specified filename to all the member devices in a stack.

**slot** *slot-number*: Saves the current configuration in the specified filename to a slave. *slot-number* represents the member ID of a member device. The value range depends on the device model. You can use the **display stack** command to view the member IDs of the member devices in a stack.

**safely**: Sets the configuration saving mode to safe. If this argument is not specified, the configuration file is saved in fast mode.

**backup**: Saves the current configuration to the startup configuration file specified in the interactive mode, and specifies the file as the backup startup configuration file to be used at the next startup of the device.

**main**: Saves the current configuration to the main startup configuration file specified in the interactive mode, and specifies the file as the main startup configuration file to be used at the next startup of the device.

### Description

Use the **save** *filename* [ **all** | **slot** *slot-number* ] command to save the current configuration to the specified configuration file, but the system will not specify the file as the startup configuration file for the next system startup. If the file specified by *filename* does not exist, the system will create the file and then save the configuration to the file; if the **all** or **slot** keyword is not specified, the configuration will be saved to the master.

Use the **save** [ **safely** ] [ **backup** | **main** ] command to save the current configuration to the root directory of the storage medium on a member device, and specify the file as the startup configuration file for the next system startup. If the **backup** or **main** keyword is not specified, the **main** keyword is used by default.

Whether the **save** [ **safely** ] [ **backup** | **main** ] command or the **save** *filename* **all** command+**Enter** takes effect on all the member devices or on the master only depends on whether the configuration file auto-save function is enabled.

Related commands: **slave auto-update config, reset saved-configuration, display current-configuration, display saved-configuration.**

## Examples

# Save the current configuration file to the specified directory, but do not specify the configuration file as the configuration file for the next startup.

```
<Sysname> save test.cfg
The current configuration will be saved to flash:/test.cfg. Continue? [Y/N]:y
Now saving current configuration to the device.
Saving configuration flash:/test.cfg. Please wait...
.....
Configuration is saved to flash successfully.
```

# Save the current configuration to the root directory of the storage medium on a member device, and specify the file as the configuration file for the next startup.

```
<Sysname> display startup
MainBoard:
  Current startup saved-configuration file: NULL
  Next main startup saved-configuration file: flash:/aa.cfg
  Next backup startup saved-configuration file: NULL
Slot 2:
  Current startup saved-configuration file: NULL
  Next main startup saved-configuration file: flash:/aa.cfg
  Next backup startup saved-configuration file: NULL
```

*// The above information indicates that the main startup configuration file for the next startup of all the member devices is **aa.cfg**.*

```
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/aa.cfg]
(To leave the existing filename unchanged, press the enter key):startup.cfg
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait.....
Saved the current configuration to mainboard device successfully.
```

```
Slot 2:
  Save next configuration file successfully
  Configuration is saved to device successfully.
<Sysname> display startup
MainBoard:
  Current startup saved-configuration file: NULL
  Next main startup saved-configuration file: flash:/startup.cfg
  Next backup startup saved-configuration file: NULL
Slot 2:
  Current startup saved-configuration file: NULL
  Next main startup saved-configuration file: flash:/startup.cfg
  Next backup startup saved-configuration file: NULL
```

*// The above information indicates that the main configuration file for the next startup of all the member devices in the stack is changed to **startup.cfg**.*

# Save the current configuration in the name of **test.cfg** to a slave (with the member ID of 2) (approach 1).

```
<Sysname> save test.cfg slot 2
The current configuration will be saved to slot2#flash:/test.cfg. Continue? [Y/N]:y
Now saving current configuration to the device.
Saving configuration slot2#flash:/test.cfg. Please wait...
.....
Configuration is saved to slot2#flash successfully.
```

Or, you can use the following command (approach 2):

```
<Sysname> save slot2#flash:/test.cfg
```

## slave auto-update config

### Syntax

**slave auto-update config**

**undo slave auto-update config**

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **slave auto-update config** command to enable the configuration file auto-save function.

Use the **undo slave auto-update config** command to disable the function.

By default, the configuration file auto-save function is enabled.

### Examples

# Enable the configuration file auto-save function.

```
<Sysname> system-view
[Sysname] slave auto-update config
```

## startup saved-configuration

### Syntax

**startup saved-configuration** *cfgfile* [ **backup** | **main** ]

**undo startup saved-configuration**

### View

User view

## Default Level

2: System level

## Parameters

*cfgfile*: Configuration file name. The file must be a file with an extension .cfg stored in the root directory of the storage medium.

**backup**: Sets the configuration file as the backup startup configuration file that will be used at the next startup of the device.

**main**: Sets the configuration file as the main startup configuration file that will be used at the next startup of the device.

## Description

Use the **startup saved-configuration** command to specify a startup configuration file (the configuration file to be used at the next system startup) for all the member devices.

Use the **undo startup saved-configuration** command to configure all the member devices to start up with the null configuration, that is, the factory configuration.

The startup configuration file for the next startup of all the member devices must be the same. Therefore, before using the command, ensure that the specified configuration file has been saved to the root directories of the storage media of all the member devices; otherwise, the command will fail.

- The **startup saved-configuration** and **startup saved-configuration main** commands have the same effect: Both of them are used to specify the main startup configuration file.
- The main and backup startup configuration files can be specified as the same file. However, it is recommended you use different files, or, save the same configuration as two files using different file names, one specified as the main startup configuration file, and the other specified as the backup.
- If you execute the **undo startup saved-configuration** command, the system will set the main and backup startup configuration file as NULL, but will not delete the two configuration files.

Related commands: **display startup**.

## Examples

# Specify a startup configuration file for the next system startup.

```
<Sysname> startup saved-configuration testcfg.cfg
Please wait ...
Setting the master board .....
... Done!
Setting the slave board ...
Slot 2:
Set next configuration file successfully
```

# 2 FTP Configuration Commands

---

## FTP Server Configuration Commands

### display ftp-server

#### Syntax

display ftp-server

#### View

Any view

#### Default Level

3: Manage level

#### Parameters

None

#### Description

Use the **display ftp-server** command to display the FTP server configuration.

After configuring FTP server parameters, you may verify them with this command.

Related commands: **ftp server enable**, **ftp timeout**, **ftp update**.

#### Examples

# Display the FTP server configuration.

```
<Sysname> display ftp-server
  FTP server is running
  Max user number:           1
  User count:                1
  Timeout value(in minute):  30
  Put Method:                fast
```

**Table 2-1 display ftp-server** command output description

Field	Description
Max user number	Maximum number of login users at a time
User count	Number of the current login users
Timeout value (in minute)	Allowed idle time of an FTP connection. If there is no packet exchange between the FTP server and client during the whole period, the FTP connection will be disconnected.

Field	Description
Put Method	File update method of the FTP server, including: <ul style="list-style-type: none"> <li>fast: Fast update</li> <li>normal: Normal update</li> </ul>

## display ftp-user

### Syntax

**display ftp-user**

### View

Any view

### Default Level

3: Manage level

### Parameters

None

### Description

Use the **display ftp-user** command to display the detailed information of current FTP users.

### Examples

# Display the detailed information of FTP users.

```
<Sysname> display ftp-user
  UserName           HostIP      Port      Idle           HomeDir
  ftp                192.168.1.54  1190      0              flash:
```

# If the name of the logged-in user exceeds 10 characters, the exceeded characters will be displayed in the next line and right justified, for example, if the logged-in user name is **administrator**, the information is displayed as follows:

```
<Sysname> display ftp-user
  UserName           HostIP      Port      Idle           HomeDir
administra
  tor                192.168.0.152  1031      0              flash:
```

**Table 2-2 display ftp-user command output description**

Field	Description
UserName	Name of the currently logged-in user
HostIP	IP address of the currently logged-in user
Port	Port which the currently logged-in user is using
Idle	Duration time of the current FTP connection, in minutes
HomeDir	Authorized path of the present logged-in user

## free ftp user

### Syntax

```
free ftp user username
```

### View

User view

### Default Level

3: Manage level

### Parameters

*username*: Username. You can use the **display ftp-user** command to view the logged-in user name of the current FTP connection.

### Description

Use the **free ftp user** command to manually release the FTP connection established with the specified username.

Note that if the user to be released is transmitting a file, the connection between the user and the FTP server is terminated after the file transmission.

### Examples

```
# Manually release the FTP connection established with username ftpuser.
```

```
<Sysname> free ftp user ftpuser  
Are you sure to free FTP user ftpuser? [Y/N]:y  
<Sysname>
```

## ftp server acl

### Syntax

```
ftp server acl acl-number  
undo ftp server acl
```

### View

System view

### Default Level

3: Manage level

### Parameters

*acl-number*: Basic access control list (ACL) number, in the range 2000 to 2999.

### Description

Use the **ftp server acl** command to control the access to the device from FTP clients through ACL.

Use the **undo ftp server acl** command to restore the default.

By default, the access to the device from FTP clients is not controlled.

Associated with an ACL, the FTP server can deny the FTP requests of some FTP clients and only permit the access of clients allowed by the ACL rules. This configuration only filters the FTP connections to be established, and has no effect on the established FTP connections and operations. If you execute the command for multiple times, the last specified ACL takes effect.

## Examples

```
# Associate the FTP service with ACL 2001 to allow only the client 1.1.1.1 to access the device through FTP.
```

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule 0 permit source 1.1.1.1 0
[Sysname-acl-basic-2001] rule 1 deny source any
[Sysname-acl-basic-2001] quit
[Sysname] ftp server acl 2001
```

## ftp server enable

### Syntax

```
ftp server enable
```

```
undo ftp server
```

### View

System view

### Default Level

3: Manage level

### Parameters

None

### Description

Use the **ftp server enable** command to enable the FTP server and allow the login of FTP users.

Use the **undo ftp server** command to disable the FTP server.

By default, the FTP server is disabled to prevent attacks.

## Examples

```
# Enable the FTP server.
```

```
<Sysname> system-view
[Sysname] ftp server enable
```

## ftp timeout

### Syntax

```
ftp timeout minute
```

```
undo ftp timeout
```

## View

System view

## Default Level

3: Manage level

## Parameters

*minute*: Idle-timeout timer in minutes, in the range 1 to 35791.

## Description

Use the **ftp timeout** command to set the idle-timeout timer.

Use the **undo ftp timeout** command to restore the default.

By default, the FTP idle time is 30 minutes.

After you log in to an FTP server, if the connection is disrupted and the FTP server is not notified, the system will maintain the connection, which will cause the occupation of the system resources and affect the login of other FTP users. To address this problem, you can set an idle-timeout timer so that the FTP server can disconnect from the user if no information is received or/and transmitted before the timer expires.

## Examples

```
# Set the idle-timeout timer to 36 minutes.
```

```
<Sysname> system-view  
[Sysname] ftp timeout 36
```

## ftp update

### Syntax

```
ftp update { fast | normal }
```

```
undo ftp update
```

### View

System view

### Default Level

3: Manage level

### Parameters

**fast**: Fast update.

**normal**: Normal update.

### Description

Use the **ftp update** command to set the file update mode that the FTP server uses while receiving data.

Use the **undo ftp update** command to restore the default, namely, the normal mode.

## Examples

```
# Set the FTP update mode to normal.
<Sysname> system-view
[Sysname] ftp update normal
```

## FTP Client Configuration Commands

---



### Note

- In this section, the configuration procedure of entering FTP client view is omitted. You must use the **ftp** command to enter FTP client view for configurations under this view. For details, refer to [ftp](#).
  - Before executing the FTP client configuration commands in this section, make sure you have configured the proper authority for users on the FTP server, such as view the files under the current directory, read/download the specified file, create directory/upload files, rename/remove files, and so on.
  - The prompt information in the examples of this section varies with FTP server types.
- 

## ascii

### Syntax

**ascii**

### View

FTP client view

### Default Level

3: Manage level

### Parameters

None

### Description

Use the **ascii** command to set the file transfer mode to ASCII.

By default, the file transfer mode is ASCII.

The carriage return characters vary with operating systems. For example, to indicate the end of a line and transfer to the next line, the 3Com device system and Windows system use characters **/r/n**, and the Linux system uses characters **/n**. Therefore, after the file transmission between two systems that use different carriage return characters, such as Linux system and 3Com device system, the FTP transmission mode must be applied to ensure the correct resolution of the files.

FTP transfers files in two modes:

- Binary mode: for program file or picture transmission.
- ASCII mode: for text file transmission.

Related commands: **binary**.

## Examples

```
# Set the file transfer mode to ASCII.  
[ftp] ascii  
200 Type set to A.
```

## binary

### Syntax

**binary**

### View

FTP client view

### Default Level

3: Manage level

### Parameters

None

### Description

Use the **binary** command to set the file transfer mode to binary (also called flow mode).

By default, the transfer mode is ASCII mode.

Related commands: **ascii**.

## Examples

```
# Set the file transfer mode to binary.  
[ftp] binary  
200 Type set to I.
```

## bye

### Syntax

**bye**

### View

FTP client view

### Default Level

3: Manage level

### Parameters

None

## Description

Use the **bye** command to disconnect from the remote FTP server and return to user view.

## Examples

```
# Terminate the connection with the remote FTP server and return to user view.
```

```
[ftp] bye  
221 Server closing.
```

## cd

### Syntax

```
cd { directory | .. | / }
```

### View

FTP client view

### Default Level

3: Manage level

### Parameters

*directory*: Name of the target directory, in the format of [*drive*:][*/*]*path*. *drive* represents the name of the storage medium, which is flash for the 3Com Switch 4800G. If *drive* is not specified, it indicates the file or subfolder under the current directory.

..: Returns to the upper directory, the function same as **cdup**. If the current working directory is the root directory, or there is no such an upper directory, the current working directory is not changed after the execution of the **cd** command. No command line help for this keyword.

/: Returns to the root directory of the storage medium. No command line help for this keyword.

## Description

Use the **cd** command to change the current working directory on the remote FTP server.

You can use this command to access another authorized directory on the FTP server.

Related commands: **pwd**.

## Examples

```
# Change the working directory to the sub-directory logfile of the current directory.
```

```
[ftp] cd logfile  
250 CWD command successful.
```

```
# Change the working directory to the sub-directory folder of the authorized directory.
```

```
[ftp] cd /folder  
250 CWD command successful.
```

## cdup

### Syntax

```
cdup
```

## View

FTP client view

## Default Level

3: Manage level

## Parameters

None

## Description

Use the **cdup** command to exit the current directory and enter the upper directory of the FTP server. Execution of this command will not change the working directory if the current directory is already the authorized directory (that is, **work-directory**).

Related commands: **cd**, **pwd**.

## Examples

```
# Change the current working directory path to the upper directory.
```

```
[ftp] cdup
200 CDUP command successful.
```

## close

### Syntax

**close**

## View

FTP client view

## Default Level

3: Manage level

## Parameters

None

## Description

Use the **close** command to terminate the connection to the FTP server, but remain in FTP client view.

This command is equal to the **disconnect** command.

## Examples

```
# Terminate the connection to the FTP server and remain in FTP client view.
```

```
[ftp] close
221 Server closing.
[ftp]
```

## debugging

### Syntax

**debugging**

**undo debugging**

### View

FTP client view

### Default Level

3: Manage level

### Parameters

None

### Description

Use the **debugging** command to enable FTP client debugging.

Use the **undo debugging** command to disable FTP client debugging.

By default, FTP client debugging is disabled.

### Examples

# The device serves as the FTP client. Enable FTP client debugging and use the active mode to download file **sample.file** from the current directory of the FTP server.

```
<Sysname> terminal monitor
<Sysname> terminal debugging
<Sysname> ftp 192.168.1.46
Trying 192.168.1.46 ...
Press CTRL+K to abort
Connected to 192.168.1.46.
220 FTP service ready.
User(192.168.1.46:(none)):ftp
331 Password required for ftp.
Password:
230 User logged in.

[ftp]undo passive
[ftp] debugging
[ftp] get sample.file

---> PORT 192,168,1,44,4,21
200 Port command okay.
The parsed reply is 200
---> RETR sample.file
150 Opening ASCII mode data connection for /sample.file.
The parsed reply is 150
FTPC: File transfer started with the signal light turned on.
FTPC: File transfer completed with the signal light turned off.
```

```
.226 Transfer complete.
```

```
FTP: 3304 byte(s) received in 4.889 second(s), 675.00 byte(s)/sec.
```

```
[ftp]
```

**Table 2-3 debugging** command output description

Field	Description
---> PORT	Give an FTP order, with data port numbers being...
The parsed reply is	The received reply code, which is defined in RFC 959.
---> RETR	Download the file
FTPC: File transfer started with the signal light turned on.	File transfer starts, and the signal light is turned on.
FTPC: File transfer completed with the signal light turned off.	File transfer is completed, and the signal light is turned off.

## delete

### Syntax

```
delete remotefile
```

### View

FTP client view

### Default Level

3: Manage level

### Parameters

*remotefile*: File name.

### Description

Use the **delete** command to permanently delete a specified file on the remote FTP server.

To do this, you must be a user with the delete permission on the FTP server.

### Examples

```
# Delete file temp.c.  
[ftp] delete temp.c  
250 DELE command successful.
```

## dir

### Syntax

```
dir [ remotefile [ localfile ] ]
```

## View

FTP client view

## Default Level

3: Manage level

## Parameters

*remotefile*: Name of the file or directory on the remote FTP server.

*localfile*: Name of the local file to save the displayed information.

## Description

Use the **dir** command to view the detailed information of the files and subdirectories under the current directory on the remote FTP server.

Use the **dir remotefile** command to display the detailed information of the specified file or directory on the remote FTP server.

Use the **dir remotefile localfile** command to display the detailed information of the specified file or directory on the remote FTP server, and save the displayed information into a local file specified by the *localfile* argument.



### Note

You can use the **dir** command to display the folder- and file-related information, such as the size, and the date they were created. If you only need to view the name of all the files and subdirectories under the current directory, you can use the **ls** command.

---

## Examples

# View the detailed information of the files and subdirectories under the current directory on the remote FTP server.

```
[ftp] dir
227 Entering Passive Mode (192,168,1,46,5,68).
125 ASCII mode data connection already open, transfer starting for /*.
drwxrwxrwx  1 noone  nogroup          0 Aug 08  2006 logfile
-rwxrwxrwx  1 noone  nogroup  20471748 May 11 10:21 test.bin
-rwxrwxrwx  1 noone  nogroup    4001 Dec 08  2007 config.cfg
-rwxrwxrwx  1 noone  nogroup    3608 Jun 13  2007 startup.cfg
drwxrwxrwx  1 noone  nogroup          0 Dec 03  2007 test
-rwxrwxrwx  1 noone  nogroup    299 Oct 15  2007 key.pub
226 Transfer complete.
FTP: 394 byte(s) received in 0.189 second(s), 2.00K byte(s)/sec.
```

```
[ftp]
```

# View the information of the file **ar-router.cfg**, and save the result to **aa.txt**.

```
[ftp] dir ar-router.cfg aa.txt
```

```
227 Entering Passive Mode (192,168,1,50,17,158).
125 ASCII mode data connection already open, transfer starting for /ar-router.cfg.
....226 Transfer complete.
FTP: 67 byte(s) received in 4.600 second(s), 14.00 byte(s)/sec.
```

View the content of **aa.txt**.

```
[ftp] quit
<Sysname> more aa.txt
-rwxrwxrwx  1 noone  nogroup      3077 Jun 20 15:34 ar-router.cfg
```

## disconnect

### Syntax

```
disconnect
```

### View

FTP client view

### Default Level

3: Manage level

### Parameters

None

### Description

Use the **disconnect** command to disconnect from the remote FTP server but remain in FTP client view.

This command is equal to the **close** command.

### Examples

```
# Disconnect from the remote FTP server but remain in FTP client view.
[ftp] disconnect
221 Server closing.
```

## display ftp client configuration

### Syntax

```
display ftp client configuration
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

## Description

Use the **display ftp client configuration** command to display the configuration information of the FTP client.



### Note

Currently this command displays the configured source IP address or source interface of the FTP client.

---

Related commands: **ftp client source**.

## Examples

# Display the current configuration information of the FTP client.

```
<Sysname> display ftp client configuration
The source IP address is 192.168.0.123
```

## ftp

### Syntax

```
ftp [ server-address [ service-port ] [ source { interface interface-type interface-number | ip source-ip-address } ] ]
```

### View

User view

### Default Level

3: Manage level

### Parameters

*server-address*: IP address or host name (a string of 1 to 20 characters) of a remote FTP server.

*service-port*: TCP port number of the remote FTP server, in the range 0 to 65535. The default value is 21.

**interface** *interface-type interface-number*: Specifies the source interface by its type and number. The primary IP address configured on this interface is the source address of the transmitted packets. If no primary IP address is configured on the source interface, the connection fails.

**ip** *source-ip-address*: The source IP address of the current FTP client. This source address must be the one that has been configured on the device.

## Description

Use the **ftp** command to log in to the remote FTP server and enter FTP client view.

Note that:

- This command applies to IPv4 networks.
- If you use this command without specifying any parameters, you will simply enter the FTP client view without logging in to the FTP server.

- If you specify the parameters, you will be prompted to enter the username and password for accessing the FTP server.
- The priority of the source address specified with this command is higher than that with the **ftp client source** command. If you specify the source address with the **ftp client source** command first and then with the **ftp** command, the source address specified with the **ftp** command is used to communicate with the FTP server.

Related commands: **ftp client source**.

## Examples

# Log in from the current device **Sysname1** to the device **Sysname2** with the IP address of 192.168.0.211. The source IP address of the packets sent is 192.168.0.212.

```
<Sysname> ftp 192.168.0.211 source ip 192.168.0.212
Trying 192.168.0.211 ...
Press CTRL+K to abort
Connected to 192.168.0.211.
220 FTP Server ready.
User(192.168.0.211:(none)):abc
331 Password required for abc
Password:
230 User logged in.

[ftp]
```

## ftp client source

### Syntax

```
ftp client source { interface interface-type interface-number | ip source-ip-address }
undo ftp client source
```

### View

System view

### Default Level

2: System level

### Parameters

**interface** *interface-type interface-number*: Source interface for the FTP connection, including interface type and interface number. The primary IP address configured on the source interface is the source IP address of the packets sent by FTP. If no primary IP address is configured on the source interface, the connection fails.

**ip** *source-ip-address*: Source IP address of the FTP connection. It must be an IP address that has been configured on the device.

### Description

Use the **ftp client source** command to configure the source address of the transmitted FTP packets from the FTP client.

Use the **undo ftp client source** command to restore the default.

By default, a device uses the IP address of the interface determined by the matched route as the source IP address to communicate with an FTP server.

Note that:

- The source address can be specified as the source interface and the source IP address. If you use the **ftp client source** command to specify the source interface and then the source IP address, the newly specified source IP address overwrites the configured source interface and vice versa.
- If the source address is specified with the **ftp client source** command and then with the **ftp** command, the source address specified with the latter one is used to communicate with the FTP server.
- The source address specified with the **ftp client source** command is valid for all FTP connections and the source address specified with the **ftp** command is valid only for the current FTP connection.

Related commands: **display ftp client configuration**.

## Examples

# Specify the source IP address of the FTP client as 2.2.2.2.

```
<Sysname> system-view
[Sysname] ftp client source ip 2.2.2.2
```

# Specify the source interface of the FTP client as Vlan-interface 1.

```
<Sysname> system-view
[Sysname] ftp client source interface vlan-interface 1
```

## ftp ipv6

### Syntax

```
ftp ipv6 [ server-address [ service-port ] [ source ipv6 source-ipv6-address ] [ -i interface-type interface-number ] ]
```

### View

User view

### Default Level

3: Manage level

### Parameters

*server-address*: IP address or host name of the remote FTP server.

*service-port*: TCP port number of the FTP server, in the range 0 to 65535. The default value is 21.

**source ipv6** *source-ipv6-address*: Specifies a source IPv6 address for transmitted FTP packets. This address must be an IPv6 address that has been configured on the device.

**-i** *interface-type interface-number*: Specifies the type and number of the egress interface. This parameter can be used only in case that the FTP server address is a link local address and the specified egress interface must have a link local address (For the configuration of link local addresses, see *IPv6 Basics* in the *IP Services Volume*).

## Description

Use the **ftp ipv6** command to log in to the FTP server and enter FTP client view.

Note that:

- This command applies to IPv6 networks.
- If you use this command without specifying any parameters, you will simply enter the FTP client view without logging in to an FTP server.
- If you specify the parameters, you will be asked to enter the username and password for accessing the FTP server.

## Examples

```
# Log in to the FTP server with IPv6 address 3000::200.
```

```
<Sysname> ftp ipv6 3000::200
Trying 3000::200 ...
Press CTRL+K to abort
Connected to 3000::200.
220 Welcome!
User(3000::200:(none)): MY_NAME
331 Please specify the password.
Password:
230 Login successful.
[ftp]
```

## get

### Syntax

```
get remotefile [ localfile ]
```

### View

FTP client view

### Default Level

3: Manage level

### Parameters

*remotefile*: Name of the file to be downloaded.

*localfile*: File name used after a file is downloaded and saved locally. If this argument is not specified, the file is saved locally using the source file name to the current working directory, namely the directory where the user executes the **ftp** command.

## Description

Use the **get** command to download a file from a remote FTP server and save it.

## Examples

```
# Download file testcfg.cfg to the root directory of the storage medium of the master, and save it as newest.cfg.
```

```
[ftp] get startup.cfg newest.cfg
```

```
227 Entering Passive Mode (192,168,1,46,4,47).
```

```
125 ASCII mode data connection already open, transfer starting for /startup.cfg.
```

```
..226 Transfer complete.
```

```
FTP: 3608 byte(s) received in 2.050 second(s), 1.00K byte(s)/sec.
```

# Download file **testcfg.cfg** to the root directory of the storage medium of the slave (with the member ID 2), and save it as **newest.cfg**.

```
[ftp] get startup.cfg slot2#flash:/newest.cfg
```

```
227 Entering Passive Mode (192,168,1,46,4,48).
```

```
125 ASCII mode data connection already open, transfer starting for /startup.cfg.
```

```
226 Transfer complete.
```

```
FTP: 3608 byte(s) received in 2.322 second(s), 1.00K byte(s)/sec.
```

## lcd

### Syntax

```
lcd
```

### View

FTP client view

### Default Level

3: Manage level

### Parameters

None

### Description

Use the **lcd** command to display the local working directory of the FTP client.

### Examples

```
# Display the local working directory.
```

```
[ftp] lcd
```

```
FTP: Local directory now flash:/clienttemp.
```

The above information indicates that the working directory of the FTP client before execution of the **ftp** command is **flash:/clienttemp**.

## ls

### Syntax

```
ls [ remotefile [ localfile ] ]
```

### View

FTP client view

## Default Level

3: Manage level

## Parameters

*remotefile*: Filename or directory on the remote FTP server.

*localfile*: Name of a local file used to save the displayed information.

## Description

Use the **ls** command to view the information of all the files and subdirectories under the current directory of the remote FTP server. The file names and subdirectory names are displayed.

Use the **ls remotefile** command to view the information of a specified file or subdirectory.

Use the **ls remotefile localfile** command to view the information of a specified file or subdirectory, and save the result to a local file specified by the *localfile* argument.



### Note

The **ls** command can only display the names of files and directories on the FTP server, whereas the **dir** command can display other related information of the files and directories, such as the size, and the date they were created.

---

## Examples

# View the information of all files and subdirectories under the current directory of the FTP server.

```
[ftp] ls
227 Entering Passive Mode (192,168,1,50,17,165).
125 ASCII mode data connection already open, transfer starting for /*.
ar-router.cfg
logfile
mainar.bin
arbasicbtm.bin
ftp
test
bb.cfg
testcfg.cfg
226 Transfer complete.
FTP: 87 byte(s) received in 0.132 second(s) 659.00 byte(s)/sec.
```

# View the information of directory **logfile**, and save the result to file **aa.txt**.

```
[ftp] ls logfile aa.txt
227 Entering Passive Mode (192,168,1,46,4,3).
125 ASCII mode data connection already open, transfer starting for /logfile/*.
...226 Transfer complete.
FTP: 20 byte(s) received in 3.962 second(s), 5.00 byte(s)/sec.
```

# View the content of file **aa.txt**.

```
[ftp] quit
<Sysname> more aa.txt
.
..
logfile.log
```

## mkdir

### Syntax

```
mkdir directory
```

### View

FTP client view

### Default Level

3: Manage level

### Parameters

*directory*: Name of the directory to be created.

### Description

Use the **mkdir** command to create a subdirectory under the current directory on the remote FTP server. To do this, you must be a user with the permission on the FTP server.

### Examples

```
# Create subdirectory mytest on the current directory of the remote FTP server.
[ftp] mkdir mytest
257 "/mytest" new directory created.
```

## open

### Syntax

```
open server-address [ service-port ]
```

### View

FTP client view

### Default Level

3: Manage level

### Parameters

*server-address*: IP address or host name of a remote FTP server.

*service-port*: Port number of the remote FTP server, in the range 0 to 65535, with the default value of 21.

### Description

Use the **open** command to log in to the IPv4 FTP server under FTP client view.

At login, you will be asked to enter the username and password for accessing the FTP server. If your input is correct, the login succeeds; otherwise, it fails.

If you have logged in to the IPv4 FTP server currently, you cannot use the **open** command to log in to another server. You need to disconnect with the current server first, and then try to connect with another one.

Related commands: **close**.

## Examples

# In FTP client view, log in to the FTP server with the IP address of 192.168.1.50.

```
<Sysname> ftp
[ftp] open 192.168.1.50
Trying 192.168.1.50 ...
Press CTRL+K to abort
Connected to 192.168.1.50.
220 FTP service ready.
User(192.168.1.50:(none)):aa
331 Password required for aa.
Password:
230 User logged in.

[ftp]
```

## open ipv6

### Syntax

```
open ipv6 server-address [ service-port ] [ -i interface-type interface-number ]
```

### View

FTP client view

### Default Level

3: Manage level

### Parameters

*server-address*: IP address or host name of the remote FTP server.

*service-port*: Port number of the remote FTP server, in the range 0 to 65535. The default value is 21.

**-i** *interface-type interface-number*: Specifies the egress interface by its type and number. This parameter can be used only in case that the FTP server address is a link local address and the specified egress interface must have a link local address (For the configuration of link local addresses, see *IPv6 Basics* in the *IP Services Volume*).

### Description

Use the **open ipv6** command to log in to the IPv6 FTP server in FTP client view.

At login, you will be asked to enter the username and password for accessing the FTP server. If your input is correct, the login succeeds; otherwise, it fails.

Related commands: **close**.

## Examples

```
# Log in to the FTP server (with IPv6 address 3000::200) in FTP client view.
<Sysname> ftp
[ftp] open ipv6 3000::200
Trying 3000::200 ...
Press CTRL+K to abort
Connected to 3000::200.
220 Welcome!
User(3000::200:(none)): MY_NAME
331 Please specify the password.
Password:
230 Login successful.
```

## passive

### Syntax

```
passive
undo passive
```

### View

FTP client view

### Default Level

3: Manage level

### Parameters

None

### Description

Use the **passive** command to set the data transmission mode to **passive**.

Use the **undo passive** command to set the data transmission mode to **active**.

The default transmission mode is **passive**.

Data transmission modes fall into the passive mode and the active mode. The active mode means that the data connection request is initiated by a server. The passive mode means that the data connection request is initiated by a client. This command is mainly used in conjunction with a firewall to restrict the FTP session connection between private and public network users.

## Examples

```
# Set the data transmission mode to passive.
[ftp] passive
FTP: passive is on
```

## put

### Syntax

```
put localfile [ remotefile ]
```

## View

FTP client view

## Default Level

3: Manage level

## Parameters

*localfile*: Name of the local file to be uploaded.

*remotefile*: File name used after a file is uploaded and saved on the FTP server.

## Description

Use the **put** command to upload a file on the client to the remote FTP server.

If no name is assigned to the file to be saved on the FTP server, the name of the source file is used by default. After a file is uploaded, it will be saved under the user's authorized directory, which can be set with the **authorization-attribute** command.

## Examples

# Upload source file **vrpcfg.cfg** on the master to the remote FTP server and save it as **ftpclient.cfg**.

```
[ftp] put vrpcfg.cfg ftpclient.cfg
227 Entering Passive Mode (192,168,1,46,4,50).
125 ASCII mode data connection already open, transfer starting for /ftpclient.cfg.
226 Transfer complete.
FTP: 1366 byte(s) sent in 0.064 second(s), 21.00Kbyte(s)/sec.
```

# Upload source file **a.cfg** on the slave (with the member ID 2) to the remote FTP server and save it as **ftpclienta.cfg**.

```
[ftp] put slot2#flash:/a.cfg ftpclienta.cfg
227 Entering Passive Mode (192,168,1,46,4,52).
125 ASCII mode data connection already open, transfer starting for /ftpclienta.cfg.
226 Transfer complete.
FTP: 1226 byte(s) sent in 0.065 second(s), 18.00Kbyte(s)/sec.
```

## pwd

### Syntax

**pwd**

### View

FTP client view

### Default Level

3: Manage level

### Parameters

None

## Description

Use the **pwd** command to display the currently accessed directory on the remote FTP server.

## Examples

# Display the currently accessed directory on the remote FTP server.

```
[ftp] cd servertemp
[ftp] pwd
257 "/servertemp" is current directory.
```

The above information indicates that the **servertemp** folder under the root directory of the remote FTP server is being accessed by the user.

## quit

### Syntax

**quit**

### View

FTP client view

### Default Level

3: Manage level

### Parameters

None

### Description

Use the **quit** command to disconnect from the remote FTP server and exit to user view.

## Examples

# Disconnect from the remote FTP server and exit to user view.

```
[ftp] quit
221 Server closing.

<Sysname>
```

## remotehelp

### Syntax

**remotehelp** [ *protocol-command* ]

### View

FTP client view

### Default Level

3: Manage level

## Parameters

protocol-command: FTP command.

## Description

Use the **remotehelp** command to display the help information of FTP-related commands supported by the remote FTP server.

If no argument is specified, FTP-related commands supported by the remote FTP server are displayed.

## Examples

# Display FTP commands supported by the remote FTP server.

```
[ftp] remotehelp
214-Here is a list of available ftp commands
    Those with '*' are not yet implemented.
    USER  PASS  ACCT*  CWD   CDUP  SMNT*  QUIT  REIN*
    PORT   PASV  TYPE   STRU*  MODE*  RETR   STOR  STOU*
    APPE*  ALLO*  REST*  RNFR*  RNT0*  ABOR*  DELE  RMD
    MKD    PWD    LIST   NLST   SITE*  SYST   STAT*  HELP
    NOOP*  XCUP   XCWD   XMKD   XPWD   XRMD
214 Direct comments to 3Com company.
```

# Display the help information for the **user** command.

```
[ftp] remotehelp user
214 Syntax: USER <sp> <username>.

[ftp]
```

**Table 2-4 remotehelp** command output description

Field	Description
214-Here is a list of available ftp commands	The following is an available FTP command list.
Those with '*' are not yet implemented.	Those commands with "*" are not yet implemented.
USER	Username
PASS	Password
CWD	Change the current working directory
CDUP	Change to parent directory
SMNT*	File structure setting
QUIT	Quit
REIN*	Re-initialization
PORT	Port number
PASV	Passive mode
TYPE	Request type
STRU*	File structure
MODE*	Transmission mode

Field	Description
RETR	Download a file
STOR	Upload a file
STOU*	Store unique
APPE*	Appended file
ALLO*	Allocation space
REST*	Restart
RNFR*	Rename the source
RNTO*	Rename the destination
ABOR*	Abort the transmission
DELE	Delete a file
RMD	Delete a folder
MKD	Create a folder
PWD	Print working directory
LIST	List files
NLST	List file description
SITE*	Locate a parameter
SYST	Display system parameters
STAT*	State
HELP	Help
NOOP*	No operation
XCUP	Extension command, the same meaning as CUP
XCWD	Extension command, the same meaning as CWD
XMKD	Extension command, the same meaning as MKD
XPWD	Extension command, the same meaning as PWD
XRMD	Extension command, the same meaning as RMD
Syntax: USER <sp> <username>.	Syntax of the <b>user</b> command: user (keyword) + space + <i>username</i>

## rmdir

### Syntax

**rmdir** *directory*

### View

FTP client view

## Default Level

3: Manage level

## Parameters

*directory*: Directory name on the remote FTP server.

## Description

Use the **rmdir** command to remove a specified directory from the FTP server.

Note that only authorized users are allowed to use this command.

Note that:

- The directory to be deleted must be empty, meaning you should delete all files and subdirectories under the directory before you delete a directory. For the deletion of files, refer to the **delete** command.
- After you execute the **rmdir** command successfully, the files in the remote recycle bin under the directory will be automatically deleted.

## Examples

# Delete the **temp1** directory from the authorized directory on the FTP server.

```
[ftp] rmdir /temp1
200 RMD command successful.
```

## user

### Syntax

```
user username [ password ]
```

### View

FTP client view

## Default Level

3: Manage level

## Parameters

*username*: Login username.

*password*: Login password.

## Description

Use the **user** command to relog in to the currently accessed FTP server with another username.

Before using this command, you must configure the corresponding username and password on the FTP server; otherwise, your login fails and the FTP connection is closed.

## Examples

# User **ftp1** has logged in to the FTP server. Use username **ftp2** to log in to the current FTP server. (Suppose username **ftp2** and password **123123123123** have been configured on the FTP server).

```
[ftp] user ftp2
```

```
331 Password required for ftp2.  
Password:  
230 User logged in.  
  
[ftp]
```

## verbose

### Syntax

```
verbose  
undo verbose
```

### View

FTP client view

### Default Level

3: Manage level

### Parameters

None

### Description

Use the **verbose** command to enable the protocol information function to display detailed prompt information.

Use the **undo verbose** command to disable the protocol information function.

By default, the protocol information function is enabled.

### Examples

# Enable the protocol information function.

```
[ftp] verbose  
FTP: verbose is on
```

# Disable the protocol information function and perform the Get operation.

```
[ftp] undo verbose  
FTP: verbose is off
```

```
[ftp] get startup.cfg bb.cfg
```

```
FTP: 3608 byte(s) received in 0.052 second(s), 69.00K byte(s)/sec.
```

```
[ftp]
```

# Enable the protocol information function and perform the Get operation.

```
[ftp] verbose  
FTP: verbose is on
```

```
[ftp] get startup.cfg aa.cfg
```

227 Entering Passive Mode (192,168,1,46,5,85).

125 ASCII mode data connection already open, transfer starting for /startup.cfg.

226 Transfer complete.

FTP: 3608 byte(s) received in 0.193 second(s), 18.00K byte(s)/sec.

# 3 TFTP Configuration Commands

---

## TFTP Client Configuration Commands

### display tftp client configuration

#### Syntax

```
display tftp client configuration
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

None

#### Description

Use the **display tftp client configuration** command to display the configuration information of the TFTP client.

Related commands: **tftp client source**.

#### Examples

```
# Display the current configuration information of the TFTP client.
```

```
<Sysname> display tftp client configuration
```

```
The source IP address is 192.168.0.123
```



#### Note

Currently this command displays the configured source IP address or source interface of the TFTP client.

---

## tftp-server acl

#### Syntax

```
tftp-server [ ipv6 ] acl acl-number
```

```
undo tftp-server [ ipv6 ] acl
```

## View

System view

## Default Level

3: Manage level

## Parameters

**ipv6**: References an IPv6 ACL. If it is not specified, an IPv4 ACL is referenced.

*acl-number*: Number of a basic ACL, in the range 2000 to 2999.

## Description

Use the **tftp-server acl** command to control the access to the TFTP servers from the device through ACL.

Use the **undo tftp-server acl** command to restore the default.

By default, the access to the TFTP servers from the device is not controlled.

You can use the rules defined in the ACL to permit or deny the access from the device to the specified TFTP server on the network.

For more information about ACL, refer to *ACL Configuration* in the *Security Volume*.

## Examples

# In IPv4 networking environment, allow the device to access the TFTP server with the IP address of 1.1.1.1 only.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 1.1.1.1 0
[Sysname-acl-basic-2000] quit
[Sysname] tftp-server acl 2000
```

# In IPv6 networking environment, allow the device to access the TFTP server with the IP address of 2001::1 only.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2001
[Sysname-acl6-basic-2001] rule permit source 2001::1/128
[Sysname-acl6-basic-2001] quit
[Sysname] tftp-server ipv6 acl 2001
```

## tftp

### Syntax

```
tftp server-address { get | put | sget } source-filename [ destination-filename ] [ source { interface interface-type interface-number | ip source-ip-address } ]
```

## View

User view

## Default Level

3: Manage level

## Parameters

*server-address*: IP address or host name of a TFTP server.

**get**: Downloads a file in normal mode.

**put**: Uploads a file.

**sget**: Downloads a file in secure mode.

*source-filename*: Source file name.

*destination-filename*: Destination file name.

**source**: Configures parameters for source address binding.

- **interface** *interface-type interface-number*: Specifies the source interface by its type and number. The primary IP address configured on the source interface is the source IP address of the packets sent by TFTP. If no primary IP address is configured on the source interface, the transmission fails.
- **ip** *source-ip-address*: Specifies the source IP address for the current TFTP client to transmit packets. This source address must be an IP address that has been configured on the device.

## Description

Use the **tftp** command to upload files from the local device to a TFTP server or download files from the TFTP server to the local device.

- If no destination file name is specified, a file is saved using the same name as that on the remote FTP server to the current working directory of the user (namely, the working directory where the **tftp** command is executed).
- The priority of the source address specified with this command is higher than that specified with the **tftp client source** command. If you use the **tftp client source** command to specify the source address first and then with the **tftp** command, the latter one is adopted.

This command applies to IPv4 networks.

Related commands: **tftp client source**.

## Examples

# Download the **config.cfg** file from the TFTP server with the IP address of 192.168.0.98 and save it as **config.bak**. Specify the source IP address to be 192.168.0.92.

```
<Sysname> tftp 192.168.0.98 get config.cfg config.bak source ip 192.168.0.92
...
File will be transferred in binary mode
Downloading file from remote TFTP server, please wait....
TFTP:      372800 bytes received in 1 second(s)
File downloaded successfully.
```

# Upload the **config.cfg** file from the local device to the default path of the TFTP server with the IP address of 192.168.0.98 and save it as **config.bak**. Specify the source IP interface to be Vlan-interface 1.

```
<Sysname> tftp 192.168.0.98 put config.cfg config.bak source interface vlan-interface 1

File will be transferred in binary mode
```

```
    Sending file to remote TFTP server. Please wait...
    TFTP:      345600 bytes sent in 1 second(s).
File uploaded successfully.
```

# To upgrade the device, download the **test.bin** file from the TFTP server with the IP address of 192.168.1.26 and save it to both the root directory on the flash of the master and the root directory on the flash of the slave (with the member ID 2).

```
<Sysname> tftp 192.168.1.26 get newest.bin startup.bin
```

```
.
File will be transferred in binary mode
Downloading file from remote TFTP server, please wait.....
TFTP:  2737556 bytes received in 13 second(s)
File downloaded successfully.
```

// Download the BIN file from the TFTP server to the root directory on the flash of the master.

```
<Sysname> tftp 192.168.1.26 get newest.bin slot2#flash:/startup.bin
```

```
File will be transferred in binary mode
Downloading file from remote TFTP server, please wait...|
TFTP:  2737556 bytes received in 14 second(s)
File downloaded successfully.
```

// Download the BIN file from the TFTP server to the root directory on the flash of the slave.

## tftp client source

### Syntax

```
tftp client source { interface interface-type interface-number | ip source-ip-address }
undo tftp client source
```

### View

System view

### Default Level

2: System level

### Parameters

**interface** *interface-type interface-number*: Specifies the source interface by its type and number. The primary IP address configured on the source interface is the source IP address of the packets sent by TFTP. If no primary IP address is configured on the source interface, the transmission fails.

**ip** *source-ip-address*: The source IP address of TFTP connections. It must be an IP address that has been configured on the device.

### Description

Use the **tftp client source** command to configure the source address of the TFTP packets from the TFTP client.

Use the **undo telnet client source** command to restore the default.

By default, a device uses the IP address of the interface determined by the matched route as the source IP address to communicate with a TFTP server.

Note that:

- The source address can be specified as the source interface and the source IP; if you use the **tftp client source** command to specify the source interface and then the source IP, the newly specified source IP overwrites the configured source interface and vice versa.
- If the source address is specified with the **tftp client source** command and then with the **tftp** command, the source address specified with the latter one is used to communicate with the TFTP server.
- The source address specified with the **tftp client source** command is valid for all **tftp** connections and the source address specified with the **tftp** command is valid for the current **tftp** command.

Related commands: **display tftp client configuration**.

## Examples

# Specify the source IP address of the TFTP client as 2.2.2.2.

```
<Sysname> system-view
[Sysname] tftp client source ip 2.2.2.2
```

# Specify the source interface of the TFTP client as Vlan-interface 1.

```
<Sysname> system-view
[Sysname] tftp client source interface vlan-interface 1
```

## tftp ipv6

### Syntax

```
tftp ipv6 tftp-ipv6-server [ -i interface-type interface-number ] { get | put } source-file [ destination-file ]
```

### View

User view

### Default Level

3: Manage level

### Parameters

*tftp-ipv6-server*: IPv6 address or host name (a string of 1 to 46 characters) of a TFTP server.

**-i** *interface-type interface-number*: Specifies the egress interface by its type and number. This parameter can be used only in case that the TFTP server address is a link local address and the specified egress interface must have a link local address (For the configuration of link local address, see *IPv6 Basics* in the *IP Services Volume*).

**get**: Downloads a file.

**put**: Uploads a file.

*source-filename*: Source filename.

*destination-filename*: Destination filename. If not specified, this filename is the same as the source filename.

## Description

Use the **tftp ipv6** command to download a specified file from a TFTP server or upload a specified local file to a TFTP server.

This command applies to IPv6 networks.

## Examples

# Download **filetoget.txt** from the TFTP server.

```
<Sysname> tftp ipv6 fe80::250:daff:fe91:e058 -i vlan-interface 1 get filetoget.txt
...
File will be transferred in binary mode
Downloading file from remote TFTP server, please wait....
TFTP:      411100 bytes received in 2 second(s)
File downloaded successfully.
```

# Table of Contents

<b>1 HTTP Configuration Commands</b> .....	<b>1-1</b>
HTTP Configuration Commands .....	1-1
display ip http .....	1-1
ip http acl .....	1-2
ip http enable .....	1-2
ip http port .....	1-3
<b>2 HTTPS Configuration Commands</b> .....	<b>2-1</b>
HTTPS Configuration Commands .....	2-1
display ip https .....	2-1
ip https acl .....	2-2
ip https certificate access-control-policy .....	2-2
ip https enable .....	2-3
ip https port .....	2-4
ip https ssl-server-policy .....	2-4

# 1 HTTP Configuration Commands

---

## HTTP Configuration Commands

### display ip http

#### Syntax

```
display ip http
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

None

#### Description

Use the **display ip http** command to display information about HTTP.

#### Examples

```
# Display information about HTTP..
```

```
<Sysname> display ip http
```

```
HTTP port: 80
```

```
Basic ACL: 2222
```

```
Current connection: 0
```

```
Operation status: Running
```

**Table 1-1** display ip http command output description

Field	Description
HTTP port	Port number used by the HTTP service
Basic ACL	A basic ACL number associated with the HTTP service
Current connection	The number of current connections
Operation status	Operation status, which takes the following values: <ul style="list-style-type: none"><li>Running: The HTTP service is enabled.</li><li>Stopped: The HTTP service is disabled.</li></ul>

## ip http acl

### Syntax

```
ip http acl acl-number  
undo ip http acl
```

### View

System view

### Default Level

2: System level

### Parameters

*acl-number*: ACL number, in the range 2000 to 2999: basic IPv4 ACL

### Description

Use the **ip http acl** command to associate the HTTP service with an ACL.

Use the **undo ip http acl** command to remove the association.

By default, the HTTP service is not associated with any ACL.

After the HTTP service is associated with an ACL, only the clients permitted by the ACL can access the device.

Related commands: **acl number** in *ACL Commands* in the *Security Volume*.

### Examples

# Configure to associate the HTTP service with ACL 2001 and only allow the clients within the 10.10.0.0/16 network segment to access the device through the Web function.

```
<Sysname> system-view  
[Sysname] acl number 2001  
[Sysname-acl-basic-2001] rule permit source 10.10.0.0 0.0.255.255  
[Sysname-acl-basic-2001] quit  
[Sysname] ip http acl 2001
```

## ip http enable

### Syntax

```
ip http enable  
undo ip http enable
```

### View

System view

### Default Level

2: System level

### Parameters

None

## Description

Use the **ip http enable** command to enable the HTTP service.

Use the **undo ip http enable** command to disable the HTTP service.

The device can act as the HTTP server and the users can access and control the device through the Web function only after the HTTP service is enabled.

## Examples

```
# Enable the HTTP service.
```

```
<Sysname> system-view  
[Sysname] ip http enable
```

```
# Disable the HTTP service.
```

```
<Sysname> system-view  
[Sysname] undo ip http enable
```

## ip http port

### Syntax

```
ip http port port-number
```

```
undo ip http port
```

### View

System view

### Default Level

3: Manage level

### Parameters

*port-number*: Port number of the HTTP service, in the range 1 to 65535.

## Description

Use the **ip http port** command to configure the port number of the HTTP service.

Use the **undo ip http port** command to restore the default.

By default, the port number of the HTTP service is 80.

Note that this command does not check whether the configured port number conflicts with that of an existing service. Therefore, you must ensure that the port number is not used by another service before the configuration.

## Examples

```
# Configure the port number of the HTTP service as 8080.
```

```
<Sysname> system-view  
[Sysname] ip http port 8080
```

# 2 HTTPS Configuration Commands

---

## HTTPS Configuration Commands

### display ip https

#### Syntax

**display ip https**

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

None

#### Description

Use the **display ip https** command to display information about HTTPS.

#### Examples

# Display information about HTTPS.

```
<Sysname> display ip https
HTTPS port: 443
SSL server policy: test
Certificate access-control-policy:
Basic ACL: 2222
Current connection: 0
Operation status: Running
```

**Table 2-1 display ip https** command output description

Field	Description
HTTPS port	Port number used by the HTTPS service
SSL server policy	The SSL server policy associated with the HTTPS service
Certificate access-control-policy	The certificate attribute access control policy associated with the HTTPS service
Basic ACL	The basic ACL number associated with the HTTPS service
Current connection	The number of current connections

Field	Description
Operation status	Operation status, which takes the following values: <ul style="list-style-type: none"> <li>• Running: The HTTPS service is enabled.</li> <li>• Stopped: The HTTPS service is disabled.</li> </ul>

## ip https acl

### Syntax

```
ip https acl acl-number
undo ip https acl
```

### View

System view

### Default Level

3: Manage level

### Parameters

*acl-number*: ACL number, in the range 2000 to 2999: basic IPv4 ACL

### Description

Use the **ip https acl** command to associate the HTTPS service with an ACL.

Use the **undo ip https acl** command to remove the association.

By default, the HTTPS service is not associated with any ACL.

After the HTTPS service is associated with an ACL, only the clients permitted by the ACL can access the device.

Related commands: **acl number** in *ACL Commands* in the *Security Volume*

### Examples

```
# Associate the HTTPS service with ACL 2001 and only allow the clients within the 10.10.0.0/16
network segment to access the HTTPS server through the Web function.
```

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-basic-2001] quit
[Sysname] ip https acl 2001
```

## ip https certificate access-control-policy

### Syntax

```
ip https certificate access-control-policy policy-name
undo ip https certificate access-control-policy
```

## View

System view

## Default Level

3: Manage level

## Parameters

*policy-name*: Name of the certificate attribute access control policy, a string of 1 to 16 characters.

## Description

Use the **ip https certificate access-control-policy** command to associate the HTTPS service with a certificate attribute access control policy.

Use the **undo ip https certificate access-control-policy** command to remove the association.

By default, the HTTPS service is not associated with any certificate attribute access control policy.

Association of the HTTPS service with a certificate attribute access control policy can control the access rights of clients.

Related commands: **pki certificate access-control-policy**. (In *PKI Commands* in the *Security Volume*)

## Examples

```
# Associate the HTTPS server to certificate attribute access control policy myacl.
```

```
<Sysname> system-view
```

```
[Sysname] ip https certificate access-control-policy myacl
```

## ip https enable

### Syntax

```
ip https enable
```

```
undo ip https enable
```

## View

System view

## Default Level

3: Manage level

## Parameters

None

## Description

Use the **ip https enable** command to enable the HTTPS service.

Use the **undo ip https enable** command to disable the HTTPS service.

By default, the HTTPS service is disabled.

The device can act as the HTTP server and the users can access and control the device through the Web function only after the HTTP service is enabled.

Note that enabling of the HTTPS service triggers an SSL handshake negotiation process. During the process, if a local certificate of the device already exists, the SSL negotiation is successfully performed, and the HTTPS service can be started normally. If no local certificate exists, a certificate application process will be triggered by the SSL negotiation. Since the application process takes much time, the SSL negotiation often fails and the HTTPS service cannot be started normally. Therefore, the **ip https enable** command must be executed for multiple times to ensure normal startup of the HTTPS service.

## Examples

```
# Enable the HTTPS service.  
<Sysname> system-view  
[Sysname] ip https enable
```

## ip https port

### Syntax

```
ip https port port-number  
undo ip https port
```

### View

System view

### Default Level

3: Manage level

### Parameters

*port-number*: Port number of the HTTPS service, in the range 1 to 65535.

### Description

Use the **ip https port** command to configure the port number of the HTTPS service.

Use the **undo ip https port** command to restore the default.

By default, the port number of the HTTPS service is 443.

Note that this command does not check whether the configured port number conflicts with that of an existing service. Therefore, you must ensure that the port number is not used by another service before the configuration.

## Examples

```
# Configure the port number of the HTTPS service as 6000.  
<Sysname> system-view  
[Sysname] ip https port 6000
```

## ip https ssl-server-policy

### Syntax

```
ip https ssl-server-policy policy-name  
undo ip https ssl-server-policy
```

## View

System view

## Default Level

3: Manage level

## Parameters

*policy-name*: Name of an SSL server policy, a string of 1 to 16 characters.

## Description

Use the **ip https ssl-server-policy** command to associate the HTTPS service with an SSL server-end policy.

Use the **undo ip https ssl-server-policy** to remove the association between the HTTPS service and an SSL server-end policy.

By default, the HTTPS service is not associated with any SSL server-end policy.

Note that:

- The HTTPS service can be enabled only after this command is configured successfully.
- You cannot modify an SSL server-end policy or remove the association between the HTTPS service and an SSL server-end policy after the HTTPS service is enabled.

Related commands: **ssl server-policy** in *SSL Commands* in the *Security Volume*

## Examples

# Configure the HTTPS service to use SSL server-end policy **myssl**.

```
<Sysname> system-view
```

```
[Sysname] ip https ssl-server-policy myssl
```

# Table of Contents

<b>1 SNMP Configuration Commands</b> .....	<b>1-1</b>
SNMP Configuration Commands.....	1-1
display snmp-agent community.....	1-1
display snmp-agent group.....	1-2
display snmp-agent local-engineid.....	1-3
display snmp-agent mib-view.....	1-4
display snmp-agent statistics.....	1-5
display snmp-agent sys-info.....	1-7
display snmp-agent trap queue.....	1-8
display snmp-agent trap-list.....	1-8
display snmp-agent usm-user.....	1-9
enable snmp trap updown.....	1-10
snmp-agent.....	1-11
snmp-agent calculate-password.....	1-12
snmp-agent community.....	1-13
snmp-agent group.....	1-15
snmp-agent local-engineid.....	1-16
snmp-agent log.....	1-17
snmp-agent mib-view.....	1-18
snmp-agent packet max-size.....	1-19
snmp-agent sys-info.....	1-19
snmp-agent target-host.....	1-21
snmp-agent trap enable.....	1-22
snmp-agent trap if-mib link extended.....	1-24
snmp-agent trap life.....	1-25
snmp-agent trap queue-size.....	1-25
snmp-agent trap source.....	1-26
snmp-agent usm-user { v1   v2c }.....	1-27
snmp-agent usm-user v3.....	1-28
<b>2 MIB Configuration Commands</b> .....	<b>2-1</b>
MIB Configuration Commands.....	2-1
display mib-style.....	2-1
mib-style.....	2-1

# 1 SNMP Configuration Commands

---

## SNMP Configuration Commands

### display snmp-agent community

#### Syntax

```
display snmp-agent community [ read | write ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

**read:** Displays the information of communities with read-only access right.

**write:** Displays the information of communities with read and write access right.

#### Description

Use the **display snmp-agent community** command to display community information for SNMPv1 or SNMPv2c.

#### Examples

# Display the information of all the communities that have been configured.

```
<Sysname> display snmp-agent community
```

```
Community name: aa
  Group name: aa
  Acl:2001
  Storage-type: nonVolatile
```

```
Community name: bb
  Group name: bb
  Storage-type: nonVolatile
```

```
Community name: userv1
  Group name: testv1
  Storage-type: nonVolatile
```

**Table 1-1** display snmp-agent community command output description

Field	Description
Community name	Community name. <ul style="list-style-type: none"><li>• If a community name is created by using the <b>snmp-agent community</b> command, the community name will be displayed.</li><li>• If a community name is created by using the <b>snmp-agent usm-user { v1   v2c }</b> command, the user name will be displayed.</li></ul>
Group name	SNMP group name. <ul style="list-style-type: none"><li>• If a community name is created by using the <b>snmp-agent community</b> command, the group name and the community name are the same, which means the community name will be displayed.</li><li>• If a community name is created by using the <b>snmp-agent usm-user { v1   v2c }</b> command, the name of the group to which the user belongs will be displayed.</li></ul>
Acl	The number of the ACL in use. After an ACL is configured, only the Network Management Station (NMS) with the IP address that matches the ACL rule can access the device.
Storage-type	Storage type, which could be: <ul style="list-style-type: none"><li>• <i>volatile</i>: Information will be lost if the system is rebooted</li><li>• <i>nonVolatile</i>: Information will not be lost if the system is rebooted</li><li>• <i>permanent</i>: Information will not be lost if the system is rebooted. Modification is permitted, but deletion is forbidden</li><li>• <i>readOnly</i>: Information will not be lost if the system is rebooted. Read only, that is, no modification, no deletion</li><li>• <i>other</i>: Other storage types</li></ul>

## display snmp-agent group

### Syntax

```
display snmp-agent group [ group-name ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*group-name*: Specifies the SNMP group name, a string of 1 to 32 characters, case sensitive.

### Description

Use the **display snmp-agent group** command to display information for the SNMP agent group, including group name, security model, MIB view, storage type, and so on. Absence of the *group-name* parameter indicates that information for all groups will be displayed.

### Examples

```
# Display the information of all SNMP agent groups.
```

```
<Sysname> display snmp-agent group
```

```

Group name: groupv3
Security model: v3 noAuthnoPriv
Readview: ViewDefault
Writeview: <no specified>
Notifyview: <no specified>
Storage-type: nonVolatile

```

**Table 1-2 display snmp-agent group** command output description

Field	Description
Group name	SNMP group name
Security model	Security model of the SNMP group, which can be: authPriv (authentication with privacy), authNoPriv (authentication without privacy), or noAuthNoPriv (no authentication no privacy).
Readview	The read only MIB view associated with the SNMP group
Writeview	The writable MIB view associated with the SNMP group
Notifyview	The notify MIB view associated with the SNMP group, the view with entries that can generate traps
Storage-type	Storage type, which includes: volatile, nonVolatile, permanent, readOnly, and other. For detailed information, refer to <a href="#">Table 1-1</a> .

## display snmp-agent local-engineid

### Syntax

```
display snmp-agent local-engineid
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display snmp-agent local-engineid** command to display the local SNMP agent engine ID.

SNMP engine ID identifies an SNMP entity uniquely within an SNMP domain. SNMP engine is an indispensable part of an SNMP entity. It provides the SNMP message allocation, message handling, authentication, and access control.

### Examples

# Display the local SNMP agent engine ID.

```

<Sysname> display snmp-agent local-engineid
SNMP local EngineID: 800007DB7F0000013859

```

## display snmp-agent mib-view

### Syntax

```
display snmp-agent mib-view [ exclude | include | viewname view-name ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**exclude:** Displays MIB view information of the **excluded** type.

**include:** Displays MIB view information of the **included** type.

**viewname *view-name*:** Displays MIB view information with a specified MIB view name, where *view-name* is the name of the specified MIB view.

### Description

Use the **display snmp-agent mib-view** command to display MIB view information. Absence of parameters indicates that information for all MIB views will be displayed.

### Examples

# Display all SNMP MIB views of the device.

```
<Sysname> display snmp-agent mib-view
```

```
View name:ViewDefault
  MIB Subtree:iso
  Subtree mask:
  Storage-type: nonVolatile
  View Type:included
  View status:active
```

```
View name:ViewDefault
  MIB Subtree:snmpUsmMIB
  Subtree mask:
  Storage-type: nonVolatile
  View Type:excluded
  View status:active
```

```
View name:ViewDefault
  MIB Subtree:snmpVacmMIB
  Subtree mask:
  Storage-type: nonVolatile
  View Type:excluded
  View status:active
```

```
View name:ViewDefault
  MIB Subtree:snmpModules.18
```

```

Subtree mask:
Storage-type: nonVolatile
View Type:excluded
View status:active

```

ViewDefault is the default view of the device. When you access the device through the ViewDefault view, you can access all the MIB objects of the iso subtree except for the MIB objects under the snmpUsmMIB, snmpVacmMIB, and snmpModules.18 subtrees.

**Table 1-3 display snmp-agent mib-view** command output description

Field	Description
View name	MIB view name
MIB Subtree	MIB subtree corresponding to the MIB view
Subtree mask	MIB subtree mask
Storage-type	Storage type
View Type	View type, which can be <b>included</b> or <b>excluded</b> : <ul style="list-style-type: none"> <li>• Included indicates that all nodes of the MIB tree are included in current view, namely, you are allowed to access all the MIB objects of the subtree</li> <li>• Excluded indicates that none of the nodes of the MIB tree are included in current view, namely, you are allowed to access none of the MIB objects of the subtree</li> </ul>
View status	The status of MIB view

## display snmp-agent statistics

### Syntax

```
display snmp-agent statistics
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display snmp-agent statistics** command to display SNMP statistics.

### Examples

```
# Display the statistics on the current SNMP.
```

```

<Sysname> display snmp-agent statistics
1684 Messages delivered to the SNMP entity
5 Messages which were for an unsupported version
0 Messages which used a SNMP community name not known

```

```

0 Messages which represented an illegal operation for the community supplied
0 ASN.1 or BER errors in the process of decoding
1679 Messages passed from the SNMP entity
0 SNMP PDUs which had badValue error-status
0 SNMP PDUs which had genErr error-status
0 SNMP PDUs which had noSuchName error-status
0 SNMP PDUs which had tooBig error-status (Maximum packet size 1500)
16544 MIB objects retrieved successfully
2 MIB objects altered successfully
7 GetRequest-PDU accepted and processed
7 GetNextRequest-PDU accepted and processed
1653 GetBulkRequest-PDU accepted and processed
1669 GetResponse-PDU accepted and processed
2 SetRequest-PDU accepted and processed
0 Trap PDUs accepted and processed
0 Alternate Response Class PDUs dropped silently
0 Forwarded Confirmed Class PDUs dropped silently

```

**Table 1-4** display snmp-agent statistics command output description

Field	Description
Messages delivered to the SNMP entity	Number of packets delivered to the SNMP agent
Messages which were for an unsupported version	Number of packets from a device with an SNMP version that is not supported by the current SNMP agent
Messages which used a SNMP community name not known	Number of packets that use an unknown community name
Messages which represented an illegal operation for the community supplied	Number of packets carrying an operation that the community has no right to perform
ASN.1 or BER errors in the process of decoding	Number of packets with ASN.1 or BER errors in the process of decoding
Messages passed from the SNMP entity	Number of packets sent by the SNMP agent
SNMP PDUs which had badValue error-status	Number of SNMP PDUs with a badValue error
SNMP PDUs which had genErr error-status	Number of SNMP PDUs with a genErr error
SNMP PDUs which had noSuchName error-status	Number of PDUs with a noSuchName error
SNMP PDUs which had tooBig error-status (Maximum packet size 1500)	Number of PDUs with a tooBig error (the maximum packet size is 1,500 bytes)
MIB objects retrieved successfully	Number of MIB objects that have been successfully retrieved
MIB objects altered successfully	Number of MIB objects that have been successfully modified
GetRequest-PDU accepted and processed	Number of get requests that have been received and processed
GetNextRequest-PDU accepted and processed	Number of getNext requests that have been received and processed
GetBulkRequest-PDU accepted and processed	Number of getBulk requests that have been received and processed

Field	Description
GetResponse-PDU accepted and processed	Number of get responses that have been received and processed
SetRequest-PDU accepted and processed	Number of set requests that have been received and processed
Trap PDUs accepted and processed	Number of traps that have been received and processed
Alternate Response Class PDUs dropped silently	Number of dropped response packets
Forwarded Confirmed Class PDUs dropped silently	Number of forwarded packets that have been dropped

## display snmp-agent sys-info

### Syntax

```
display snmp-agent sys-info [ contact | location | version ] *
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**contact:** Displays the contact information of the current network administrator.

**location:** Displays the location information of the current device.

**version:** Displays the version of the current SNMP agent.

### Description

Use the **display snmp-agent sys-info** command to display the current SNMP system information.

If no keyword is specified, all SNMP agent system information will be displayed.

### Examples

# Display the current SNMP agent system information.

```
<Sysname> display snmp-agent sys-info
  The contact person for this managed node:
    3Com Corporation.

  The physical location of this node:
    Marlborough, MA 01752 USA

  SNMP version running in the system:
    SNMPv3
```

## display snmp-agent trap queue

### Syntax

display snmp-agent trap queue

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display snmp-agent trap queue** command to display basic information of the trap queue, including trap queue name, queue length and the number of traps in the queue currently.

Related commands: **snmp-agent trap life**, **snmp-agent trap queue-size**.

### Examples

# Display the current configuration and usage of the trap queue.

```
<Sysname> display snmp-agent trap queue
  Queue name: SNTP
  Queue size: 100
  Message number: 6
```

**Table 1-5** display snmp-agent trap queue command output description

Field	Description
Queue name	Trap queue name
Queue size	Trap queue size
Message number	Number of traps in the current trap queue

## display snmp-agent trap-list

### Syntax

display snmp-agent trap-list

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

## Description

Use the **display snmp-agent trap-list** command to display the modules that can generate traps and whether their trap function is enabled or not. If a module comprises multiple sub-modules, then as long as one sub-module has the trap function enabled, the whole module will be displayed as being enabled with the trap function.

Related commands: **snmp-agent trap enable**.

## Examples

# Display the modules that can generate traps and whether their trap function is enabled or not.

```
<Sysname> display snmp-agent trap-list
bfd trap enable
bgp trap enable
configuration trap enable
flash trap enable
ospf trap enable
standard trap enable
system trap enable
vrrp trap enable
Enable traps: 8; Disable traps: 0
```

In the above output, enable indicates that the module is allowed to generate traps whereas disable indicates the module is not allowed to generate traps. You can configure the trap function (enable or disable) of each module through command lines.

## display snmp-agent usm-user

### Syntax

```
display snmp-agent usm-user [ engineid engineid | username user-name | group group-name ] *
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**engineid** *engineid*: Displays SNMPv3 user information for a specified engine ID, where *engineid* indicates the SNMP engine ID.

**username** *user-name*: Displays SNMPv3 user information for a specified user name. It is case sensitive.

**group** *group-name*: Displays SNMPv3 user information for a specified SNMP group name. It is case sensitive.

## Description

Use the **display snmp-agent usm-user** command to display SNMPv3 user information.

## Examples

# Display SNMPv3 information of all created users.

```
<Sysname> display snmp-agent usm-user
  User name: userv3
  Group name: mygroupv3
    Engine ID: 800063A203000FE240A1A6
    Storage-type: nonVolatile
    UserStatus: active

  User name: userv3code
  Group name: groupv3code
    Engine ID: 800063A203000FE240A1A6
    Storage-type: nonVolatile
    UserStatus: active
```

**Table 1-6 display snmp-agent usm-user command output description**

Field	Description
User name	SNMP user name
Group name	SNMP group name
Engine ID	Engine ID for an SNMP entity
Storage-type	Storage type, which can be the following: <ul style="list-style-type: none"><li>• volatile</li><li>• nonvolatile</li><li>• permanent</li><li>• readOnly</li><li>• other</li></ul> See <a href="#">Table 1-1</a> for details.
UserStatus	SNMP user status

## enable snmp trap updown

### Syntax

```
enable snmp trap updown
undo enable snmp trap updown
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

## Description

Use the **enable snmp trap updown** command to enable the trap function for interface state changes.

Use the **undo enable snmp trap updown** command to disable the trap function for interface state changes.

By default, the trap function for interface state changes is enabled.

Note that:

To enable an interface to generate linkUp/linkDown traps when its state changes, you need to enable the linkUp/linkDown trap function on the interface and globally. Use the **enable snmp trap updown** command to enable this function on an interface, and use the **snmp-agent trap enable [ standard [ linkdown | linkup ] \* ]** command to enable this function globally.

Related commands: **snmp-agent target-host**, **snmp-agent trap enable**.

## Examples

# Enable the sending of linkUp/linkDown SNMP traps on port GigabitEthernet 1/0/1 and use the community name **public**.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] enable snmp trap updown
```

## snmp-agent

### Syntax

```
snmp-agent
undo snmp-agent
```

### View

System view

### Default Level

3: Manage level

### Parameters

None

### Description

Use the **snmp-agent** command to enable SNMP agent.

Use the **undo snmp-agent** command to disable SNMP agent.

By default, SNMP agent is disabled.

You can enable SNMP agent through any commands that begin with **snmp-agent**.

### Examples

# Enable SNMP agent on the device.

```
<Sysname> system-view
```

```
[Sysname] snmp-agent
```

## snmp-agent calculate-password

### Syntax

```
snmp-agent calculate-password plain-password mode { 3desmd5 | 3dessa | md5 | sha }  
{ local-engineid | specified-engineid engineid }
```

### View

System view

### Default Level

3: Manage level

### Parameters

*plain-password*: Plain text password to be encrypted, a string of 1 to 64 characters.

**mode**: Specifies the encryption algorithm and authentication algorithm. The three encryption algorithms Advanced Encryption Standard (AES), triple data encryption standard (3DES), and Data Encryption Standard (DES) are in descending order in terms of security. Higher security means more complex implementation mechanism and lower speed. DES is enough to meet general requirements. Message-Digest Algorithm 5 (MD5) and Secure Hash Algorithm (SHA-1) are the two authentication algorithms. MD5 is faster than SHA-1, while SHA-1 provides higher security than MD5.

- **3desmd5**: Converts a plain text encryption password to a cipher text encryption password. In this case, the authentication protocol must be MD5, and the encryption algorithm must be 3DES.
- **3dessa**: Converts a plain text encryption password to a cipher text encryption password. In this case, the authentication protocol must be SHA-1, and the encryption algorithm must be 3DES.
- **md5**: Converts a plain text authentication password to a cipher text authentication password. In this case, the authentication protocol must be MD5. Or, this algorithm can convert the plain text encryption password to a cipher text encryption password, In this case, the authentication protocol must be MD5, and the encryption algorithm can be either AES or DES (when the authentication protocol is specified as MD5, cipher text passwords are the same by using the encryption algorithms AES and DES).
- **sha**: Converts the plain text authentication password to a cipher text authentication password. In this case, the authentication protocol must be SHA-1. Or, this algorithm can convert the plain text encryption password to a cipher text encryption password, In this case, the authentication protocol must be SHA-1, and the encryption algorithm can be either AES or DES (when the authentication protocol is specified as SHA-1, cipher text passwords are the same by using the encryption algorithms AES and DES).

**local-engineid**: Uses local engine ID to calculate cipher text password. For engine ID-related configuration, refer to the **snmp-agent local-engineid** command.

**specified-engineid**: Uses user-defined engine ID to calculate cipher text password.

*engineid*: The engine ID string, an even number of hexadecimal characters, in the range 10 to 64. Its length must not be an odd number, and the all-zero and all-F strings are invalid.

## Description

Use the **snmp-agent calculate-password** command to convert the user-defined plain text password to a cipher text password.

Note that:

- The cipher text password converted with the **sha** keyword specified in this command is a string of 40 hexadecimal characters. For an authentication password, all of the 40 hexadecimal characters are valid; while for a privacy password, only the first 32 hexadecimal characters are valid.
- Enable SNMP on the device before executing the command.

When creating an SNMPv3 user, if you specify to use the cipher text authentication/encryption password, you can use this command to generate a cipher text password.

The converted password is associated with the engine ID, namely, the password is valid only under the specified engine ID based on which the password was configured.

Related commands: `snmp-agent usm-user v3`.

## Examples

```
# Use local engine ID and MD5 authentication protocol to convert the plain text password authkey.
```

```
<Sysname> system-view
[Sysname] snmp-agent calculate-password authkey mode md5 local-engineid
The secret key is: 09659EC5A9AE91BA189E5845E1DDE0CC
```

## snmp-agent community

### Syntax

```
snmp-agent community { read | write } community-name [ acl acl-number | mib-view view-name ] *
undo snmp-agent community { read | write } community-name
```

### View

System view

### Default Level

3: Manage level

### Parameters

**read**: Indicates that the community has read only access right to the MIB objects; that is, the NMS can perform read-only operations when it uses this community name to access the agent.

**write**: Indicates that the community has read and write access right to the MIB objects; that is, the NMS can perform read and write operations when it uses this community name to access the agent.

*community-name*: Community name, a string of 1 to 32 characters.

**acl** *acl-number*: Associates a basic ACL with the community name. *acl-number* is in the range 2,000 to 2,999. By using an ACL, you can configure to allow or prohibit the access to the agent from the NMS with the specified source IP address.

**mib-view** *view-name*: Specifies the MIB view name associated with *community-name*, where *view-name* represents the MIB view name, a string of 1 to 32 characters. If no keyword is specified, the default view is ViewDefault (The view created by the system after SNMP agent is enabled).

## Description

Use the **snmp-agent community** command to create a new SNMP community. Parameters to be configured include access right, community name, ACL, and accessible MIB views.

Use the **undo snmp-agent community** command to delete a specified community.

The community name configured with this command is only valid for the SNMP v1 and v2c agent.

A community is composed of NMSs and SNMP agents, and is identified by the community name, which functions as a password. In a community, when devices communicate with each other, they use community name for authentication. The NMS and the SNMP agent can access each other only when they are configured with the same community name. Typically, **public** is used as the read-only community name, and **private** is used as the read and write community name. For security purposes, you are recommended to configure a community name other than **public** and **private**.

- The keyword **acl** specifies that only the NMS with a qualified IP address can access the agent.
- The argument *community-name* specifies the community name used by the NMS when it accesses the agent.
- The keyword **mib-view** specifies the MIB objects which the NMS can access.
- The keywords **read** and **write** specify the access type.

Related commands: **snmp-agent mib-view**.

## Examples

# Create a community with the name of **readaccess**, allowing read-only access right using this community name.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v1 v2c
[Sysname] snmp-agent community read readaccess
```

- Set the SNMP version on the NMS to SNMPv1 or SNMPv2c
- Fill in the read-only community name **readaccess**
- Establish a connection, and the NMS can perform read-only operations to the MIB objects in the ViewDefault view on the device

# Create a community with the name of **writeaccess**, allowing only the NMS with the IP address of 1.1.1.1 to configure the values of the agent MIB objects by using this community name; other NMSs are not allowed to perform the write operations by using this community name.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[Sysname-acl-basic-2001] rule deny source any
[Sysname-acl-basic-2001] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent community write writeaccess acl 2001
```

- Set the IP address of the NMS to 1.1.1.1
- Set the SNMP version on the NMS to SNMPv2c
- Fill in the write community name **writeaccess**; namely, the NMS can perform read-only operations to the MIB objects in the ViewDefault view on the device

# Create a community with the name of **wr-sys-acc**. The NMS can perform the read and write operations to the MIB objects of the system subtree (with the OID of 1.3.6.1.2.1.1).

```
<Sysname> system-view
```

```
[Sysname] snmp-agent sys-info version v1 v2c
[Sysname] snmp-agent mib-view included test system
[Sysname] snmp-agent community write wr-sys-acc mib-view system
```

- Set the SNMP version on the NMS to SNMPv1 or SNMPv2c
- Fill in the write community name **wr-sys-acc**
- Establish a connection, and the NMS can perform read and write operations to the MIB objects in system view on the device

## snmp-agent group

### Syntax

The following syntax applies to SNMPv1 and SNMP v2c:

```
snmp-agent group { v1 | v2c } group-name [ read-view read-view ] [ write-view write-view ]
[ notify-view notify-view ] [ acl acl-number ]
```

```
undo snmp-agent group { v1 | v2c } group-name
```

The following syntax applies to SNMPv3:

```
snmp-agent group v3 group-name [ authentication | privacy ] [ read-view read-view ] [ write-view
write-view ] [ notify-view notify-view ] [ acl acl-number ]
```

```
undo snmp-agent group v3 group-name [ authentication | privacy ]
```

### View

System view

### Default Level

3: Manage level

### Parameters

**v1**: SNMPv1.

**v2c**: SNMPv2c.

**v3**: SNMPv3.

*group-name*: Group name, a string of 1 to 32 characters.

**authentication**: Specifies the security model of the SNMP group to be authentication only (without privacy).

**privacy**: Specifies the security model of the SNMP group to be authentication and privacy.

**read-view** *read-view*: Read view, a string of 1 to 32 characters. The default read view is ViewDefault.

**write-view** *write-view*: Write view, a string of 1 to 32 characters. By default, no write view is configured, namely, the NMS cannot perform the write operations to all MIB objects on the device.

**notify-view** *notify-view*: Notify view, for sending traps, a string of 1 to 32 characters. By default, no notify view is configured, namely, the agent does not send traps to the NMS.

**acl** *acl-number*: Associates a basic ACL with the group. *acl-number* is in the range 2000 to 2999. By using a basic ACL, you can restrict the source IP address of SNMP packets, that is, you can configure to allow or prohibit SNMP packets with a specific source IP address, so as to restrict the intercommunication between the NMS and the agent.

## Description

Use the **snmp-agent group** command to configure a new SNMP group and specify its access right.

Use the **undo snmp-agent group** command to delete a specified SNMP group.

By default, SNMP groups configured by the **snmp-agent group v3** command use a no-authentication-no-privacy security model.

An SNMP group defines security model, access right, and so on. A user in this SNMP group has all these public properties.

Related commands: **snmp-agent mib-view**, **snmp-agent usm-user**.

## Examples

```
# Create an SNMP group group1 on an SNMPv3 enabled device, no authentication, no privacy.
```

```
<Sysname> system-view  
[Sysname] snmp-agent group v3 group1
```

## snmp-agent local-engineid

### Syntax

```
snmp-agent local-engineid engineid
```

```
undo snmp-agent local-engineid
```

### View

System view

### Default Level

3: Manage level

### Parameters

*engineid*: Engine ID, an even number of hexadecimal characters, in the range 10 to 64. Its length must not be an odd number, and the all-zero and all-F strings are invalid.

## Description

Use the **snmp-agent local-engineid** command to configure a local engine ID for an SNMP entity.

Use the **undo snmp-agent local-engineid** command to restore the default local engine ID.

By default, the engine ID of a device is the combination of company ID and device ID. Device ID varies by product; it could be an IP address, a MAC address, or a self-defined string of hexadecimal numbers.

An engine ID has two functions:

- For all devices managed by one NMS, each device needs a unique engine ID to identify the SNMP agent. By default, each device has an engine ID. The network administrator has to ensure that there is no repeated engine ID within an SNMP domain.
- In SNMPv3, the user name and cipher text password are associated with the engine ID. Therefore, if the engine ID changes, the user name and cipher text password configured under the engine ID become invalid.

Typically, the device uses its default engine ID. For ease of remembrance, you can set engine IDs for the devices according to the network planning. For example, if both device 1 and device 2 are on the

first floor of building A, you can set the engine ID of device 1 to 000Af0010001, and that of device 2 to 000Af0010002.

Related commands: **snmp-agent usm-user**.

## Examples

```
# Configure the local engine ID as 123456789A.
<Sysname> system-view
[Sysname] snmp-agent local-engineid 123456789A
```

## snmp-agent log

### Syntax

```
snmp-agent log { all | get-operation | set-operation }
undo snmp-agent log { all | get-operation | set-operation }
```

### View

System view

### Default Level

3: Manage level

### Parameters

**all**: Enables logging of SNMP GET and SET operations.  
**get-operation**: Enables logging of SNMP GET operation.  
**set-operation**: Enables logging of SNMP SET operation.

### Description

Use the **snmp-agent log** command to enable SNMP logging.

Use the **undo snmp-agent log** command to restore the default.

By default, SNMP logging is disabled.

If specified SNMP logging is enabled, when the NMS performs a specified operation to the SNMP agent, the latter records the operation-related information and saves it to the information center. With parameters for the information center set, output rules of the SNMP logs are decided (that is, whether logs are permitted to output and the output destinations).

## Examples

```
# Enable logging of SNMP GET operation.
<Sysname> system-view
[Sysname] snmp-agent log get-operation

# Enable logging of SNMP SET operation.
<Sysname> system-view
[Sysname] snmp-agent log set-operation
```

## snmp-agent mib-view

### Syntax

```
snmp-agent mib-view { excluded | included } view-name oid-tree [ mask mask-value ]
undo snmp-agent mib-view view-name
```

### View

System view

### Default Level

3: Manage level

### Parameters

**excluded**: Indicates that no nodes of the MIB tree are included in current view.

**included**: Indicates that all nodes of the MIB tree are included in current view.

*view-name*: View name, a string of 1 to 32 characters.

*oid-tree*: MIB subtree, identified by the OID of the subtree root node, such as 1.4.5.3.1, or the name of the subtree root node, such as "system". OID is made up of a series of integers, which marks the position of the node in the MIB tree and uniquely identifies a MIB object.

**mask mask-value**: Mask for a MIB subtree, in the range 1 to 32 hexadecimal digits. It must be an even digit.

### Description

Use the **snmp-agent mib-view** command to create or update MIB view information so that MIB objects can be specified.

Use the **undo snmp-agent mib-view** command to delete the current configuration.

By default, MIB view name is ViewDefault.

MIB view is a subset of MIB, and it may include all nodes of a MIB subtree (that is, the access to all nodes of this MIB subtree is permitted), or may exclude all nodes of a MIB subtree (that is, the access to all nodes of this MIB subtree is forbidden).

You can use the **display snmp-agent mib-view** command to view the access right of the default view. Also, you can use the **undo snmp-agent mib-view** command to remove the default view, after that, however, you may not be able to read or write all MIB nodes on the agent.

Related commands: **snmp-agent group**.

### Examples

# Create a MIB view **mibtest**, which includes all objects of the subtree **mib-2**, and excludes all objects of the subtree **ip**.

```
<Sysname> system-view
[Sysname] snmp-agent mib-view included mibtest 1.3.6.1
[Sysname] snmp-agent mib-view excluded mibtest ip
[Sysname] snmp-agent community read public mib-view mibtest
```

If the SNMP version on the NMS is set to SNMPv1, when the NMS uses the community name **public** to access the device, it cannot access all objects of the **ip** subtree (such as the ipForwarding node, the ipDefaultTTL node, and so on), but it can access all objects of the **mib-2** subtree.

## snmp-agent packet max-size

### Syntax

```
snmp-agent packet max-size byte-count  
undo snmp-agent packet max-size
```

### View

System view

### Default Level

3: Manage level

### Parameters

*byte-count*: Maximum size of the SNMP packets that can be received or sent by the agent, in the range 484 to 17,940.

### Description

Use the **snmp-agent packet max-size** command to configure the maximum size of the SNMP packets that can be received or sent by the agent.

Use the **undo snmp-agent packet max-size** command to restore the default packet size.

By default, the maximum size of the SNMP packets that can be received or sent by the agent is 1,500 bytes.

If devices not supporting fragmentation exist on the routing path between the NMS and the agent, you can use the command to configure the maximum SNMP packet size, and thus to prevent giant packets from being discarded.

Typically, you are recommended to apply the default value.

### Examples

# Configure the maximum size of the SNMP packets that can be received or sent by the SNMP agent as 1,042 bytes.

```
<Sysname> system-view  
[Sysname] snmp-agent packet max-size 1042
```

## snmp-agent sys-info

### Syntax

```
snmp-agent sys-info { contact sys-contact | location sys-location | version { all | { v1 | v2c | v3 }* } }  
undo snmp-agent sys-info { contact | location | version { all | { v1 | v2c | v3 }* } }
```

### View

System view

## Default Level

3: Manage level

## Parameters

**contact** *sys-contact*: A string of 1 to 200 characters that describes the contact information for system maintenance.

**location** *sys-location*: A string of 1 to 200 characters that describes the location of the device.

**version**: The SNMP version in use.

- **all**: Specifies SNMPv1, SNMPv2c, and SNMPv3.
- **v1**: SNMPv1.
- **v2c**: SNMPv2c.
- **v3**: SNMPv3.

## Description

Use the **snmp-agent sys-info** command to configure system information, including the contact information, the location, and the SNMP version in use.

Use the **undo snmp-agent sys-info contact** and **undo snmp-agent sys-info location** command to restore the default.

Use the **undo snmp-agent sys-info version** command to disable use of the SNMP function of the specified version.

By default, the location information is Marlborough, MA 01752 USA, version is SNMPv3, and the contact is 3Com Corporation.

The device can process the SNMP packets of the corresponding version only if SNMP of a specific version is enabled. If SNMPv1 is enabled, the device will drop the received SNMPv2c packets; if SNMPv2c is enabled, the device will drop the received SNMPv1 packets. To enable the device to communicate with different NMSs, you can enable SNMP of different versions on a device.

Related commands: **display snmp-agent sys-info**.



### Note

Network maintenance engineers can use the system contact information to get in touch with the manufacturer in case of network failures. The system location information is a management variable under the system branch as defined in RFC1213-MIB, identifying the location of the managed object.

---

## Examples

# Configure the contact information as "Dial System Operator at beeper # 27345".

```
<Sysname> system-view
```

```
[Sysname] snmp-agent sys-info contact Dial System Operator at beeper # 27345
```

## snmp-agent target-host

### Syntax

```
snmp-agent target-host trap address udp-domain { ip-address | ipv6 ipv6-address } [ udp-port port-number ] [ vpn-instance vpn-instance-name ] params securityname security-string [ v1 | v2c | v3 [ authentication | privacy ] ]
```

```
undo snmp-agent target-host trap address udp-domain { ip-address | ipv6 ipv6-address } params securityname security-string [ vpn-instance vpn-instance-name ]
```

### View

System view

### Default Level

3: Manage level

### Parameters

**trap**: Specifies the host to be the target host which will receive traps and notifications from the device.

**address**: Specifies the destination IP address in the SNMP messages sent from the device.

**udp-domain**: Indicates that the trap is transmitted using UDP.

*ip-address*: The IPv4 address of the trap target host.

**ipv6** *ipv6-address*: Specifies the IPv6 address of the trap target host.

**udp-port** *port-number*: Specifies the number of the port on the target host to receive traps.

**vpn-instance** *vpn-instance-name*: Specifies the VPN where the target host resides, where *vpn-instance-name* indicates the VPN instance name and is a string of 1 to 31 characters. It is case sensitive and is applicable only in a network supporting IPv4. If you execute the command with this keyword and argument combination, you need to add the agent into this VPN domain, and ensure that the route between the agent and the NMS is available.

**params securityname** *security-string*: Specifies the authentication related parameter, which is an SNMPv1 or SNMPv2c community name or an SNMPv3 user name, a string of 1 to 32 characters.

**v1**: SNMPv1.

**v2c**: SNMPv2c.

**v3**: SNMPv3.

- **authentication**: Specifies the security model to be authentication without privacy. Authentication is a process to check whether the packet is integral and whether it has been tampered. You need to configure the authentication password when creating an SNMPv3 user.
- **privacy**: Specifies the security model to be authentication with privacy. Privacy is to encrypt the data part of a packet to prevent it from being intercepted. You need to configure the authentication password and privacy password when creating an SNMPv3 user.

### Description

Use the **snmp-agent target-host** command to configure the related settings for a trap target host.

Use the **undo snmp-agent target-host** command to remove the current settings. According to the networking requirements, you can use this command for multiple times to configure different settings for a target host, enabling the device to send trap messages to different NMSs.

- If **udp-port** *port-number* is not specified, port number 162 is used.
- If the key words **v1**, **v2** and **v3** are not specified, v1 is used.
- If the key words **authentication** and **privacy** are not specified, the authentication mode is no authentication, no privacy.

Related commands: enable snmp trap updown, snmp-agent trap enable, snmp-agent trap source, snmp-agent trap life.

## Examples

# Enable the device to send SNMP traps to 10.1.1.1, using the community name of **public**.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable standard
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public
```

# Enable the device to send SNMP traps to the device which is in VPN 1 and has an IP address of 10.1.1.1, using the community name of **public**.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable standard
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 vpn-instance vpn1 params securityname public
```

## snmp-agent trap enable

### Syntax

**snmp-agent trap enable** [ **bfd** | **bgp** | **configuration** | **flash** | **ospf** [ *process-id* ] [ **ifauthfail** | **ifcfgerror** | **ifrxbadpkt** | **ifstatechange** | **iftxretransmit** | **lsdbapproachoverflow** | **lsdboverflow** | **maxagelsa** | **nbrstatechange** | **originatelsa** | **vifcfgerror** | **virifauthfail** | **virifrxbadpkt** | **virifstatechange** | **viriftxretransmit** | **virnbrstatechange** ]\* | **standard** [ **authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart** ]\* | **system** | **vrp** [ **authfailure** | **newmaster** ] ]

**undo snmp-agent trap enable** [ **bfd** | **bgp** | **configuration** | **flash** | **ospf** [ *process-id* ] [ **ifauthfail** | **ifcfgerror** | **ifrxbadpkt** | **ifstatechange** | **iftxretransmit** | **lsdbapproachoverflow** | **lsdboverflow** | **maxagelsa** | **nbrstatechange** | **originatelsa** | **vifcfgerror** | **virifauthfail** | **virifrxbadpkt** | **virifstatechange** | **viriftxretransmit** | **virnbrstatechange** ]\* | **standard** [ **authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart** ]\* | **system** | **vrp** [ **authfailure** | **newmaster** ] ]

### View

System view

### Default Level

3: Manage level

### Parameters

**bfd**: Enables the sending of traps of the BFD module.

**bgp**: Enables the sending of traps of the BGP module.

**configuration**: Enables the sending of configuration traps.

**flash**: Enables the sending of FLASH-related traps.

**ospf**: Enables the sending of traps of the OSPF module.

- *process-id*: OSPF process ID, in the range 1 to 65535.
- **ifauthfail**: Traps for interface authentication failure.
- **ifcfgerror**: Traps for interface configuration error.
- **ifrxbadpkt**: Traps for receiving incorrect packets.
- **ifstatechange**: Traps for interface state change.
- **iftxretransmit**: Traps for the interface to receive and forward packets.
- **lsdbapproachoverflow**: Traps for LSDB to be overflowed.
- **lsdboverflow**: Traps for LSDB overflow.
- **maxagelsa**: Traps for LSA max age.
- **nbrstatechange**: Traps for neighbor state change.
- **originatelsa**: Traps for local LSA generation.
- **vifcfgerror**: Traps for virtual interface configuration error.
- **virifauthfail**: Traps for virtual interface authentication failure.
- **virifrxbadpkt**: Traps for virtual interface receiving error packets.
- **virifstatechange**: Traps for virtual interface state changes.
- **viriftxretransmit**: Traps for virtual interface receiving and forwarding packets.
- **virnbrstatechange**: Traps for neighbor state change of the virtual interface.

**standard**: Standard traps.

- **authentication**: Enables the sending of authentication failure traps in the event of authentication failure.
- **coldstart**: Sends coldstart traps when the device restarts.
- **linkdown**: Sends linkdown traps when the port is in a linkdown status. It should be configured globally.
- **linkup**: Sends linkup traps when the port is in a linkup status. It should be configured globally.
- **warmstart**: Sends warmstart traps when the SNMP restarts.

**system**: Sends 3Com-SYS-MAN-MIB (a private MIB) traps.

**vrrp**: Traps of the VRRP module.

- **authfailure**: Traps for VRRP authentication failure.
- **newmaster**: Enables the sending of VRRP newmaster traps when the device becomes the master.

## Description

Use the **snmp-agent trap enable** command to enable the trap function globally.

Use the **undo snmp-agent trap enable** command to disable the trap function globally.

By default, the trap function of other modules is enabled.

Only after the trap function is enabled can each module generate corresponding traps.

Note that:

To enable an interface to generate Linkup/Linkdown traps when its state changes, you need to enable the linkUp/linkDown trap function on the interface and globally. Use the **enable snmp trap updown** command to enable this function on an interface, and use the **snmp-agent trap enable [ standard [ linkdown | linkup ] \* ]** command to enable this function globally.

Related commands: **snmp-agent target-host**, **enable snmp trap updown**.

## Examples

```
# Enable the device to send SNMP authentication failure packets to 10.1.1.1, using the community name public.
```

```
<Sysname> system-view
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public
[Sysname] snmp-agent trap enable standard authentication
```

## snmp-agent trap if-mib link extended

### Syntax

**snmp-agent trap if-mib link extended**

**undo snmp-agent trap if-mib link extended**

### View

System view

### Default Level

3: Manage level

### Parameters

None

### Description

Use the **snmp-agent trap if-mib link extended** command to extend the standard linkUp/linkDown traps defined in RFC. An extended linkUp/linkDown trap is the standard linkUp/linkDown trap defined in RFC appended with the interface description and interface type information.

Use the **undo snmp-agent trap if-mib link extended** command to restore the default.

By default, standard linkUp/linkDown traps defined in RFC are used.

- A standard linkUp trap is in the following format:

```
#Apr 24 11:48:04:896 2008 Sysname IFNET/4/INTERFACE UPDOWN:
```

```
Trap 1.3.6.1.6.3.1.1.5.4<linkUp>: Interface 983555 is Up, ifAdminStatus is 1, ifOperStatus is 1
```

- An extended linkUp trap is in the following format:

```
#Apr 24 11:43:09:896 2008 Sysname IFNET/4/INTERFACE UPDOWN:
```

```
Trap 1.3.6.1.6.3.1.1.5.4<linkUp>: Interface 983555 is Up, ifAdminStatus is 1, ifOperStatus is 1, ifDescr is GigabitEthernet1/0/1, ifType is 6
```

- A standard linkDown trap is in the following format:

```
#Apr 24 11:47:35:224 2008 Sysname IFNET/4/INTERFACE UPDOWN:
```

```
Trap 1.3.6.1.6.3.1.1.5.3<linkDown>: Interface 983555 is Down, ifAdminStatus is 2, ifOperStatus is 2
```

- An extended linkDown trap is in the following format:

```
#Apr 24 11:42:54:314 2008 AR29.46 IFNET/4/INTERFACE UPDOWN:
```

```
Trap 1.3.6.1.6.3.1.1.5.3<linkDown>: Interface 983555 is Down, ifAdminStatus is 2, ifOperStatus is 2, ifDescr is GigabitEthernet1/0/1, ifType is 6
```

The format of an extended linkup/ linkDown trap is the standard format followed with the ifDescr and ifType information, facilitating problem location.

Note that after this command is configured, the device sends extended linkUp/linkDown traps. If the extended messages are not supported on NMS, the device may not be able to resolve the messages.

## Examples

```
# Extend standard linkUp/linkDown traps defined in RFC.
<Sysname> system-view
[Sysname] snmp-agent trap if-mib link extended
```

## snmp-agent trap life

### Syntax

```
snmp-agent trap life seconds
undo snmp-agent trap life
```

### View

System view

### Default Level

3: Manage level

### Parameters

*seconds*: Timeout time, in the range 1 to 2,592,000 seconds.

### Description

Use the **snmp-agent trap life** command to configure the holding time of the traps in the queue. Traps will be discarded when the holding time expires.

Use the **undo snmp-agent trap life** command to restore the default holding time of traps in the queue. By default, the holding time of SNMP traps in the queue is 120 seconds.

The SNMP module sends traps in queues. As soon as the traps are saved in the trap queue, a timer is started. If traps are not sent out until the timer times out (namely, the holding time configured by using this command expires), the system removes the traps from the trap sending queue.

Related commands: snmp-agent trap enable, snmp-agent target-host.

## Examples

```
# Configure the holding time of traps in the queue as 60 seconds.
<Sysname> system-view
[Sysname] snmp-agent trap life 60
```

## snmp-agent trap queue-size

### Syntax

```
snmp-agent trap queue-size size
undo snmp-agent trap queue-size
```

### View

System view

## Default Level

3: Manage level

## Parameters

**size**: Number of traps that can be stored in the trap sending queue, in the range 1 to 1,000.

## Description

Use the **snmp-agent trap queue-size** command to set the size of the trap sending queue.

Use the **undo snmp-agent trap queue-size** command to restore the default queue size.

By default, up to 100 traps can be stored in the trap sending queue.

After traps are generated, they will be saved into the trap sending queue. The size of the queue determines the maximum number of the traps that can be stored in the queue. When the size of the trap sending queue reaches the configured value, the newly generated traps are saved into the queue, and the earliest ones are discarded.

Related commands: snmp-agent trap enable, snmp-agent target-host, snmp-agent trap life.

## Examples

```
# Set the maximum number of traps that can be stored in the trap sending queue to 200.
```

```
<Sysname> system-view  
[Sysname] snmp-agent trap queue-size 200
```

## snmp-agent trap source

### Syntax

```
snmp-agent trap source interface-type interface-number
```

```
undo snmp-agent trap source
```

### View

System view

## Default Level

3: Manage level

## Parameters

*interface-type interface-number*: Specifies the interface type and interface number.

## Description

Use the **snmp-agent trap source** command to specify the source IP address contained in the trap.

Use the **undo snmp-agent trap source** command to restore the default.

By default, SNMP chooses the IP address of an interface to be the source IP address of the trap.

Upon the execution of this command, the system uses the primary IP address of the specified interface as the source IP address of the traps, and the NMS will use this IP address to uniquely identify the agent. Even if the agent sends out traps through different interfaces, the NMS uses this IP address to filter all traps sent from the agent.

Use this command to trace a specific event by the source IP address of a trap.

Note that:

Before you can configure the IP address of a particular interface as the source IP address of the trap, ensure that the interface already exists and that it has a legal IP address. Otherwise, if the configured interface does not exist, the configurations will fail; if the specified IP address is illegal, the configuration will be invalid. After a legal IP address is configured for the interface, the configuration becomes valid automatically.

Related commands: **snmp-agent trap enable**, **snmp-agent target-host**.

## Examples

# Configure the IP address of Vlan-interface 1 as the source address for traps.

```
<Sysname> system-view
[Sysname] snmp-agent trap source Vlan-interface 1
```

## snmp-agent usm-user { v1 | v2c }

### Syntax

```
snmp-agent usm-user { v1 | v2c } user-name group-name [ acl acl-number ]
undo snmp-agent usm-user { v1 | v2c } user-name group-name
```

### View

System view

### Default Level

3: Manage level

### Parameters

**v1**: The configured user name should be applied in the SNMPv1 networking environment. If the agent and the NMS use SNMPv1 packets to communicate with each other, this keyword is needed.

**v2c**: The configured user name should be applied in the SNMPv2c networking environment. If the agent and the NMS use SNMPv2c packets to communicate with each other, this keyword is needed..

*user-name*: User name, a string of 1 to 32 characters. It is case sensitive.

*group-name*: Group name, a string of 1 to 32 characters. It is case sensitive.

**acl** *acl-number*: Associates a basic ACL with the user. *acl-number* is in the range 2000 to 2999. By using a basic ACL, you can restrict the source IP address of SNMP packets, that is, you can configure to allow or prohibit SNMP packets with a specific source IP address, so as to allow or prohibit the specified NMS to access the agent by using this user name.

### Description

Use the **snmp-agent usm-user { v1 | v2c }** command to add a user to an SNMP group.

Use the **undo snmp-agent usm-user { v1 | v2c }** command to delete a user from an SNMP group.

As defined in the SNMP protocol, in SNMPv1 and SNMPv2c networking applications, the NMS and the agent use community name to authenticate each other; in SNMPv3 networking applications, they use user name to authenticate each other. If you prefer using the user name in the authentication, the device supports configuration of SNMPv1 and SNMPv2c users. Creating an SNMPv1 or SNMPv2c user

equals adding of a new read-only community name. After you add the user name into the read-only community name field of the NMS, the NMS can establish SNMP connection with the device.

To make the configured user take effect, create an SNMP group first.

Related commands: `snmp-agent group`, `snmp-agent community`, `snmp-agent usm-user v3`.

## Examples

# Create a v2c user **userv2c** in group **readCom**.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent group v2c readCom
[Sysname] snmp-agent usm-user v2c userv2c readCom
```

- Set the SNMP version on the NMS to SNMPv2c
- Fill in the read community name **userv2c**, and then the NMS can access the agent

# Create a v2c user **userv2c** in group **readCom**, allowing only the NMS with the IP address of 1.1.1.1 to access the agent by using this user name; other NMSs are not allowed to access the agent by using this user name.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[Sysname-acl-basic-2001] rule deny source any
[Sysname-acl-basic-2001] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent group v2c readCom
[Sysname] snmp-agent usm-user v2c userv2c readCom acl 2001
```

- Set the IP address of the NMS to 1.1.1.1
- Set the SNMP version on the NMS to SNMPv2c
- Fill in both the read community and write community options with **userv2c**, and then the NMS can access the agent.

## snmp-agent usm-user v3

### Syntax

```
snmp-agent usm-user v3 user-name group-name [ cipher ] [ authentication-mode { md5 | sha }
auth-password [ privacy-mode { 3des | aes128 | des56 } priv-password ] [ acl acl-number ]
undo snmp-agent usm-user v3 user-name group-name { local | engineid engineid-string }
```

### View

System view

### Default Level

3: Manage level

### Parameters

*user-name*: User name, a string of 1 to 32 characters. It is case sensitive.

*group-name*: Group name, a string of 1 to 32 characters. It is case sensitive.

**cipher:** Specifies that *auth-password* and *priv-password* are cipher text passwords, which can be calculated by using the **snmp-agent calculate-password** command.

**authentication-mode:** Specifies the security model to be authentication. MD5 is faster than SHA, while SHA provides a higher security than MD5.

- **md5:** Specifies the authentication protocol as MD5.
- **sha:** Specifies the authentication protocol as SHA-1.

*auth-password:* Authentication password. If the **cipher** keyword is not specified, *auth-password* indicates a plain text password, which is a string of 1 to 64 visible characters. If the **cipher** keyword is specified, *auth-password* indicates a cipher text password. If the **md5** keyword is specified, *auth-password* is a string of 32 hexadecimal characters. If the **sha** keyword is specified, *auth-password* is a string of 40 hexadecimal characters.

**privacy-mode:** Specifies the security model to be privacy. The three encryption algorithms AES, 3DES, and DES are in descending order in terms of security. Higher security means more complex implementation mechanism and lower speed. DES is enough to meet general requirements.

- **3des:** Specifies the privacy protocol as 3DES.
- **des56:** Specifies the privacy protocol as DES.
- **aes128:** Specifies the privacy protocol as AES.

*priv-password:* The privacy password. If the **cipher** keyword is not specified, *priv-password* indicates a plain text password, which is a string of 1 to 64 characters; if the **cipher** keyword is specified, *priv-password* indicates a cipher text password; if the **3des** keyword is specified, *priv-password* is a string of 80 hexadecimal characters; if the **aes128** keyword is specified, *priv-password* is a string of 40 hexadecimal characters; if the **des56** keyword is specified, *priv-password* is a string of 40 hexadecimal characters.

**acl** *acl-number:* Associates a basic ACL with the user. *acl-number* is in the range 2000 to 2999. By using a basic ACL, you can restrict the source IP address of SNMP packets, that is, you can configure to allow or prohibit SNMP packets with a specific source IP address, so as to allow or prohibit the specified NMS to access the agent by using this user name.

**local:** Represents a local SNMP entity user.

**engineid** *engineid-string:* The engine ID string, an even number of hexadecimal characters, in the range 10 to 64. Its length must not be an odd number, and the all-zero and all-F strings are invalid.

## Description

Use the **snmp-agent usm-user v3** command to add a user to an SNMP group.

Use the **undo snmp-agent usm-user v3** command to delete a user from an SNMP group.

The user name configured by using this command is applicable to the SNMPv3 networking environments. If the agent and the NMS use SNMPv3 packets to communicate with each other, you need to create an SNMPv3 user.

To make the configured user valid, create an SNMP group first. Configure the authentication and encryption modes when you create a group, and configure the authentication and encryption passwords when you create a user.

- If you specify the **cipher** keyword, the system considers the arguments *auth-password* and *priv-password* as cipher text passwords. In this case, the command supports copy and paste, meaning if the engine IDs of the two devices are the same, you can copy and paste the SNMPv3 configuration commands in the configuration file on device A to device B and execute the

commands on device B. The cipher text password and plain text password on the two devices are the same.

- If you do not specify the **cipher** keyword, the system considers the arguments *auth-password* and *priv-password* as plain text passwords. In this case, if you perform the copy and paste operation, the system will encrypt these two passwords, resulting in inconsistency of the cipher text and plain text passwords of the two devices.

Note that:

- If you use the **snmp-agent usm-user v3 cipher** command, the *priv-password* argument in this command can be obtained by the **snmp-agent calculate-password** command. To make the calculated cipher text password applicable to the **snmp-agent usm-user v3 cipher** command and have the same effect as that in the **snmp-agent usm-user v3 cipher** command, ensure that the same privacy protocol is specified for the two commands and the local engine ID specified in the **snmp-agent usm-user v3 cipher** command is consistent with the SNMP entity engine ID specified in the **snmp-agent calculate-password** command.
- If you execute this command repeatedly to configure the same user (namely, the user names are the same, no limitation to other keywords and arguments), the last configuration takes effect.
- A plain text password is required when the NMS accesses the device; therefore, please remember the user name and the plain text password when you create a user.

Related commands: `snmp-agent calculate-password`, `snmp-agent group`, `snmp-agent usm-user { v1 | v2c }`.

## Examples

# Add a user **testUser** to the SNMPv3 group **testGroup**. Configure the security model as **authentication without privacy**, the authentication protocol as **MD5**, the plain-text authentication password as **authkey**.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 testGroup authentication
[Sysname] snmp-agent usm-user v3 testUser testGroup authentication-mode md5 authkey
```

- Set the SNMP version on the NMS to SNMPv3
- Fill in the user name **testUser**,
- Set the authentication protocol to **MD5**
- Set the authentication password to **authkey**
- Establish a connection, and the NMS can access the MIB objects in the ViewDefault view on the device

# Add a user **testUser** to the SNMPv3 group **testGroup**. Configure the security model as **authentication and privacy**, the authentication protocol as MD5, the privacy protocol as DES56, the plain-text authentication password as **authkey**, and the plain-text privacy password as **prikey**.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 testGroup privacy
[Sysname] snmp-agent usm-user v3 testUser testGroup authentication-mode md5 authkey
privacy-mode des56 prikey
```

- Set the SNMP version on the NMS to SNMPv3
- Fill in the user name **testUser**,
- Set the authentication protocol to **MD5**
- Set the authentication password to **authkey**
- Set the privacy protocol to **DES**

- Set the privacy password to **prikey**
- Establish a connection, and the NMS can access the MIB objects in the ViewDefault view on the device

# Add a user **testUser** to the SNMPv3 group **testGroup** with the **cipher** keyword specified. Configure the security model as **authentication and privacy**, the authentication protocol as MD5, the privacy protocol as DES56, the plain-text authentication password as **authkey**, and the plain-text privacy password as **prikey**

```
<Sysname> system-view
[Sysname] snmp-agent group v3 testGroup privacy
[Sysname] snmp-agent calculate-password authkey mode md5 local-engineid
The secret key is: 09659EC5A9AE91BA189E5845E1DDE0CC
[Sysname] snmp-agent calculate-password prikey mode md5 local-engineid
The secret key is: 800D7F26E786C4BECE61BF01E0A22705
[Sysname] snmp-agent usm-user v3 testUser testGroup cipher authentication-mode md5
09659EC5A9AE91BA189E5845E1DDE0CC privacy-mode des56 800D7F26E786C4BECE61BF01E0A22705
```

- Set the SNMP version on the NMS to SNMPv3
- Fill in the user name **testUser**,
- Set the authentication protocol to **MD5**
- Set the authentication password to **authkey**
- Set the privacy protocol to **DES**
- Set the privacy password to **prikey**
- Establish a connection, and the NMS can access the MIB objects in the ViewDefault view on the device

# 2 MIB Configuration Commands

---

## MIB Configuration Commands

### display mib-style

#### Syntax

**display mib-style**

#### View

Any view

#### Default Level

3: Manage level

#### Parameters

None

#### Description

Use the **display mib-style** command to display the MIB style of the device.

Two MIB styles are available on the device: **new** and **compatible**. After obtaining the MIB style, you can select matched 3Com network management software based on the MIB style.

Related commands: **mib-style**.

#### Examples

# After getting the device ID from node **sysObjectID**, you find that it is an 3Com device, and hope to know the current MIB style or the MIB style after next boot of the device.

```
<Sysname> display mib-style
Current MIB style: new
Next reboot MIB style: new
```

The above output information indicates that the current MIB style of the device is **new**, and the MIB style after next boot is still **new**.

### mib-style

#### Syntax

**mib-style [ new | compatible ]**

#### View

System view

## Default Level

3: Manage level

## Parameters

**new**: Specifies the MIB style of the device as 3Com **new**; that is, both sysOID and private MIB of the device are located under the 3Com enterprise ID 25506.

**compatible**: Specifies the MIB style of the device as 3Com **compatible**; that is, sysOID of the device is located under the 3Com enterprise ID 25506, and private MIB is located under the enterprise ID 2011.

## Description

Use the **mib-style** command to set the MIB style of the device.

By default, the MIB style of the device is **new**.

Note that the configuration takes effect only after the device reboots.

## Examples

# Modify the MIB style of the device as **compatible**.

```
<Sysname> system-view
[Sysname] mib-style compatible
[Sysname] quit
<Sysname> display mib-style
  Current MIB style: new
  Next reboot MIB style: compatible
<Sysname> reboot
```

# Table of Contents

<b>1 RMON Configuration Commands</b> .....	<b>1-1</b>
RMON Configuration Commands .....	1-1
display rmon alarm .....	1-1
display rmon event .....	1-2
display rmon eventlog.....	1-3
display rmon history.....	1-4
display rmon prialarm .....	1-7
display rmon statistics .....	1-8
rmon alarm .....	1-10
rmon event.....	1-12
rmon history.....	1-13
rmon prialarm .....	1-14
rmon statistics.....	1-16

# 1 RMON Configuration Commands

---

## RMON Configuration Commands

### display rmon alarm

#### Syntax

```
display rmon alarm [ entry-number ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

*entry-number*: Index of an RMON alarm entry, in the range 1 to 65535. If no entry is specified, the configuration of all alarm entries is displayed.

#### Description

Use the **display rmon alarm** command to display the configuration of the specified or all RMON alarm entries.

Related commands: **rmon alarm**.

#### Examples

# Display the configuration of all RMON alarm table entries.

```
<Sysname> display rmon alarm
AlarmEntry 1 owned by user1 is VALID.
  Samples type           : absolute
  Variable formula       : 1.3.6.1.2.1.16.1.1.1.4.1<etherStatsOctets.1>
  Sampling interval      : 10(sec)
  Rising threshold       : 50(linked with event 1)
  Falling threshold      : 5(linked with event 2)
  When startup enables   : risingOrFallingAlarm
  Latest value           : 0
```

**Table 1-1 display rmon alarm** command output description

Field	Description
AlarmEntry	Alarm entry, corresponding to the management information base (MIB) node alarmIndex.
owned by	Owner of the entry, user1 in this example, corresponding to the MIB node alarmOwner.

Field	Description
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the <b>display rmon</b> command to view the invalid entry, while with the <b>display current-configuration</b> and <b>display this</b> commands you cannot view the corresponding <b>rmon</b> commands.), corresponding to the MIB node alarmStatus.
Samples type	The sampling type (the value can be absolute or delta), corresponding to the MIB node alarmSampleType.
Variable formula	Alarm variable, namely, the monitored MIB node, corresponding to the MIB node alarmVariable.
Sampling interval	Sampling interval, in seconds, corresponding to the MIB node alarmInterval.
Rising threshold	Alarm rising threshold (When the sampling value is bigger than or equal to this threshold, a rising alarm is triggered.), corresponding to the MIB node alarmRisingThreshold.
Falling threshold	Alarm falling threshold (When the sampling value is smaller than or equal to this threshold, a falling alarm is triggered.), corresponding to the MIB node alarmFallingThreshold.
When startup enables	How an alarm can be triggered, corresponding to the MIB node alarmStartupAlarm.
Latest value	The last sampled value, corresponding to the MIB node alarmValue.

## display rmon event

### Syntax

**display rmon event** [ *entry-number* ]

### View

Any view

### Default Level

1: Monitor level

### Parameters

*entry-number*: Index of an RMON event entry, in the range 1 to 65535. If no entry is specified, the configuration of all event entries is displayed.

### Description

Use the **display rmon event** command to display the configuration of the specified or all RMON event entries.

Displayed information includes event index, event owner, event description, action triggered by the event (such as sending log or trap messages), and last time the event occurred (the elapsed time since system initialization/startup) in seconds.

Related commands: **rmon event**.

## Examples

```
# Display the configuration of RMON event table.
```

```
<Sysname> display rmon event
```

```
EventEntry 1 owned by user1 is VALID.
```

```
  Description: null.
```

```
  Will cause log-trap when triggered, last triggered at 0days 00h:02m:27s.
```

**Table 1-2 display rmon event** command output description

Field	Description
EventEntry	Event entry, corresponding to the MIB node eventIndex.
owned by	Owner of the entry, corresponding to the MIB node eventOwner.
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the <b>display rmon</b> command to view the invalid entry; while with the <b>display current-configuration</b> and <b>display this</b> commands you cannot view the corresponding <b>rmon</b> commands.), corresponding to the MIB node eventStatus.
Description	Description for the event, corresponding to the MIB node eventDescription.
cause log-trap when triggered	The actions that the system will take when the event is triggered: <ul style="list-style-type: none"><li>• none: The system will take no action</li><li>• log: The system will log the event</li><li>• snmp-trap: The system will send a trap to the NMS</li><li>• log-and-trap: The system will log the event and send a trap to the NMS</li></ul> This field corresponds to the MIB node eventType.
last triggered at	Time when the last event was triggered, corresponding to the MIB node eventLastTimeSent.

## display rmon eventlog

### Syntax

```
display rmon eventlog [ entry-number ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*entry-number*: Index of an event entry, in the range 1 to 65535.

### Description

Use the **display rmon eventlog** command to display log information for the specified or all event entries.

If *entry-number* is not specified, the log information for all event entries is displayed.

If you use the **rmon event** command to configure the system to log an event when the event is triggered, the event is recorded into the RMON log. You can use this command to display the details of the log table: event index, current event state, time the event was logged (the elapsed time in seconds since system initialization/startup), and event description.

## Examples

# Display the RMON log information for event entry 1.

```
<Sysname> display rmon eventlog 1
LogEntry 1 owned by null is VALID.
  Generates eventLog 1.1 at 0day(s) 00h:00m:33s.
  Description: The alarm formula defined in prialarmEntry 1,
    uprise 80 with alarm value 85. Alarm sample type is absolute.
  Generates eventLog 1.2 at 0day(s) 00h:42m:03s.
  Description: The alarm formula defined in prialarmEntry 2,
    less than(or =) 5 with alarm value 0. Alarm sample type is delta.
```

**Table 1-3 display rmon eventlog command output description**

Field	Description
LogEntry	Event log entry, corresponding to the MIB node logIndex.
owned by	Owner of the entry, corresponding to the MIB node eventOwner.
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the <b>display rmon</b> command to view the invalid entry; while with the <b>display current-configuration</b> and <b>display this</b> commands you cannot view the corresponding <b>rmon</b> commands.), corresponding to the MIB node eventStatus.
Generates eventLog at	Time when the log was created (Time passed since the device was booted), corresponding to the MIB node logTime.
Description	Log description, corresponding to the MIB node logDescription.

The above example shows that event 1 has generated two logs:

- eventLog 1.1, generated by private alarm entry 1, which is triggered because the alarm value (85) exceeds the rising threshold (80). The sampling type is **absolute**.
- eventLog 1.2, generated by private alarm entry 2, which is triggered because the alarm value (0) is lower than the falling threshold (5). The sampling type is **delta**.

## display rmon history

### Syntax

```
display rmon history [ interface-type interface-number ]
```

### View

Any view

### Default Level

1: Monitor level

## Parameters

*interface-type interface-number*. Specifies an interface by its type and number.

## Description

Use the **display rmon history** command to display RMON history control entry and history sampling information.

After you have created history control entry on an interface, the system calculates the information of the interface periodically and saves this information to the etherHistoryEntry table. You can use this command to display the entries in this table.

You can configure the number of history sampling records that can be displayed and the history sampling interval through the **rmon history** command.

Related commands: **rmon history**.

## Examples

# Display RMON history control entry and history sampling information for interface GigabitEthernet 1/0/1.

```
<Sysname> display rmon history GigabitEthernet 1/0/1
HistoryControlEntry 1 owned by null is VALID
  Samples interface      : GigabitEthernet1/0/1<ifIndex.1>
  Sampling interval     : 10(sec) with 5 buckets max
  Sampled values of record 1 :
    dropevents          : 0          , octets          : 0
    packets              : 0          , broadcast packets : 0
    multicast packets    : 0          , CRC alignment errors : 0
    undersize packets    : 0          , oversize packets    : 0
    fragments            : 0          , jabbers             : 0
    collisions           : 0          , utilization          : 0
  Sampled values of record 2 :
    dropevents          : 0          , octets          : 0
    packets              : 0          , broadcast packets : 0
    multicast packets    : 0          , CRC alignment errors : 0
    undersize packets    : 0          , oversize packets    : 0
    fragments            : 0          , jabbers             : 0
    collisions           : 0          , utilization          : 0
  Sampled values of record 3 :
    dropevents          : 0          , octets          : 0
    packets              : 0          , broadcast packets : 0
    multicast packets    : 0          , CRC alignment errors : 0
    undersize packets    : 0          , oversize packets    : 0
    fragments            : 0          , jabbers             : 0
    collisions           : 0          , utilization          : 0
  Sampled values of record 4 :
    dropevents          : 0          , octets          : 0
    packets              : 0          , broadcast packets : 0
    multicast packets    : 0          , CRC alignment errors : 0
    undersize packets    : 0          , oversize packets    : 0
```

```

    fragments      : 0      , jabbers      : 0
    collisions     : 0      , utilization  : 0
Sampled values of record 5 :
    dropevents    : 0      , octets      : 0
    packets       : 0      , broadcast packets : 0
    multicast packets : 0      , CRC alignment errors : 0
    undersize packets : 0      , oversize packets : 0
    fragments     : 0      , jabbers     : 0
    collisions    : 0      , utilization  : 0

```

**Table 1-4 display rmon history** command output description

Field	Description
HistoryControlEntry	History control entry, corresponding to the MIB node etherHistoryIndex.
owned by	Owner of the entry, corresponding to the MIB node historyControlOwner.
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the <b>display rmon</b> command to view the invalid entry; while with the <b>display current-configuration</b> and <b>display this</b> commands you cannot view the corresponding <b>rmon</b> commands.), corresponding to the MIB node historyControlStatus.
Samples Interface	The sampled interface
Sampling interval	Sampling period, in seconds, corresponding to the MIB node historyControlInterval. The system samples the information of an interface periodically.
buckets max	The maximum number of history table entries that can be saved, corresponding to the MIB node historyControlBucketsGranted. If the specified value of the <b>buckets</b> argument exceeds the history table size supported by the device, the supported history table size is displayed. If the current number of the entries in the table has reached the maximum number, the system will delete the earliest entry to save the latest one.
Sampled values of record <i>number</i>	The ( <i>number</i> )th statistics recorded in the system cache. Statistics records are numbered according to the order of time they are saved into the cache.
dropevents	Dropped packets during the sampling period, corresponding to the MIB node etherHistoryDropEvents.
octets	Number of octets received during the sampling period, corresponding to the MIB node etherHistoryOctets.
packets	Number of packets received during the sampling period, corresponding to the MIB node etherHistoryPkts.
broadcastpackets	Number of broadcasts received during the sampling period, corresponding to the MIB node etherHistoryBroadcastPkts.
multicastpackets	Number of multicasts received during the sampling period, corresponding to the MIB node etherHistoryMulticastPkts.

Field	Description
CRC alignment errors	Number of packets received with CRC alignment errors during the sampling period, corresponding to the MIB node etherHistoryCRCAlignErrors.
undersize packets	Number of undersize packets received during the sampling period, corresponding to the MIB node etherHistoryUndersizePkts.
oversize packets	Number of oversize packets received during the sampling period, corresponding to the MIB node etherHistoryOversizePkts.
fragments	Number of fragments received during the sampling period, corresponding to the MIB node etherHistoryFragments.
jabbers	Number of jabbers received during the sampling period corresponding to the MIB node etherHistoryJabbers.
collisions	Number of colliding packets received during the sampling period, corresponding to the MIB node etherHistoryCollisions.
utilization	Bandwidth utilization during the sampling period, corresponding to the MIB node etherHistoryUtilization.

## display rmon prialarm

### Syntax

**display rmon prialarm** [ *entry-number* ]

### View

Any view

### Default Level

1: Monitor level

### Parameters

*entry-number*: Private alarm entry index, in the range 1 to 65535. If no entry is specified, the configuration of all private alarm entries is displayed.

### Description

Use the **display rmon prialarm** command to display the configuration of the specified or all private alarm entries.

Related commands: **rmon prialarm**.

### Examples

# Display the configuration of all private alarm entries.

```
<Sysname> display rmon prialarm
PrialarmEntry 1 owned by user1 is VALID.
  Samples type           : absolute
  Variable formula       : (.1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1)
  Description            : ifUtilization.GigabitEthernet1/0/1
```

```

Sampling interval      : 10(sec)
Rising threshold      : 80(linked with event 1)
Falling threshold     : 5(linked with event 2)
When startup enables  : risingOrFallingAlarm
This entry will exist : forever
Latest value          : 85

```

**Table 1-5 display rmon prialarm command output description**

Field	Description
PrialarmEntry	The entry of the private alarm table
owned by	Owner of the entry, user1 in this example
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the <b>display rmon</b> command to view the invalid entry; while with the <b>display current-configuration</b> and <b>display this</b> commands you cannot view the corresponding <b>rmon</b> commands.)
Samples type	Sampling type, whose value can be absolute or delta.
Sampling interval	Sampling interval, in seconds. The system performs absolute sample or delta sample to sampling variables according to the sampling interval.
Rising threshold	Alarm rising threshold. An event is triggered when the sampled value is greater than or equal to this threshold.
Falling threshold	Alarm falling threshold. An event is triggered when the sampled value is less than or equal to this threshold.
linked with event	Event index associated with the prialarm
When startup enables	How can an alarm be triggered
This entry will exist	The lifetime of the entry, which can be forever or span the specified period
Latest value	The count result of the last sample

## display rmon statistics

### Syntax

```
display rmon statistics [ interface-type interface-number ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*interface-type interface-number*. Specifies an interface by its type and number.

### Description

Use the **display rmon statistics** command to display RMON statistics.

This command displays the interface statistics during the period from the time the statistics entry is created to the time the command is executed. The statistics are cleared after the device reboots.

Related commands: **rmon statistics**.

## Examples

# Display RMON statistics for interface GigabitEthernet 1/0/1.

```
<Sysname> display rmon statistics GigabitEthernet 1/0/1
EtherStatsEntry 1 owned by null is VALID.
  Interface : GigabitEthernet1/0/1<ifIndex.3>
  etherStatsOctets      : 43393306 , etherStatsPkts      : 619825
  etherStatsBroadcastPkts : 503581 , etherStatsMulticastPkts : 44013
  etherStatsUndersizePkts : 0 , etherStatsOversizePkts : 0
  etherStatsFragments   : 0 , etherStatsJabbers     : 0
  etherStatsCRCAlignErrors : 0 , etherStatsCollisions  : 0
  etherStatsDropEvents (insufficient resources): 0
  Packets received according to length:
  64 : 0 , 65-127 : 0 , 128-255 : 0
  256-511: 0 , 512-1023: 0 , 1024-1518: 0
```

**Table 1-6 display rmon statistics** command output description

Field	Description
EtherStatsEntry	The entry of the statistics table, corresponding to the MIB node etherStatsIndex.
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the <b>display rmon</b> command to view the invalid entry; while with the <b>display current-configuration</b> and <b>display this</b> commands you cannot view the corresponding <b>rmon</b> commands.), corresponding to the MIB node etherStatsStatus.
Interface	Interface on which statistics are gathered, corresponding to the MIB node etherStatsDataSource.
etherStatsOctets	Number of octets received and sent by the interface during the statistical period, corresponding to the MIB node etherStatsOctets.
etherStatsPkts	Number of packets received and sent by the interface during the statistical period, corresponding to the MIB node etherStatsPkts.
etherStatsBroadcastPkts	Number of broadcast packets received and sent by the interface during the statistical period, corresponding to the MIB node etherStatsBroadcastPkts.
etherStatsMulticastPkts	Number of multicast packets received and sent by the interface during the statistical period, corresponding to the MIB node etherStatsMulticastPkts.
etherStatsUndersizePkts	Number of undersize packets received and sent by the interface during the statistical period, corresponding to the MIB node etherStatsUndersizePkts.
etherStatsOversizePkts	Number of oversize packets received and sent by the interface during the statistical period, corresponding to the MIB node etherStatsOversizePkts.

Field	Description
etherStatsFragments	Number of undersize packets with CRC errors received and sent by the interface during the statistical period, corresponding to the MIB node etherStatsFragments.
etherStatsJabbers	Number of oversize packets with CRC errors received and sent by the interface during the statistical period, corresponding to the MIB node etherStatsJabbers.
etherStatsCRCAlignErrors	Number of packets with CRC errors received and sent on the interface during the statistical period, corresponding to the MIB node etherStatsCRCAlignErrors.
etherStatsCollisions	Number of collisions received and sent on the interface during the statistical period, corresponding to the MIB node etherStatsCollisions.
etherStatsDropEvents	Total number of drop events received and sent on the interface during the statistical period, corresponding to the MIB node etherStatsDropEvents.
Packets received according to length: 64 :0 , 65-127 :0 , 128-255 :0 256-511:0 , 512-1023: 0 , 1024-1518:0	<p>Statistics of packets received and sent according to length during the statistical period (Hardware support is needed for the statistics. If the hardware does not support the function, all statistics are displayed as 0.), in which:</p> <ul style="list-style-type: none"> <li>• Information of the field 64 corresponds to the MIB node etherStatsPkts64Octets</li> <li>• Information of the field 65-127 corresponds to the MIB node etherStatsPkts65to127Octets</li> <li>• Information of the field 128-255 corresponds to the MIB node etherStatsPkts128to255Octets</li> <li>• Information of the field 256-511 corresponds to the MIB node etherStatsPkts256to511Octets</li> <li>• Information of the field 512-1023 corresponds to the MIB node etherStatsPkts512to1023Octets</li> <li>• Information of the field 1024-1518 corresponds to the MIB node etherStatsPkts1024to1518Octets</li> </ul>

## rmon alarm

### Syntax

**rmon alarm** *entry-number alarm-variable sampling-interval* { **absolute** | **delta** } **rising-threshold** *threshold-value1 event-entry1 falling-threshold threshold-value2 event-entry2* [ **owner text** ]

**undo rmon alarm** *entry-number*

### View

System view

### Default Level

2: System level

### Parameters

*entry-number*: Alarm entry index, in the range 1 to 65535.

*alarm-variable*: Alarm variable, a string of 1 to 256 characters. It can be in dotted object identifier (OID) format (in the format of *entry.integer.instance* or *leaf node name.instance*, for example,

1.3.6.1.2.1.2.1.10.1), or a node name like ifInOctets.1. Only variables that can be parsed into INTEGER (INTEGER, Counter, Gauge, or Time Ticks) in the ASN.1 can be used for the *alarm-variable* argument, such as the instance of the leaf node (like etherStatsOctets, etherStatsPkts, etherStatsBroadcastPkts, and so on) of the etherStatsEntry entry, the instance of the leaf node (like ifInOctets, ifInUcastPkts, ifInNUcastPkts, and so on) of the ifEntry entry.

*sampling-interval*: Sampling interval, in the range 5 to 65,535 seconds.

**absolute**: Sets the sampling type to **absolute**, namely, the system obtains the value of the variable when the sampling time is reached.

**delta**: Sets the sampling type to **delta**, namely, the system obtains the variation value of the variable during the sampling interval when the sampling time is reached.

**rising-threshold** *threshold-value1 event-entry1*: Sets the rising threshold, where *threshold-value1* represents the rising threshold, in the range -2,147,483,648 to +2,147,483,647, and *event-entry1* represents the index of the event triggered when the rising threshold is reached. *event-entry1* ranges from 0 to 65,535, with 0 meaning no corresponding event is triggered and no event action is taken when an alarm is triggered.

**falling-threshold** *threshold-value2 event-entry2*: Sets the falling threshold, where *threshold-value2* represents the falling threshold, in the range -2,147,483,648 to +2,147,483,647 and *event-entry2* represents the index of the event triggered when the falling threshold is reached. *event-entry2* ranges from 1 to 65,535.

**owner text**: Owner of the entry, a string of 1 to 127 characters. It is case sensitive and space is supported.

## Description

Use the **rmon alarm** command to create an entry in the RMON alarm table.

Use the **undo rmon alarm** command to remove a specified entry from the RMON alarm table.

This command defines an alarm entry, so as to trigger the specified event when abnormality occurs. The event defines how to deal with the abnormality.

The following is how the system handles alarm entries:

- 1) Samples the alarm variables at the specified interval.
- 2) Compares the sampled values with the predefined threshold and does the following:
  - If the rising threshold is reached, triggers the event specified by the *event-entry1* argument.
  - If the falling threshold is reached, triggers the event specified by the *event-entry2* argument.



### Note

- Before creating an alarm entry, define the events to be referenced in the event table with the **rmon event** command.
  - When you create an entry, if the values of the specified alarm variable (*alarm-variable*), sampling interval (*sampling-interval*), sampling type (**absolute** or **delta**), rising threshold (*threshold-value1*) and falling threshold (*threshold-value2*) are identical to those of the existing alarm entry, the system considers their configurations are the same and the creation fails.
  - You can create up to 60 alarm entries.
-

Related commands: **display rmon alarm**, **rmon event**, **rmon history**, **rmon statistics**.

## Examples

# Add entry 1 in the alarm table and sample the node 1.3.6.1.2.1.16.1.1.1.4.1 at a sampling interval of 10 seconds in absolute sampling type. Trigger event 1 when the sampled value is greater than or equal to the rising threshold of 5000, and event 2 when the sampled value is less than or equal to the falling threshold of 5. Set the owner of the entry to be **user1**.

```
<Sysname> system-view
[Sysname] rmon event 1 log
[Sysname] rmon event 2 none
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 1
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 10 absolute rising-threshold 5000 1
falling-threshold 5 2 owner user1
```

1.3.6.1.2.1.16.1.1.1.4 is the OID of the leaf node etherStatsOctets. It represents the statistics of the received packets on the interface, in bytes. In the above example, you can use etherStatsOctets.1 to replace the parameter 1.3.6.1.2.1.16.1.1.1.4.1, where 1 indicates the serial number of the interface statistics entry. Therefore, if you execute the **rmon statistics 5** command, you can use etherStatsOctets.5 to replace the parameter.

The above configuration implements the following:

- Sampling and monitoring interface GigabitEthernet 1/0/1
- Obtaining the absolute value of the number of received packets. If the total bytes of the received packets reach 5,000, the system will log the event; if the total bytes of the received packets are no more than 5, the system will take no action.

## rmon event

### Syntax

```
rmon event entry-number [ description string ] { log | log-trap log-trapcommunity | none | trap trap-community } [ owner text ]
```

```
undo rmon event entry-number
```

### View

System view

### Default Level

2: System level

### Parameters

*entry-number*: Event entry index, in the range 1 to 65,535.

**description** *string*: Event description, a string of 1 to 127 characters.

**log**: Logs the event when it occurs.

**log-trap** *log-trapcommunity*: Log and trap events. The system performs both logging and trap sending when the event occurs. *log-trapcommunity* indicates the community name of the network management station that receives trap messages, a string of 1 to 127 characters.

**none:** Performs no action when the event occurs.

**trap** *trap-community*: Trap event. The system sends a trap with a community name when the event occurs. *trap-community* specifies the community name of the network management station that receives trap messages, a string of 1 to 127 characters.

**owner** *text*: Owner of the entry, a string of 1 to 127 characters. It is case sensitive and space is supported.

## Description

Use the **rmon event** command to create an entry in the RMON event table.

Use the **undo rmon event** command to remove a specified entry from the RMON event table.

When create an event entry, you can define the actions that the system will take when the event is triggered by its associated alarm in the alarm table. According to your configuration, the system can log the event, send a trap, do both, or do neither at all.

Related commands: **display rmon event**, **rmon alarm**, **rmon prialarm**.



### Note

- When you create an entry, if the values of the specified event description (**description string**), event type (**log**, **trap**, **logtrap** or **none**), and community name (*trap-community* or *log-trapcommunity*) are identical to those of the existing event entry, the system considers their configurations are the same and the creation fails.
  - You can create up to 60 alarm entries.
- 

## Examples

```
# Create event 10 in the RMON event table.  
<Sysname> system-view  
[Sysname] rmon event 10 log owner user1
```

## rmon history

### Syntax

```
rmon history entry-number buckets number interval sampling-interval [ owner text ]  
undo rmon history entry-number
```

### View

Ethernet interface view

### Default Level

2: System level

### Parameters

*entry-number*: History control entry index, in the range 1 to 65535.

**buckets** *number*: History table size for the entry, in the range 1 to 65,535.

**interval** *sampling-interval*: Sampling period, in the range 5 to 3600 seconds.

**owner** *text*: Owner of the entry, a string of 1 to 127 characters. It is case sensitive and space is supported.

## Description

Use the **rmon history** command to create an entry in the RMON history control table.

Use the **undo rmon history** command to remove a specified entry from the RMON history control table.

After an entry is created, the system periodically samples the number of packets received/sent on the current interface, and saves the statistics as an instance under the leaf node of the etherHistoryEntry table. The maximum number of history entries can be saved in the table is specified by **buckets number**. If the number of the entries in the table has reached the maximum number, the system will delete the earliest entry to save the latest one. The statistics include total number of received packets on the current interface, total number of broadcast packets, and total number of multicast packets in a sampling period,

When you create an entry in the history table, if the specified history table size exceeds that supported by the device, the entry will be created. However, the validated value of the history table size corresponding to the entry is that supported by the device. You can use the **display rmon history** command to view the configuration result.



### Note

- When you create an entry, if the value of the specified sampling interval (**interval** *sampling-interval*) is identical to that of the existing history entry, the system considers their configurations are the same and the creation fails.
  - You can create up to 100 alarm entries.
- 

Related commands: **display rmon history**.

## Examples

# Create RMON history control entry 1 for interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon history 1 buckets 10 interval 5 owner user1
```

## rmon prialarm

### Syntax

```
rmon prialarm entry-number prialarm-formula prialarm-des sampling-interval { absolute | changeratio | delta } rising-threshold threshold-value1 event-entry1 falling-threshold threshold-value2 event-entry2 entrytype { forever | cycle cycle-period } [ owner text ]
```

```
undo rmon prialarm entry-number
```

## View

System view

## Default Level

2: System level

## Parameters

*entry-number*: Index of a private alarm entry, in the range 1 to 65535.

*prialarm-formula*: Private alarm variable formula, a string of 1 to 256 characters. The variables in the formula must be represented in OID format that starts with a point ".", the formula (.1.3.6.1.2.1.2.1.10.1)\*8 for example. You may perform the basic operations of addition, subtraction, multiplication, and division on these variables. The operations should yield a long integer. To prevent errors, make sure that the result of each calculating step falls into the value range for long integers.

*prialarm-des*: Private alarm entry description, a string of 1 to 127 characters.

*sampling-interval*: Sampling interval, in the range 10 to 65,535 seconds.

**absolute** | **changeratio** | **delta** : Sets the sampling type to absolute, delta, or change ratio. Absolute sampling is to obtain the value of the variable when the sampling time is reached; delta sampling is to obtain the variation value of the variable during the sampling interval when the sampling time is reached; change ratio sampling is not supported at present.

**rising-threshold** *threshold-value1 event-entry1*: Sets the rising threshold, where *threshold-value1* represents the rising threshold, in the range -2,147,483,648 to +2,147,483,647, and *event-entry1* represents the index of the event triggered when the rising threshold is reached. *event-entry1* ranges from 0 to 65,535, with 0 meaning no corresponding event is triggered and no event action is taken when an alarm is triggered.

**falling-threshold** *threshold-value2 event-entry2*: Sets the falling threshold, where *threshold-value2* represents the falling threshold, in the range -2,147,483,648 to +2,147,483,647 and *event-entry2* represents the index of the event triggered when the falling threshold is reached. *event-entry2* ranges from 1 to 65,535.

**forever**: Indicates that the lifetime of the private alarm entry is infinite.

**cycle** *cycle-period*: Sets the lifetime period of the private alarm entry, in the range 0 to 2,147,483,647 seconds.

**owner text**: Owner of the entry, a string of 1 to 127 characters. It is case sensitive and space is supported.

## Description

Use the **rmon prialarm** command to create an entry in the private alarm table of RMON.

Use the **undo rmon prialarm** command to remove a private alarm entry from the private alarm table of RMON.

The following is how the system handles private alarm entries:

- 1) Samples the private alarm variables in the private alarm formula at the specified sampling interval.
- 2) Performs calculation on the sampled values with the formula.
- 3) Compares the calculation result with the predefined thresholds and does the following:
  - If the result is equal to or greater than the rising threshold, triggers the event specified by the *event-entry1* argument.

- If the result is equal to or smaller than the falling threshold, triggers the event specified by the *event-entry2* argument.



#### Note

- Before creating an alarm entry, define the events to be referenced in the event table with the **rmon event** command.
- When you create an entry, if the values of the specified alarm variable formula (*prialarm-formula*), sampling type (**absolute changeratio** or **delta**), rising threshold (*threshold-value1*) and falling threshold (*threshold-value2*) are identical to those of the existing alarm entry, the system considers their configurations are the same and the creation fails.
- You can create up to 50 pri-alarm entries.

---

Related commands: **display rmon prialarm**, **rmon event**, **rmon history**, **rmon statistics**.

### Examples

# Create entry 5 in the private alarm table. Calculate the private alarm variables with the (1.3.6.1.2.1.16.1.1.1.6.1\*100/.1.3.6.1.2.1.16.1.1.1.5.1) formula and sample the corresponding variables at intervals of 10 seconds. Rising threshold of 80 corresponds to event 1 (and record the event into the log table); falling threshold of 5 corresponds to event 2 (but neither log it nor send a trap). Set the lifetime of the entry to **forever** and owner to **user1**.

```
<Sysname> system-view
[Sysname] rmon event 1 log
[Sysname] rmon event 2 none
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 1
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] rmon prialarm 1 (1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1)
packet GigabitEthernet1/0/1 10 absolute rising_threshold 80 1 falling_threshold 5 2 entrytype
forever owner user1
```

1.3.6.1.2.1.16.1.1.1.6.1 is the OID of the node etherStatsBroadcastPkts.1, and 1.3.6.1.2.1.16.1.1.1.5.1 is the OID of the node etherStatsPkts.1. 1 indicates the serial number of the interface statistics entry. Therefore, if you execute the **rmon statistics 5** command, you should use 1.3.6.1.2.1.16.1.1.1.6.5 and 1.3.6.1.2.1.16.1.1.1.5.5.

The above configuration implements the following:

- Sampling and monitoring interface GigabitEthernet1/0/1
- If the portion of broadcast packets received in the total packets is greater than or equal to 80%, the system will log the event; if the portion is less than or equal to 5%, the system will take no action.

You can view the event log using the **display rmon eventlog** command.

### rmon statistics

#### Syntax

```
rmon statistics entry-number [ owner text ]
```

**undo rmon statistics** *entry-number*

## View

Ethernet interface view

## Default Level

2: System level

## Parameters

*entry-number*: Index of statistics entry, in the range 1 to 65535.

**owner** *text*: Owner of the entry, a string of 1 to 127 characters. It is case sensitive and space is supported.

## Description

Use the **rmon statistics** command to create an entry in the RMON statistics table.

Use the **undo rmon statistics** command to remove a specified entry from the RMON statistics table.

After an entry is created, the system continuously calculates the information of the interface. It provides statistics about network collisions, CRC alignment errors, undersize/oversize packets, broadcasts, multicasts, bytes received, packets received, bytes sent, packets sent, and so on. The statistics are cleared after the device reboots.

To display information for the RMON statistics table, use the **display rmon statistics** command.



### Note

- Only one statistics entry can be created on one interface.
  - You can create up to 100 statistics entries.
- 

## Examples

# Create an entry in the RMON statistics table for interface GigabitEthernet 1/0/1. The index of the entry is 20, and the owner of the entry is **user1**.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 20 owner user1
```

# Table of Contents

<b>1 MAC Address Table Management Configuration Commands</b> .....	<b>1-1</b>
MAC Address Table Management Configuration Commands .....	1-1
display mac-address .....	1-1
display mac-address aging-time .....	1-2
mac-address (Interface view) .....	1-3
mac-address (system view) .....	1-4
mac-address mac-learning disable .....	1-5
mac-address max-mac-count (Interface view) .....	1-6
mac-address timer .....	1-7
<b>2 MAC Information Configuration Commands</b> .....	<b>2-1</b>
MAC Information Configuration Commands .....	2-1
mac-address information enable (Ethernet interface view) .....	2-1
mac-address information enable (system view) .....	2-2
mac-address information interval .....	2-2
mac-address information mode .....	2-3
mac-address information queue-length .....	2-4

# 1 MAC Address Table Management Configuration Commands

---



## Note

Interfaces that MAC address table management involves can only be Ethernet ports.

---

## MAC Address Table Management Configuration Commands

### display mac-address

#### Syntax

```
display mac-address blackhole [ vlan vlan-id ] [ count ]
```

```
display mac-address [ mac-address [ vlan vlan-id ] ] [ dynamic | static ] [ interface interface-type  
interface-number ] [ vlan vlan-id ] [ count ] ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

**blackhole:** Destination blackhole MAC address entries. These entries do not age but you can add or remove them. The packets whose destination MAC addresses match destination blackhole MAC address entries are dropped.

**vlan *vlan-id*:** Displays MAC address entries of the specified VLAN, where *vlan-id* is in the range 1 to 4094.

**count:** Displays the total number of MAC addresses in the MAC address table.

***mac-address*:** Displays MAC address entries in a specified MAC address, in the format of H-H-H.

**dynamic:** Displays dynamic MAC address entries. Aging time is set for these entries.

**static:** Displays static MAC address entries. Similar to blackhole MAC address entries, these entries do not age but you can add or remove them.

**interface *interface-type interface-number*:** Displays MAC address learning status of the specified interface. *interface-type interface-number* specifies an interface by its type and number.

## Description

Use the **display mac-address** command to display information about the MAC address table.

Related commands: **mac-address (system view)**, **mac-address (Ethernet interface view)**, **mac-address timer**.

## Examples

# Display the MAC address table entry for MAC address 000f-e201-0101.

```
<Sysname> display mac-address 000f-e201-0101
MAC ADDR          VLAN ID  STATE          PORT INDEX          AGING TIME(s)
000f-e201-0101    1        Learned        GigabitEthernet1/0/1  AGING
```

**Table 1-1 display mac-address command output description**

Field	Description
MAC ADDR	MAC address
VLAN ID	ID of the VLAN to which the MAC address belongs
STATE	State of a MAC address, includes: <ul style="list-style-type: none"><li>• Config static: static entry configured by the user manually</li><li>• Config dynamic: dynamic entry configured by the user manually</li><li>• Learned: entry learned by the device</li><li>• Blackhole: destination blackhole entry</li><li>• Source-Blackhole: source blackhole entry</li></ul>
PORT INDEX	Number of the port corresponding to the MAC address, that is, packets destined to this MAC address will be sent out from this port. (Displayed as N/A for a blackhole MAC address entry).
AGING TIME(s)	Aging time, which could be: <ul style="list-style-type: none"><li>• <i>AGING</i>, indicates that the entry is aging.</li><li>• <i>NOAGED</i>, indicates that the entry does not age.</li></ul>

## display mac-address aging-time

### Syntax

```
display mac-address aging-time
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

## Description

Use the **display mac-address aging-time** command to display the aging time of dynamic entries in the MAC address table.

Related commands: **mac-address (system view)**, **mac-address (Ethernet interface view)**, **mac-address timer**, **display mac-address**.

## Examples

# Display the aging time of dynamic entries in the MAC address table.

```
<Sysname> display mac-address aging-time  
Mac address aging time: 300s
```

The above information indicates that the aging time of dynamic entries in the MAC address table is 300 seconds.

## mac-address (Interface view)

### Syntax

```
mac-address { dynamic | static } mac-address vlan vlan-id  
undo mac-address { dynamic | static } mac-address vlan vlan-id
```

### View

Ethernet interface view, Layer-2 aggregate interface view

### Default Level

2: System level

### Parameters

**dynamic**: Dynamic MAC address entries. Aging time is set for these entries.

**static**: Static MAC address entries. They do not age but you can add or remove them.

*mac-address*: Specifies a MAC address in the format of H-H-H, where 0s at the beginning of each H (16-bit hexadecimal digit) can be omitted; for example, inputting “f-e2-1” indicates that the MAC address is “000f-00e2-0001”.

**vlan** *vlan-id*: Specifies an existing VLAN to which the Ethernet interface belongs, where *vlan-id* is the specified VLAN ID, in the range 1 to 4094.

### Description

Use the **mac-address** command to add or modify a MAC address entry on a specified interface.

Use the **undo mac-address** command to remove a MAC address entry on the interface.

Note that, as your MAC address entries configuration cannot survive a reboot, save it after completing the configuration. The dynamic MAC address table entries however will be lost whether you save the configuration or not.

Related commands: **display mac-address**.

## Examples

# Add a static entry for MAC address 000f-e201-0101 on port GigabitEthernet 1/0/1 that belongs to VLAN 2.

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] mac-address static 000f-e201-0101 vlan 2
```

# Add a static entry for MAC address 000f-e201-0102 on port Bridge-Aggregation 1 that belongs to VLAN 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] mac-address static 000f-e201-0102 vlan 1
```

## mac-address (system view)

### Syntax

**mac-address blackhole** *mac-address* **vlan** *vlan-id*

**mac-address** { **dynamic** | **static** } *mac-address* **interface** *interface-type* *interface-number* **vlan** *vlan-id*

**undo mac-address** [ { **dynamic** | **static** } *mac-address* **interface** *interface-type* *interface-number* **vlan** *vlan-id* ]

**undo mac-address** [ **blackhole** | **dynamic** | **static** ] [ *mac-address* ] **vlan** *vlan-id*

**undo mac-address** [ **dynamic** | **static** ] *mac-address* **interface** *interface-type* *interface-number* **vlan** *vlan-id*

**undo mac-address** [ **dynamic** | **static** ] **interface** *interface-type* *interface-number*

### View

System view

### Default Level

2: System level

### Parameters

**blackhole**: Destination blackhole MAC address entries. These entries do not age but you can add or remove them. The packets whose destination MAC addresses match destination blackhole MAC address entries are dropped.

*mac-address*: Specifies a MAC address in the format of H-H-H, where 0s at the beginning of each H (16-bit hexadecimal digit) can be omitted; for example, inputting “f-e2-1” indicates that the MAC address is “000f-00e2-0001”.

**vlan** *vlan-id*: Specifies an existing VLAN to which the Ethernet interface belongs, where *vlan-id* is the specified VLAN ID, in the range 1 to 4094.

**dynamic**: Dynamic MAC address entries. Aging time is set for these entries.

**static**: Static MAC address entries. These entries do not age but you can add or remove them.

**interface** *interface-type* *interface-number*: Outbound interface, with *interface-type* *interface-number* representing the interface type and number.

### Description

Use the **mac-address** command to add or modify a MAC address entry.

Use the **undo mac-address** command to remove one or all MAC address entries.

Note that a static or blackhole entry will not be overwritten by a dynamic entry, but a dynamic entry can be overwritten by a static or blackhole entry. However, you can delete any type of MAC address entries.

As your MAC address entries configuration cannot survive a reboot, save it after completing the configuration. The dynamic entries however will be lost whether you save the configuration or not.

Related commands: **display mac-address**.

## Examples

# Add a static entry for MAC address 000f-e201-0101. All frames destined to this MAC address are sent out of port GigabitEthernet 1/0/1 which belongs to VLAN 2.

```
<Sysname> system-view  
[Sysname] mac-address static 000f-e201-0101 interface gigabitethernet 1/0/1 vlan 2
```

## mac-address mac-learning disable

### Syntax

```
mac-address mac-learning disable  
undo mac-address mac-learning disable
```

### View

VLAN view

### Default Level

2: System level

### Parameters

None

### Description

Use the **mac-address mac-learning disable** command to disable MAC address learning on a VLAN. Use the **undo mac-address mac-learning disable** command to enable MAC address learning on a VLAN.

By default, MAC address learning is enabled on all VLANs.

Note that:

- You may need to disable MAC address learning sometimes to prevent the MAC address table from being saturated, for example, when your device is being attacked by a great deal of packets with different source MAC addresses. This somewhat affects update of the MAC address table.
- As disabling MAC address learning may result in broadcast storms, you need to enable broadcast storm suppression after you disable MAC address learning on a port.

Related commands: **display mac-address mac-learning**.



### Note

Once MAC learning is disabled in a VLAN, all MAC address entries learnt in the VLAN are removed.

---

## Examples

```
# Disable MAC address learning on VLAN 10.
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] mac-address mac-learning disable
```

## mac-address max-mac-count (Interface view)

### Syntax

```
mac-address max-mac-count count
undo mac-address max-mac-count
```

### View

Ethernet interface view, port group view

### Default Level

2: System level

### Parameters

*count*: Maximum number of MAC addresses that can be learned on a port, ranging from 0 to 4096. When the argument takes 0, the VLAN is not allowed to learn MAC addresses.

**disable-forwarding**: Disables forwarding of frames with unknown source MAC addresses after the number of learned MAC addresses reaches the upper limit. Frames with the source MAC addresses listed in the MAC address table will be forwarded normally.

### Description

Use the **mac-address max-mac-count** *count* command to configure the maximum number of MAC addresses that can be learned on an Ethernet port.

Use the **undo mac-address max-mac-count** command to restore the default maximum number of MAC addresses that can be learned on an Ethernet port.

By default, the maximum number of MAC addresses that can be learned on an Ethernet port is not configured.

If the command is executed in interface view, the configuration takes effect on the current interface; if the command is executed in port group view, the configuration takes effect on all ports belonging to the port group.

Related commands: **mac-address**, **mac-address timer**.

## Examples

# Set the maximum number of MAC addresses that can be learned on port GigabitEthernet 1/0/1 to 600. After this upper limit is reached, frames received with unknown source MAC addresses on the port will not be forwarded.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address max-mac-count 600
[Sysname-GigabitEthernet1/0/1] mac-address max-mac-count disable-forwarding
```

## mac-address timer

### Syntax

```
mac-address timer { aging seconds | no-aging }  
undo mac-address timer aging
```

### View

System view

### Default Level

2: System level

### Parameters

**aging** *seconds*: Sets an aging timer in seconds for dynamic MAC address entries. The *seconds* argument ranges from 10 to 1000000.

**no-aging**: Sets dynamic MAC address entries not to age.

### Description

Use the **mac-address timer** command to configure the aging timer for dynamic MAC address entries.

Use the **undo mac-address timer** command to restore the default.

By default the default aging timer is 300 seconds.

Set the aging timer appropriately: a long aging interval may cause the MAC address table to retain outdated entries and fail to accommodate the latest network changes; a short interval may result in removal of valid entries and hence unnecessary broadcasts which may affect device performance.

### Examples

```
# Set the aging timer for dynamic MAC address entries to 500 seconds.
```

```
<Sysname> system-view  
[Sysname] mac-address timer aging 500
```

# 2 MAC Information Configuration Commands

---



## Note

Currently, MAC Information applies to only Layer-2 Ethernet interfaces.

---

## MAC Information Configuration Commands

### mac-address information enable (Ethernet interface view)

#### Syntax

```
mac-address information enable { added | deleted }
undo mac-address information enable { added | deleted }
```

#### View

Ethernet interface view

#### Default Level

1: Monitor level

#### Parameters

**added:** Enables the device to record security information when a new MAC address is learned on the Ethernet port.

**deleted:** Enables the device to record security information when an existing MAC address is deleted.

#### Description

Use the **mac-address information enable** command to enable MAC Information on the Layer-2 Ethernet interface.

Use the **undo mac-address information enable** command to disable MAC Information on the Layer-2 Ethernet interface.

By default, MAC Information is disabled on a Layer-2 Ethernet interface.

Note that:

- This command is not supported on aggregate interfaces.
- To enable MAC Information on an Ethernet interface, enable MAC Information globally first.

#### Examples

```
# Enable MAC Information on GigabitEthernet1/0/1.
```

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address information enable added
```

## mac-address information enable (system view)

### Syntax

```
mac-address information enable
undo mac-address information enable
```

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **mac-address information enable** command to enable MAC Information globally.

Use the **undo mac-address information enable** command to disable MAC Information globally.

By default, MAC Information is disabled globally.

### Examples

```
# Enable MAC Information globally.
```

```
<Sysname> system-view
[Sysname] mac-address information enable
```

## mac-address information interval

### Syntax

```
mac-address information interval value
undo mac-address information interval
```

### View

System view

### Default Level

2: System level

### Parameters

*value*: Interval for sending Syslog or Trap messages (in seconds). The range for this argument is 1 to 20000.

## Description

Use the **mac-address information interval** command to set the interval for sending Syslog or Trap messages.

Use the **undo mac-address information interval** command to restore the default interval for sending Syslog or Trap messages.

By default, the interval for sending Syslog or Trap messages is 1 second.

## Examples

```
# Set the interval for sending Syslog or Trap messages to 200 seconds.
```

```
<Sysname> system-view
[Sysname] mac-address information interval 200
```

## mac-address information mode

### Syntax

```
mac-address information mode { syslog | trap }
undo mac-address information mode
```

### View

System view

### Default Level

2: System level

### Parameters

**syslog**: Specifies that the device sends Syslog messages to inform the remote network management device of MAC address changes.

**trap**: Specifies that the device sends trap messages to inform the remote network management device of MAC address changes.

## Description

Use the **mac-address information mode** command to set the MAC Information mode, that is, whether to use Syslog messages or Trap messages to inform the remote network management device of MAC address changes.

Use the **undo mac-address information mode** command to restore the default.

By default, trap messages are sent to inform the remote network management device of MAC address changes.

## Examples

```
# Configure the device to send trap messages to inform the remote network management device of
MAC address changes.
```

```
<Sysname> system-view
[Sysname] mac-address information mode trap
```

## mac-address information queue-length

### Syntax

```
mac-address information queue-length value  
undo mac-address information queue-length
```

### View

System view

### Default Level

2: System level

### Parameters

*value*: MAC Information queue length. The value range is 0 to 1000.

### Description

Use the **mac-address information queue-length** command to set the MAC Information queue length.

Use the **undo mac-address information queue-length** command to restore the default.

By default, the MAC Information queue length is 50.

Setting the MAC Information queue length to 0 indicates that the device sends a Syslog or Trap message to the network management device as soon as a new MAC address is learned or an existing MAC address is deleted.

### Examples

```
# Set the MAC Information queue length to 600.
```

```
<Sysname> system-view
```

```
[Sysname] mac-address information queue-length 600
```

# Table of Contents

<b>1 System Maintaining and Debugging Commands</b> .....	<b>1-1</b>
System Maintaining Commands .....	1-1
ping .....	1-1
ping ipv6 .....	1-4
tracert.....	1-6
tracert ipv6.....	1-7
System Debugging Commands .....	1-8
debugging.....	1-8
display debugging.....	1-9

# 1 System Maintaining and Debugging Commands

---

## System Maintaining Commands

### ping

#### Syntax

```
ping [ ip ] [ -a source-ip | -c count | -f | -h ttl | -i interface-type interface-number | -m interval | -n | -p pad | -q | -r | -s packet-size | -t timeout | -tos tos | -v | -vpn-instance vpn-instance-name ] * remote-system
```

#### View

Any view

#### Default Level

0: Visit level

#### Parameters

**ip**: Supports IPv4 protocol.

**-a source-ip**: Specifies the source IP address of an ICMP echo request (ECHO-REQUEST). It must be a legal IP address configured on the device.

**-c count**: Specifies the number of times that an ICMP echo request is sent, in the range 1 to 4294967295. The default value is 5.

**-f**: Discards packets larger than the MTU of a given interface, that is, the ICMP echo request is not allowed to be fragmented.

**-h ttl**: Specifies the TTL value for an ICMP echo request, in the range 1 to 255. The default value is 255.

**-i interface-type interface-number**: Specifies the ICMP echo request sending interface by its type and number.

**-m interval**: Specifies the interval (in milliseconds) to send an ICMP echo response, in the range 1 to 65535. The default value is 200 ms.

- If a response from the destination is received within the timeout time, the interval to send the next echo request equals the actual response period plus the value of *interval*.
- If no response from the destination is received within the timeout time, the interval to send the next echo request equals the *timeout* value plus the value of *interval*.

**-n**: Specifies that the Domain Name System (DNS) is disabled. DNS is enabled by default, that is, the *hostname* is translated into an address.

**-p pad**: Specifies the value of the **pad** field in an ICMP echo request, in hexadecimal format, 1 to 8 bits, in the range 0 to fffffff. If the specified value is less than 8 bits, 0s will be added in front of the value to extend it to 8 bits. For example, if *pad* is configured as 0x2f, then the packets will be padded with 0x0000002f repeatedly to make the total length of the packet meet the requirements of the device. By default, the padded value starts from 0x01 up to 0xff, where another round starts again if necessary, like 0x010203...feff01....

**-q:** Presence of this parameter indicates that only statistics are displayed. By default, all information is displayed.

**-r:** Records routes. By default, routes are not recorded.

**-s packet-size:** Specifies length (in bytes) of an ICMP echo request, in the range 20 to 8100. The default value is 56.

**-t timeout:** Specifies the timeout value (in milliseconds) of an ICMP echo reply (ECHO-REPLY), in the range 0 to 65535. It defaults to 2000.

**-tos tos:** Specifies type of service (ToS) of an echo request, in the range 0 to 255. The default value is 0.

**-v:** Displays non ICMP echo reply received. By default, the system does not display non ICMP echo reply.

**-vpn-instance vpn-instance-name:** Specifies the name of an MPLS VPN instance, which is a string of 1 to 31 characters. It is case sensitive.

*remote-system:* IP address or host name (a string of 1 to 20 characters) of the destination device.

## Description

Use the **ping** command to verify whether the destination device in an IP network is reachable, and to display the related statistics.

Note that:

- You must use the command in the form of **ping ip ip** instead of **ping ip** if the destination name is a key word, such as **ip**.
- Only the directly connected segment address can be pinged if the outgoing interface is specified with the **-i** argument.

During the execution of the command, you can press **Ctrl+C** to abort the ping operation.

## Examples

**# Check whether the device with an IP address of 10.1.1.5 is reachable.**

```
<Sysname> ping 10.1.1.5
PING 10.1.1.5 : 56 data bytes, press CTRL_C to break
Reply from 10.1.1.5 : bytes=56 Sequence=1 ttl=255 time=1 ms
Reply from 10.1.1.5 : bytes=56 Sequence=2 ttl=255 time=2 ms
Reply from 10.1.1.5 : bytes=56 Sequence=3 ttl=255 time=1 ms
Reply from 10.1.1.5 : bytes=56 Sequence=4 ttl=255 time=3 ms
Reply from 10.1.1.5 : bytes=56 Sequence=5 ttl=255 time=2 ms

--- 10.1.1.5 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 1/2/3 ms
```

The above information indicates the following:

- The destination host was reachable
- All probe packets sent by the source device got responses
- The minimum time, average time, and maximum time for the packet's roundtrip time are 1 ms, 2 ms, and 3 ms respectively

# Check whether the device with an IP address of 3.3.3.2 is reachable. Only the check results are displayed.

```
<Sysname> ping -q 3.3.3.2
  PING 3.3.3.2: 56 data bytes, press CTRL_C to break

  --- 3.3.3.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 1/1/1 ms
```

# Check whether the device with an IP address of 3.3.3.2 is reachable. The route information is required to be displayed.

```
<Sysname> ping -r 3.3.3.2
  PING 3.3.3.2: 56 data bytes, press CTRL_C to break
    Reply from 3.3.3.2: bytes=56 Sequence=1 ttl=255 time=2 ms
      Record Route:
        3.3.3.2
        3.3.3.1
    Reply from 3.3.3.2: bytes=56 Sequence=2 ttl=255 time=1 ms
      Record Route:
        3.3.3.2
        3.3.3.1
    Reply from 3.3.3.2: bytes=56 Sequence=3 ttl=255 time=1 ms
      Record Route:
        3.3.3.2
        3.3.3.1
    Reply from 3.3.3.2: bytes=56 Sequence=4 ttl=255 time=2 ms
      Record Route:
        3.3.3.2
        3.3.3.1
    Reply from 3.3.3.2: bytes=56 Sequence=5 ttl=255 time=1 ms
      Record Route:
        3.3.3.2
        3.3.3.1

  --- 3.3.3.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 1/1/2 ms
```

The above information indicates the following:

- The destination host was reachable
- The IP address 3.3.3.1 was reached first, and then 3.3.3.2.

**Table 1-1 ping command output description**

Field	Description
PING 10.1.1.5	Check whether the device with IP address 10.1.1.5 is reachable
56 data bytes	Number of data bytes in the ICMP echo request
press CTRL_C to break	During the execution of the command, you can press <b>Ctrl+C</b> to abort the ping operation.
Reply from 10.1.1.5 : bytes=56 Sequence=1 ttl=255 time=1 ms	Received the ICMP reply from the device whose IP address is 10.1.1.5. If no reply is received during the timeout period, "Request time out" will be displayed. <ul style="list-style-type: none"> <li>• bytes= indicates the number of data bytes in the ICMP reply.</li> <li>• Sequence= indicates the packet sequence.</li> <li>• ttl= indicates the TTL value in the ICMP reply.</li> <li>• time= indicates the response time.</li> </ul>
Record Route:	The routers through which the ICMP echo request passed. They are displayed in inversed order, that is, the router with a smaller distance to the destination is displayed first.
--- 10.1.1.5 ping statistics ---	Statistics on data received and sent in the ping operation
5 packet(s) transmitted	Number of ICMP echo requests sent
5 packet(s) received	Number of ICMP echo requests received
0.00% packet loss	Percentage of packets not responded to the total packets sent
round-trip min/avg/max = 0/4/20 ms	Minimum/average/maximum response time, in ms

## ping ipv6

### Syntax

```
ping ipv6 [ -a source-ipv6 | -c count | -m interval | -s packet-size | -t timeout ] * remote-system [ -i interface-type interface-number ]
```

### View

Any view

### Default Level

0: Visit level

### Parameters

**-a source-ipv6:** Specifies the source IPv6 address of an ICMP echo request. It must be a legal IPv6 address configured on the device.

**-c count:** Specifies the number of times that an ICMPv6 echo request is sent, in the range 1 to 4294967295. The default value is 5.

**-m interval:** Specifies the interval (in milliseconds) to send an ICMPv6 echo reply, in the range 1 to 65535. The default value is 200 ms.

- If a response from the destination is received within the timeout time, the interval to send the next echo request equals the actual response period plus the value of *interval*.

- If no response from the destination is received within the timeout time, the interval to send the next echo request equals the *timeout* value plus the value of *interval*.

**-s packet-size:** Specifies length (in bytes) of an ICMPv6 echo request, in the range 20 to 8100. It defaults to 56.

**-t timeout:** Specifies the timeout value (in milliseconds) of an ICMPv6 echo reply, in the range 0 to 65535. It defaults to 2000.

*remote-system:* IPv6 address or host name of the destination device, a string of 1 to 46 characters.

**-i interface-type interface-number:** Specifies an outgoing interface by its type and number. This parameter can be used only in case that the destination address is the link local address and the specified outgoing interface must have a link local address (For the configuration of link local address, see *IPv6 Basics* in the *IP Services Volume*).

## Description

Use the **ping ipv6** command to verify whether an IPv6 address is reachable, and display the corresponding statistics.

You must use the command in the form of **ping ipv6 ipv6** instead of **ping ipv6** if the destination name is an ipv6 name.

During the execution of the command, you can press **Ctrl+C** to abort the ping ipv6 operation.

## Examples

# Verify whether the IPv6 address 2001::1 is reachable.

```
<Sysname> ping ipv6 2001::1
PING 1::2 : 56 data bytes, press CTRL_C to break
  Reply from 1::2
    bytes=56 Sequence=1 hop limit=64 time = 4 ms
  Reply from 1::2
    bytes=56 Sequence=2 hop limit=64 time = 2 ms
  Reply from 1::2
    bytes=56 Sequence=3 hop limit=64 time = 2 ms
  Reply from 1::2
    bytes=56 Sequence=4 hop limit=64 time = 2 ms
  Reply from 1::2
    bytes=56 Sequence=5 hop limit=64 time = 2 ms

--- 1::2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 2/2/4 ms
```

The “hop limit” field in this prompt information has the same meaning as the “ttl” field in the prompt information displayed by the IPv4 **ping** command, indicating the TTL value in the ICMPv6 echo request. For the description on other fields, refer to [Table 1-1](#).

## tracert

### Syntax

```
tracert [ -a source-ip | -f first-ttl | -m max-ttl | -p port | -q packet-number | -vpn-instance vpn-instance-name | -w timeout ] * remote-system
```

### View

Any view

### Default Level

0: Visit level

### Parameters

**-a source-ip:** Specifies the source IP address of a tracert packet. It must be a legal IP address configured on the device.

**-f first-ttl:** Specifies the first TTL, that is, the allowed number of hops for the first packet, in the range 1 to 255. It defaults to 1 and must be less than the maximum TTL.

**-m max-ttl:** Specifies the maximum TTL, that is, the maximum allowed number of hops for a packet, in the range 1 to 255. It defaults to 30, and must be greater than the first TTL.

**-p port:** Specifies the UDP port number of the destination device, in the range 1 to 65535. The default value is 33434. You do not need to modify this parameter.

**-q packet-number:** Specifies the number of probe packets sent each time, in the range 1 to 65535. The default value is 3.

**-vpn-instance vpn-instance-name:** Specifies the name of an MPLS VPN instance, which is a string of 1 to 31 characters.

**-w timeout:** Specifies the timeout time of the reply packet of a probe packet, in the range 1 to 65535, in milliseconds. The default value is 5000 ms.

*remote-system:* IP address or host name (a string of 1 to 20 characters) of the destination device.

### Description

Use the **tracert** command to trace the path the packets traverse from the source to the destination device.

After having identified network failure with the **ping** command, you can use the **tracert** command to determine the failed node(s).

Output information of the **tracert** command includes IP addresses of all the Layer 3 devices the packets traverse from the source to the destination device. If a device times out, "\* \* \*" will be displayed.

During the execution of the command, you can press **Ctrl+C** to abort the tracert operation.

### Examples

# Display the path the packets traverse from the source device to the destination device with an IP address of 18.26.0.115.

```
<Sysname> tracert 18.26.0.115
traceroute to 18.26.0.115(18.26.0.115) 30 hops max,40 bytes packet, press CTRL_C to break
 1  128.3.112.1  10 ms 10 ms 10 ms
 2  128.32.210.1  19 ms 19 ms 19 ms
```

```

3 128.32.216.1 39 ms 19 ms 19 ms
4 128.32.136.23 19 ms 39 ms 39 ms
5 128.32.168.22 20 ms 39 ms 39 ms
6 128.32.197.4 59 ms 119 ms 39 ms
7 131.119.2.5 59 ms 59 ms 39 ms
8 129.140.70.13 80 ms 79 ms 99 ms
9 129.140.71.6 139 ms 139 ms 159 ms
10 129.140.81.7 199 ms 180 ms 300 ms
11 129.140.72.17 300 ms 239 ms 239 ms
12 * * *
13 128.121.54.72 259 ms 499 ms 279 ms
14 * * *
15 * * *
16 * * *
17 * * *
18 18.26.0.115 339 ms 279 ms 279 ms

```

**Table 1-2** `tracert` command output description

Field	Description
tracert to 18.26.0.115(18.26.0.115)	Display the route the IP packets traverse from the current device to the device whose IP address is 18.26.0.115.
30 hops max	Maximum number of hops of the probe packets, which can be set through the <b>-m</b> keyword
60 bytes packet	Number of bytes of a probe packet
press CTRL_C to break	During the execution of the command, you can press <b>Ctrl+C</b> to abort the <code>tracert</code> operation.
1 128.3.112.1 10 ms 10 ms 10 ms	The probe result of the probe packets whose TTL is 1, including the IP address of the device and the roundtrip time of three probe packets. The number of packets that can be sent in each probe can be set through the <b>-q</b> keyword.
12 * * *	The probe result of the probe packets whose TTL is 12. The result is: timeout

## tracert ipv6

### Syntax

```
tracert ipv6 [ -f first-ttl | -m max-ttl | -p port | -q packet-number | -w timeout ] * remote-system
```

### View

Any view

### Default Level

0: Visit level

## Parameters

**-f first-ttl:** Specifies the first TTL, that is, the allowed number of hops for the first packet, in the range 1 to 255. It defaults to 1 and must be less than the maximum TTL.

**-m max-ttl:** Specifies the maximum TTL, that is, the maximum allowed number of hops for a packet, in the range 1 to 255. It defaults to 30 and must be greater than the first TTL.

**-p port:** Specifies the UDP port number of the destination device, in the range 1 to 65535. The default value is 33434. It is unnecessary to modify this parameter.

**-q packet-number:** Specifies the number of probe packets sent each time, in the range 1 to 65535, defaulting to 3.

**-w timeout:** Specifies the timeout time of the reply packet of a probe packet, in the range 1 to 65535, in milliseconds. The default value is 5000 ms.

**remote-system:** IPv6 address or host name of the destination device, a string of 1 to 46 characters.

## Description

Use the **tracert ipv6** command to view the path the IPv6 packets traverse from the source to the destination device.

After having identified network failure with the **ping** command, you can use the **tracert** command to determine the failed node(s).

Output information of the **tracert ipv6** command includes IPv6 addresses of all the Layer 3 devices the packets traverse from the source to the destination device. If a device times out, "\*\*\*" will be displayed.

During the execution of the command, you can press **Ctrl+C** to abort the tracert operation.

## Examples

# View the path the packets traverse from the source to the destination with IPv6 address 3002::1.

```
<Sysname> tracert ipv6 3002::1
  traceroute to 3002::1 30 hops max,60 bytes packet, press CTRL_C to break
  1 3003::1 30 ms 10 ms 10 ms
  2 3002::1 10 ms 11 ms 9 ms
```

For description on the fields in the above output information, refer to [Table 1-2](#).

# System Debugging Commands

## debugging

### Syntax

```
debugging { all [ timeout time ] | module-name [ option ] }
undo debugging { all | module-name [ option ] }
```

### View

User view

### Default Level

1: Monitor level

## Parameters

**all**: All debugging functions.

**timeout** *time*: Specifies the timeout time for the **debugging all** command. When all debugging is enabled, the system automatically executes the **undo debugging all** command after the *time*. The value ranges from 1 to 1440, in minutes.

*module-name*: Module name, such as arp or device. You can use the **debugging ?** command to display the current module name.

*option*: The debugging option for a specific module. Different modules have different debugging options in terms of their number and content. You can use the **debugging module-name ?** command to display the currently supported options.

## Description

Use the **debugging** command to enable the debugging of a specific module.

Use the **undo debugging** command to disable the debugging of a specific module.

By default, debugging functions of all modules are disabled.

Note the following:

- Output of the debugging information may degrade system efficiency, so you are recommended to enable the debugging of a specific module for diagnosing network failure, and not to enable the debugging of multiple modules at the same time.
- **Default Level** describes the default level of the **debugging all** command. Different **debugging** commands may have different default levels.
- You must configure the **debugging**, **terminal debugging** and **terminal monitor** commands first to display detailed debugging information on the terminal. For the detailed description on the **terminal debugging** and **terminal monitor** commands, refer to *Information Center Commands* in the *System Volume*.

Related commands: **display debugging**.

## Examples

```
# Enable IP packet debugging.  
<Sysname> debugging ip packet
```

## display debugging

### Syntax

```
display debugging [ interface interface-type interface-number ] [ module-name ]
```

### View

Any view

### Default Level

1: Monitor level

## Parameters

**interface** *interface-type interface-number*: Displays the debugging settings of the specified interface, where *interface-type interface-number* represents the interface type and number.

*module-name*: Module name.

## Description

Use the **display debugging** command to display enabled debugging functions.

Related commands: **debugging**.

## Examples

# Display all enabled debugging functions.

```
<Sysname> display debugging
```

```
IP packet debugging is on
```

# Table of Contents

<b>1 Information Center Configuration Commands</b> .....	<b>1-1</b>
Information Center Configuration Commands .....	1-1
display channel .....	1-1
display info-center .....	1-2
display logbuffer .....	1-4
display logbuffer summary .....	1-6
display trapbuffer .....	1-7
enable log updown .....	1-8
info-center channel name .....	1-9
info-center console channel .....	1-9
info-center enable .....	1-10
info-center logbuffer .....	1-11
info-center loghost .....	1-11
info-center loghost source .....	1-12
info-center monitor channel .....	1-13
info-center snmp channel .....	1-14
info-center source .....	1-15
info-center synchronous .....	1-17
info-center timestamp .....	1-19
info-center timestamp loghost .....	1-20
info-center trapbuffer .....	1-20
reset logbuffer .....	1-21
reset trapbuffer .....	1-22
terminal debugging .....	1-22
terminal logging .....	1-23
terminal monitor .....	1-24
terminal trapping .....	1-24

# 1 Information Center Configuration Commands

---

## Information Center Configuration Commands

### display channel

#### Syntax

**display channel** [ *channel-number* | *channel-name* ]

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

*channel-number*: Displays information of the channel with a specified number, where *channel-number* represents the channel number, in the range 0 to 9.

*channel-name*: Displays information of the channel with a specified name, where *channel-name* represents the channel name, which could be a default name or a self-defined name. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to the **info-center channel name** command.

**Table 1-1** Information channels for different output destinations

Output destination	Information channel number	Default channel name
Console	0	console
Monitor terminal	1	monitor
Log host	2	loghost
Trap buffer	3	trapbuffer
Log buffer	4	logbuffer
SNMP module	5	snmpagent

#### Description

Use the **display channel** command to display channel information.

If no channel is specified, information for all channels is displayed.

#### Examples

```
# Display information for channel 0.
```

```
<Sysname> display channel 0
```

```
channel number:0, channel name:console
MODU_ID  NAME      ENABLE LOG_LEVEL  ENABLE TRAP_LEVEL  ENABLE DEBUG_LEVEL
ffff0000 default  Y      warnings    Y      debugging  Y      debugging
```

The above information indicates to output log information with the severity from 0 to 4, trap information with the severity from 0 to 7 and debugging information with the severity from 0 to 7 to the console. The information source modules are all modules (default).

**Table 1-2 display channel** command output description

Field	Description
channel number	A specified channel number, in the range 0 to 9.
channel name	A specified channel name, which varies with user's configuration. For more information, refer to the <b>info-center channel name</b> command.
MODU_ID	The ID of the module to which the information permitted to pass through the current channel belongs
NAME	The name of the module to which the information permitted to pass through the current channel belongs Default means all modules are allowed to output system information, but the module type varies with devices.
ENABLE	Indicates whether to enable or disable the output of log information, which could be Y or N.
LOG_LEVEL	The severity of log information, refer to <a href="#">Table 1-4</a> for details.
ENABLE	Indicates whether to enable or disable the output of trap information, which could be Y or N.
TRAP_LEVEL	The severity of trap information, refer to <a href="#">Table 1-4</a> for details.
ENABLE	Indicates whether to enable or disable the output of debugging information, which could be Y or N.
DEBUG_LEVEL	The severity of debugging information, refer to <a href="#">Table 1-4</a> for details.

## display info-center

### Syntax

```
display info-center
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display info-center** command to display the information of each output destination.

## Examples

# Display configurations on each output destination.

```
<Sysname> display info-center
Information Center:enabled
Log host:
    2.2.2.2, channel number : 8, channel name : channel8,
    host facility local7
Console:
    channel number : 0, channel name : console
Monitor:
    channel number : 1, channel name : monitor
SNMP Agent:
    channel number : 5, channel name : snmpagent
Log buffer:
    enabled,max buffer size 1024, current buffer size 512,
    current messages 512, dropped messages 0, overwritten messages 740
    channel number : 4, channel name : logbuffer
Trap buffer:
    enabled,max buffer size 1024, current buffer size 256,
    current messages 216, dropped messages 0, overwritten messages 0
    channel number : 3, channel name : trapbuffer
Information timestamp setting:
    log - date, trap - date, debug - date,
    loghost - date
```

**Table 1-3 display info-center command output description**

Field	Description
Information Center	The current state of the information center, which could be enabled or disabled.
Log host: 2.2.2.2, channel number : 8, channel name : channel8, host facility local7	Configurations on the log host destination (It can be displayed only when the <b>info-center loghost</b> command is configured), including IP address of the log host, the channel number and channel name used, and logging facility used.)
Console: channel number : 0, channel name : console	Configurations on the console destination, including the channel number and channel name used
Monitor: channel number : 1, channel name : monitor	Configurations on the monitor terminal destination, including the channel number and channel name used
SNMP Agent: channel number : 5, channel name : snmpagent	Configurations on the SNMP module destination, including the channel number and channel name used

Field	Description
Log buffer: enabled,max buffer size 1024, current buffer size 512, current messages 512, dropped messages 0, overwritten messages 740 channel number : 4, channel name : logbuffer	Configurations on the log buffer destination, including whether information output to this destination is enabled or disabled, the maximum capacity, the current capacity, the current number of messages, the number of dropped messages, the number of messages that have been overwritten, and the channel number and channel name used.
Trap buffer: enabled,max buffer size 1024, current buffer size 256, current messages 216, dropped messages 0, overwritten messages 0 channel number : 3, channel name : trapbuffer	Configurations on the trap buffer destination, including whether information output to this destination is enabled or disabled, the maximum capacity, the current capacity, the current number of messages, the number of dropped messages, the number of messages that have been overwritten, and the channel number and channel name used.
Information timestamp setting	The timestamp configurations, specifying the timestamp format for log, trap, debug, and log host information.

## display logbuffer

### Syntax

```
display logbuffer [ reverse ] [ level severity | size buffersize | slot slot-number ] * [ { begin | exclude | include } regular-expression ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**reverse:** Displays log entries chronologically, with the most recent entry at the top. If this keyword is not specified, the log entries will be displayed chronologically, with the oldest entry at the top.

**level severity:** Displays information of the log with specified level, where *severity* represents information level, in the range 0 to 7.

**Table 1-4** Severity description

Severity	Value	Description
Emergency	0	The system is unusable.
Alert	1	Action must be taken immediately
Critical	2	Critical conditions
Error	3	Error conditions
Warning	4	Warning conditions
Notice	5	Normal but significant condition

Severity	Value	Description
Informational	6	Informational messages
Debug	7	Debug-level messages

**size** *buffersize*: Displays specified number of the latest log messages in the log buffer, where *buffersize* represents the number of the latest log messages to be displayed in the log buffer, in the range 1 to 1,024.

**slot** *slot-number*: Displays the log information in the log buffer of the specified device. If the device is in an IRF stack, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF stack, the *slot-number* argument represents the device ID.

|: Uses a regular expression to filter the output information. For detailed information about regular expression, refer to section CLI Display in *Basic System Configuration* in the *System Volume*.

- **begin**: Displays the line that matches the regular expression and all the subsequent lines.
- **exclude**: Displays the lines that do not match the regular expression.
- **include**: Displays the lines that match the regular expression.

*regular-expression*: Regular expression, a string of 1 to 256 characters. Note that this argument is case-sensitive and can have spaces included.

## Description

Use the **display logbuffer** command to display the state of the log buffer and the log information recorded. Absence of the **size buffersize** argument indicates that all log information recorded in the log buffer is displayed.

## Examples

# Display the state of the log buffer and the log information recorded on the device.

```
<Sysname> display logbuffer
Logging buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 512
Channel number : 4 , Channel name : logbuffer
Dropped messages : 0
Overwritten messages : 718
Current messages : 512

%Jun 17 15:57:09:578 2006 Sysname IC/7/SYS_RESTART:
System restarted --
```

The rest is omitted here.

**Table 1-5 display logbuffer command output description**

Field	Description
Logging buffer configuration and contents	Indicates the current state of the log buffer and its contents, which could be enabled or disabled.
Allowed max buffer size	The maximum buffer size allowed
Actual buffer size	The actual buffer size

Field	Description
Channel number	The channel number of the log buffer, defaults to 4.
Channel name	The channel name of the log buffer, defaults to logbuffer.
Dropped messages	The number of dropped messages
Overwritten messages	The number of overwritten messages (when the buffer size is not big enough to hold all messages, the latest messages overwrite the old ones).
Current messages	The number of the current messages

## display logbuffer summary

### Syntax

**display logbuffer summary** [ *level severity* | *slot slot-number* ] \*

### View

Any view

### Default Level

1: Monitor level

### Parameters

**level severity**: Displays the summary of the log buffer, where *severity* represents information level, in the range 0 to 7.

**slot slot-number**: Displays the summary of the log buffer of the specified device. If the device is in an IRF stack, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF stack, the *slot-number* argument represents the device ID.

### Description

Use the **display logbuffer summary** command to display the summary of the log buffer.

### Examples

# Display the summary of the log buffer on the device.

```
<Sysname> display logbuffer summary
  SLOT EMERG ALERT  CRIT ERROR  WARN NOTIF  INFO DEBUG
    0    0    0    0    0    0    0    0    0
    1    0    0    0    0    0    0    0    0
    2    0    0    0    0    0    0    0    0
    3    0    0    0    0    16   0    1    0
```

**Table 1-6 display logbuffer summary** command output description

Field	Description
SLOT	Slot number
EMERG	Represents emergency, refer to <a href="#">Table 1-4</a> for details

Field	Description
ALERT	Represents alert, refer to <a href="#">Table 1-4</a> for details
CRIT	Represents critical, refer to <a href="#">Table 1-4</a> for details
ERROR	Represents error, refer to <a href="#">Table 1-4</a> for details
WARN	Represents warning, refer to <a href="#">Table 1-4</a> for details
NOTIF	Represents notice, refer to <a href="#">Table 1-4</a> for details
INFO	Represents informational, refer to <a href="#">Table 1-4</a> for details
DEBUG	Represents debug, refer to <a href="#">Table 1-4</a> for details

## display trapbuffer

### Syntax

```
display trapbuffer [ reverse ] [ size buffersize ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**reverse:** Displays trap entries chronologically, with the most recent entry at the top. If this keyword is not specified, trap entries will be displayed chronologically, with the oldest entry at the top.

**size buffersize:** Displays specified number of the latest trap messages in a trap buffer, where *buffersize* represents the number of the latest trap messages in a trap buffer, in the range 1 to 1,024.

### Description

Use the **display trapbuffer** command to display the state and the trap information recorded.

Absence of the **size buffersize** argument indicates that all trap information is displayed.

### Examples

# Display the state of the trap buffer and the trap information recorded.

```
<Sysname> display trapbuffer
Trapping buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 2

#Aug 7 14:47:35:636 2008 Sysname IFNET/4/INTERFACE UPDOWN:
```

```

Trap 1.3.6.1.6.3.1.1.5.3<linkDown>: Interface 983041 is Down, ifAdminStatus is 2,
ifOperStatus is 2
#Aug 7 14:47:47:724 2008 Sysname IFNET/4/INTERFACE UPDOWN:
Trap 1.3.6.1.6.3.1.1.5.4<linkUp>: Interface 983041 is Up, ifAdminStatus is 1, ifOperStatus
is 1

```

**Table 1-7 display trapbuffer command output description**

Field	Description
Trapping buffer configuration and contents	Indicates the current state of the trap buffer and its contents, which could be enabled or disabled.
Allowed max buffer size	The maximum buffer size allowed
Actual buffer size	The actual buffer size
Channel number	The channel number of the trap buffer, defaults to 3.
channel name	The channel name of the trap buffer, defaults to trapbuffer.
Dropped messages	The number of dropped messages
Overwritten messages	The number of overwritten messages (when the buffer size is not big enough to hold all messages, the latest messages overwrite the old ones).
Current messages	The number of the current messages

## enable log updown

### Syntax

```

enable log updown
undo enable log updown

```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **enable log updown** command to allow a port to generate link up/down logging information when the port state changes.

Use the **undo enable log updown** command to disable a port from generating link up/down logging information when the port state changes.

By default, all the ports are allowed to generate port link up/down logging information when the port state changes.

## Examples

```
# Disable port GigabitEthernet 1/0/1 from generating link up/down logging information.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo enable log updown
```

## info-center channel name

### Syntax

```
info-center channel channel-number name channel-name
undo info-center channel channel-number
```

### View

System view

### Default Level

2: System level

### Parameters

*channel-number*: Specifies a channel number, in the range 0 to 9.

*channel-name*: Specifies a channel name, a string of 1 to 30 characters. It must be a combination of letters and numbers, and start with a letter and is case insensitive.

### Description

Use the **info-center channel name** command to name a channel with a specified channel number.

Use the **undo info-center channel** command to restore the default name for a channel with a specified channel number.

Refer to [Table 1-1](#) for details of default channel names and channel numbers.

## Examples

```
# Name channel 0 as abc.
<Sysname> system-view
[Sysname] info-center channel 0 name abc
```

## info-center console channel

### Syntax

```
info-center console channel { channel-number | channel-name }
undo info-center console channel
```

### View

System view

### Default Level

2: System level

## Parameters

*channel-number*: Specifies a channel number, in the range 0 to 9.

*channel-name*: Specifies a channel name, which could be a default name or a self-defined name. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to the **info-center channel name** command.

## Description

Use the **info-center console channel** command to specify the channel to output system information to the console.

Use the **undo info-center console channel** command to restore the default output channel to the console.

By default, output of information to the console is enabled with channel 0 as the default channel (known as console).

Note that the **info-center console channel** command takes effect only after the information center is enabled first with the **info-center enable** command.

## Examples

```
# Set channel 0 to output system information to the console.
```

```
<Sysname> system-view  
[Sysname] info-center console channel 0
```

## info-center enable

### Syntax

```
info-center enable
```

```
undo info-center enable
```

### View

```
System view
```

### Default Level

```
2: System level
```

### Parameters

```
None
```

### Description

Use the **info-center enable** command to enable information center.

Use the **undo info-center enable** command to disable the information center.

The system outputs information to the log host or the console only after the information center is enabled first.

By default, the information center is enabled.

## Examples

```
# Enable the information center.
```

```
<Sysname> system-view
[Sysname] info-center enable
% Information center is enabled
```

## info-center logbuffer

### Syntax

```
info-center logbuffer [ channel { channel-number | channel-name } | size buffersize ] *
undo info-center logbuffer [ channel | size ]
```

### View

System view

### Default Level

2: System level

### Parameters

*channel-number*: A specified channel number, in the range 0 to 9.

*channel-name*: Specifies a channel name, which could be a default name or a self-defined name. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to the **info-center channel name** command.

*buffersize*: Specifies the maximum number of log messages that can be stored in a log buffer, in the range 0 to 1,024 with 512 as the default value.

### Description

Use the **info-center logbuffer** command to enable information output to a log buffer and set the corresponding parameters.

Use the **undo info-center logbuffer** command to disable information output to a log buffer.

By default, information is output to the log buffer with the default channel of channel 4 (logbuffer) and the default buffer size of 512.

Note that the **info-center logbuffer** command takes effect only after the information center is enabled with the **info-center enable** command.

### Examples

# Configure the system to output information to the log buffer through channel 4, and set the log buffer size to 50.

```
<Sysname> system-view
[Sysname] info-center logbuffer size 50
```

## info-center loghost

### Syntax

```
info-center loghost host-ip [ channel { channel-number | channel-name } | facility local-number ] *
undo info-center loghost host-ip
```

## View

System view

## Default Level

2: System level

## Parameters

*host-ip*: The IP address of the log host.

**channel**: Specifies the channel through which system information can be output to the log host.

*channel-number*: Specifies a channel number, in the range 0 to 9.

*channel-name*: Specifies a channel name, which could be a default name or a self-defined name. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to the **info-center channel name** command.

**facility local-number**: The logging facility of the log host. The value can be local0 to local7 and defaults to local7. Logging facility is mainly used to mark different logging sources, query and filter the logs of the corresponding log source.

## Description

Use the **info-center loghost** command to specify a log host and to configure the related parameters.

Use the **undo info-center loghost** command to restore the default configurations on a log host.

By default, output of system information to the log host is disabled. When it is enabled, the default channel name will be loghost and the default channel number will be 2.

Note that:

- The **info-center loghost** command takes effect only after the information center is enabled with the **info-center enable** command.
- Ensure to input a correct IP address while using the **info-center loghost** command to configure the IP address for a log host. System will prompt an invalid address if the loopback address (127.0.0.1) is input.
- A maximum number of 4 hosts (different) can be designated as the log host.

## Examples

```
# Output log information to a Unix station with the IP address being 1.1.1.1/16.
```

```
<Sysname> system-view  
[Sysname] info-center loghost 1.1.1.1
```

## info-center loghost source

### Syntax

```
info-center loghost source interface-type interface-number
```

```
undo info-center loghost source
```

### View

System view

## Default Level

2: System level

## Parameters

*interface-type interface-number*: Specifies the egress interface for log information by the interface type and interface number.

## Description

Use the **info-center loghost source** command to specify the source IP address for log information.

Use the **undo info-center loghost source** command to restore the default.

By default, the interface for sending log information is determined by the matched route, and the primary IP address of this interface is the source IP address of the log information.

After the source IP address of log information is specified, no matter the log information is actually output through which physical interface, the source IP address of the log information is the primary IP address of the specified interface. If you want to display the source IP address in the log information, you can configure it by using this command.

Note that:

- The **info-center loghost source** command takes effect only after the information center is enabled with the **info-center enable** command.
- The IP address of the specified source interface must be configured; otherwise, although the **info-center loghost source** command can be configured successfully, the log host will not receive any log information.

## Examples

By default, the log information in the following format is displayed on the log host:

```
<188>Jul 22 05:58:06 2008 Sysname %%10IFNET/4/LINK UPDOWN(1): GigabitEthernet1/0/3: link status is UP
```

# Specify the primary IP address of VLAN-interface1 as the source IP address of log information.

```
<Sysname> system-view
[Sysname] interface Vlan-interface1
[Sysname-Vlan-interface1] ip address 2.2.2.2
[Sysname-Vlan-interface1] quit
[Sysname] info-center loghost source Vlan-interface1
```

After the above configuration, the log information in the following format is displayed on the log host (compared with the default format, the following format has the **-DevIP=2.2.2.2** field):

```
<188>Jul 22 06:11:31 2008 Sysname %%10IFNET/4/LINK UPDOWN(1):-DevIP=2.2.2.2;
GigabitEthernet1/0/3: link status is UP0
```

## info-center monitor channel

### Syntax

**info-center monitor channel** { *channel-number* | *channel-name* }

**undo info-center monitor channel**

## View

System view

## Default Level

2: System level

## Parameters

*channel-number*: Specifies a channel number, in the range 0 to 9.

*channel-name*: Specifies a channel name, which could be a default name or a self-defined name. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to the **info-center channel name** command.

## Description

Use the **info-center monitor channel** command to configure the channel to output system information to the monitor.

Use the **undo info-center monitor channel** command to restore the default channel to output system information to the monitor.

By default, output of system information to the monitor is enabled with a default channel name of monitor and a default channel number of 1.

Note that the **info-center monitor channel** command takes effect only after the information center is enabled with the **info-center enable** command.

## Examples

```
# Output system information to the monitor through channel 0.
```

```
<Sysname> system-view
```

```
[Sysname] info-center monitor channel 0
```

## info-center snmp channel

### Syntax

```
info-center snmp channel { channel-number | channel-name }
```

```
undo info-center snmp channel
```

### View

System view

### Default Level

2: System level

### Parameters

*channel-number*: Specifies a channel number, in the range 0 to 9.

*channel-name*: Specifies a channel name, which could be a default name or a self-defined name. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to the **info-center channel name** command.

## Description

Use the **info-center snmp channel** command to configure the channel to output system information to the SNMP module.

Use the **undo info-center snmp channel** command to restore the default channel to output system information to the SNMP module.

By default, output of system information to the SNMP module is enabled with a default channel name of snmpagent and a default channel number of 5.

For more information, refer to the **display snmp-agent** command in the *SNMP Commands* in the *System Volume*.

## Examples

```
# Output system information to the SNMP module through channel 6.
```

```
<Sysname> system-view
[Sysname] info-center snmp channel 6
```

## info-center source

### Syntax

```
info-center source { module-name | default } channel { channel-number | channel-name } [ debug
{ level severity | state state } * | log { level severity | state state } * | trap { level severity | state state }
* ] *
```

```
undo info-center source { module-name | default } channel { channel-number | channel-name }
```

### View

System view

### Default Level

2: System level

### Parameters

*module-name*: Specifies the output rules of the system information of the specified modules. For instance, if information on ARP module is to be output, you can configure this argument as ARP. You can use the **info-center source ?** command to view the modules supported by the device.

**default**: Specifies the output rules of the system information of all the modules allowed to output the system information, including all the modules displayed by using the **info-center source ?** command.

**debug**: Debugging information.

**log**: Log information.

**trap**: Trap information.

**level severity**: Specifies the severity of system information, refer to [Table 1-4](#) for details. With this keyword, you can specify the severity level of the information allowed/denied to output.

**state state**: Configures whether to output the system information, which could be **on** (enabled) or **off** (disabled). With this keyword, you can specify whether to output the specified system information.

*channel-number*: Specifies a channel number, in the range 0 to 9.

*channel-name*: Specifies a channel name, which could be a default name or a self-defined name. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to the **info-center channel name** command.

## Description

Use the **info-center source** command to specify the output rules of the system information.

Use the **undo info-center source** command to remove the specified output rules.

By default, the output rules for the system information are listed in [Table 1-8](#).

This command can be used to set the filter and redirection rules of log, trap and debugging information.

For example, the user can set to output log information with severity higher than warning to the log host, and information with severity higher than informational to the log buffer. The user can also set to output trap information of the IP module to a specified output destination.

Note that:

- If you do not use the *module-name* argument to set output rules for a module, the module uses the default output rules or the output rules set by the **default** keyword; otherwise the module uses the output rules separately set for it.
- If you use the **default** keyword to set the output rules for all the modules without specifying the **debug**, **log**, and **trap** keywords, the default output rules for the modules are used. Refer to [Table 1-8](#) for details.
- If you use the *module-name* argument to set the output rules for a module without specifying the **debug**, **log**, and **trap** keywords, the default output rules for the module are as follows: the output of log and trap information is enabled, with severity being informational; the output of debugging information is disabled, with severity being debug. For example, if you execute the command **info-center source snmp channel 5**, the command is actually equal to the command **info-center source snmp channel 5 debug level debugging state off log level informational state on trap level informational state on**.
- If you repeatedly use the command to set the output rules for a module or for all the modules with the **default** keyword, the last configured output rules take effect
- After you separately set the output rules for a module, you must use the *module-name* argument to modify or remove the rules. The new configuration by using the **default** keyword is invalid on the module.
- You can configure to output the log, trap and debugging information to the trap buffer, but the trap buffer only receives the trap information and discards the log and debugging information.
- You can configure to output the log, trap and debugging information to the log buffer, but the log buffer only receives the log and debugging information and discards the trap information.
- You can configure to output the log, trap and debugging information to the SNMP module, but the SNMP module only receives the trap information and discards the log and debugging information.

**Table 1-8** Default output rules for different output destinations

Output destination	Modules allowed	LOG		TRAP		DEBUG	
		Enabled/disabled	Severity	Enabled/disabled	Severity	Enabled/disabled	Severity
Console	default (all modules)	Enabled	Warning	Enabled	Debug	Enabled	Debug

Output destination	Modules allowed	LOG		TRAP		DEBUG	
		Enabled/disabled	Severity	Enabled/disabled	Severity	Enabled/disabled	Severity
Monitor terminal	default (all modules)	Enabled	Warning	Enabled	Debug	Enabled	Debug
Log host	default (all modules)	Enabled	Informational	Enabled	Debug	Disabled	Debug
Trap buffer	default (all modules)	Disabled	Informational	Enabled	Warning	Disabled	Debug
Log buffer	default (all modules)	Enabled	Warning	Disabled	Debug	Disabled	Debug
SNMP module	default (all modules)	Disabled	Debug	Enabled	Warning	Disabled	Debug

## Examples

# Set the output channel for the log information of VLAN module to **snmpagent** and to output information with severity being **emergency**. Log information of other modules cannot be output to this channel; other types of information of this module may or may not be output to this channel.

```
<Sysname> system-view
[Sysname] info-center source default channel snmpagent log state off
[Sysname] info-center source vlan channel snmpagent log level emergencies state on
```

# Set the output channel for the log information of VLAN module to **snmpagent** and to output information with severity being **emergency**. Log information of other modules and all the other system information cannot be output to this channel.

```
<Sysname> system-view
[Sysname] info-center source default channel snmpagent debug state off log state off trap state off
[Sysname] info-center source vlan channel snmpagent log level emergencies state on
```

## info-center synchronous

### Syntax

**info-center synchronous**

**undo info-center synchronous**

### View

System view

### Default Level

2: System level

## Parameters

None

## Description

Use the **info-center synchronous** command to enable synchronous information output.

Use the **undo info-center synchronous** command to disable the synchronous information output.

By default, the synchronous information output is disabled.



### Note

- If system information, such as log information, is output before you input any information under a current command line prompt, the system will not display the command line prompt after the system information output.
  - If system information is output when you are inputting some interactive information (non Y/N confirmation information), then after the system information output, the system will not display the command line prompt but your previous input in a new line.
- 

## Examples

# Enable the synchronous information output function, and then input the **display interface gigabitethernet** command to view Ethernet interface information.

```
<Sysname> system-view
[Sysname] info-center synchronous
% Info-center synchronous output is on
[Sysname] display interface gigabitethernet
```

At this time, the system receives log messages, and it then displays the log messages first. After the system displays all the log messages, it displays the user's previous input, which is **display interface gigabitethernet** in this example.

```
%Apr 29 08:12:44:71 2007 Sysname IFNET/4/LINK UPDOWN:
 GigabitEthernet1/0/1: link status is UP
[Sysname] display interface gigabitethernet
```

# Enable the synchronous information output function, and then save the current configuration (input interactive information).

```
<Sysname> system-view
[Sysname] info-center synchronous
% Info-center synchronous output is on
[Sysname] save
The current configuration will be written to the device. Are you sure? [Y/N]:
```

At this time, the system receives the log information, and it then displays the log information first. After the system displays all the log information, it displays the user's previous input, which is [Y/N] in this example.

```
%May 21 14:33:19:425 2007 Sysname SHELL/4/LOGIN: VTY login from 192.168.1.44
[Y/N]:
```

## info-center timestamp

### Syntax

```
info-center timestamp { debugging | log | trap } { boot | date | none }
undo info-center timestamp { debugging | log | trap }
```

### View

System view

### Default Level

2: System level

### Parameters

**debugging**: Sets the timestamp format of the debugging information.

**log**: Sets the timestamp output format of the log information.

**trap**: Sets the timestamp output format of the trap information.

**boot**: The time taken to boot up the system, in the format of xxxxxx.yyyyyy, in which xxxxxx represents the most significant 32 bits of the time taken to boot up the system (in milliseconds) whereas yyyyyy is the least significant 32 bits. For example, 0.21990989 equals Jun 25 14:09:26:881 2007.

**date**: The current system date and time, in the format of "Mmm dd hh:mm:ss:sss yyyy".

- Mmm: The abbreviations of the months in English, which could be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, or Dec.
- dd: The date, starting with a space if less than 10, for example " 7".
- hh:mm:ss:sss: The local time, with hh ranging from 00 to 23, mm and ss ranging from 00 to 59, and sss ranging from 0 to 999.
- yyyy: Represents the year.

**none**: Indicates no time information is provided.

### Description

Use the **info-center timestamp** command to configure the timestamp format.

Use the **undo info-center timestamp** command to restore the default.

By default, the timestamp format of log, trap and debugging information is **date**.

### Examples

# Configure the timestamp format for log information as **boot**.

```
<Sysname> system-view
[Sysname] info-center timestamp log boot
```

At this time, if you execute the **shutdown** command on GigabitEthernet1/0/1 that is in the UP state, the log information generated is as follows:

```
%0.1382605158 Sysname IFNET/4/LINK UPDOWN:
GigabitEthernet1/0/1: link status is DOWN
```

# Configure the timestamp format for log information as **date**.

```
<Sysname> system-view
[Sysname] info-center timestamp log date
```

At this time, if you execute the **shutdown** command on GigabitEthernet1/0/1 that is in the UP state, the log information generated is as follows:

```
%Sep 29 17:19:11:188 2007 Sysname IFNET/4/LINK UPDOWN:  
GigabitEthernet1/0/1: link status is DOWN
```

# Configure the timestamp format for log information as **none**.

```
<Sysname> system-view  
[Sysname] info-center timestamp log none
```

At this time, if you execute the **shutdown** command on GigabitEthernet1/0/1 that is in the UP state, the log information generated is as follows:

```
% Sysname IFNET/4/LINK UPDOWN:  
GigabitEthernet1/0/1: link status is DOWN
```

## info-center timestamp loghost

### Syntax

```
info-center timestamp loghost { date | no-year-date | none }  
undo info-center timestamp loghost
```

### View

System view

### Default Level

2: System level

### Parameters

**date**: Indicates the current system date and time, in the format of "Mmm dd hh:mm:ss:ms yyyy". However, the display format depends on the log host.

**no-year-date**: Indicates the current system date and time (year exclusive).

**none**: Indicates that no time stamp information is provided.

### Description

Use the **info-center timestamp loghost** command to configure the time stamp format of the system information sent to the log host.

Use the **undo info-center timestamp loghost** command to restore the default.

By default, the time stamp format for system information sent to the log host is **date**.

### Examples

# Configure that the system information output to the log host does not include the year information.

```
<Sysname> system-view  
[Sysname] info-center timestamp loghost no-year-date
```

## info-center trapbuffer

### Syntax

```
info-center trapbuffer [ channel { channel-number | channel-name } | size buffersize ] *
```

**undo info-center trapbuffer [ channel | size ]**

## View

System view

## Default Level

2: System level

## Parameters

**size** *buffersize*: Specifies the maximum number of trap messages in a trap buffer, in the range 0 to 1,024 with 256 as the default value.

*channel-number*: Specifies a channel number, in the range 0 to 9.

*channel-name*: Specifies a channel name, which could be a default name or a self-defined name. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to the **info-center channel name** command.

## Description

Use the **info-center trapbuffer** command to enable information output to the trap buffer and set the corresponding parameters.

Use the **undo info-center trapbuffer** command to disable information output to the trap buffer.

By default, information output to the trap buffer is enabled with channel 3 (trapbuffer) as the default channel and a maximum buffer size of 256.

Note that the **info-center trapbuffer** command takes effect only after the information center is enabled with the **info-center enable** command.

## Examples

# Configure the system to output information to the trap buffer through the default channel, and set the trap buffer size to 30.

```
<Sysname> system-view  
[Sysname] info-center trapbuffer size 30
```

## reset logbuffer

### Syntax

**reset logbuffer**

### View

User view

### Default Level

3: Manage level

### Parameters

None

## Description

Use the **reset logbuffer** command to reset the log buffer contents.

## Examples

```
# Reset the log buffer contents.  
<Sysname> reset logbuffer
```

## reset trapbuffer

### Syntax

```
reset trapbuffer
```

### View

User view

### Default Level

3: Manage level

### Parameters

None

## Description

Use the **reset trapbuffer** command to reset the trap buffer contents.

## Examples

```
# Reset the trap buffer contents.  
<Sysname> reset trapbuffer
```

## terminal debugging

### Syntax

```
terminal debugging  
undo terminal debugging
```

### View

User view

### Default Level

1: Monitor level

### Parameters

None

## Description

Use the **terminal debugging** command to enable the display of debugging information on the current terminal.

Use the **undo terminal debugging** command to disable the display of debugging information on the current terminal.

By default, the display of debugging information on the current terminal is disabled.

Note that:

- The debugging information is displayed (using the **terminal debugging** command) only after the monitoring of system information is enabled on the current terminal first (using the **terminal monitor** command).
- The configuration of this command is valid for only the current connection between the terminal and the device. If a new connection is established, the display of debugging information on the terminal restores the default.

## Examples

```
# Enable the display of debugging information on the current terminal.
```

```
<Sysname> terminal debugging
```

```
% Current terminal debugging is on
```

## terminal logging

### Syntax

```
terminal logging
```

```
undo terminal logging
```

### View

```
User view
```

### Default Level

```
1: Monitor level
```

### Parameters

```
None
```

### Description

Use the **terminal logging** command to enable the display of log information on the current terminal.

Use the **undo terminal logging** command to disable the display of log information on the current terminal.

By default, the display of log information on the current terminal is disabled.

Note that:

- The log information is displayed (using the **terminal logging** command) only after the monitoring of system information is enabled on the current terminal first (using the **terminal monitor** command).
- The configuration of this command is valid for only the current connection between the terminal and the device. If a new connection is established, the display of log information on the terminal restores the default.

## Examples

```
# Disable the display of log information on the current terminal.  
<Sysname> undo terminal logging  
% Current terminal logging is off
```

## terminal monitor

### Syntax

```
terminal monitor  
undo terminal monitor
```

### View

User view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **terminal monitor** command to enable the monitoring of system information on the current terminal.

Use the **undo terminal monitor** command to disable the monitoring of system information on the current terminal.

By default, monitoring of the system information on the console is enabled and that on the monitor terminal is disabled.

Note that:

- You need to configure the **terminal monitor** command before you can display the log, trap, and debugging information.
- Configuration of the **undo terminal monitor** command automatically disables the monitoring of log, trap, and debugging information.
- The configuration of this command is valid for only the current connection between the terminal and the device. If a new connection is established, the monitoring of system information on the terminal restores the default.

## Examples

```
# Enable the monitoring of system information on the current terminal.  
<Sysname> terminal monitor  
% Current terminal monitor is on
```

## terminal trapping

### Syntax

```
terminal trapping
```

## undo terminal trapping

### View

User view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **terminal trapping** command to enable the display of trap information on the current terminal.

Use the **undo terminal trapping** command to disable the display of trap information on the current terminal.

By default, the display of trap information on the current terminal is enabled.

Note that:

- The trap information is displayed (using the **terminal trapping** command) only after the monitoring of system information is enabled on the current terminal first (using the **terminal monitor** command).
- The configuration of this command is valid for only the current connection between the terminal and the device. If a new connection is established, the display of trap information on the terminal restores the default.

### Examples

```
# Enable the display of trap information on the current terminal.
```

```
<Sysname> terminal trapping
```

```
% Current terminal trapping is on
```

# Table of Contents

<b>1 PoE Configuration Commands</b> .....	<b>1-1</b>
PoE Configuration Commands .....	1-1
apply poe-profile .....	1-1
apply poe-profile interface .....	1-2
display poe device .....	1-2
display poe interface .....	1-3
display poe interface power .....	1-6
display poe pse .....	1-8
display poe pse interface .....	1-9
display poe pse interface power .....	1-10
display poe-profile .....	1-11
display poe-profile interface .....	1-14
poe disconnect .....	1-15
poe enable .....	1-15
poe legacy enable .....	1-16
poe max-power .....	1-17
poe mode .....	1-17
poe pd-description .....	1-18
poe pd-policy priority .....	1-19
poe priority .....	1-19
poe update .....	1-20
poe utilization-threshold .....	1-21
poe-profile .....	1-22

# 1 PoE Configuration Commands

---

## PoE Configuration Commands

### apply poe-profile

#### Syntax

```
apply poe-profile { index index | name profile-name }  
undo apply poe-profile { index index | name profile-name }
```

#### View

PoE interface view

#### Default Level

2: System level

#### Parameters

**index** *index*: Index number of the PoE configuration file, in the range 1 to 100.

**name** *profile-name*: Name of the PoE configuration file, a string of 1 to 15 characters.

#### Description

Use the **apply poe-profile** command to apply the PoE configuration file to the current PoE interface.

Use the **undo apply poe-profile** command to remove the application of the PoE configuration file to the current PoE interface.

Note that the index number, instead of the name, of the PoE configuration file is displayed when you execute the **display this** command.

Related commands: **display poe-profile**, **apply poe-profile interface**.

#### Examples

# Apply the PoE configuration file named **A20** to the PoE interface GigabitEthernet 1/0/1.

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] apply poe-profile name A20  
[Sysname-GigabitEthernet1/0/1] display this  
#  
interface GigabitEthernet1/0/1  
port link-mode route  
apply poe-profile index 1  
#
```

## apply poe-profile interface

### Syntax

```
apply poe-profile { index index | name profile-name } interface interface-range  
undo apply poe-profile { index index | name profile-name } interface interface-range
```

### View

System view

### Default Level

2: System level

### Parameters

**index** *index*: Index number of the PoE configuration file, in the range 1 to 100.

**name** *profile-name*: Name of the PoE configuration file, a string of 1 to 15 characters.

*interface-range*: Range of Ethernet interface numbers, indicating multiple Ethernet interfaces. The expression is *interface-range* = *interface-type interface-number* [ **to** *interface-type interface-number* ], where *interface-type interface-number* represents the interface type and interface number. The start interface number should be smaller than the end interface number. Ethernet interface numbers can be in any range. If any interface in the specified range does not support PoE, it is ignored when the PoE configuration file is applied.

### Description

Use the **apply poe-profile interface** command to apply the PoE configuration file to one or more PoE interfaces.

Use the **undo apply poe-profile interface** command to remove the application of the PoE configuration file to the specified PoE interface(s).

Related commands: **display poe-profile interface**, **apply poe-profile**.

### Examples

```
# Apply the PoE configuration file named ABC to the PoE interface GigabitEthernet 1/0/1.
```

```
<Sysname> system-view  
[Sysname] apply poe-profile name ABC interface gigabitethernet 1/0/1
```

```
# Apply the indexed PoE configuration file to PoE interfaces GigabitEthernet 1/0/2 through GigabitEthernet 1/0/8.
```

```
<Sysname> system-view  
[Sysname] apply poe-profile index 5 interface gigabitethernet 1/0/2 to gigabitethernet 1/0/8
```

## display poe device

### Syntax

```
display poe device
```

### View

Any view

## Default Level

1: Monitor level

## Parameters

None

## Description

Use the **display poe device** command to display the mapping between ID, module, and member ID of all the power sourcing equipments (PSEs).

## Examples

# Display the mapping between ID, module, and member ID of each PSE.

```
<Sysname> display poe device
```

```
PSE ID  SlotNo  SubSNo  PortNum  MaxPower(W)  State  Model
5       4       0       24       200           on    LSP1POEA
6       5       0       16       200           on    LSP1POEA
```

**Table 1-1** display poe device command output description

Field	Description
PSE ID	ID of the PSE
SlotNo	Member ID number of the PSE
SubSNo	SubSlot number of the PSE
PortNum	Number of PoE interfaces on the PSE
MaxPower(W)	Maximum power of the PSE (W)
State	PSE state: on: The PSE is supplying power. off: The PSE stops supplying power. faulty: The PSE fails.
Model	PSE model

## display poe interface

### Syntax

```
display poe interface [ interface-type interface-number ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*interface-type interface-number*: Specifies an interface by its type and number.

## Description

Use the **display poe interface** command to display the power information of the specified interface. If no interface is specified, the power information of all PoE interfaces is displayed.

## Examples

# Display the power state of GigabitEthernet 1/0/1.

```
<Sysname> display poe interface gigabitethernet 1/0/1
Port Power Enabled           : enable
Port Power Priority          : critical
Port Operating Status       : on
Port IEEE Class             : 1
Port Detection Status       : delivering-power
Port Power Mode             : signal
Port Current Power          : 11592    mW
Port Average Power          : 11610    mW
Port Peak Power             : 11684    mW
Port Max Power              : 15400    mW
Port Current                : 244      mA
Port Voltage                : 51.7     V
Port PD Description         : IP Phone For Room 101
```

**Table 1-2** display poe interface ethernet command output description

Field	Description
Port Power Enabled	PoE state: enabled/disabled <ul style="list-style-type: none"><li>enable: PoE is enabled.</li><li>disable: PoE is disabled.</li></ul>
Port Power Priority	Power priority of the PoE interface: <ul style="list-style-type: none"><li>critical (highest)</li><li>high</li><li>low</li></ul>
Port Operating Status	Operating state of a PoE interface: <ul style="list-style-type: none"><li>off: PoE is disabled.</li><li>on: Power is supplied for a PoE interface normally.</li><li>power lack: The guaranteed remaining power of the PSE is not high enough to supply power for a critical PoE interface.</li><li>power-deny: The PSE refuses to supply power. The power required by the powered device (PD) is higher than the configured power.</li><li>power-itself: The external equipment is supplying power for itself.</li><li>power-limit: The PSE is supplying a limited power. The power required by the PD is higher than the configured power and the PSE still supplies the configured power.</li></ul> Port operating status varies with devices.
Port IEEE class	PD power class: 0, 1, 2, 3, 4, and - - indicates not supported.

Field	Description
Port Detection Status	<p>Power detection state of a PoE interface:</p> <ul style="list-style-type: none"> <li>disabled: The PoE function is disabled.</li> <li>searching: The PoE interface is searching for the PD.</li> <li>delivering-power: The PoE interface is supplying power for the PD.</li> <li>fault: There is a fault defined in 802.3af.</li> <li>test: The PoE interface is under test.</li> <li>other-fault: There is a fault other than defined in 802.3af.</li> <li>pd-disconnect: The PD is disconnected.</li> </ul> <p>Port detection status varies with devices.</p>
Port Power Mode	<p>Power mode of a PoE interface:</p> <ul style="list-style-type: none"> <li>signal: Power is supplied over signal cables.</li> <li>spare: Power is supplied over spare cables.</li> </ul> <p>3Com Switch 4800G only support for signal mode.</p>
Port Current Power	<p>Current power of a PoE interface, including PD consumption power and transmission loss</p> <p>The transmission loss usually does not exceed one watt. The specific loss varies with devices.</p>
Port Average Power	Average power of a PoE interface
Port Peak Power	Peak power of a PoE interface
Port Max Power	Maximum power of a PoE interface
Port Current	Current of a PoE interface
Port Voltage	Voltage of a PoE interface
Port PD Description	Description of the PD connected to the PoE interface, which is used to identify the type and location of the PD.

# Display the state of all PoE interfaces.

```
<Sysname> display poe interface
```

```

Interface  Enable   Priority  CurPower  Operating  IEEE  Detection
          (W)      Status   class    Status
GE1/1     enable  low      4.4       on         1     delivering-power
GE1/2     enable  critical 0         on         -     disabled
GE1/3     enable  low      0         on         -     disabled
GE1/4     enable  critical 0         on         -     searching
GE1/5     enable  low      4.0       on         2     delivering-power
GE1/6     enable  low      0         on         -     disabled
GE1/7     disable low      0         off        -     fault
GE1/8     disable low      0         off        -     disabled
GE1/9     disable low      0         off        -     disabled
GE1/10    disable low      0         off        -     disabled
GE1/11    disable low      0         off        -     disabled
GE1/12    disable low      0         off        -     disabled

```

```
--- 2 port(s) on, 8.4(W) consumed, 171.6(W) Remaining ---
```

**Table 1-3 display poe interface** command output description

Field	Description
Interface	Shortened form of a PoE interface
Enable	PoE state: enabled/disabled <ul style="list-style-type: none"> <li>enable: PoE is enabled.</li> <li>disable: PoE is disabled.</li> </ul>
Priority	Power priority of a PoE interface: <ul style="list-style-type: none"> <li>critical (highest)</li> <li>high</li> <li>low</li> </ul>
CurPower	Current power of a PoE interface
Operating Status	Operating state of a PoE interface <ul style="list-style-type: none"> <li>off: PoE is disabled.</li> <li>on: Power is supplied for a PoE interface normally.</li> <li>power lack: The guaranteed remaining power of the PSE is not high enough to supply power for a critical PoE interface.</li> <li>power-deny: The PSE refuses to supply power. The power required by the powered device (PD) is higher than the configured power.</li> <li>power-itself: The external equipment is supplying power for itself.</li> <li>power-limit: The PSE is supplying a limited power. The power required by the PD is higher than the configured power and the PSE still supplies the configured power.</li> </ul> Port operation status varies with devices.
IEEE class	PD power class defined by IEEE
Detection Status	Power detection state of a PoE interface: <ul style="list-style-type: none"> <li>disabled: The PoE function is disabled.</li> <li>searching: The PoE interface is searching for the PD.</li> <li>delivering-power: The PoE interface is supplying power for the PD.</li> <li>fault: There is a fault defined in 802.3af.</li> <li>test: The PoE interface is under test.</li> <li>There is a fault other than defined in 802.3af.</li> <li>pd-disconnect: The PD is disconnected.</li> </ul> Power detection state varies with devices.
port(s) on	Number of PoE interfaces that are supplying power
consumed	Power consumed by the current PoE interface
Remaining	Total remaining power of the system

## display poe interface power

### Syntax

```
display poe interface power [ interface-type interface-number ]
```

### View

Any view

## Default Level

1: Monitor level

## Parameters

*interface-type interface-number*: Specifies an interface by its type and number.

## Description

Use the **display poe interface power** command to display the power information of a PoE interface(s).

If no interface is specified, the power information of all PoE interfaces will be displayed.

## Examples

# Display the power information of GigabitEthernet 1/0/1.

```
<Sysname> display poe interface power gigabitethernet 1/0/1
Interface  CurPower  PeakPower  MaxPower  PD Description
          (W)         (W)         (W)
Eth1/1    15.0        15.3        15.4      Access Point on Room 509 for Peter
```

# Display the power information of all PoE interfaces.

```
<Sysname> display poe interface power
Interface  CurPower  PeakPower  MaxPower  PD Description
          (W)         (W)         (W)
GE1/0/25   4.4        4.5        4.6       IP Phone on Room 309 for Peter Smith
GE1/0/26   4.4        4.5        15.4      IP Phone on Room 409 for Peter Pan
GE1/0/27   15.0       15.3       15.4      Access Point on Room 509 for Peter
GE1/0/28   0          0          0         IP Phone on Room 609 for Peter John
GE1/0/29   0          0          0         IP Phone on Room 709 for Jack
GE1/0/30   0          0          0         IP Phone on Room 809 for Alien
```

```
--- 3 port(s) on, 23.8(W) consumed, 776.2(W) Remaining ---
```

**Table 1-4 display poe interface power** command output description

Field	Description
Interface	Shortened form of a PoE interface
CurPower	Current power of a PoE interface
PeakPower	Peak power of a PoE interface
MaxPower	Maximum power of a PoE interface
PD Description	Description of the PD connected with a PoE interface When the description contains more than 34 characters, the first 30 characters followed by four dots are displayed.
port(s) on	Number of PoE interfaces that are supplying power
consumed	Power currently consumed by all PoE interfaces
Remaining	Total remaining power of the system

## display poe pse

### Syntax

```
display poe pse [ pse-id ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*pse-id*: PSE ID. You can use the **display poe device** command to view the mapping between PSE ID and member ID. If you enter a PSE ID, the information of the PSE is displayed. Otherwise, the information of all PSEs on the device is displayed.

### Description

Use the **display poe pse** command to display the information of the specified PSE.

### Examples

```
# Display the information of PSE 6.
```

```
<Sysname> display poe pse 6
PSE ID                : 6
PSE Slot No           : 5
PSE Model              : LSBMPOEGV48TP
PSE Power Enabled     : enable
PSE Power Preempted   : no
PSE Power Priority     : low
PSE Current Power     : 130      W
PSE Average Power     : 20       W
PSE Peak Power        : 240      W
PSE Max Power         : 200      W
PSE Remaining Guaranteed : 120    W
PSE CPLD Version      : 100
PSE Software Version  : 200
PSE Hardware Version  : 100
PSE Legacy Detection  : disable
PSE Utilization-threshold : 80
PSE Pd-policy Mode    : disable
PSE PD Disconnect Detect Mode : DC
```

**Table 1-5 display poe pse** command output description

Field	Description
PSE ID	ID of the PSE
PSE Slot No	Member ID number of the PSE
PSE Model	Model of the PSE module

Field	Description
PSE Power Enabled	PoE is enabled for the PSE
PSE Power Preempted	PSE power preempted state <ul style="list-style-type: none"> <li>no: The power of the PSE is not preempted.</li> <li>yes: The power of the PSE is preempted so that it cannot supply power, although PoE is enabled for the PSE</li> </ul>
PSE Power Priority	Power priority of the PSE
PSE Current Power	Current power of the PSE
PSE Average Power	Average power of the PSE
PSE Peak Power	Peak power of the PSE
PSE Max Power	Maximum power of the PSE
PSE Remaining Guaranteed	Guaranteed remaining power of the PSE = Maximum power of the PSE– the sum of the maximum power of the critical PoE interfaces of the PSE
PSE CPLD Version	PSE CPLD version
PSE Software Version	PSE software version number
PSE Hardware Version	PSE hardware version number
PSE Legacy Detection	Nonstandard PD detection by the PSE: <ul style="list-style-type: none"> <li>enable: Enabled</li> <li>disable: Disabled</li> </ul>
PSE Utilization-threshold	PSE power alarm threshold
PSE Pd-policy Mode	PD power management policy mode
PSE PD Disconnect Detect Mode	PD disconnection detection mode

## display poe pse interface

### Syntax

**display poe pse** *pse-id* **interface**

### View

Any view

### Default Level

1: Monitor level

### Parameters

**pse** *pse-id*: Specifies a PSE ID. You can use the **display poe device** command to view the mapping between PSE ID and member ID.

### Description

Use the **display poe pse interface** command to display the state of all PoE interfaces connected to the specified PSE.

## Examples

# Display the state of all PoE interfaces connected to PSE 1.

```
<Sysname> display poe pse 1 interface
```

Interface	Enable	Priority	CurPower (W)	Operating Status	IEEE class	Detection Status
GE1/1	enable	low	4.4	on	1	delivering-power
GE1/2	enable	critical	0	power-lack	-	disabled
GE1/3	enable	low	0	power-deny	-	disabled
GE1/4	enable	critical	0	on	-	searching
GE1/5	enable	low	4.0	power-limit	2	delivering-power
GE1/6	enable	low	0	power-itself	-	disabled
GE1/7	disable	low	0	off	-	fault
GE1/8	disable	low	0	off	-	disabled
GE1/9	disable	low	0	off	-	disabled
GE1/10	disable	low	0	off	-	disabled
GE1/11	disable	low	0	off	-	disabled
GE1/12	disable	low	0	off	-	disabled

```
--- 2 port(s) on, 8.4(W) consumed, 171.6(W) Remaining ---
```

**Table 1-6 display poe pse interface** command output description

Field	Description
Interface	Shortened form of a PoE interface
Enable	PoE enabled/disabled state. For the value, see <a href="#">Table 1-2</a> .
Priority	Priority of a PoE interface. For the value, see <a href="#">Table 1-2</a> .
CurPower	Current power of a PoE interface
Operating	Operating state of a PoE interface. For the value, see <a href="#">Table 1-2</a> .
IEEE	PD power class
Detection	Power detection state of a PoE interface. For the value, see <a href="#">Table 1-2</a> .
port(s) on	Number of PoE interfaces that are supplying power
consumed	Power consumed by PoE interfaces on the PSE
Remaining	Remaining power on the PSE

## display poe pse interface power

### Syntax

```
display poe pse pse-id interface power
```

### View

Any view

## Default Level

1: Monitor level

## Parameters

**pse** *pse-id*: Specifies a PSE ID. You can use the **display poe device** command to view the mapping between PSE ID and member ID.

## Description

Use the **display poe pse interface power** command to display the power information of PoE interfaces connected with the PSE.

## Examples

# Display the power information of PoE interfaces connected with PSE 1.

```
<Sysname> display poe pse 1 interface power
Interface  CurPower  PeakPower  MaxPower  PD Description
          (W)      (W)        (W)
GE1/0/25   4.4        4.5        4.6       IP Phone on Room 309 for Peter Smith
GE1/0/26   4.4        4.5        15.4      IP Phone on Room 409 for Peter Pan
GE1/0/27   15.0       15.3       15.4      Access Point on Room 509 for Peter
GE1/0/28   0          0          5         IP Phone on Room 609 for Peter John
GE1/0/29   0          0          4         IP Phone on Room 709 for Jack
GE1/0/30   0          0          5         IP Phone on Room 809 for Alien

--- 3 port(s) on, 23.8(W) consumed, 776.2(W) Remaining ---
```

**Table 1-7** display poe pse interface power command output description

Field	Description
Interface	Shortened form of a PoE interface
CurPower	Current power of a PoE interface
PeakPower	Peak power of a PoE interface
MaxPower	Maximum power of a PoE interface
PD Description	Description of the PD connected with a PoE interface. When the description contains more than 34 characters, the first 30 characters followed by four dots are displayed.
port(s) on	Number of PoE interfaces that are supplying power
consumed	Power currently consumed by all PoE interfaces
Remaining	Remaining power on the PSE

## display poe-profile

### Syntax

```
display poe-profile [ index index | name profile-name ]
```

## View

Any view

## Default Level

1: Monitor level

## Parameters

**index** *index*: Index number of the PoE configuration file, in the range 1 to 100.

**name** *profile-name*: Name of the PoE configuration file, a string of 1 to 15 characters.

## Description

Use the **display poe-profile** command to display all information of the configurations and applications of the PoE configuration file.

If no argument is specified, all information of the configurations and applications of existing PoE configuration files is displayed.

## Examples

# Display all information of the configurations and applications of the current PoE configuration file.

```
<Sysname> display poe-profile
Poe-profile      Index  ApplyNum  Interface  Configuration
AA3456789012345  1      3          GE1/1      poe enable
                  GE1/2      poe priority critical
                  GE1/3
poe-profileAA    2      1          GE1/24     poe enable
                  poe max-power 12300
poe-profileBB    3      0          poe enable
                  poe priority critical
                  poe max-power 15400

--- 3 poe-profile(s) created, 4 port(s) applied ---
```

**Table 1-8 display poe-profile** command output description

Field	Description
Poe-profile	Name of the PoE configuration file
Index	Index number of the PoE configuration file
ApplyNum	Number of PoE interfaces to which a PoE configuration file is applied
Interface	Shortened form of the PoE interface to which the PoE configuration is applied
Configuration	Configurations of the PoE configuration file
poe-profile(s) created	Number of PoE configuration files
port(s) applied	Sum of the number of PoE interfaces to which all PoE configuration files are respectively applied

# Display all information of the configurations and applications of the PoE configuration file whose index number is 1.

```
<Sysname> display poe-profile index 1
Poe-profile      Index  ApplyNum  Interface  Configuration
AA3456789012345  1      2          GE1/2      poe enable
                                     GE1/24     poe priority critical
                                               poe max-power 12300

--- 2 port(s) applied ---
```

**Table 1-9 display poe-profile index** command output description

Field	Description
Poe-profile	Name of the PoE configuration file
Index	Index number of the PoE configuration file
ApplyNum	Number of PoE interfaces to which a PoE configuration file is applied
Interface	Shortened form of the PoE interface to which the PoE configuration is applied
Configuration	Configurations of the PoE configuration file
port(s) applied	Sum of the number of PoE interfaces to which all PoE configuration files are respectively applied

# Display all information of the configurations and applications of the PoE configuration file named **AA**.

```
<Sysname> display poe-profile name AA
Poe-profile      Index  ApplyNum  Interface  Configuration
AA               1      2          GE1/1      poe enable
                                     GE1/2      poe priority critical
                                               poe max-power 12300

--- 2 port(s) applied ---
```

**Table 1-10 display poe-profile name** command output description

Field	Description
Poe-profile	Name of the PoE configuration file
Index	Index number of the PoE configuration file
ApplyNum	Number of PoE interfaces to which a PoE configuration file is applied
Interface	Shortened form of the PoE interface to which the PoE configuration is applied
Configuration	Configurations of the PoE configuration file
port(s) applied	Sum of the number of PoE interfaces to which all PoE configuration files are respectively applied

## display poe-profile interface

### Syntax

**display poe-profile interface** *interface-type interface-number*

### View

Any view

### Default Level

1: Monitor level

### Parameters

*interface-type interface-number*. Specifies an interface by its type and number.

### Description

Use the **display poe-profile interface** command to display all information of the configurations and applications of the PoE configuration file that currently takes effect on the specified PoE interface.

### Examples

# Display all information of the configurations and applications of the current PoE configuration file applied to GigabitEthernet 1/0/1.

```
<Sysname> display poe-profile interface gigabitethernet 1/0/1
Poe-profile      Index  ApplyNum  Interface  Current Configuration
AA3456789012345  1      2          GE1/2      poe enable
                                     poe priority critical
```

**Table 1-11** display poe-profile interface command output description

Field	Description
Poe-profile	Name of the PoE configuration file
Index	Index number of the PoE configuration file
ApplyNum	Number of PoE interfaces to which the PoE configuration file is applied
Interface	Shortened form of the PoE interface to which the PoE configuration is applied
Current Configuration	Configurations of the PoE configuration file that currently take effect on a PoE interface



### Note

Because not all the configurations of a PoE configuration file can be applied successfully, only the configurations that currently take effect on the interface are displayed.

## **poe disconnect**

### **Syntax**

```
poe disconnect { ac | dc }  
undo poe disconnect
```

### **View**

System view

### **Default Level**

2: System level

### **Parameters**

**ac**: Specifies the PD disconnection detection mode as **ac**.

**dc**: Specifies the PD disconnection detection mode as **dc**.

### **Description**

Use the **poe disconnect** command to configure a PD disconnection detection mode.

Use the **undo poe disconnect** command to restore the default.

The default PD disconnection detection mode varies with devices.

Note that change to the PD disconnection detection mode may lead to power-off of some PDs.

### **Examples**

```
# Set the PD disconnection detection mode to dc.
```

```
<Sysname> system-view  
[Sysname] poe disconnect dc
```

## **poe enable**

### **Syntax**

```
poe enable  
undo poe enable
```

### **View**

PoE interface view, PoE-profile file view

### **Default Level**

2: System level

### **Parameters**

None

### **Description**

Use the **poe enable** command to enable PoE on a PoE interface.

Use the **undo poe enable** command to disable PoE on a PoE interface.

By default, PoE is disabled on a PoE interface.

---

### Caution

- If a PoE configuration file is already applied to a PoE interface, you need to remove the application of the file to the PoE interface before configuring the interface in PoE-profile view.
  - If a PoE configuration file is applied to a PoE interface, you need to remove the application of the file to the PoE interface before configuring the interface in PoE interface view.
- 

## Examples

# Enable PoE on a PoE interface.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe enable
```

# Enable PoE on a PoE interface through a PoE configuration file.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe enable
[Sysname-poe-profile-abc-1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] apply poe-profile name abc
```

## poe legacy enable

### Syntax

```
poe legacy enable pse pse-id
undo poe legacy enable pse pse-id
```

### View

System view

### Default Level

2: System level

### Parameters

**pse** *pse-id*: Specifies a PSE ID.

### Description

Use the **poe legacy enable** command to enable the PSE to detect nonstandard PDs.

Use the **undo poe legacy enable** command to disable the PSE from detecting nonstandard PDs.

By default, the PSE is disabled from detecting nonstandard PDs.

## Examples

```
# Enable PSE 2 to detect nonstandard PDs.
<Sysname> system-view
[Sysname] poe legacy enable pse 2
```

## poe max-power

### Syntax

```
poe max-power max-power
undo poe max-power
```

### View

PoE interface view, PoE-profile file view

### Default Level

2: System level

### Parameters

*max-power*: Maximum power in milliwatts allocated to a PoE interface. The range of this argument varies with devices.

### Description

Use the **poe max-power** command to configure the maximum power for a PoE interface.

Use the **undo poe max-power** command to restore the default.

By default, the maximum power of the PoE interface is 15,400 milliwatts.

## Examples

```
# Set the maximum power of GigabitEthernet 1/0/1 to 12,000 milliwatts.
```

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe max-power 12000
```

```
# Set the maximum power of GigabitEthernet 1/0/1 to 12,000 milliwatts through a PoE configuration file.
```

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe max-power 12000
[Sysname-poe-profile-abc-1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] apply poe-profile name abc
```

## poe mode

### Syntax

```
poe mode signal
undo poe mode
```

## View

PoE interface view, PoE-profile file view

## Default Level

2: System level

## Parameters

**signal**: Specifies the PoE mode as **signal** (power over signal cables).

## Description

Use the **poe mode** command to configure a PoE mode.

Use the **undo poe mode** command to restore the default.

By default, the PoE mode is **signal** (power over signal cables).

The PSE supplies power for a PoE interface in the following two modes: **signal** and **spare**.

- In the signal mode, lines in Category 3 and 5 twisted pair cables used for transmitting data are also used for supplying DC power.
- In the spare mode, lines in Category 3 and 5 twisted pair cables not in use are used for supplying DC power.
- 3Com Switch 4800G only support for signal mode.

## Examples

# Set the PoE mode to **signal** (power over signal cables).

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe mode signal
```

# Set the PoE mode to **signal** (power over signal cables) through a PoE configuration file.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe mode signal
[Sysname-poe-profile-abc-1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] apply poe-profile name abc
```

## poe pd-description

### Syntax

**poe pd-description** *string*

**undo poe pd-description**

### View

PoE interface view

### Default Level

2: System level

## Parameters

*string*: Description of the PD connected to a PoE interface, a string of 1 to 80 characters.

## Description

Use the **poe pd-description** command to configure a description for the PD connected to a PoE interface.

Use the **undo poe pd-description** command to restore the default.

By default, no description is available for the PD connected to a PoE interface.

## Examples

# Configure the description for the PD connected to GigabitEthernet 1/0/1 as IP Phone for Room 101.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe pd-description IP Phone For Room 101
```

## poe pd-policy priority

### Syntax

```
poe pd-policy priority
undo poe pd-policy priority
```

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **poe pd-policy priority** command to configure a PD power management priority policy.

Use the **undo poe pd-policy priority** command to remove the PD power management priority policy.

By default, no PD power management priority policy is configured.

### Examples

# Configure a PD power management priority policy

```
<Sysname> system-view
[Sysname] poe pd-policy priority
```

## poe priority

### Syntax

```
poe priority { critical | high | low }
undo poe priority
```

## View

PoE interface view, PoE-profile file view

## Default Level

2: System level

## Parameters

**critical**: Sets the power priority of a PoE interface to **critical**. The PoE interface whose power priority level is **critical** works in guaranteed mode, that is, power is first supplied to the PD connected to this critical PoE interface.

**high**: Sets the power priority of a PoE interface to **high**.

**low**: Sets the power priority of a PoE interface to **low**.

## Description

Use the **poe priority** command to configure a power priority level for a PoE interface.

Use the **undo poe priority** command to restore the default.

By default, the power priority of a PoE interface is **low**.

Note that:

- When the PoE power is insufficient, power is first supplied to PoE interfaces with a higher priority level.
- If a PoE configuration file is already applied to a PoE interface, you need to remove the application of the file to the PoE interface before configuring the interface in PoE-profile view.
- If a PoE configuration file is applied to a PoE interface, you need to remove the application of the file to the PoE interface before configuring the interface in PoE interface view.
- If two PoE interfaces have the same priority level, the PoE interface with a smaller ID has the higher priority level.

## Examples

# Set the power priority of GigabitEthernet 1/0/1 to **critical**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe priority critical
```

# Set the power priority of GigabitEthernet 1/0/1 to **critical** through a PoE configuration file.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe priority critical
[Sysname-poe-profile-abc-1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] apply poe-profile name abc
```

## poe update

### Syntax

**poe update** { **full** | **refresh** } *filename* **pse** *pse-id*

## View

System view

## Default Level

2: System level

## Parameters

**full**: Specifies to upgrade the PSE processing software in full mode when the software is unavailable.

**refresh**: Specifies to upgrade the PSE processing software in refresh mode when the software is available.

**filename**: Name of the upgrade file, a string of 1 to 64 characters. This file must be under the root directory of the file system of the device. The extension of the upgrade file varies with devices.

**pse *pse-id***: Specifies a PSE ID.

## Description

Use the **poe update** command to upgrade the PSE processing software online.



### Caution

- The **full** mode is used only in the case that anomalies occur when you use the **refresh** mode to upgrade the PSE processing software. Do not use the full mode in other circumstances.
  - You can use the **full** mode to upgrade the PSE processing software to restore the PSE firmware when the the PSE processing software is unavailable (it means that none of the PoE commands are executed successfully).
- 

## Examples

# Upgrade the processing software of PSE 2 online.

```
<Sysname> system-view
```

```
[Sysname] poe update refresh 0400_001.S19 pse 2
```

```
This command will refresh firmware on the specific PSE(s), Continue? [Y/N]:y
```

```
System is downloading firmware into the hardware. Please wait .....
```

```
.....
```

```
.....
```

```
Refresh firmware on the specific PSE(s) successfully!
```

## poe utilization-threshold

### Syntax

**poe utilization-threshold** *utilization-threshold-value* **pse** *pse-id*

**undo poe utilization-threshold** **pse** *pse-id*

### View

System view

## Default Level

2: System level

## Parameters

*utilization-threshold-value*: Power alarm threshold in percentage, in the range 1 to 99.

**pse** *pse-id*: Specifies a PSE ID.

## Description

Use the **poe utilization-threshold** command to configure a power alarm threshold for the PSE.

Use the **undo poe utilization-threshold** command to restore the default power alarm threshold of the PSE.

By default, the power alarm threshold for the PSE is 80%.

The system sends a Trap message when the percentage of power utilization exceeds the alarm threshold. If the percentage of the power utilization always keeps above the alarm threshold, the system does not send any Trap message. Instead, when the percentage of the power utilization drops below the alarm threshold, the system sends a Trap message again.

## Examples

```
# Set the power alarm threshold of PSE 2 to 90%.
```

```
<Sysname> system-view  
[Sysname] poe utilization-threshold 90 pse 2
```

## poe-profile

### Syntax

```
poe-profile profile-name [ index ]  
undo poe-profile { index index | name profile-name }
```

### View

System view

### Default Level

2: System level

### Parameters

*profile-name*: Name of a PoE configuration file, a string of 1 to 15 characters. A PoE configuration file name begins with a letter (a through z or A through Z) and must not contain reserved keywords such as **undo**, **all**, **name**, **interface**, **user**, **poe**, **disable**, **max-power**, **mode**, **priority** and **enable**.

*index*: Index number of a PoE configuration file, in the range 1 to 100.

### Description

Use the **poe-profile** *profile-name* command to create a PoE configuration file and enter PoE-profile view.

Use the **undo poe-profile** command to delete the specified PoE configuration file.

If no index is specified, the system automatically assigns an index to the PoE configuration file, starting from 1.

Note that if a PoE configuration file is already applied to a PoE interface, you cannot delete it. To delete the file, you must first execute the **undo apply poe-profile** command to remove the application of the PoE configuration file to the PoE interface.

### Examples

# Create a PoE configuration file, name it **abc**, and specify the index number as **3**.

```
<Sysname> system-view  
[Sysname] poe-profile abc 3
```

# Table of Contents

<b>1 Track Configuration Commands</b> .....	<b>1-1</b>
Track Configuration Commands .....	1-1
display track.....	1-1
track bfd echo .....	1-2
track nqa.....	1-3

# 1 Track Configuration Commands

---

## Track Configuration Commands

### display track

#### Syntax

```
display track { track-entry-number | all }
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

*track-entry-number*: Displays information about the specified Track object, in the range 1 to 1024.

**all**: Displays information about all the Track objects.

#### Description

Use the **display track** command to display Track object information.

#### Examples

# Display information about all the Track objects.

```
<Sysname> display track all
Track ID: 1
  Status: Positive
  Reference Object:
    NQA Entry: admin test
    Reaction: 10
Track ID: 2
  Status: Invalid
  Reference Object:
    BFD Session:
    Packet type: Echo
    Interface   : vlan-interface2
    Remote IP   : 192.168.40.1
    Local IP    : 192.168.40.2
```

**Table 1-1 display track command output description**

Field	Description
Track ID	ID of a Track object
Status	Status of a Track object: <ul style="list-style-type: none"><li>• Positive: The Track object is normal.</li><li>• Invalid: The Track object is invalid.</li><li>• Negative: The Track object is abnormal.</li></ul>
Reference Object	The objects referenced by the Track object
NQA Entry	The NQA test group referenced by the Track object
Reaction	The Reaction entry referenced by the Track object
BFD session	Information about the BFD object associated with the Track object
Packet type	Type of the BFD packet, which can only be Echo currently.
Interface	Outgoing interface of BFD echo packets
Remote IP	Remote IP address of the BFD echo packets
Local IP	Local IP address of the BFD echo packets

## track bfd echo

### Syntax

```
track track-entry-number bfd echo interface interface-type interface-number remote ip remote-ip  
local ip local-ip  
undo track track-entry-number
```

### View

System view

### Default Level

2: System level

### Parameters

*track-entry-number*: Track object ID, in the range 1 to 1024.

**interface** *interface-type interface-number*: Specifies the outgoing interface for BFD echo packets. *interface-type interface-number* represents the interface type and interface number.

**remote ip** *remote-ip*: Specifies the remote IP address of the BFD echo packets.

**local ip** *local-ip*: Specifies the local IP address of the BFD echo packets.

### Description

Use the **track bfd echo** command to create the Track object associated with the BFD session, and specify to use echo packets in BFD probes.

Use the **undo track** command to remove the created Track object.

By default, no Track object is associated with BFD session.

## Examples

# Create Track object 1 to associate it with BFD session, which makes a probe using echo packets; the outgoing interface is VLAN-interface 2; the remote IP address is 192.168.40.1; and the local IP address is 192.168.40.2.

```
<Sysname> system-view
[Sysname] track 1 bfd echo interface vlan-interface 2 remote ip 192.168.40.1 local ip
192.168.40.2
```

## track nqa

### Syntax

**track** *track-entry-number* **nqa entry** *admin-name operation-tag* **reaction** *item-num*

**undo track** *track-entry-number*

### View

System view

### Default Level

2: System level

### Parameters

*track-entry-number*: Track object ID, in the range 1 to 1024.

**entry** *admin-name operation-tag*: Specifies the NQA test group to be associated with the Track object. *admin-name* is the name of the administrator creating the NQA operation, a string of 1 to 32 characters, case-insensitive. *operation-tag* is the NQA operation tag, a string of 1 to 32 characters, case-insensitive.

**reaction** *item-num*: Specifies the Reaction entry to be associated with the Track object. *item-num* is the Reaction entry ID, in the range 1 to 10.

### Description

Use the **track** command to create the Track object to be associated with the specified Reaction entry of the NQA test group.

Use the **undo track** command to remove the created Track object.

By default, no Track object is created.

Note that after a Track object is created, you cannot modify it using the **track** command.

Related commands: **nqa**, and **reaction** in *NQA Commands* in the *System Volume*.

## Examples

# Create Track object 1 to associate it with Reaction entry 3 of the NQA test group (admin-test).

```
<Sysname> system-view
[Sysname] track 1 nqa entry admin test reaction 3
```

# Table of Contents

<b>1 NQA Configuration Commands</b> .....	<b>1-1</b>
NQA Client Configuration Commands .....	1-1
advantage-factor .....	1-1
codec-type .....	1-1
data-fill .....	1-2
data-size .....	1-3
description (any NQA test type view) .....	1-4
destination ip .....	1-5
destination port .....	1-5
display nqa history .....	1-6
display nqa result .....	1-7
display nqa statistics .....	1-11
filename .....	1-16
frequency .....	1-16
history-records .....	1-17
http-version .....	1-18
next-hop .....	1-18
nqa .....	1-19
nqa agent enable .....	1-19
nqa agent max-concurrent .....	1-20
nqa schedule .....	1-21
operation (FTP test type view) .....	1-22
operation (HTTP test type view) .....	1-22
operation interface .....	1-23
password (FTP test type view) .....	1-24
probe count .....	1-24
probe packet-interval .....	1-25
probe packet-number .....	1-26
probe packet-timeout .....	1-26
probe timeout .....	1-27
reaction .....	1-28
reaction trap .....	1-29
route-option bypass-route .....	1-29
source interface .....	1-30
source ip .....	1-31
source port .....	1-32
statistics hold-time .....	1-32
statistics max-group .....	1-33
statistics interval .....	1-34
tos .....	1-34
ttl .....	1-35
type .....	1-36
url .....	1-36

username (FTP test type view) .....	1-37
vpn-instance (ICMP echo test type view) .....	1-38
NQA Server Configuration Commands.....	1-38
display nqa server status.....	1-38
nqa server enable.....	1-39
nqa server tcp-connect.....	1-40
nqa server udp-echo.....	1-41

# 1 NQA Configuration Commands

---

## NQA Client Configuration Commands

### advantage-factor

#### Syntax

**advantage-factor** *factor*

**undo advantage-factor**

#### View

Voice test type view

#### Default Levels

2: System level

#### Parameter

*factor*: Advantage factor, used to count Mean Opinion Scores (MOS) and Calculated Planning Impairment Factor (ICPIF) values. It is in the range 0 to 20.

#### Description

Use the **advantage-factor** command to configure the advantage factor which is used to count MOS and ICPIF values.

Use the **undo advantage-factor** command to restore the default.

By default, the advantage factor is 0.

The evaluation of voice quality depends on users' tolerance to voice quality, and this factor should be taken into consideration. For users with higher tolerance to voice quality, you can use the **advantage-factor** command to configure the advantage factor. When the system calculates the ICPIF value, this advantage factor is subtracted to modify ICPIF and MOS values and thus both the objective and subjective factors are considered when you evaluate the voice quality.

#### Example

```
# Configure the advantage factor for a voice test as 10.
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type voice
[Sysname-nqa-admin-test-voice] advantage-factor 10
```

### codec-type

#### Syntax

**codec-type** { **g711a** | **g711u** | **g729a** }

## undo codec-type

### View

Voice test type view

### Default Level

2: System level

### Parameters

**g711a**: G.711 A-law codec type.

**g711u**: G.711  $\mu$ -law codec type

**g729a**: G.729 A-law codec type.

### Description

Use the **codec-type** command to configure the codec type for a voice test.

Use the **undo codec-type** command to restore the default.

By default, the codec type for a voice test is G.711 A-law.

### Examples

# Configure the codec type for a voice test as **g729a**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type voice
[Sysname-nqa-admin-test-voice] codec-type g729a
```

## data-fill

### Syntax

**data-fill** *string*

**undo data-fill**

### View

ICMP echo, UDP echo, UDP jitter, voice test type view

### Default Level

2: System level

### Parameters

*string*: String used to fill a probe packet, in the range 1 to 200. It is case sensitive.

### Description

Use the **data-fill** command to configure the string used to fill a probe packet.

Use the **undo data-fill** command to restore the default.

By default, the string used to fill a probe packet is the hexadecimal number 00010203040506070809.

- If the data field of a probe packet is smaller than the fill data, the system uses only the first part of the character string to encapsulate the packet.
- If the data field of a probe packet is larger than the fill data, the system fills the character string cyclically to encapsulate the packet until it is full.

For example, when the fill data is **abcd** and the size of the data field of a probe packet is 3 byte, **abc** is used to fill the packet. When the data field of a probe packet is 6 byte, **abcdab** is used to fill the packet.

- In an ICMP echo test, the configured character string is used to fill the data field in an ICMP echo message.
- In a UDP echo test, because the first five bytes of the data field of a UDP packet have some specific usage, the configured character string is used to fill the remaining bytes in the UDP packet.
- In a UDP jitter test, because the first 68 bytes of the data field of a UDP packet have some specific usage, the configured character string is used to fill the remaining bytes in the UDP packet.
- In a voice test, because the first 16 bytes of the data field of a UDP packet have some specific usage, the configured character string is used to fill the remaining bytes in the UDP packet.

## Examples

# Configure the string used to fill an ICMP echo probe packet as **abcd**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] data-fill abcd
```

## data-size

### Syntax

**data-size** *size*

**undo data-size**

### View

ICMP echo, UDP echo, UDP jitter, voice test type view

### Default Level

2: System level

### Parameters

*size*: Size of a probe packet in bytes, in the range 20 to 8100 for an ICMP echo or a UDP echo test, in the range 68 to 8100 for a UDP jitter test and in the range 16 to 1500 for a voice test.

### Description

Use the **data-size** command to configure the size of a probe packet to be sent.

Use the **undo data-size** command to restore the default.

The default values are as shown in [Table 1-1](#).

**Table 1-1** Default values of the size of test packets sent

Test Type	Codec type	Default value (in bytes)
ICMP	None	100
UDP echo	None	100
UDP jitter	None	100
Voice	G.711 A-law	172
Voice	G.711 $\mu$ -law	172
Voice	G.729 A-law	32

- For an ICMP echo test, the size of a probe packet is the length of the data field in an ICMP echo message.
- For a UDP echo test, UDP jitter test and voice test, the size of a probe packet is the length of the data field in a UDP packet.

### Examples

```
# Configure the size of an ICMP echo probe packet as 80 bytes.
```

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] data-size 80
```

### description (any NQA test type view)

#### Syntax

```
description text
undo description
```

#### View

Any NQA test type view

#### Default Level

2: System level

#### Parameters

*text*: Descriptive string of a test group, in the range 1 to 200. It is case sensitive.

#### Description

Use the **description** command to give a brief description of a test group, usually, the test type or test purpose of a test group.

Use the **undo description** command to remove the configured description information.

By default, no descriptive string is available for a test group.

### Examples

```
# Configure the descriptive string for a test group as icmp-probe.
```

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] description icmp-probe
```

## destination ip

### Syntax

**destination ip** *ip-address*

**undo destination ip**

### View

DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice test type view

### Default Level

2: System level

### Parameters

*ip-address*: Destination IP address of a test operation.

### Description

Use the **destination ip** command to configure a destination IP address for a test operation.

Use the **undo destination ip** command to remove the configured destination IP address.

By default, no destination IP address is configured for a test operation.

### Examples

# Configure the destination IP address of an ICMP echo test operation as 10.1.1.1.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] destination ip 10.1.1.1
```

## destination port

### Syntax

**destination port** *port-number*

**undo destination port**

### View

TCP, UDP echo, UDP jitter, voice test type view

### Default Level

2: System level

### Parameters

*port-number*: Destination port number of a test operation, in the range 1 to 65535.

## Description

Use the **destination port** command to configure a destination port number for a test operation.

Use the **undo destination port** command to remove the configured destination port number.

By default, no destination port number is configured for a test operation.

Note that you are not recommended to perform a UDP jitter test and a voice test on ports from 1 to 1023 (known ports). Otherwise, the NQA test will fail or the corresponding services of this port will be unavailable.

## Examples

# Configure the destination port number of a test operation as 9000.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-echo
[Sysname-nqa-admin-test-udp-echo] destination port 9000
```

## display nqa history

### Syntax

```
display nqa history [ admin-name operation-tag ]
```

### View

Any view

### Default Level

2: System level

### Parameters

*admin-name operation-tag*: Displays history records of a test group. If these two arguments are not specified, history records of all test groups are displayed. *admin-name* represents the name of the administrator who creates the NQA operation. It is a string of 1 to 32 characters, case-insensitive. *operation-tag* represents the test operation tag. It is a string of 1 to 32 characters, case-insensitive.

## Description

Use the **display nqa history** command to display history records of NQA tests.

The **display nqa history** command cannot show you the results of voice tests and UDP jitter tests. Therefore, to know the result of a voice test or a UDP jitter test, you are recommended to use the **display nqa result** command to view the probe results of the latest NQA test, or use the **display nqa statistics** command to view the statistics of NQA tests.

## Examples

# Display the history records of the NQA test in which the administrator name is **administrator**, and the operation tag is **test**.

```
<Sysname> display nqa history administrator test
NQA entry(admin administrator, tag test) history record(s):
  Index      Response      Status          Time
  ---      -
  10         329           Succeeded       2007-04-29 20:54:26.5
```

9	344	Succeeded	2007-04-29 20:54:26.2
8	328	Succeeded	2007-04-29 20:54:25.8
7	328	Succeeded	2007-04-29 20:54:25.5
6	328	Succeeded	2007-04-29 20:54:25.1
5	328	Succeeded	2007-04-29 20:54:24.8
4	328	Succeeded	2007-04-29 20:54:24.5
3	328	Succeeded	2007-04-29 20:54:24.1
2	328	Succeeded	2007-04-29 20:54:23.8
1	328	Succeeded	2007-04-29 20:54:23.4

**Table 1-2 display nqa history** command output description

Field	Description
Index	History record number
Response	Roundtrip delay of a test packet in the case of a successful test, timeout time in the case of timeout, or 0 in the case that a test cannot be completed (in milliseconds)
Status	Status value of test results, including: <ul style="list-style-type: none"> <li>• Succeeded</li> <li>• Unknown error</li> <li>• Internal error</li> <li>• Timeout</li> </ul>
Time	Time when the test is completed

## display nqa result

### Syntax

```
display nqa result [ admin-name operation-tag ]
```

### View

Any view

### Default Level

2: System level

### Parameters

*admin-name operation-tag*: Displays results of the last test of a test group. If this argument is not specified, results of the last tests of all test groups are displayed. *admin-name* represents the name of the administrator who creates the NQA operation. It is a string of 1 to 32 characters, case-insensitive. *operation-tag* represents the test operation tag. It is a string of 1 to 32 characters, case-insensitive.

### Description

Use the **display nqa result** command to display results of the last NQA test.

### Examples

```
# Display the results of the last UDP jitter test.
```

```
<Sysname> display nqa result admin test
```

NQA entry(admin admin, tag test) test results:

Destination IP address: 192.168.1.42

Send operation times: 10                      Receive response times: 10

Min/Max/Average round trip time: 15/46/26

Square-Sum of round trip time: 8103

Last succeeded probe time: 2008-05-29 10:56:38.7

Extended results:

Packet lost in test: 0%

Failures due to timeout: 0

Failures due to disconnect: 0

Failures due to no connection: 0

Failures due to sequence error: 0

Failures due to internal error: 0

Failures due to other errors: 0

Packet(s) arrived late: 0

UDP-jitter results:

RTT number: 10

Min positive SD: 8

Min positive DS: 8

Max positive SD: 18

Max positive DS: 8

Positive SD number: 5

Positive DS number: 2

Positive SD sum: 75

Positive DS sum: 32

Positive SD average: 15

Positive DS average: 16

Positive SD square sum: 1189

Positive DS square sum: 640

Min negative SD: 8

Min negative DS: 1

Max negative SD: 24

Max negative DS: 30

Negative SD number: 4

Negative DS number: 7

Negative SD sum: 56

Negative DS sum: 99

Negative SD average: 14

Negative DS average: 14

Negative SD square sum: 946

Negative DS square sum: 1495

One way results:

Max SD delay: 22

Max DS delay: 23

Min SD delay: 7

Min DS delay: 7

Number of SD delay: 10

Number of DS delay: 10

Sum of SD delay: 125

Sum of DS delay: 132

Square sum of SD delay: 1805

Square sum of DS delay: 1988

SD lost packet(s): 0

DS lost packet(s): 0

Lost packet(s) for unknown reason: 0

## # Display the results of the last voice test.

<Sysname> display nqa result admin test

NQA entry(admin admin, tag test) test results:

Destination IP address: 192.168.1.42

Send operation times: 1000                      Receive response times: 0

Min/Max/Average round trip time: 0/0/0

Square-Sum of round trip time: 0

Last succeeded probe time: 0-00-00 00:00:00.0

Extended results:

Packet lost in test: 100%

```

Failures due to timeout: 1000
Failures due to disconnect: 0
Failures due to no connection: 0
Failures due to sequence error: 0
Failures due to internal error: 0
Failures due to other errors: 0
Packet(s) arrived late: 0
Voice results:
RTT number: 0
Min positive SD: 0           Min positive DS: 0
Max positive SD: 0           Max positive DS: 0
Positive SD number: 0        Positive DS number: 0
Positive SD sum: 0           Positive DS sum: 0
Positive SD average: 0       Positive DS average: 0
Positive SD square sum: 0    Positive DS square sum: 0
Min negative SD: 0           Min negative DS: 0
Max negative SD: 0           Max negative DS: 0
Negative SD number: 0        Negative DS number: 0
Negative SD sum: 0           Negative DS sum: 0
Negative SD average: 0       Negative DS average: 0
Negative SD square sum: 0    Negative DS square sum: 0
One way results:
Max SD delay: 0             Max DS delay: 0
Min SD delay: 0             Min DS delay: 0
Number of SD delay: 0       Number of DS delay: 0
Sum of SD delay: 0          Sum of DS delay: 0
Square sum of SD delay: 0   Square sum of DS delay: 0
SD lost packet(s): 0        DS lost packet(s): 0
Lost packet(s) for unknown reason: 1000
Voice scores:
MOS value: 0.99             ICPIF value: 87

```

**Table 1-3 display nqa result command output description**

Field	Description
Destination IP address	IP address of the destination
Send operation times	Number of probe packets sent
Receive response times	Number of response packets received
Min/Max/Average round trip time	Minimum/maximum/average roundtrip time, in milliseconds
Square-Sum of round trip time	Square sum of roundtrip time
Last succeeded probe time	Time when the last successful probe was finished
Packet lost in test	Average packet loss ratio
Failures due to timeout	Number of timeout occurrences in a test
Failures due to disconnect	Number of disconnections by the peer
Failures due to no connection	Number of failures to connect with the peer

Field	Description
Failures due to sequence error	Number of failures owing to out-of-sequence packets
Failures due to internal error	Number of failures owing to internal errors
Failures due to other errors	Failures due to other errors
Packet(s) arrived late	Number of packets that arrived late
UDP-jitter results	UDP jitter test results, available only in UDP jitter tests.
Voice results	Voice test results, available only in voice tests.
RTT number	Number of response packets received
Min positive SD	Minimum positive jitter delay from source to destination
Min positive DS	Minimum positive jitter delay from destination to source
Max positive SD	Maximum positive jitter delay from source to destination
Max positive DS	Maximum positive jitter delay from destination to source
Positive SD number	Number of positive jitter delays from source to destination
Positive DS number	Number of positive jitter delays from destination to source
Positive SD sum	Sum of positive jitter delays from source to destination
Positive DS sum	Sum of positive jitter delays from destination to source
Positive SD average	Average of positive jitter delays from source to destination
Positive DS average	Average of positive jitter delays from destination to source
Positive SD square sum	Square sum of positive jitter delays from source to destination
Positive DS square sum	Square sum of positive jitter delays from destination to source
Min negative SD	Minimum absolute value among negative jitter delays from source to destination
Min negative DS	Minimum absolute value among negative jitter delays from destination to source
Max negative SD	Maximum absolute value among negative jitter delays from source to destination
Max negative DS	Maximum absolute value among negative jitter delays from destination to source
Negative SD number	Number of negative jitter delays from source to destination
Negative DS number	Number of negative jitter delays from destination to source
Negative SD sum	Sum of absolute values of negative jitter delays from source to destination
Negative DS sum	Sum of absolute values of negative jitter delays from destination to source

Field	Description
Negative SD average	Average absolute value of negative jitter delays from source to destination
Negative DS average	Average absolute value of negative jitter delays from destination to source
Negative SD square sum	Square sum of negative jitter delays from source to destination
Negative DS square sum	Square sum of negative jitter delays from destination to source
One way results	Uni-direction delay test result, displayed in a UDP jitter or voice test
Max SD delay	Maximum delay from source to destination
Max DS delay	Maximum delay from destination to source
Min SD delay	Minimum delay from source to destination
Min DS delay	Minimum delay from destination to source
Number of SD delay	Number of delays from source to destination
Number of DS delay	Number of delays from destination to source
Sum of SD delay	Sum of delays from source to destination
Sum of DS delay	Sum of delays from destination to source
Square sum of SD delay	Square sum of delays from source to destination
Square sum of DS delay	Square sum of delays from destination to source
SD lost packet(s)	Number of lost packets from the source to the destination
DS lost packet(s)	Number of lost packets from the destination to the source
Lost packet(s) for unknown reason	Number of lost packets for unknown reasons
Voice scores	Voice parameters, displayed only in a voice test
MOS value	MOS value calculated for a voice test
ICPIF value	ICPIF value calculated for a voice test

## display nqa statistics

### Syntax

**display nqa statistics** [ *admin-name operation-tag* ]

### View

Any view

### Default Level

2: System level

## Parameters

*admin-name operation-tag*: Displays statistics of the specified test group. If this argument is not specified, statistics of all test groups are displayed. *admin-name* represents the name of the administrator who creates the NQA operation. It is a string of 1 to 32 characters, case-insensitive. *operation-tag* represents the test operation tag. It is a string of 1 to 32 characters, case-insensitive.

## Description

Use the **display nqa statistics** command to display statistics of NQA test or tests.

After the test operation begins, if not all the probes in the first test have been finished, statistics cannot be generated. In this case, if you display the statistics using this command, the statistics is displayed as all 0s.

## Examples

# Display statistics of UDP jitter tests.

```
<Sysname> display nqa statistics admin test
NQA entry(admin admin, tag test) test statistics:
NO. : 1
Destination IP address: 192.168.1.42
Start time: 2008-05-29 11:33:29.9
Life time: 8
Send operation times: 70          Receive response times: 70
Min/Max/Average round trip time: 1/63/19
Square-Sum of round trip time: 36330
Extended results:
Packet lost in test: 0%
Failures due to timeout: 0
Failures due to disconnect: 0
Failures due to no connection: 0
Failures due to sequence error: 0
Failures due to internal error: 0
Failures due to other errors: 0
Packet(s) arrived late: 0
UDP-jitter results:
RTT number: 70
Min positive SD: 1          Min positive DS: 1
Max positive SD: 24        Max positive DS: 22
Positive SD number: 34     Positive DS number: 27
Positive SD sum: 415       Positive DS sum: 362
Positive SD average: 12    Positive DS average: 13
Positive SD square sum: 6593 Positive DS square sum: 6450
Min negative SD: 1         Min negative DS: 1
Max negative SD: 40        Max negative DS: 64
Negative SD number: 28     Negative DS number: 35
Negative SD sum: 28        Negative DS sum: 35
Negative SD average: 13    Negative DS average: 12
Negative SD square sum: 7814 Negative DS square sum: 420
One way results:
```

Max SD delay: 31	Max DS delay: 31
Min SD delay: 7	Min DS delay: 7
Number of SD delay: 70	Number of DS delay: 70
Sum of SD delay: 628	Sum of DS delay: 656
Square sum of SD delay: 8156	Square sum of DS delay: 8704
SD lost packet(s): 0	DS lost packet(s): 0
Lost packet(s) for unknown reason: 0	

## # Display statistics of voice tests.

<Sysname> display nqa statistics admin test

NQA entry(admin admin, tag test) test statistics:

NO. : 1

Destination IP address: 192.168.1.42

Start time: 2008-05-29 11:00:03.6

Life time: 638

Send operation times: 10000

Receive response times: 0

Min/Max/Average round trip time: 0/0/0

Square-Sum of round trip time: 0

Extended results:

Packet lost in test: 100%

Failures due to timeout: 10000

Failures due to disconnect: 0

Failures due to no connection: 0

Failures due to sequence error: 0

Failures due to internal error: 0

Failures due to other errors: 0

Packet(s) arrived late: 0

Voice results:

RTT number: 0

Min positive SD: 0

Min positive DS: 0

Max positive SD: 0

Max positive DS: 0

Positive SD number: 0

Positive DS number: 0

Positive SD sum: 0

Positive DS sum: 0

Positive SD average: 0

Positive DS average: 0

Positive SD square sum: 0

Positive DS square sum: 0

Min negative SD: 0

Min negative DS: 0

Max negative SD: 0

Max negative DS: 0

Negative SD number: 0

Negative DS number: 0

Negative SD sum: 0

Negative DS sum: 0

Negative SD average: 0

Negative DS average: 0

Negative SD square sum: 0

Negative DS square sum: 0

One way results:

Max SD delay: 0

Max DS delay: 0

Min SD delay: 0

Min DS delay: 0

Number of SD delay: 0

Number of DS delay: 0

Sum of SD delay: 0

Sum of DS delay: 0

Square sum of SD delay: 0

Square sum of DS delay: 0

SD lost packet(s): 0

DS lost packet(s): 0

Lost packet(s) for unknown reason: 10000

Voice scores:

Max MOS value: 0.99

Min MOS value: 0.99

Max ICPIF value: 87

Min ICPIF value: 87

**Table 1-4 display nqa statistics** command output description

Field	Description
No.	Statistics group number
Destination IP address	IP address of the destination
Start time	Test start time
Life time	Duration of the test, in seconds
Send operation times	Number of probe packets sent
Receive response times	Number of response packets received
Min/Max/Average round trip time	Minimum/maximum/average roundtrip time, in milliseconds
Square-Sum of round trip time	Square sum of roundtrip time
Packet lost in test	Average packet loss ratio
Failures due to timeout	Number of timeout occurrences in a test
Failures due to disconnect	Number of disconnections by the peer
Failures due to no connection	Number of failures to connect with the peer
Failures due to sequence error	Number of failures owing to out-of-sequence packets
Failures due to internal error	Number of failures owing to internal errors
Failures due to other errors	Failures due to other errors
Packet(s) arrived late	Number of response packets received after a probe times out
UDP-jitter results	UDP jitter test results, available only in UDP jitter tests.
Voice results	Voice test results, available only in voice tests.
RTT number	Number of response packets received
Min positive SD	Minimum positive jitter delay from source to destination
Min positive DS	Minimum positive jitter delay from destination to source
Max positive SD	Maximum positive jitter delay from source to destination
Max positive DS	Maximum positive jitter delay from destination to source
Positive SD number	Number of positive jitter delays from source to destination
Positive DS number	Number of positive jitter delays from destination to source
Positive SD sum	Sum of positive jitter delays from source to destination
Positive DS sum	Sum of positive jitter delays from destination to source
Positive SD average	Average of positive jitter delays from source to destination
Positive DS average	Average of positive jitter delays from destination to source
Positive SD square sum	Square sum of positive jitter delays from source to destination

<b>Field</b>	<b>Description</b>
Positive DS square sum	Square sum of positive jitter delays from destination to source
Min negative SD	Minimum absolute value among negative jitter delays from source to destination
Min negative DS	Minimum absolute value among negative jitter delays from destination to source
Max negative SD	Maximum absolute value among negative jitter delays from source to destination
Max negative DS	Maximum absolute value among negative jitter delays from destination to source
Negative SD number	Number of negative jitter delays from source to destination
Negative DS number	Number of negative jitter delays from destination to source
Negative SD sum	Sum of absolute values of negative jitter delays from source to destination
Negative DS sum	Sum of absolute values of negative jitter delays from destination to source
Negative SD average	Average absolute value of negative jitter delays from source to destination
Negative DS average	Average absolute value of negative jitter delays from destination to source
Negative SD square sum	Square sum of negative jitter delays from source to destination
Negative DS square sum	Square sum of negative jitter delays from destination to source
One way results	Uni-direction delay test result, displayed on in a UDP-Jitter or voice test
Max SD delay	Maximum delay from source to destination
Max DS delay	Maximum delay from destination to source
Min SD delay	Minimum delay from source to destination
Min DS delay	Minimum delay from destination to source
Number of SD delay	Number of delays from source to destination
Number of DS delay	Number of delays from destination to source
Sum of SD delay	Sum of delays from source to destination
Sum of DS delay	Sum of delays from destination to source
Square sum of SD delay	Square sum of delays from source to destination
Square sum of DS delay	Square sum of delays from destination to source
SD lost packet(s)	Number of lost packets from the source to the destination
DS lost packet(s)	Number of lost packets from the destination to the source
Lost packet(s) for unknown reason	Number of lost packets for unknown reasons
Voice scores	Voice parameters, displayed only in a voice test

## filename

### Syntax

**filename** *filename*

**undo filename**

### View

FTP test type view

### Default Level

2: System level

### Parameters

*filename*: Name of the file transferred between the FTP server and the FTP client, a string of 1 to 200 characters. It is case sensitive.

### Description

Use the **filename** command to specify a file to be transferred between the FTP server and the FTP client.

Use the **undo filename** command to restore the default.

By default, no file is specified.

### Examples

# Specify the file to be transferred between the FTP server and the FTP client as config.txt.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] filename config.txt
```

## frequency

### Syntax

**frequency** *interval*

**undo frequency**

### View

Any NQA test type view

### Default Level

2: System level

### Parameters

*interval*: Interval between two consecutive tests, in milliseconds, in the range 0 to 604800000. If the interval is 0, it indicates that only one test is performed, and no statistics are generated.

## Description

Use the **frequency** command to configure the interval between two consecutive tests for a test group.

Use the **undo frequency** command to restore the default.

By default, the interval between two consecutive voice tests is 60000 milliseconds, and the interval between two consecutive tests of other types is 0 milliseconds, that is, only one test is performed.

After you use the **nqa schedule** command to start an NQA test, one test is started at *interval*.

If the last test is not completed when the interval specified by the **frequency** command is reached, a new test is not started.

## Examples

```
# Configure the interval between two consecutive tests as 1000 milliseconds.
```

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] frequency 1000
```

## history-records

### Syntax

**history-records** *number*

**undo history-records**

### View

Any NQA test type view

### Default Level

2: System level

### Parameters

*number*: Maximum number of history records that can be saved in a test group, in the range 0 to 50.

## Description

Use the **history-records** command to configure the maximum number of history records that can be saved in a test group.

Use the **undo history-records** command to restore the default.

By default, the maximum number of records that can be saved in a test group is 50.

If the number of history records exceeds the maximum number, the earliest history record for a probe will be discarded.

## Examples

```
# Configure the maximum number of history records that can be saved in a test group as 10.
```

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] history-records 10
```

## http-version

### Syntax

```
http-version v1.0
undo http-version
```

### View

HTTP test type view

### Default Level

2: System level

### Parameters

**v1.0**: The HTTP version is 1.0 in an HTTP test.

### Description

Use the **http-version** command to configure the HTTP version used in an HTTP test.

Use the **undo http-version** command to restore the default.

By default, HTTP 1.0 is used in an HTTP test.

### Examples

```
# Configure the HTTP version as 1.0 in an HTTP test.
```

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] http-version v1.0
```

## next-hop

### Syntax

```
next-hop ip-address
undo next-hop
```

### View

ICMP echo test type view

### Default Level

2: System level

### Parameters

*ip-address*: IP address of the next hop.

### Description

Use the **next-hop** command to configure the next hop IP address for an IP packet.

Use the **undo next-hop** command to remove the configured next hop IP address.

By default, no next hop IP address is configured.

## Examples

```
# Configure the next hop IP address as 10.1.1.1.
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] next-hop 10.1.1.1
```

## nqa

### Syntax

```
nqa entry admin-name operation-tag
undo nqa { all | entry admin-name operation-tag }
```

### View

System view

### Default Level

2: System level

### Parameters

*admin-name*: Specifies the name of the administrator who creates the NQA test operation, a string of 1 to 32 characters, with "-" excluded. It is case-insensitive.

*operation-tag*: Specifies the tag of a test operation, a string of 1 to 32 characters, with "-" excluded. It is case-insensitive.

**all**: All NQA test groups.

### Description

Use the **nqa** command to create an NQA test group and enter NQA test group view.

Use the **undo nqa** command to remove the test group.

Note that if the test type has been configured for the test group, you will directly enter NQA test type view when you execute the **nqa** command.

## Examples

```
# Create an NQA test group whose administrator name is admin and whose operation tag is test and enter NQA test group view.
```

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test]
```

## nqa agent enable

### Syntax

```
nqa agent enable
undo nqa agent enable
```

## View

System view

## Default Level

2: System level

## Parameters

None

## Description

Use the **nqa agent enable** command to enable the NQA client.

Use the **undo nqa agent enable** command to disable the NQA client and stop all the tests being performed.

By default, the NQA client is enabled.

Related commands: **nqa server enable**.

## Examples

```
# Enable the NQA client.  
<Sysname> system-view  
[Sysname] nqa agent enable
```

## nqa agent max-concurrent

### Syntax

```
nqa agent max-concurrent number  
undo nqa agent max-concurrent
```

## View

System view

## Default Level

2: System level

## Parameters

*number*: Maximum number of the tests that the NQA client can simultaneously perform, in the range 1 to 5. The default value is 2..

## Description

Use the **nqa agent max-concurrent** command to configure the maximum number of tests that the NQA client can simultaneously perform.

Use the **undo nqa agent max-concurrent** command to restore the default.

From the beginning to the end of a test, the NQA test is in the test status; from the end of a test to the beginning of the next test, the NQA test is in the waiting status.

## Examples

```
# Configure the maximum number of the tests that the NQA client can simultaneously perform as 3.
<Sysname> system-view
[Sysname] nqa agent max-concurrent 3
```

## nqa schedule

### Syntax

```
nqa schedule admin-name operation-tag start-time { hh:mm:ss [ yyyy/mm/dd ] | now } lifetime
{ lifetime | forever }
undo nqa schedule admin-name operation-tag
```

### View

System view

### Default Level

2: System level

### Parameters

*admin-name*: Specifies the name of the administrator who creates the NQA test operation, a string of 1 to 32 characters. It is case-insensitive.

*operation-tag*: Specifies the test operation tag, a string of 1 to 32 characters. It is case-insensitive.

**start-time**: Specifies the start time and date of a test.

*hh:mm:ss*: Start time of a test.

*yyyy/mm/dd*: Start date of a test. The default value is the current system time, and *yyyy* ranges from 2000 to 2035.

**now**: Starts the tests for a test group immediately.

**lifetime**: Specifies the duration of the test operation.

*lifetime*: Duration of the test operation in seconds, in the range 1 to 2147483647.

**forever**: Specifies that the tests are performed for a test group forever.

### Description

Use the **nqa schedule** command to configure the test start time and test duration for a test group.

Use the **undo nqa schedule** command to stop the test for the test group.

Note that:

- It is not allowed to enter test group view or test type view after a test group is scheduled.
- A test group performs a test when the system time is between the start time and the end time (the start time plus test duration). If the system time is behind the start time when you execute the **nqa schedule** command, a test is started when the system time reaches the start time; if the system time is between the start time and the end time, a test is started at once; if the system time is ahead of the end time, no test is started. You can use the **display clock** command to view the current system time.

For the related configurations, refer to the **display clock** command in Basic System Configuration Commands in the System Volume.

## Examples

# Start the tests for the test group with the administrator name **admin** and operation tag **test**. The start time and duration of the tests are 08:08:08 2008/08/08 and 1000 seconds respectively.

```
<Sysname> system-view
[Sysname] nqa schedule admin test start-time 08:08:08 2008/08/08 lifetime 1000
```

## operation (FTP test type view)

### Syntax

```
operation { get | put }
undo operation
```

### View

FTP test type view

### Default Level

2: System level

### Parameters

**get**: Obtains a file from the FTP server.

**put**: Transfers a file to the FTP server.

### Description

Use the **operation** command to configure the FTP operation type.

Use the **undo operation** command to restore the default.

By default, the FTP operation type is **get**.

## Examples

# Configure the FTP operation type as **put**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] operation put
```

## operation (HTTP test type view)

### Syntax

```
operation { get | post }
undo operation
```

### View

HTTP test type view

### Default Level

2: System level

## Parameters

**get**: Obtains data from the HTTP server.

**post**: Transfers data to the HTTP server.

## Description

Use the **operation** command to configure the HTTP operation type.

Use the **undo operation** command to restore the default.

By default, the HTTP operation type is **get**.

## Examples

# Configure the HTTP operation type as **post**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] operation post
```

## operation interface

### Syntax

**operation interface** *interface-type interface-number*

**undo operation interface**

### View

DHCP test type view

### Default Level

2: System level

## Parameters

*interface-type interface-number*. Type and number of the interface that is performing a DHCP test.

## Description

Use the **operation interface** command to specify the interface to perform a DHCP test.

Use the **undo operation interface** command to restore the default.

By default, no interface is specified to perform a DHCP test.

Note that the specified interface must be up; otherwise, the test will fail.

## Examples

# Specify the interface to perform a DHCP test as VLAN-interface 2.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type dhcp
[Sysname-nqa-admin-test-dhcp] operation interface vlan-interface 2
```

## password (FTP test type view)

### Syntax

```
password password  
undo password
```

### View

FTP test type view

### Default Level

2: System level

### Parameters

*password*: Password used to log onto the FTP server, a string of 1 to 32 characters. It is case sensitive.

### Description

Use the **password** command to configure a password used to log onto the FTP server.

Use the **undo password** command to remove the configured password.

By default, no password is configured for logging onto the FTP server.

Related commands: **username**, **operation**.

### Examples

# Configure the password used for logging onto the FTP server as **ftpuser**.

```
<Sysname> system-view  
[Sysname] nqa entry admin test  
[Sysname-nqa-admin-test] type ftp  
[Sysname-nqa-admin-test-ftp] password ftpuser
```

## probe count

### Syntax

```
probe count times  
undo probe count
```

### View

DHCP, DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter test type view

### Default Level

2: System level

### Parameters

*times*: Number of probes in an NQA test, in the range 1 to 15.

### Description

Use the **probe count** command to configure the number of probes in an NQA test.

Use the **undo probe count** command to restore the default.

By default, one probe is performed in an NQA test.

- For a TCP or DLSw test, one probe means one connection;
- For a UDP jitter test or a voice test, the number of packets sent in one probe depends on the **probe packet-number** command;
- For an FTP, HTTP or DHCP test, one probe means to carry out a corresponding function;
- For an ICMP echo or UDP echo test, one packet is sent in one probe;
- For an SNMP test, three packets are sent in a probe.

If the number of probes in a test is greater than 1, the system performs a second probe after it performs the first probe and receives a response packet. If the system does not receive a response packet, it waits for the test timer to expire before performing a second probe. The process is repeated until the specified probes are completed.

Note that this command is not supported in a voice test. Only one probe can be made in a voice test.

## Examples

# Configure the number of probes in an ICMP echo test as 10.

```
<Sysname> system-view
[Sysname] nqa entry admin-test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] probe count 10
```

## probe packet-interval

### Syntax

**probe packet-interval** *packet-interval*

**undo probe packet-interval**

### View

UDP jitter, voice test type view

### Default Level

2: System level

### Parameters

*packet-interval*: Interval for packets sent in a probe in a test, in milliseconds, in the range 10 to 60000.

### Description

Use the **probe packet-interval** command to configure the interval for sending packets in a probe in a test.

Use the **undo probe-interval** command to restore the default.

By default, the interval is 20 milliseconds.

## Examples

# Configure the interval for sending packets in a probe in a UDP jitter test as 100 milliseconds.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
```

```
[Sysname-nqa-admin-test-udp-jitter] probe packet-interval 100
```

## probe packet-number

### Syntax

```
probe packet-number packet-number  
undo probe packet-number
```

### View

UDP jitter, voice test type view

### Default Level

2: System level

### Parameters

*packet-number*: Number of packets sent in a UDP jitter probe or a voice probe. For a UDP jitter test, it is in the range 10 to 1000; for a voice test, it is in the range 10 to 60000.

### Description

Use the **probe packet-number** command to configure the number of packets sent in a UDP jitter probe or a voice probe.

Use the **undo probe packet-number** command to restore the default.

By default, the number of packets sent in a probe is 10 in a UDP jitter test and 1000 in a voice test.

### Examples

```
# Configure the number of packets sent in a UDP jitter probe as 100.
```

```
<Sysname> system-view  
[Sysname] nqa entry admin test  
[Sysname-nqa-admin-test] type udp-jitter  
[Sysname-nqa-admin-test-udp-jitter] probe packet-number 100
```

## probe packet-timeout

### Syntax

```
probe packet-timeout packet-timeout  
undo probe packet-timeout
```

### View

UDP jitter, voice test type view

### Default Level

2: System level

### Parameters

*packet-timeout*: Timeout time for waiting for responses in a UDP jitter or voice test, in the range 10 to 3600000 milliseconds.

## Description

Use the **probe packet-timeout** command to configure the timeout time for waiting for responses in a UDP jitter or voice test.

Use the **undo probe packet-timeout** command to restore the default.

By default, the timeout time in a UDP jitter and a voice test is 3000 and 5000 milliseconds respectively.

## Examples

```
# Configure the timeout time for waiting for responses in a UDP jitter test as 100 milliseconds.
```

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] probe packet-timeout 100
```

## probe timeout

### Syntax

```
probe timeout timeout
```

```
undo probe timeout
```

### View

DHCP, DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo test type view

### Default Level

2: System level

### Parameters

*timeout*: Timeout time in a probe except UDP jitter probe, in milliseconds. For an FTP or HTTP probe, the value range is 10 to 86400000; for a DHCP, DLSw, ICMP echo, SNMP, TCP or UDP echo probe, the value range is 10 to 3600000.

## Description

Use the **probe timeout** command to configure the timeout time in a probe.

Use the **undo probe timeout** command to restore the default.

By default, the timeout time is 3000 milliseconds.

After an NQA probe begins, if the NQA probe is not finished within the time specified in the **probe timeout** command, then the probe times out.

## Examples

```
# Configure the timeout time in a DHCP probe as 10000 milliseconds.
```

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type dhcp
[Sysname-nqa-admin-test-dhcp] probe timeout 10000
```

## reaction

### Syntax

```
reaction item-num checked-element probe-fail threshold-type consecutive occurrences  
[ action-type { none | trigger-only } ]
```

```
undo reaction item-num
```

### View

DHCP, DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo test type view

### Default Level

2: System level

### Parameters

*item-num*: Number of the reaction entry, in the range 1 to 10.

**checked-element**: Type of the monitored element in collaboration. At present, the type of the monitored element can be probe failure only.

**probe-fail**: The type of the monitored element is probe failure.

**threshold-type consecutive**: Threshold type is consecutive probe failures.

*occurrences*: Number of consecutive probe failures, in the range 1 to 16.

**action-type**: Triggered action type, defaulting to **none**.

**none**: No actions.

**trigger-only**: Triggers collaboration between other modules only.

### Description

Use the **reaction** command to establish a collaboration entry to monitor the probe results of the current test group. If the number of consecutive probe failures reaches the threshold, collaboration with other modules is triggered.

Use the **undo reaction** command to remove the collaboration entry.

By default, no collaboration entries are configured.

Note that:

- You cannot modify the content of a collaboration object using the **reaction** command after the collaboration object is created.
- The collaboration function is not supported in a UDP jitter or voice test.

Related commands: **track** in the *Track Commands* in the *System Volume*.

### Examples

```
# Create collaboration object 1. If the number of consecutive probe failures reaches 3, collaboration  
with other modules is triggered.
```

```
<Sysname> system-view  
[Sysname] nqa entry admin test  
[Sysname-nqa-admin-test] type tcp  
[Sysname-nqa-admin-test-tcp] reaction 1 checked-element probe-fail threshold-type  
consecutive 3 action-type trigger-only
```

## reaction trap

### Syntax

```
reaction trap { probe-failure consecutive-probe-failures | test-complete | test-failure  
cumulate-probe-failures }
```

```
undo reaction trap { probe-failure | test-complete | test-failure }
```

### View

Any NQA test type view

### Default Level

2: System level

### Parameters

**probe-failure** *consecutive-probe-failures*: Specifies to send a trap indicating a probe failure to the network management server after consecutive probe failures in an NQA test. *consecutive-probe-failures* is the number of consecutive probe failures in a test, in the range 1 to 15.

**test-complete**: Specifies to send a trap to indicate that the test is completed.

**test-failure** *cumulate-probe-failures*: Specifies to send a trap indicating a probe failure to the network management server if the total number of probe failures in an NQA test is larger than or equal to *cumulate-probe-failures*. For one test, the trap is sent only when the test is completed. *cumulate-probe-failures* is the total number of consecutive probe failures in a test, in the range 1 to 15.

### Description

Use the **reaction trap** command to configure to send traps to network management server under specified conditions.

Use the **undo reaction trap** command to restore the default.

By default, no traps are sent to the network management server.

Note that only the **reaction trap test-complete** command is supported in a voice test, namely, in a voice test, traps are sent to the NMS only if the test succeeds.

### Examples

```
# Configure to send a trap indicating a probe failure after five consecutive probe failures in an ICMP  
echo test.
```

```
<Sysname> system-view  
[Sysname] nqa entry admin test  
[Sysname-nqa-admin-test] type icmp-echo  
[Sysname-nqa-admin-test-icmp-echo] reaction trap probe-failure 5
```

## route-option bypass-route

### Syntax

```
route-option bypass-route
```

```
undo route-option bypass-route
```

## View

DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice test type view

## Default Level

2: System level

## Parameters

None

## Description

Use the **route-option bypass-route** command to enable the routing table bypass function to test the direct connectivity to the direct destination.

Use the **undo route-option bypass-route** command to disable the routing table bypass function.

By default, the routing table bypass function is disabled.

Note that after this function is enabled, the routing table is not searched, and the packet is directly sent to the destination in a directly connected network.

## Examples

# Enable the routing table bypass function.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] route-option bypass-route
```

## source interface

### Syntax

**source interface** *interface-type interface-number*

**undo source interface**

### View

ICMP echo test type view

### Default Level

2: System level

### Parameters

*interface-type interface-number*: Interface type and the interface number of the source interface of a probe packet.

### Description

Use the **source interface** command to specify the IP address of an interface as the source IP address of ICMP echo probe requests.

Use the **undo source interface** command to remove the IP address of an interface as the source IP address of ICMP echo probe requests.

By default, no interface address is specified as the source IP address of ICMP test request packets.

Note that:

- If you use the **source ip** command to configure the source IP address of ICMP probe requests, the **source interface** command is invalid.
- The interface specified by the **source interface** command must be up; otherwise, the probe fails.

Related commands: **source ip**.

## Examples

# Specify the IP address of interface VLAN-interface 2 as the source IP address of ICMP echo probe requests.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] source interface vlan-interface 2
```

## source ip

### Syntax

**source ip** *ip-address*

**undo source ip**

### View

DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice test type view

### Default Level

2: System level

### Parameters

*ip-address*: Source IP address of a test operation.

### Description

Use the **source ip** command to configure the source IP address of ICMP probe requests in a test operation.

Use the **undo source ip** command to remove the configured source address. That is, the IP address of the interface sending a probe request serves as the source IP address of the probe request.

By default, no source IP address is specified.

Note that:

- For an ICMP echo test, if no source IP address is specified, but the source interface is specified, the IP address of the source interface is taken as the source IP address of ICMP probe requests.
- The source IP address specified by the **source ip** command must be the IP address of an interface on the device, and the interface must be up; otherwise, the test fails.

Related commands: **source interface**.

## Examples

# Configure the source IP address of an ICMP echo probe request as 10.1.1.1.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] source ip 10.1.1.1
```

## source port

### Syntax

**source port** *port-number*

**undo source port**

### View

SNMP, UDP echo, UDP jitter, voice test type view

### Default Level

2: System level

### Parameters

*port-number*: Source port number for a test operation, in the range 1 to 50000.

### Description

Use the **source port** command to configure the source port of ICMP probe requests in a test operation.

Use the **undo source port** command to remove the configured port number.

By default, no source port number is specified.

### Examples

# Configure the source port number of a probe request as 8000.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-echo
[Sysname-nqa-admin-test-udp-echo] source port 8000
```

## statistics hold-time

### Syntax

**statistics hold-time** *hold-time*

**undo statistics hold-time**

### View

DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice test type view

### Default Levels

2: System level

### Parameters

*hold-time*: Hold time of a statistics group in minutes, in the range 1 to 1440.

## Description

Use the **statistics hold-time** command to configure the hold time of a statistics group.

Use the **undo statistics hold-time** command to restore the default.

By default, the hold time of a statistics group is 120 minutes.

A statistics group has the aging mechanism. A statistics group will be deleted after it is kept for a period of time so that information of a new statistics group will be recorded.

Note that this command is supported on all types of tests except DHCP tests.

## Examples

```
# Configure the hold time of a statistics group as 3 minutes.
```

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] statistics hold-time 3
```

## statistics max-group

### Syntax

```
statistics max-group number
```

```
undo statistics max-group
```

### View

DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice test type view

### Default Levels

2: System level

### Parameters

*number*: Maximum number of statistics groups that can be kept, in the range 0 to 100.

## Description

Use the **statistics max-group** command to configure the maximum number of statistics groups that can be kept.

Use the **undo statistics max-group** command to restore the default.

By default, the maximum number of statistics groups that can be kept is 2.

When the number of statistics groups kept reaches the upper limit, if a new statistics group is generated, the statistics group that is kept the longest is deleted.

Note that:

- This command is supported in all tests except DHCP tests.
- The value of 0 indicates that no statistics are collected.

## Examples

```
# Configure the maximum number of statistics groups that can be kept as 5.
```

```
<Sysname> system-view
```

```
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] statistics max-group 5
```

## statistics interval

### Syntax

```
statistics interval interval
undo statistics interval
```

### View

DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice test type view

### Default Levels

2: System level

### Parameters

*interval*: Interval for collecting statistics of the test results in minutes, in the range 1 to 35791394.

### Description

Use the **statistics interval** command to configure the interval for collecting statistics of the test results.

Use the **undo statistics interval** command to restore the default.

By default, the interval is 60 minutes.

NQA puts the NQA tests completed in a certain interval into one group, and calculates the statistics of the test results of the group. These statistics form a statistics group. You can use the **display nqa statistics** command to display information of the statistics group.

Note that this command is supported on all types of tests except DHCP tests.

### Examples

# Configure the interval for collecting statistics of the test results as 2 minutes.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] statistics interval 2
```

## tos

### Syntax

```
tos value
undo tos
```

### View

DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice test type view

### Default Level

2: System level

## Parameters

*value*: Value of the ToS field in the IP header in an NQA probe packet, in the range 0 to 255.

## Description

Use the **tos** command to configure the value of the ToS field in the IP header in an NQA probe packet.

Use the **undo tos** command to restore the default.

By default, the ToS field in the IP header of an NQA probe packet is 0.

## Examples

# Configure the ToS field in a IP packet header in an NQA probe packet as 1.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] tos 1
```

## ttl

### Syntax

**ttl** *value*

**undo ttl**

### View

DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice test type view

### Default Level

2: System level

## Parameters

*value*: Maximum number of hops a probe packet traverses in the network, in the range 1 to 255.

## Description

Use the **ttl** command to configure the maximum number of hops a probe packet traverses in the network.

Use the **undo ttl** command to restore the default.

By default, the maximum number of hops that a probe packet can traverse in a network is 20.

Note that after you configure the **route-option bypass-route** command, the maximum number of hops a probe packet traverses in the network is 1, and the **ttl** command does not take effect.

## Examples

# Configure the maximum number of hops that a probe request can traverse in a network as 16.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] ttl 16
```

## type

### Syntax

```
type { dhcp | dlsw | ftp | http | icmp-echo | snmp | tcp | udp-echo | udp-jitter | voice }
```

### View

NQA test group view

### Default Level

2: System level

### Parameters

**dhcp**: DHCP test.

**dlsw**: DLSw test.

**ftp**: FTP test.

**http**: HTTP test.

**icmp-echo**: ICMP echo test.

**snmp**: SNMP test.

**tcp**: TCP test.

**udp-echo**: UDP echo test.

**udp-jitter**: UDP jitter test.

**voice**: Voice test.

### Description

Use the **type** command to configure the test type of the current test group and enter test type view.

By default, no test type is configured.

### Examples

# Configure the test type of a test group as **FTP** and enter test type view.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp]
```

## url

### Syntax

```
url url
```

```
undo url
```

### View

HTTP test type view

## Default Level

2: System level

## Parameters

*url*: Website that an HTTP test visits, a string of 1 to 185 characters. It is case sensitive.

## Description

Use the **url** command to configure the website an HTTP test visits.

Use the **undo url** command to remove the configured website an HTTP test visits.

Note that the character string of the configured URL cannot contain spaces.

## Examples

```
# Configure the website that an HTTP test visits as /index.htm.
```

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] url /index.htm
```

## username (FTP test type view)

### Syntax

```
username username
```

```
undo username
```

### View

FTP test type view

### Default Level

2: System level

### Parameters

*username*: Username used to log onto the FTP server, a string of 1 to 32 characters. It is case sensitive.

### Description

Use the **username** command to configure a username used to log onto the FTP server.

Use the **undo username** command to remove the configured username.

By default, no username is configured for logging onto the FTP server.

Related commands: **password**, **operation**.

### Examples

```
# Configure the login username as administrator.
```

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] username administrator
```

## vpn-instance (ICMP echo test type view)

### Syntax

**vpn-instance** *instance*

**undo vpn-instance**

### View

ICMP echo test type view

### Default Level

2: System level

### Parameters

*instance*: VPN instance name, a string of 1 to 31 characters. It is case sensitive.

### Description

Use the **vpn-instance** command to specify a VPN instance.

Use the **undo vpn-instance** command to restore the default.

By default, no VPN instance is specified.

After you specify a VPN instance, NQA will test the connectivity of the specified VPN tunnel.

### Examples

# Specify the VPN instance **vpn1**.

```
<Sysname> system-view
```

```
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type icmp-echo
```

```
[Sysname-nqa-admin-test-icmp-echo] vpn-instance vpn1
```

## NQA Server Configuration Commands



### Note

You only need to configure the NQA server for UDP jitter, TCP, UDP echo and voice tests.

---

## display nqa server status

### Syntax

**display nqa server status**

### View

Any view

## Default Level

2: System level

## Parameters

None

## Description

Use the **display nqa server status** command to display NQA server status.

## Examples

```
# Display NQA server status.
```

```
<Sysname> display nqa server status
nqa server is: enabled
tcp-connect:
  IP Address      Port      Status
  2.2.2.2         2000     active
udp-echo:
  IP Address      Port      Status
  3.3.3.3         3000     inactive
```

**Table 1-5** display nqa server status command output description

Field	Description
tcp-connect	NQA server status in the NQA TCP test
udp-echo	NQA server status in the NQA UDP test
IP Address	IP address specified for the TCP/UDP listening service on the NQA server
Port	Port number of the TCP/UDP listening service on the NQA server
Status	Listening service status: <b>active</b> : Listening service is ready; <b>inactive</b> : Listening service is not ready.

## nqa server enable

### Syntax

```
nqa server enable
undo nqa server enable
```

### View

System view

## Default Level

2: System level

## Parameters

None

## Description

Use the **nqa server enable** command to enable the NQA server.

Use the **undo nqa server enable** command to disable the NQA server.

By default, the NQA server is disabled.

Related commands: **nqa server tcp-connect**, **nqa server udp-echo** and **display nqa server status**.

## Examples

```
# Enable the NQA server.
<Sysname> system-view
[Sysname] nqa server enable
```

## nqa server tcp-connect

### Syntax

```
nqa server tcp-connect ip-address port-number
undo nqa server tcp-connect ip-address port-number
```

### View

System view

### Default Level

2: System level

### Parameters

*ip-address*: IP address specified for the TCP listening service on the NQA server.

*port-number*: Port number specified for the TCP listening service on the NQA server, in the range 1 to 50000.-

## Description

Use the **nqa-server tcp-connect** command to create a TCP listening service on the NQA server.

Use the **undo nqa-server tcp-connect** command to remove the TCP listening service created.

Note that:

- You need to configure the command on the NQA server for TCP tests only.
- The IP address and port number must be consistent with those on the NQA client and must be different from those for an existing listening service.
- The IP address must be that of an interface on the NQA server. Otherwise, the configuration will be invalid.

Related commands: **nqa server enable** and **display nqa server status**.

## Examples

```
# Create a TCP listening service by using the IP address 169.254.10.2 and port 9000.
<Sysname> system-view
[Sysname] nqa server tcp-connect 169.254.10.2 9000
```

## nqa server udp-echo

### Syntax

```
nqa server udp-echo ip-address port-number  
undo nqa server udp-echo ip-address port-number
```

### View

System view

### Default Level

2: System level

### Parameters

*ip-address*: IP address specified for the UDP listening service on the NQA server.

*port-number*: Port number specified for the UDP listening service on the NQA server, in the range 1 to 50000.

### Description

Use the **nqa-server udp-echo** command to create a UDP listening service on the NQA server.

Use the **undo nqa-server udp-echo** command to remove the UDP listening service created.

Note that:

- You need to configure the command on the NQA server for UDP jitter, UDP echo and voice tests only.
- The IP address and port number must be consistent with those configured on the NQA client and must be different from those of an existing listening service.
- The IP address must be that of an interface on the NQA server. Otherwise, the configuration will be invalid.

Related commands: **nqa server enable** and **display nqa server status**.

### Examples

# Create a UDP listening service by using the IP address 169.254.10.2 and port 9000.

```
<Sysname> system-view  
[Sysname] nqa server udp-echo 169.254.10.2 9000
```

# Table of Contents

<b>1 NTP Configuration Commands</b> .....	<b>1-1</b>
NTP Configuration Commands .....	1-1
display ntp-service sessions .....	1-1
display ntp-service status .....	1-2
display ntp-service trace .....	1-4
ntp-service access .....	1-5
ntp-service authentication enable .....	1-6
ntp-service authentication-keyid .....	1-7
ntp-service broadcast-client .....	1-8
ntp-service broadcast-server .....	1-8
ntp-service in-interface disable .....	1-9
ntp-service max-dynamic-sessions .....	1-9
ntp-service multicast-client .....	1-10
ntp-service multicast-server .....	1-11
ntp-service reliable authentication-keyid .....	1-12
ntp-service source-interface .....	1-12
ntp-service unicast-peer .....	1-13
ntp-service unicast-server .....	1-14

# 1 NTP Configuration Commands

---

## NTP Configuration Commands

### display ntp-service sessions

#### Syntax

```
display ntp-service sessions [ verbose ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

**verbose:** Displays the detailed information of all NTP sessions. If you do not specify this keyword, only the brief information of the NTP sessions will be displayed.

#### Description

Use the **display ntp-service sessions** command to view the information of all NTP sessions.

#### Examples

# View the brief information of NTP sessions.

```
<Sysname> display ntp-service sessions
      source      reference  stra reach  poll now  offset  delay disper
*****
[12345]1.1.1.1    127.127.1.0  3    377    64 178    0.0    40.1    22.8
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations : 1
```

**Table 1-1** display ntp-service sessions command output description

Field	Description
source	IP address of the clock source
reference	Reference clock ID of the clock source 1) If the reference clock is the local clock, the value of this field is related to the value of the <b>stra</b> field: <ul style="list-style-type: none"> <li>When the value of the <b>stra</b> field is 0 or 1, this field will be "LOCL";</li> <li>When the <b>stra</b> field has another value, this field will be the IP address of the local clock.</li> </ul> 2) If the reference clock is the clock of another device on the network, the value of this field will be the IP address of that device.
stra	Stratum level of the clock source, which determines the clock precision. The value range is 1 to 16. The clock precision decreases from stratum 1 to stratum 16. A stratum 1 clock has the highest precision, and a stratum 16 clock is not synchronized and cannot be used as a reference clock.
reach	Reachability count of the clock source. 0 indicates that the clock source is unreachable.
poll	Poll interval in seconds, namely, the maximum interval between successive NTP messages.
now	The length of time from when the last NTP message was received or when the local clock was last updated to the current time The time is in second by default. If the time length is greater than 2048 seconds, it is displayed in minute; if greater than 300 minutes, in hour; if greater than 96 hours, in day.
offset	The offset of the system clock relative to the reference clock, in milliseconds
delay	the roundtrip delay from the local device to the clock source, in milliseconds
disper	The maximum error of the system clock relative to the reference source.
[12345]	1: Clock source selected by the system, namely, the current reference source, with a system clock stratum level less than or equal to 15 2: Stratum level of the clock source is less than or equal to 15. 3: This clock source has passed the clock selection process. 4: This clock source is a candidate clock source. 5: This clock source was created by a configuration command.
Total associations	Total number of associations

**Note**

When a device is working in the NTP broadcast/multicast server mode, the **display ntp-service sessions** command executed on the device will not display the NTP session information corresponding to the broadcast/multicast server, but the sessions will be counted in the total number of associations.

**display ntp-service status****Syntax**

```
display ntp-service status
```

## View

Any view

## Default Level

1: Monitor level

## Parameters

None

## Description

Use the **display ntp-service status** command to view the NTP service status information.

## Examples

# View the NTP service status information.

```
<Sysname> display ntp-service status
Clock status: unsynchronized
Clock stratum: 16
Reference clock ID: none
Nominal frequency: 100.0000 Hz
Actual frequency: 100.0000 Hz
Clock precision: 2^18
Clock offset: 0.0000 ms
Root delay: 0.00 ms
Root dispersion: 0.00 ms
Peer dispersion: 0.00 ms
Reference time: 00:00:00.000 UTC Jan 1 1900(00000000.00000000)
```

**Table 1-2 display ntp-service status command output description**

Field	Description
Clock status	Status of the system clock, including <ul style="list-style-type: none"><li>• Synchronized: The system clock has been synchronized.</li><li>• Unsynchronized: The system clock has not been synchronized.</li></ul>
Clock stratum	Stratum level of the system clock
Reference clock ID	After the system clock is synchronized to a remote time server, this field indicates the address of the remote time server; after the system clock is synchronized to a local reference source, this field indicates the address of the local clock source: <ul style="list-style-type: none"><li>• When the local clock has a stratum level of 1, the value of this field is "LOCL";</li><li>• When the stratum of the local clock has another value, the value of this field is the IP address of the local clock.</li></ul>
Nominal frequency	The nominal frequency of the local system hardware clock, in Hz
Actual frequency	The actual frequency of the local system hardware clock, in Hz
Clock precision	The precision of the system clock
Clock offset	The offset of the system clock relative to the reference source, in milliseconds

Field	Description
Root delay	The roundtrip delay from the local device to the primary reference source, in milliseconds
Root dispersion	The maximum error of the system clock relative to the primary reference source, in milliseconds
Peer dispersion	The maximum error of the system clock relative to the reference source, in milliseconds
Reference time	Reference timestamp

## display ntp-service trace

### Syntax

**display ntp-service trace**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display ntp-service trace** command view the brief information of each NTP server along the NTP server chain from the local device back to the primary reference source.

The **display ntp-service trace** command takes effect only if routes are available between the local device and all the devices on the NTP server chain; otherwise, this command will fail to display all the NTP servers on the NTP chain due to timeout.

### Examples

# View the brief information of each NTP server from the local device back to the primary reference source.

```
<Sysname> display ntp-service trace
server 127.0.0.1,stratum 2, offset -0.013500, synch distance 0.03154
server 133.1.1.1,stratum 1, offset -0.506500, synch distance 0.03429
refid LOCL
```

The information above shows an NTP server chain for the server 127.0.0.1: The server 127.0.0.1 is synchronized to the server 133.1.1.1, and the server 133.1.1.1 is synchronized to the local clock source.

**Table 1-3 display ntp-service trace command output description**

Field	Description
server	IP address of the NTP server

Field	Description
stratum	The stratum level of the corresponding system clock
offset	The clock offset relative to the upper-level clock, in seconds
synch distance	The synchronization distance relative to the upper-level clock, in seconds, and calculated from dispersion and roundtrip delay values.
refid	Identifier of the primary reference source. When the stratum level of the primary reference clock is 0, it is displayed as LOCL; otherwise, it is displayed as the IP address of the primary reference clock.

## ntp-service access

### Syntax

```
ntp-service access { peer | query | server | synchronization } acl-number
undo ntp-service access { peer | query | server | synchronization }
```

### View

System view

### Default Level

2: System level

### Parameters

**peer:** Specifies to permit full access. This level of right permits the peer devices to perform synchronization and control query to the local device and also permits the local device to synchronize its clock to that of a peer device. Control query refers to query of NTP status information, such as alarm information, authentication status, and clock source information.

**query:** Specifies to permit control query. This level of right permits the peer devices to perform control query to the NTP service on the local device but does not permit a peer device to synchronize its clock to that of the local device.

**server:** Specifies to permit server access and query. This level of right permits the peer devices to perform synchronization and control query to the local device but does not permit the local device to synchronize its clock to that of a peer device.

**synchronization:** Specifies to permit server access only. This level of right permits a peer device to synchronize its clock to that of the local device but does not permit the peer devices to perform control query.

*acl-number:* Basic ACL number, in the range of 2000 to 2999

### Description

Use the **ntp-service access** command to configure the access-control right for the peer devices to access the NTP services of the local device.

Use the **undo ntp-service access** command to remove the configured NTP service access-control right to the local device.

By default, the access-control right for the peer devices to access the NTP services of the local device is set to **peer**.

From the highest NTP service access-control right to the lowest one are **peer**, **server**, **synchronization**, and **query**. When a device receives an NTP request, it will match against the access-control right in this order and will use the first matched right.

Note that:

- The **ntp-service access** command provides only a minimum degree of security protection. A more secure method is identity authentication. The related command is **ntp-service authentication enable**.
- Before specifying an ACL number in the **ntp-service access** command, make sure you have already created and configured this ACL.

## Examples

# Configure the peer devices on subnet 10.10.0.0/16 to have the full access right to the local device.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-basic-2001] quit
[Sysname] ntp-service access peer 2001
```

## ntp-service authentication enable

### Syntax

```
ntp-service authentication enable
undo ntp-service authentication enable
```

### View

System view

### Default Level

2: System level

### Parameters

None

### Description

Use the **ntp-service authentication enable** command to enable NTP authentication.

Use the **undo ntp-service authentication enable** command to disable NTP authentication.

By default, NTP authentication is disabled.

Related commands: **ntp-service authentication-keyid**, **ntp-service reliable authentication-keyid**.

## Examples

# Enable NTP authentication.

```
<Sysname> system-view
[Sysname] ntp-service authentication enable
```

## ntp-service authentication-keyid

### Syntax

```
ntp-service authentication-keyid keyid authentication-mode md5 value  
undo ntp-service authentication-keyid keyid
```

### View

System view

### Default Level

2: System level

### Parameters

*keyid*: Authentication key ID, in the range of 1 to 4294967295.

**authentication-mode md5** *value*: Specifies to use the MD5 algorithm for key authentication, where *value* represents authentication key and is a string of 1 to 32 characters.

### Description

Use the **ntp-service authentication-keyid** command to set the NTP authentication key.

Use the **undo ntp-service authentication-keyid** command to remove the set NTP authentication key.

By default, no NTP authentication key is set.

In a network where there is a high security demand, the NTP authentication feature should be enabled for a system running NTP. This feature enhances the network security by means of the client-server key authentication, which prohibits a client from synchronizing with a device that has failed authentication.

After the NTP authentication key is configured, you need to configure the key as a trusted key by using the **ntp-service reliable authentication-keyid** command.



#### Caution

- Presently the system supports only the MD5 algorithm for key authentication.
  - You can set a maximum of 1,024 keys for each device.
  - If an NTP authentication key is specified as a trusted key, the key automatically changes to untrusted after you delete the key. In this case, you do not need to execute the **undo ntp-service reliable authentication-keyid** command.
- 

Related commands: **ntp-service reliable authentication-keyid**.

### Examples

# Set an MD5 authentication key, with the key ID of 10 and key value of **BetterKey**.

```
<Sysname> system-view  
[Sysname] ntp-service authentication enable  
[Sysname] ntp-service authentication-keyid 10 authentication-mode md5 BetterKey
```

## ntp-service broadcast-client

### Syntax

```
ntp-service broadcast-client
undo ntp-service broadcast-client
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **ntp-service broadcast-client** command to configure the device to work in the NTP broadcast client mode and use the current interface to receive NTP broadcast packets.

Use the **undo ntp-service broadcast-client** command to remove the configuration.

By default, the device does not work in the NTP broadcast client mode.

### Examples

```
# Configure the device to work in the broadcast client mode and receive NTP broadcast messages on
VLAN-interface 1.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service broadcast-client
```

## ntp-service broadcast-server

### Syntax

```
ntp-service broadcast-server [ authentication-keyid keyid | version number ] *
undo ntp-service broadcast-server
```

### View

Interface view

### Default Level

2: System level

### Parameters

**authentication-keyid** *keyid*: Specifies the key ID to be used for sending broadcast messages to broadcast clients, where *keyid* is in the range of 1 to 4294967295. This parameter is not meaningful if authentication is not required.

**version** *number*: Specifies the NTP version, where *number* is in the range of 1 to 3 and defaults to 3.

## Description

Use the **ntp-service broadcast-server** command to configure the device to work in the NTP broadcast server mode and use the current interface to send NTP broadcast packets.

Use the **undo ntp-service broadcast-server** command to remove the configuration.

By default, the device does not work in the NTP broadcast server mode.

## Examples

# Configure the device to work in the broadcast server mode and send NTP broadcast messages on VLAN-interface 1, using key 4 for encryption, and set the NTP version to 3.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service broadcast-server authentication-keyid 4 version 3
```

## ntp-service in-interface disable

### Syntax

```
ntp-service in-interface disable
undo ntp-service in-interface disable
```

### View

Interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **ntp-service in-interface disable** command to disable an interface from receiving NTP messages.

Use the **undo ntp-service in-interface disable** command to restore the default.

By default, all interfaces are enabled to receive NTP messages.

## Examples

# Disable VLAN-interface 1 from receiving NTP messages.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service in-interface disable
```

## ntp-service max-dynamic-sessions

### Syntax

```
ntp-service max-dynamic-sessions number
undo ntp-service max-dynamic-sessions
```

## View

System view

## Default Level

2: System level

## Parameters

*number*: Maximum number of dynamic NTP sessions that are allowed to be established, in the range of 0 to 100.

## Description

Use the **ntp-service max-dynamic-sessions** command to set the maximum number of dynamic NTP sessions that are allowed to be established locally.

Use the **undo ntp-service max-dynamic-sessions** command to restore the maximum number of dynamic NTP sessions to the system default.

By default, the number is 100.

A single device can have a maximum of 128 associations at the same time, including static associations and dynamic associations. A static association refers to an association that a user has manually created by using an NTP command, while a dynamic association is a temporary association created by the system during operation. A dynamic association will be removed if the system fails to receive messages from it over a specific long time. In the client/server mode, for example, when you carry out a command to synchronize the time to a server, the system will create a static association, and the server will just respond passively upon the receipt of a message, rather than creating an association (static or dynamic). In the symmetric mode, static associations will be created at the symmetric-active peer side, and dynamic associations will be created at the symmetric-passive peer side; in the broadcast or multicast mode, static associations will be created at the server side, and dynamic associations will be created at the client side.

## Examples

# Set the maximum number of dynamic NTP sessions allowed to be established to 50.

```
<Sysname> system-view  
[Sysname] ntp-service max-dynamic-sessions 50
```

## ntp-service multicast-client

### Syntax

```
ntp-service multicast-client [ ip-address ]  
undo ntp-service multicast-client [ ip-address ]
```

### View

Interface view

### Default Level

2: System level

## Parameters

*ip-address*: Multicast IP address, defaulting to 224.0.1.1.

## Description

Use the **ntp-service multicast-client** command to configure the device to work in the NTP multicast client mode and use the current interface to receive NTP multicast packets.

Use the **undo ntp-service multicast-client** command to remove the configuration.

By default, the device does not work in the NTP multicast client mode.

## Examples

# Configure the device to work in the multicast client mode and receive NTP multicast messages on VLAN-interface 1, and set the multicast address to 224.0.1.1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service multicast-client 224.0.1.1
```

## ntp-service multicast-server

### Syntax

**ntp-service multicast-server** [ *ip-address* ] [ **authentication-keyid** *keyid* | **ttl** *tll-number* | **version** *number* ] \*

**undo ntp-service multicast-server** [ *ip-address* ]

### View

Interface view

### Default Level

2: System level

## Parameters

*ip-address*: Multicast IP address, defaulting to 224.0.1.1.

**authentication-keyid** *keyid*: Specifies the key ID to be used for sending multicast messages to multicast clients, where *keyid* is in the range of 1 to 4294967295. This parameter is not meaningful if authentication is not required.

**tll** *tll-number*: Specifies the TTL of NTP multicast messages, where *tll-number* is in the range of 1 to 255 and defaults to 16.

**version** *number*: Specifies the NTP version, where *number* is in the range of 1 to 3 and defaults to 3.

## Description

Use the **ntp-service multicast-server** command to configure the device to work in the NTP multicast server mode and use the current interface to send NTP multicast packets.

Use the **undo ntp-service multicast-server** command to remove the configuration.

By default, the device does not work in the NTP multicast server mode.

## Examples

# Configure the device to work in the multicast server mode and send NTP multicast messages on VLAN-interface 1 to the multicast address 224.0.1.1, using key 4 for encryption, and set the NTP version to 3.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service multicast-server 224.0.1.1 version 3
authentication-keyid 4
```

## ntp-service reliable authentication-keyid

### Syntax

```
ntp-service reliable authentication-keyid keyid
undo ntp-service reliable authentication-keyid keyid
```

### View

System view

### Default Level

2: System level

### Parameters

*keyid*: Authentication key number, in the range of 1 to 4294967295.

### Description

Use the **ntp-service reliable authentication-keyid** command to specify that the created authentication key is a trusted key. When NTP authentication is enabled, a client can be synchronized only to a server that can provide a trusted authentication key.

Use the **undo ntp-service reliable authentication-keyid** command to remove the configuration.

No authentication key is configured to be trusted by default.

## Examples

# Enable NTP authentication, specify to use MD5 encryption algorithm, with the key ID of 37 and key value of **BetterKey**.

```
<Sysname> system-view
[Sysname] ntp-service authentication enable
[Sysname] ntp-service authentication-keyid 37 authentication-mode md5 BetterKey
```

# Specify this key as a trusted key.

```
[Sysname] ntp-service reliable authentication-keyid 37
```

## ntp-service source-interface

### Syntax

```
ntp-service source-interface interface-type interface-number
undo ntp-service source-interface
```

## View

System view

## Default Level

2: System level

## Parameters

*interface-type interface-number*: Specifies an interface by its interface type and interface number.

## Description

Use the **ntp-service source-interface** command to specify the source interface for NTP messages.

Use the **undo ntp-service source-interface** command to restore the default.

By default, no source interface is specified for NTP messages, and the system uses the IP address of the interface determined by the matched route as the source IP address of NTP messages.

If you do not wish the IP address of a certain interface on the local device to become the destination address of response messages, you can use this command to specify the source interface for NTP messages, so that the source IP address in NTP messages is the primary IP address of this interface.

## Examples

# Specify the source interface of NTP messages as VLAN-interface 1.

```
<Sysname> system-view  
[Sysname] ntp-service source-interface vlan-interface 1
```

## ntp-service unicast-peer

### Syntax

```
ntp-service unicast-peer [ vpn-instance vpn-instance-name ] { ip-address | peer-name }  
[ authentication-keyid keyid | priority | source-interface interface-type interface-number | version  
number ] *
```

```
undo ntp-service unicast-peer [ vpn-instance vpn-instance-name ] { ip-address | peer-name }
```

## View

System view

## Default Level

2: System level

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies a VPN instance by its name, where *vpn-instance-name* is a string of 1 to 31 characters.

*ip-address*: IP address of the symmetric-passive peer. It must be a unicast address, rather than a broadcast address, a multicast address or the IP address of the local clock.

*peer-name*: Host name of the symmetric-passive peer, a string of 1 to 20 characters.

**authentication-keyid** *keyid*: Specifies the key ID to be used for sending NTP messages to the peer, where *keyid* is in the range of 1 to 4294967295.

**priority:** Specifies the peer designated by *ip-address* or *peer-name* as the first choice under the same condition.

**source-interface** *interface-type interface-number*. Specifies the source interface for NTP messages. In an NTP message the local device sends to its peer, the source IP address is the primary IP address of this interface. *interface-type interface-number* represents the interface type and number.

**version** *number*. Specifies the NTP version, where *number* is in the range of 1 to 3 and defaults to 3.

## Description

Use the **ntp-service unicast-peer** command to designate a symmetric-passive peer for the device.

Use the **undo ntp-service unicast-peer** command to remove the symmetric-passive peer designated for the device.

No symmetric-passive peer is designated for the device by default.



### Note

- To synchronize the switch to another device in a VPN, you need to provide **vpn-instance** *vpn-instance-name* in your command.
  - If you include **vpn-instance** *vpn-instance-name* in the **undo ntp-service unicast-peer** command, the command will remove the symmetric-passive peer with the IP address of *ip-address* in the specified VPN; if you do not include **vpn-instance** *vpn-instance-name* in this command, the command will remove the symmetric-passive peer with the IP address of *ip-address* in the public network.
- 

## Examples

# Designate the device with the IP address of 10.1.1.1 as the symmetric-passive peer of the device, configure the device to run NTP version 3, and specify the source interface of NTP messages as VLAN-interface 1.

```
<Sysname> system-view
[Sysname] ntp-service unicast-peer 10.1.1.1 version 3 source-interface vlan-interface 1
```

## ntp-service unicast-server

### Syntax

```
ntp-service unicast-server [ vpn-instance vpn-instance-name ] { ip-address | server-name }
[ authentication-keyid keyid | priority | source-interface interface-type interface-number | version
number ] *
```

```
undo ntp-service unicast-server [ vpn-instance vpn-instance-name ] { ip-address | server-name }
```

### View

System view

### Default Level

2: System level

## Parameters

**vpn-instance** *vpn-instance-name*: Specifies a VPN instance by its name, where *vpn-instance-name* is a string of 1 to 31 characters.

*ip-address*: IP address of the NTP server. It must be a unicast address, rather than a broadcast address, a multicast address or the IP address of the local clock.

*server-name*: Host name of the NTP server, a string of 1 to 20 characters.

**authentication-keyid** *keyid*: Specifies the key ID to be used for sending NTP messages to the NTP server, where *keyid* is in the range of 1 to 4294967295.

**priority**: Specifies this NTP server as the first choice under the same condition.

**source-interface** *interface-type interface-number*: Specifies the source interface for NTP messages. In an NTP message the local device sends to the NTP server, the source IP address is the primary IP address of this interface. *interface-type interface-number* represents the interface type and number.

**version** *number*: Specifies the NTP version, where *number* is in the range of 1 to 3 and defaults to 3.

## Description

Use the **ntp-service unicast-server** command to designate an NTP server for the device.

Use the **undo ntp-service unicast-server** command to remove an NTP server designated for the device.

No NTP server is designated for the device by default.



### Note

- To synchronize the switch to another device in a VPN, you need to provide **vpn-instance** *vpn-instance-name* in your command.
  - If you include **vpn-instance** *vpn-instance-name* in the **undo ntp-service unicast-server** command, the command will remove the NTP server with the IP address of *ip-address* in the specified VPN; if you do not include **vpn-instance** *vpn-instance-name* in this command, the command will remove the NTP server with the IP address of *ip-address* in the public network.
- 

## Examples

# Designate NTP server 10.1.1.1 for the device, and configure the device to run NTP version 3.

```
<Sysname> system-view
[Sysname] ntp-service unicast-server 10.1.1.1 version 3
```

# Table of Contents

<b>1 VRRP Configuration Commands</b> .....	<b>1-1</b>
IPv4-Based VRRP Configuration Commands .....	1-1
display vrrp .....	1-1
display vrrp statistics .....	1-3
reset vrrp statistics.....	1-5
vrrp method .....	1-6
vrrp un-check ttl .....	1-6
vrrp vrid authentication-mode .....	1-7
vrrp vrid preempt-mode .....	1-8
vrrp vrid priority .....	1-9
vrrp vrid timer advertise .....	1-10
vrrp vrid track .....	1-11
vrrp vrid track interface .....	1-12
vrrp vrid virtual-ip .....	1-13
VRRP Configuration Commands for IPv6.....	1-14
display vrrp ipv6.....	1-14
display vrrp ipv6 statistics.....	1-16
reset vrrp ipv6 statistics .....	1-18
vrrp ipv6 method.....	1-18
vrrp ipv6 vrid authentication-mode .....	1-19
vrrp ipv6 vrid preempt-mode .....	1-20
vrrp ipv6 vrid priority .....	1-21
vrrp ipv6 vrid timer advertise .....	1-22
vrrp ipv6 vrid track interface .....	1-23
vrrp ipv6 vrid virtual-ip .....	1-24

# 1 VRRP Configuration Commands

---



## Note

- The term router in this document refers to a router in a generic sense or a Layer 3 switch.
  - At present, the interfaces that VRRP involves can only be VLAN interfaces unless otherwise specified.
- 

## IPv4-Based VRRP Configuration Commands

### display vrrp

#### Syntax

```
display vrrp [ verbose ] [ interface interface-type interface-number [ vrid virtual-router-id ] ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

**verbose**: Displays detailed state information of VRRP group(s).

**interface** *interface-type interface-number*: Displays VRRP group state information of the specified interface. *interface-type interface-number* specifies an interface by its type and number.

**vrid** *virtual-router-id*: Displays state information of the specified VRRP group. *virtual-router-id* specifies a VRRP group by its group number, in the range 1 to 255.

#### Description

Use the **display vrrp** command to display the state information of VRRP group(s).

If you do not specify **verbose**, only the brief state information of VRRP group is displayed.

If you specify both an interface and a VRRP group, only the state information of the specified VRRP group on the interface is displayed; if you only specify an interface, the state information of all the VRRP groups on the interface is displayed; if you specify neither, the state information of all the VRRP groups on the device is displayed.

#### Examples

```
# Display brief information about all VRRP groups on the device.
```

```

<Sysname> display vrrp
IPv4 Standby Information:
Run Method      : VIRTUAL-MAC
Total number of virtual routers: 1
Interface       VRID  State      Run      Adver.   Auth      Virtual
                Pri   Time      Type     IP
-----
Vlan100         1    Master    100     1        NONE     10.10.10.2

```

# Display detailed information about all VRRP groups on the device.

```

<Sysname> display vrrp verbose
IPv4 Standby Information:
Run Method      : VIRTUAL-MAC
Total number of virtual routers: 1
Interface       : Vlan-interface100
VRID            : 1                      Adver. Timer   : 1
Admin Status    : UP                      State          : Master
Config Pri     : 100                    Run Pri        : 100
Preempt Mode    : YES                    Delay Time     : 0
Auth Type      : NONE
Track IF        : Vlan200                Pri Reduced    : 10
Track Object    : 1                      Pri Reduced    : 10
Track Object    : 2                      Switchover
Virtual IP      : 10.10.10.2
Virtual MAC     : 0000-5e00-0101
Master IP      : 10.10.10.1

```

**Table 1-1 display vrrp command output description**

Field	Description
Run Method	Current VRRP running mode, including <ul style="list-style-type: none"> <li>REAL-MAC: real MAC mode, that is, the virtual IP address of the VRRP group is associated with the real MAC address of the interface</li> <li>VIRTUAL-MAC: virtual MAC mode, that is, the virtual IP address of the VRRP group is associated with the virtual router MAC address</li> </ul>
Total number of virtual routers	Number of VRRP groups
Interface	Interface to which the VRRP group belongs
VRID	Serial number of the VRRP group
Adver. Timer	VRRP advertisement interval, in seconds
Admin Status	Administrative state: UP or DOWN
State	Status of the router in the VRRP group, master, backup, or initialize
Config Pri	Configured priority
Run Pri	Running priority

Field	Description
Preempt Mode	Preemptive mode, including <ul style="list-style-type: none"> <li>• YES: The router in the VRRP group works in preemptive mode</li> <li>• NO: The router in the VRRP group works in non preemptive mode</li> </ul>
Delay Time	Preemption delay, in seconds
Auth Type	Authentication type, including <ul style="list-style-type: none"> <li>• NONE: No authentication</li> <li>• SIMPLE TEXT: Simple text authentication</li> <li>• MD5: MD5 authentication</li> </ul>
Track IF	The interface to be tracked. It is displayed only after the execution of the <b>vrrp vrid track interface</b> command.
Track Object	The object to be tracked. After the execution of the <b>vrrp vrid track</b> command, it is displayed if the specified Track object to be monitored exists.
Pri Reduced	The priority value that is reduced when the monitored interface is down or when the status of the monitored Track object turns to <b>negative</b> . It may be displayed when the Track IF or Track Object field is displayed.
Switchover	Switchover mode. If the status of the monitored Track object turns to <b>negative</b> , the backup will switch to the master immediately. It may be displayed when the Track Object field is displayed.
Virtual IP	Virtual IP addresses of the VRRP group
Virtual MAC	Virtual MAC address corresponding to the virtual IP address of the VRRP group. It is displayed only when the router is in the state of master.
Master IP	Primary IP address of the interface which belongs to the router in the state of master

## display vrrp statistics

### Syntax

**display vrrp statistics** [ **interface** interface-type interface-number [ **vrid** virtual-router-id ] ]

### View

Any view

### Default Level

1: Monitor level

### Parameters

**interface** *interface-type interface-number*: Displays VRRP group statistics of the specified interface. *interface-type interface-number* specifies an interface by its type and number.

**vrid** *virtual-router-id*: Displays statistics of the specified VRRP group. *virtual-router-id* specifies a VRRP group by its group number, in the range 1 to 255.

## Description

Use the **display vrrp statistics** command to display statistics about VRRP group(s).

If you specify both an interface and a VRRP group, only the statistics about the specified VRRP group on the interface are displayed; if you only specify an interface, the statistics about all the VRRP groups on the interface are displayed; if you specify neither, the statistics about all the VRRP groups on the device are displayed.

You can use the **reset vrrp statistics** command to clear the VRRP group statistics.

Related commands: **reset vrrp statistics**.

## Examples

# Display the statistics about all VRRP groups.

```
<Sysname> display vrrp statistics
Interface          : Vlan-interface100
VRID               : 1
Checksum Errors    : 16          Version Errors          : 0
Invalid Type Pkts Rcvd : 0          Advertisement Interval Errors : 0
IP TTL Errors      : 0          Auth Failures           : 0
Invalid Auth Type  : 0          Auth Type Mismatch      : 0
Packet Length Errors : 0        Address List Errors     : 0
Become Master      : 1          Priority Zero Pkts Rcvd  : 0
Advertise Rcvd     : 16        Priority Zero Pkts Sent  : 0
Advertise Sent     : 40

Interface          : Vlan-interface200
VRID               : 105
Checksum Errors    : 0          Version Errors          : 0
Invalid Type Pkts Rcvd : 0        Advertisement Interval Errors : 0
IP TTL Errors      : 0          Auth Failures           : 0
Invalid Auth Type  : 0          Auth Type Mismatch      : 0
Packet Length Errors : 0        Address List Errors     : 0
Become Master      : 0          Priority Zero Pkts Rcvd  : 0
Advertise Rcvd     : 0          Priority Zero Pkts Sent  : 0
Advertise Sent     : 30

Global statistics
Checksum Errors    : 16
Version Errors     : 0
VRID Errors       : 20
```

**Table 1-2 display vrrp statistics** command output description

Field	Description
Interface	Interface to which the VRRP group belongs
VRID	Serial number of the VRRP group
Checksum Errors	Number of packets with checksum errors
Version Errors	Number of packets with version errors

Field	Description
Invalid Type Pkts Rcvd	Number of packets with incorrect packet type
Advertisement Interval Errors	Number of packets with advertisement interval errors
IP TTL Errors	Number of packets with TTL errors
Auth Failures	Number of packets with authentication failures
Invalid Auth Type	Number of packets with authentication failures due to invalid authentication types
Auth Type Mismatch	Number of packets with authentication failures due to mismatching authentication types
Packet Length Errors	Number of packets with VRRP packet length errors
Address List Errors	Number of packets with virtual IP address list errors
Become Master	Number of times that the router worked as the master
Priority Zero Pkts Rcvd	Number of received advertisements with the priority of 0
Advertise Rcvd	Number of received advertisements
Advertise Sent	Number of advertisements sent
Global statistics	Statistics about all VRRP groups
Checksum Errors	Total number of packets with checksum errors
Version Errors	Total number of packets with version errors
VRID Errors	Total number of packets with VRID errors

## reset vrrp statistics

### Syntax

```
reset vrrp statistics [ interface interface-type interface-number [ vrid virtual-router-id ] ]
```

### View

User view

### Default Level

1: Monitor level

### Parameters

**interface** *interface-type interface-number*: Clears VRRP group statistics of a specified interface. *interface-type interface-number* specifies an interface by its type and number.

**vrid** *virtual-router-id*: Clears VRRP statistics of the specified VRRP group. *virtual-router-id* specifies a VRRP group by its group number, in the range 1 to 255.

### Description

Use the **reset vrrp statistics** command to clear VRRP group statistics.

If you specify both an interface and a VRRP group, the statistics about the specified VRRP group on the specified interface are cleared; if you specify only the interface, the statistics about all the VRRP groups

on the interface are cleared; if you specify neither, the statistics about all the VRRP groups on the device are cleared.

Related commands: **display vrrp statistics**.

## Examples

```
# Clear the statistics about all the VRRP groups on the device.
```

```
<Sysname> reset vrrp statistics
```

## vrrp method

### Syntax

```
vrrp method { real-mac | virtual-mac }
```

```
undo vrrp method
```

### View

System view

### Default Level

2: System level

### Parameters

**real-mac**: Associates the real MAC address of the interface with the virtual IP addresses of the VRRP groups.

**virtual-mac**: Associates the virtual MAC address of a VRRP group with the virtual IP address of the VRRP group.

### Description

Use the **vrrp method** command to set the association between the virtual IP addresses and the MAC addresses of the VRRP groups.

Use the **undo vrrp method** command to restore the default association.

By default, the virtual MAC address of a VRRP group is associated with the virtual IP address of the VRRP group.

Note that you need to configure the association between the virtual IP address and the MAC address before creating any VRRP group. Otherwise, your configuration will fail.

## Examples

```
# Associate the virtual IP address of a VRRP group with the real MAC address of the interface.
```

```
<Sysname> system-view
```

```
[Sysname] vrrp method real-mac
```

## vrrp un-check ttl

### Syntax

```
vrrp un-check ttl
```

```
undo vrrp un-check ttl
```

## View

Interface view

## Default Level

2: System level

## Parameters

None

## Description

Use the **vrrp un-check ttl** command to disable TTL check on VRRP packets.

Use the **undo vrrp un-check ttl** command to enable TTL check on VRRP packets.

By default, TTL check on VRRP packets is enabled.

The master of a VRRP group periodically sends VRRP advertisements to indicate its existence. The VRRP advertisements are multicast onto the local network segment and not forwarded by a router, and therefore the packet TTL value will not be changed. When the master of a VRRP group advertises VRRP packets, it sets the packet TTL to 255. After you configure to check the VRRP packet TTL, when the backups of the VRRP group receive VRRP packets, they check the packet TTL and drop the VRRP packets whose TTL is smaller than 255, so as to prevent attacks from other network segments.

As devices of different vendors may achieve VRRP in a different way, when the device is interoperating with devices of other vendors, VRRP packet TTL check may result in dropping packets that should not be dropped. In this case, you can use the command to disable TTL check on VRRP packets.

## Examples

# Disable TTL check on VRRP packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp un-check ttl
```

## vrrp vrid authentication-mode

### Syntax

**vrrp vrid** *virtual-router-id* **authentication-mode** { **md5** | **simple** } *key*

**undo vrrp vrid** *virtual-router-id* **authentication-mode**

### View

Interface view

### Default Level

2: System level

### Parameters

*virtual-router-id*: VRRP group number, in the range 1 to 255.

**simple**: Plain text authentication mode.

**md5**: Authentication using the MD5 algorithm.

*key*: Authentication key, which is case sensitive.

- When **simple** authentication applies, the authentication key is in plain text with a length of 1 to 8 characters.
- When **md5** authentication applies, the authentication key is in MD5 cipher text or in plain text and the length of the key depends on its input format. If the key is input in plain text, its length is 1 to 8 characters, such as 1234567; if the key is input in cipher text, its length must be 24 characters, such as `_(TT8F)Y\5SQ=^Q`MAF4<1!!`.

## Description

Use the **vrpp vrid authentication-mode** command to configure authentication mode and authentication key for a VRRP group to send and receive VRRP packets.

Use the **undo vrpp vrid authentication-mode** command to restore the default.

By default, authentication is disabled.

Note that:

- Before executing the command, create a VRRP group on an interface and configure the virtual IP address of the VRRP group.
- You may configure different authentication modes and authentication keys for the VRRP groups on an interface. However, the members of the same VRRP group must use the same authentication mode and authentication key.

## Examples

# Set the authentication mode to **simple** and authentication key to **Sysname** for VRRP group 1 on interface VLAN-interface 2 to send and receive VRRP packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrpp vrid 1 virtual-ip 10.1.1.1
[Sysname-Vlan-interface2] vrpp vrid 1 authentication-mode simple Sysname
```

## vrpp vrid preempt-mode

### Syntax

```
vrpp vrid virtual-router-id preempt-mode [ timer delay delay-value ]
```

```
undo vrpp vrid virtual-router-id preempt-mode [ timer delay ]
```

### View

Interface view

### Default Level

2: System level

### Parameters

*virtual-router-id*: Virtual router ID or VRRP group number, in the range 1 to 255.

**timer delay** *delay-value*: Sets preemption delay. The *delay-value* argument is in the range of 0 to 255 seconds and defaults to 0 seconds.

## Description

Use the **vrp vrid preempt-mode** command to enable preemption on the router and configure its preemption delay in the specified VRRP group.

Use the **undo vrrp vrid preempt-mode** command to disable preemption on the router in the specified VRRP group, that is, specify the router to work in the non-preemptive mode.

Use the **undo vrrp vrid preempt-mode timer delay** command to restore the default preemption delay, that is, zero seconds.

The default mode is immediate preemption without delay.

On an unstable network, the VRRP group member in the backup state may not normally receive the packets from the master due to network congestion, resulting in frequent master/backup state transition of the VRRP group members. Preemption delay is introduced to solve this problem. With a preemption delay set, if the backup member does not receive the packet from the master member on time, it waits for a period to see whether it can receive any packet from the master. If the specified period elapses but it still receives no packet from the master, it becomes the master.

Note that before executing the command, you need to create a VRRP group on an interface and configure the virtual IP address of the VRRP group.

## Examples

```
# Enable preemption on the router in VRRP group 1, and set the preemption delay to five seconds.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

## vrp vrid priority

### Syntax

**vrp vrid** virtual-router-id **priority** priority-value

**undo vrrp vrid** *virtual-router-id* **priority**

### View

Interface view

### Default Level

2: System level

### Parameters

*virtual-router-id*: VRRP group number, in the range 1 to 255.

*priority-value*: Priority value of the router in the specified VRRP group, in the range 1 to 254, A higher number indicates a higher priority.

## Description

Use the **vrp vrid priority** command to configure the priority of the router in the specified VRRP group.

Use the **undo vrrp vrid priority** command to restore the default.

By default, the priority of a router in a VRRP group is 100.

- Before executing the command, create a VRRP group on an interface and configure the virtual IP address of the VRRP group.
- In VRRP, the role that a router plays in a VRRP group depends on its priority. A higher priority means that the router is more likely to become the master. Note that priority 0 is reserved for special use and 255 for the IP address owner.
- If the router is the IP address owner, its priority is always 255. Therefore, it will be the master so long as it is functioning normally.

## Examples

```
# Set the priority of VRRP group 1 on interface VLAN-interface 2 to 150.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Vlan-interface2] vrrp vrid 1 priority 150
```

## vrrp vrid timer advertise

### Syntax

```
vrrp vrid virtual-router-id timer advertise adver-interval
```

```
undo vrrp vrid virtual-router-id timer advertise
```

### View

Interface view

### Default Level

2: System level

### Parameters

*virtual-router-id*: VRRP group number, in the range 1 to 255.

*adver-interval*: Interval at which the master in the specified VRRP group sends VRRP advertisements. It ranges from 1 to 255 seconds.

### Description

Use the **vrrp vrid timer advertise** command to configure the Adver\_Timer of the specified VRRP group.

Use the **undo vrrp vrid timer advertise** command to restore the default.

By default the Adver\_Timer is 1 second.

The Adver\_Timer controls the interval at which the master sends VRRP packets.

Note that:

- Before executing the command, create a VRRP group on an interface and configure the virtual IP address of the VRRP group.
- Routers in the same VRRP group must use the same Adver\_Timer setting.

## Examples

```
# Set the master in VRRP group 1 to send VRRP advertisements at intervals of five seconds.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Vlan-interface2] vrrp vrid 1 timer advertise 5
```

## vrrp vrid track

### Syntax

```
vrrp vrid virtual-router-id track track-entry-number [ reduced priority-reduced | switchover ]
undo vrrp vrid virtual-router-id track [ track-entry-number ]
```

### View

Interface view

### Default Level

2: System level

### Parameters

*virtual-router-id*: VRRP group number, in the range 1 to 255.

**track** *track-entry-number*: Specifies a Track object to be monitored by its number. *track-entry-number* ranges from 1 to 1024.

**reduced** *priority-reduced*: Specifies the value by which the priority decreases. *priority-reduced* ranges from 1 to 255 and defaults to 10.

**switchover**: Switchover mode of a router. If the status of the monitored Track object turns to **negative** and the router is a backup in the VRRP group, it turns to the master immediately.

### Description

Use the **vrrp vrid track** command to specify the Track object to be monitored. If the status of the monitored Track object changes to negative, the priority of the router decreases by a specified value or the router immediately switches to the master.

Use the **undo vrrp vrid track** command to cancel the specified Track object.

By default, no Track object is specified to be monitored.

Note that:

- Before executing the command, create a VRRP group on an interface and configure the virtual IP address of the VRRP group.
- When the router is the IP address owner, you cannot perform the configuration.
- When the status of the monitored Track object turns from negative to positive, the corresponding router restores its priority automatically.
- The Track object specified in this command can be nonexistent. You can use the **vrrp vrid track** command to specify a Track object, and then create the Track object using the **track** command.



## Note

- If the Track object specified in the **vrrp vrid track** command does not exist, this configuration is saved (you can see the configuration by using the **display this** command), but the monitoring function does not take effect. After that, if you create the specified Track object on the device, the monitoring function will take effect, and you can see the Track object by using the **display vrrp verbose** command.
  - For details of the Track object, refer to *Track Configuration* in the *System Volume*.
- 

## Examples

# Configure to monitor Track object 1, making the priority of VRRP group 1 on VLAN-interface 2 decrease by 50 when Track object 1 turns to negative.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Vlan-interface2] vrrp vrid 1 track 1 reduced 50
```

## vrrp vrid track interface

### Syntax

**vrrp vrid** virtual-router-id **track interface** interface-type interface-number [ **reduced** priority-reduced ]  
**undo vrrp vrid** virtual-router-id **track** [ **interface** interface-type interface-number ]

### View

Interface view

### Default Level

2: System level

### Parameters

*virtual-router-id*: VRRP group number, in the range 1 to 255.

**interface** *interface-type interface-number*: Specifies an interface to be tracked by its type and number.

**reduced** *priority-reduced*: Value by which the priority decrements. *priority-reduced* ranges from 1 to 255 and defaults to 10.

### Description

Use the **vrrp vrid track interface** command to configure to track the specified interface.

Use the **undo vrrp vrid track interface** command to disable tracking the specified interface.

By default, no interface is tracked.

If the uplink interface of a router in a VRRP group fails, normally the VRRP group cannot be aware of the uplink failure. If the router is the master of the VRRP group, hosts on the LAN will not be able to access the external network because of the uplink failure. You can solve the problem through the function of tracing a specified interface. In this case, it is the uplink interface. After you configure to monitor the

uplink interface, when the uplink interface goes down, the priority of the master is automatically decreased by a specified value, allowing a higher priority router in the VRRP group to become the master.

Note that:

- Before executing the command, create a VRRP group on an interface and configure the virtual IP address of the VRRP group.
- When the router is the owner of the IP address, you cannot perform the configuration.
- When the status of the tracked interface turns from down to up, the corresponding router restores its priority automatically.

## Examples

# On interface VLAN-interface 2, set the interface to be tracked as VLAN-interface 1, making the priority of VRRP group 1 on interface VLAN-interface 2 decrement by 50 when VLAN-interface 1 goes down.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Vlan-interface2] vrrp vrid 1 track interface vlan-interface 1 reduced 50
```

## vrrp vrid virtual-ip

### Syntax

```
vrrp vrid virtual-router-id virtual-ip virtual-address
undo vrrp vrid virtual-router-id [ virtual-ip virtual-address ]
```

### View

Interface view

### Default Level

2: System level

### Parameters

*virtual-router-id*: VRRP group number, in the range 1 to 255.

*virtual-address*: Virtual IP address.

### Description

Use the **vrrp vrid virtual-ip** command to create a VRRP group, and configure a virtual IP address for it, or, add another virtual IP address for an existing VRRP group.

Use the **undo vrrp vrid virtual-ip** command to remove an existing VRRP group or the virtual IP address of the VRRP group.

By default, no VRRP group is created.

Note that:

- The system removes a VRRP group after you delete all the virtual IP addresses in it.
- The virtual IP address of the VRRP group cannot be 0.0.0.0, 255.255.255.255, loopback address, non A/B/C address and other illegal IP addresses such as 0.0.0.1.

- Only when the configured virtual IP address and the interface IP address belong to the same segment and are legal host addresses can the VRRP group operate normally. If they are not in the same network segment, or the configured IP address is the network address or network broadcast address of the network segment that the interface IP address belongs to, though you can perform the configuration successfully, the state of the VRRP group is always **Initialize**, that is, VRRP does not take effect in this case.

## Examples

```
# Create VRRP group 1 and set its virtual IP address to 10.10.10.10.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.10.10.10
```

```
# Add virtual IP address 10.10.10.11 to VRRP group 1.
```

```
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.10.10.11
```

## VRRP Configuration Commands for IPv6

### display vrrp ipv6

#### Syntax

```
display vrrp ipv6 [ verbose ] [ interface interface-type interface-number [ vrid virtual-router-id ] ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

**verbose**: Displays detailed state information of VRRP group(s).

**interface** *interface-type interface-number*: Displays VRRP group state information of the specified interface. *interface-type interface-number* specifies an interface by its type and number.

**vrid** *virtual-router-id*: Displays state information of the specified VRRP group. *virtual-router-id* specifies a VRRP group by its group number, in the range 1 to 255.

#### Description

Use the **display vrrp ipv6** command to display the state information of VRRP group(s) for IPv6.

If you do not specify **verbose**, only the brief state information of VRRP group(s) is displayed.

If you specify both an interface and a VRRP group, only the state information of the specified VRRP group on the interface is displayed; if you only specify an interface, the state information of all the VRRP groups on the interface is displayed; if you specify neither, the state information of all the VRRP groups on the device is displayed.

## Examples

```
# Display brief information about all VRRP groups on the device for IPv6.
```

```
<Sysname> display vrrp ipv6
```

```

IPv6 Standby Information:
Run Method      : VIRTUAL-MAC
Total number of virtual routers: 1
Interface       VRID  State      Run      Adver.   Auth      Virtual
                Pri   Time      Type     Type     IP
-----
Vlan100         1    Master    100     100     NONE     FE80::1

```

# Display detailed information about all VRRP groups on the device.

```

<Sysname> display vrrp ipv6 verbose
IPv6 Standby Information:
Run Method      : VIRTUAL-MAC
Total number of virtual routers: 1
Interface       : Vlan-interface100
VRID            : 1
Admin Status    : UP
Config Pri      : 100
Preempt Mode    : YES
Auth Type       : NONE
Track IF        : Vlan200
Virtual IP      : FE80::1
Virtual MAC     : 0000-5e00-0201
Master IP       : FE80::20F:E2FF:FE49:8060
Adver. Timer    : 100
State           : Master
Run Pri         : 100
Delay Time      : 0
Pri Reduced     : 10

```

**Table 1-3 display vrrp ipv6 command output description**

Field	Description
Run Method	Current VRRP running mode, including <ul style="list-style-type: none"> <li>REAL-MAC: real MAC mode, that is, the virtual IP address of the VRRP group is associated with the real MAC address of the interface</li> <li>VIRTUAL-MAC: virtual MAC mode, that is, the virtual IP address of the VRRP group is associated with the virtual router MAC address</li> </ul>
Total number of virtual routers	Number of VRRP groups
Interface	Interface to which the VRRP group belongs
VRID	Series number of the VRRP group
Adver. Timer	VRRP advertisement interval in centiseconds
Admin Status	Administrative state: UP or DOWN
State	Status of the router in the VRRP group, master, backup, or initialize
Config Pri	Configured priority
Run Pri	Running priority
Preempt Mode	Preemptive mode, including <ul style="list-style-type: none"> <li>YES: The router in the VRRP group works in preemptive mode</li> <li>NO: The router in the VRRP group works in non preemptive mode</li> </ul>
Delay Time	Preemption delay, in seconds

Field	Description
Auth Type	Authentication type, including <ul style="list-style-type: none"> <li>• NONE: No authentication</li> <li>• SIMPLE TEXT: Simple text authentication</li> </ul>
Track IF	The interface to be tracked. It is displayed only after the execution of the <b>vrrp ipv6 vrid track interface</b> command.
Pri Reduced	The priority value that is reduced when the interface being tracked is down. It is displayed only after the execution of the <b>vrrp ipv6 vrid track interface</b> command.
Virtual IP	Virtual IPv6 addresses of the VRRP group
Virtual MAC	Virtual MAC address corresponding to the virtual IPv6 address of the VRRP group. It is displayed only when the router is in the state of master.
Master IP	Primary IPv6 address of the interface which belongs to the router in the state of master

## display vrrp ipv6 statistics

### Syntax

```
display vrrp ipv6 statistics [ interface interface-type interface-number [ vrid virtual-router-id ] ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**interface** *interface-type interface-number*: Displays VRRP group statistics information of the specified interface. *interface-type interface-number* specifies an interface by its type and number.

**vrid** *virtual-router-id*: Displays statistics information of the specified VRRP group. *virtual-router-id* specifies a VRRP group by its group number, in the range 1 to 255.

### Description

Use the **display vrrp ipv6 statistics** command to display statistics about VRRP group(s) for IPv6.

If you specify both an interface and a VRRP group, only the statistics about the specified VRRP group on the interface are displayed; if you only specify an interface, the statistics about all the VRRP groups on the interface are displayed; if you specify neither, the statistics about all the VRRP groups on the device are displayed.

You can use the **reset vrrp ipv6 statistics** command to clear the VRRP group statistics.

Related commands: **reset vrrp ipv6 statistics**.

### Examples

```
# Display the statistics about all VRRP groups for IPv6.
```

```

<Sysname> display vrrp ipv6 statistics
Interface          : Vlan-interface100
VRID               : 80
Checksum Errors   : 0           Version Errors           : 0
Invalid Type Pkts Rcvd : 0       Advertisement Interval Errors : 0
Hop Limit Errors  : 0           Auth Failures             : 0
Invalid Auth Type : 0           Auth Type Mismatch        : 0
Packet Length Errors : 0       Address List Errors        : 0
Become Master     : 1           Priority Zero Pkts Rcvd    : 0
Advertise Rcvd    : 0           Priority Zero Pkts Sent    : 0
Advertise Sent    : 20

Interface          : Vlan-interface200
VRID               : 10
Checksum Errors   : 0           Version Errors           : 0
Invalid Type Pkts Rcvd : 0       Advertisement Interval Errors : 0
Hop Limit Errors  : 0           Auth Failures             : 0
Invalid Auth Type : 0           Auth Type Mismatch        : 0
Packet Length Errors : 0       Address List Errors        : 0
Become Master     : 1           Priority Zero Pkts Rcvd    : 0
Advertise Rcvd    : 0           Priority Zero Pkts Sent    : 0
Advertise Sent    : 30

Global statistics
Checksum Errors   : 0
Version Errors    : 0
VRID Errors       : 1439

```

**Table 1-4** display vrrp ipv6 statistics command output description

Field	Description
Interface	Interface to which the VRRP group belongs
VRID	Serial number of the VRRP group
Checksum Errors	Number of packets with checksum errors
Version Errors	Number of packets with version errors
Invalid Type Pkts Rcvd	Number of packets with incorrect packet type
Advertisement Interval Errors	Number of packets with advertisement interval errors
Hop Limit Errors	Number of packets with hop limit errors
Auth Failures	Number of packets with authentication failures
Invalid Auth Type	Number of packets with authentication failures due to invalid authentication types
Auth Type Mismatch	Number of packets with authentication failures due to mismatching authentication types
Packet Length Errors	Number of packets with VRRP packet length errors
Address List Errors	Number of packets with virtual IPv6 address list errors
Become Master	Number of times that the router worked as the master

Field	Description
Priority Zero Pkts Rcvd	Number of received advertisements with the priority of 0
Advertise Rcvd	Number of received advertisements
Advertise Sent	Number of advertisements sent
Global statistics	Statistics about all VRRP groups
Checksum Errors	Total number of packets with checksum errors
Version Errors	Total number of packets with version errors
VRID Errors	Total number of packets with VRID errors

## reset vrrp ipv6 statistics

### Syntax

```
reset vrrp ipv6 statistics [ interface interface-type interface-number [ vrid virtual-router-id ] ]
```

### View

User view

### Default Level

1: Monitor level

### Parameters

**interface** *interface-type interface-number*: Clears VRRP group statistics of a specific interface. *interface-type interface-number* specifies an interface by its type and number.

**vrid** *virtual-router-id*: Clears VRRP statistics of the specified VRRP group. *virtual-router-id* specifies a VRRP group by its group number, in the range 1 to 255.

### Description

Use the **reset vrrp ipv6 statistics** command to clear VRRP group statistics.

If you specify both an interface and a VRRP group, the statistics about the specified VRRP group on the specified interface are cleared; if you specify only an interface, the statistics about all the VRRP groups on the interface are cleared; if you specify neither, the statistics about all the VRRP groups on the device are cleared.

Related commands: **display vrrp ipv6 statistics**.

### Examples

```
# Clear the statistics about all the VRRP groups on the device.
```

```
<Sysname> reset vrrp ipv6 statistics
```

## vrrp ipv6 method

### Syntax

```
vrrp ipv6 method { real-mac | virtual-mac }
```

```
undo vrrp ipv6 method
```

## View

System view

## Default Level

2: System level

## Parameters

**real-mac:** Associates the real MAC address of the interface with the virtual IPv6 addresses of the VRRP groups.

**virtual-mac:** Associates the virtual MAC address of a VRRP group with the virtual IPv6 address of the VRRP group.

## Description

Use the **vrpp ipv6 method** command to set the association between the virtual IPv6 addresses and the MAC addresses of the VRRP groups.

Use the **undo vrpp ipv6 method** command to restore the default association.

By default, the virtual MAC address of a VRRP group is associated with the virtual IP address of the VRRP group.

Note that you need to configure the association between the virtual IPv6 address and the MAC address before creating any VRRP group. Otherwise, your configuration will fail.

## Examples

# Associate the virtual IPv6 address of a VRRP group with the real MAC address of the interface.

```
<Sysname> system-view  
[Sysname] vrpp ipv6 method real-mac
```

## vrpp ipv6 vrid authentication-mode

### Syntax

**vrpp ipv6 vrid** *virtual-router-id* **authentication-mode simple** *key*

**undo vrpp ipv6 vrid** *virtual-router-id* **authentication-mode**

### View

Interface view

### Default Level

2: System level

### Parameters

*virtual-router-id:* VRRP group number, in the range 1 to 255.

**simple:** Sets the authentication mode to plain text authentication.

*key:* Authentication key of 1 to 8 case-sensitive characters in plain text.

## Description

Use the **vrrip ipv6 vrid authentication-mode** command to configure authentication mode and authentication key for the VRRP groups to send and receive VRRP packets.

Use the **undo vrrip ipv6 vrid authentication-mode** command to restore the default.

By default, authentication is disabled.

Note that:

- Before executing the command, create a VRRP group on an interface and configure the virtual IP address of the VRRP group.
- You may configure different authentication types and authentication keys for the VRRP groups on an interface. However, the members of the same VRRP group must use the same authentication mode and authentication key.

## Examples

# Set the authentication mode to **simple** and authentication key to **test** for VRRP group 10 on interface VLAN-interface 2 to send and receive VRRP packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrip ipv6 vrid 10 virtual-ip fe80::2 link-local
[Sysname-Vlan-interface2] vrrip ipv6 vrid 10 authentication-mode simple test
```

## vrrip ipv6 vrid preempt-mode

### Syntax

**vrrip ipv6 vrid** *virtual-router-id* **preempt-mode** [ **timer delay** *delay-value* ]

**undo vrrip ipv6 vrid** *virtual-router-id* **preempt-mode** [ **timer delay** ]

### View

Interface view

### Default Level

2: System level

### Parameters

*virtual-router-id*: Virtual router ID or VRRP group number, in the range 1 to 255.

**timer delay** *delay-value*: Sets preemption delay. The *delay-value* argument is in the range of 0 to 255 seconds and defaults to 0 seconds.

## Description

Use the **vrrip ipv6 vrid preempt-mode** command to configure preemption on the router and configure its preemption delay in the specified VRRP group.

Use the **undo vrrip ipv6 vrid preempt-mode** command to disable preemption on the router in the specified VRRP group, that is, specify the router to work in the non-preemptive mode.

Use the **undo vrrip ipv6 vrid preempt-mode timer delay** command to restore the default preemption delay, that is, zero seconds.

The default mode is immediate preemption without delay.

If you set the router in the VRRP group to work in non-preemptive mode, the delay period changes to zero seconds automatically.

On an unstable network, the VRRP group member in the backup state may not normally receive the packets from the master member due to network congestion, resulting in frequent master/backup state transition of the VRRP group members. Preemption delay is introduced to solve this problem. With a preemption delay set, if the backup member does not receive the packet from the master member duly, it waits for a period to see whether it can receive any packet from the master. If the specified period elapses but it still receives no packet from the master, it becomes the master.

Note that before executing the command, you need to create a VRRP group on an interface and configure the virtual IPv6 address of the VRRP group.

## Examples

# Enable preemption on the router in VRRP group 80 and set the preemption delay to five seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 80 virtual-ip fe80::2 link-local
[Sysname-Vlan-interface2] vrrp ipv6 vrid 80 preempt-mode timer delay 5
```

## vrrp ipv6 vrid priority

### Syntax

**vrrp ipv6 vrid** *virtual-router-id* **priority** *priority-value*

**undo vrrp ipv6 vrid** *virtual-router-id* **priority**

### View

Interface view

### Default Level

2: System level

### Parameters

*virtual-router-id*: VRRP group number, in the range 1 to 255.

*priority-value*: Priority value of the router in the specified VRRP group, in the range 1 to 254. A higher number indicates a higher priority.

### Description

Use the **vrrp ipv6 vrid priority** command to configure the priority of the router in the specified VRRP group.

Use the **undo vrrp ipv6 vrid priority** command to restore the default.

By default, the priority of a router in a VRRP group is 100.

- Before executing the command, create a VRRP group on an interface and configure the virtual IPv6 address of the VRRP group.
- In VRRP, the role that a router plays in a VRRP group depends on its priority. A higher priority means that the router is more likely to become the master. Note that priority 0 is reserved for special use and 255 for the IP address owner.

- If the router is the IP address owner, its priority is always 255. Therefore, it will be the master so long as it is functioning normally.

## Examples

# Set the priority of VRRP group 1 on interface VLAN-interface 2 to 150.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::2 link-local
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 priority 150
```

## vrrp ipv6 vrid timer advertise

### Syntax

**vrrp ipv6 vrid** *virtual-router-id* **timer advertise** *adver-interval*

**undo vrrp ipv6 vrid** *virtual-router-id* **timer advertise**

### View

Interface view

### Default Level

2: System level

### Parameters

*virtual-router-id*: VRRP group number, in the range 1 to 255.

*adver-interval*: Interval at which the master in the specified VRRP group sends VRRP advertisements. It ranges from 100 to 4095 centiseconds.

### Description

Use the **vrrp ipv6 vrid timer advertise** command to configure the Adver\_Timer of the specified VRRP group.

Use the **undo vrrp ipv6 vrid timer advertise** command to restore the default.

By default the Adver\_Timer is 100 centiseconds.

The Adver\_Timer controls the interval at which the master sends VRRP packets.

- Before executing the command, create a VRRP group on an interface and configure the virtual IPv6 address of the VRRP group.
- Routers in the same VRRP group must use the same Adver\_Timer setting.

## Examples

# Set the master in VRRP group 1 to send VRRP advertisements at intervals of 500 centiseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::2 link-local
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 timer advertise 500
```

## vrrp ipv6 vrid track interface

### Syntax

```
vrrp ipv6 vrid virtual-router-id track interface interface-type interface-number [ reduced priority-reduced ]
```

```
undo vrrp ipv6 vrid virtual-router-id track [ interface interface-type interface-number ]
```

### View

Interface view

### Default Level

2: System level

### Parameters

*virtual-router-id*: VRRP group number, in the range 1 to 255.

**interface** *interface-type* *interface-number*: Specifies an interface by its type and number.

**reduced** *priority-reduced*: Value by which the priority decrements. *priority-reduced* ranges from 1 to 255 and defaults to 10.

### Description

Use the **vrrp ipv6 vrid track interface** command to configure to track the specified interface.

Use the **undo vrrp ipv6 vrid track interface** command to disable tracking the specified interface.

By default, no interface is being tracked.

If the uplink interface of a router in a VRRP group fails, normally the VRRP group cannot be aware of the uplink failure. If the router is the master of the VRRP group, hosts on the LAN will not be able to access the external network because of the uplink failure. You can solve the problem through the function of tracing a specified interface. In this case, it is the uplink interface. After you configure to monitor the uplink interface, when the uplink interface goes down, the priority of the master is automatically decreased by a specified value, allowing a higher priority router in the VRRP group to become the master.

Note that:

- Before executing the command, create a VRRP group on an interface and configure the virtual IPv6 address of the VRRP group.
- When the router is the owner of the IP address, you cannot perform the configuration.
- When the status of the tracked interface turns from down to up, the corresponding router restores its priority automatically.

### Examples

# On interface VLAN-interface 2, set the interface to be tracked as VLAN-interface 1, making the priority of VRRP group 1 on interface VLAN-interface 2 decrement by 50 when VLAN-interface 1 goes down.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::2 link-local
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 track interface vlan-interface 1 reduced 50
```

## vrrip ipv6 vrid virtual-ip

### Syntax

```
vrrip ipv6 vrid virtual-router-id virtual-ip virtual-address [ link-local ]  
undo vrrip ipv6 vrid virtual-router-id [ virtual-ip virtual-address [ link-local ] ]
```

### View

Interface view

### Default Level

2: System level

### Parameters

*virtual-router-id*: VRRP group number, in the range 1 to 255.

*virtual-address*: Virtual IPv6 address.

**link-local**: Indicates that the virtual IPv6 address of the VRRP group is a link local address.

### Description

Use the **vrrip ipv6 vrid virtual-ip** command to create a VRRP group, and configure a virtual IPv6 address for it, or, add another virtual IPv6 address for an existing VRRP group.

Use the **undo vrrip ipv6 vrid virtual-ip** command to remove an existing VRRP group or the virtual IPv6 address of the VRRP group.

By default, no VRRP group is created.

Note that:

- The first virtual IPv6 address assigned to a VRRP group must be a link local address and only one such address is allowed in a VRRP group.
- After you remove all virtual IPv6 addresses, the VRRP group is automatically removed. The first address assigned to the group must be removed the last.

### Examples

```
# Create VRRP group 1, and configure its virtual IPv6 address as fe80::10.
```

```
<Sysname> system-view  
[Sysname] interface vlan-interface 2  
[Sysname-Vlan-interface2] vrrip ipv6 vrid 1 virtual-ip fe80::10
```

```
# Configure the virtual IPv6 address of VRRP group 1 as 1::10.
```

```
[Sysname-Vlan-interface2] vrrip ipv6 vrid 1 virtual-ip 1::10
```

# Table of Contents

<b>1 Hotfix Configuration Commands</b> .....	<b>1-1</b>
Hotfix Configuration Commands .....	1-1
display patch information .....	1-1
patch active .....	1-2
patch deactivate .....	1-2
patch delete .....	1-3
patch install .....	1-4
patch load .....	1-5
patch location .....	1-5
patch run .....	1-6

# 1 Hotfix Configuration Commands

## Hotfix Configuration Commands

### display patch information

#### Syntax

display patch information

#### View

Any view

#### Default Level

3: Manage level

#### Parameters

None

#### Description

Use the **display patch information** command to display the hotfix information.

#### Examples

# Display hotfix information.

```
<Sysname> display patch information
```

```
The location of patches: flash:/
```

```
Slot Version   Temporary Common Current Active Running Start-Address
-----
1     XXX002     0           1     1     0     0     0x4accf74
2     XXX       0           0     0     0     0     0x4accf74
```

**Table 1-1 display patch information** command output description

Field	Description
The location of patches	Patch file location. You can configure it using the <b>patch location</b> command.
Slot	Member ID
Version	Patch version. The first three characters represent the suffix of the PATCH-FLAG. For example, if the PATCH-FLAG of the a board is PATCH-RPE, "RPE" is displayed. The following three digits, if any, represent the patch number. (The patch number can be read after the patch is loaded.)
Temporary	Number of temporary patches
Common	Number of common patches

Field	Description
Current	Total number of patches
Running	Number of patches in the RUNNING state
Active	Number of patches in the ACTIVE state
Start-Address	Starting address of the memory patch area in the memory

## patch active

### Syntax

**patch active** *patch-number* **slot** *slot-number*

### View

System view

### Default Level

3: Manage level

### Parameters

*patch-number*: Sequence number of a patch. The valid values of this argument depend on the patch file used.

**slot** *slot-number*: Specifies a member device by its member ID. The value range of this argument varies with the device model and can be displayed through the **display irf** command.

### Description

Use the **patch active** command to activate the specified patch, namely, the system will run the patch.

After you execute the command, all the DEACTIVE patches before the specified patch number are activated.

Note that:

- The command is not applicable to patches in the DEACTIVE state.
- After a system reboot, the original ACTIVE patches change to DEACTIVE and become invalid. To make them effective, you need to activate them again.

### Examples

# Activate patch 3 and all the DEACTIVE patches before patch 3 on the device with member ID being 1.

```
<Sysname> system-view
[Sysname] patch active 3 slot 1
```

## patch deactive

### Syntax

**patch deactive** *patch-number* **slot** *slot-number*

### View

System view

## Default Level

3: Manage level

## Parameters

*patch-number*: Sequence number of a patch. The valid values of this argument depend on the patch file used.

**slot** *slot-number*: Specifies a member device by its member ID. The value range of this argument varies with the device model and can be displayed through the **display irf** command.

## Description

Use the **patch deactivate** command to stop running the specified patch and all the ACTIVE patches before the specified patch number, and the system will run at the original software version.

All the ACTIVE patches (including the specified patch) turn to DEACTIVE state.

This command is not applicable to the patches in the RUNNING state.

## Examples

```
# Stop running patch 3 and all the ACTIVE patches before patch 3 on the device with member ID being 1.
```

```
<Sysname> system-view  
[Sysname] patch deactivate 3 slot 1
```

## patch delete

### Syntax

```
patch delete patch-number slot slot-number
```

### View

System view

## Default Level

3: Manage level

## Parameters

*patch-number*: Sequence number of a patch. The valid values of this argument depend on the patch file used.

**slot** *slot-number*: Specifies a member device by its member ID. The value range of this argument varies with the device model and can be displayed through the **display irf** command.

## Description

Use the **patch delete** command to delete the specified patch and all the patches before the specified patch number.

This command only removes the patches from the memory patch area, and it does not delete them from the storage medium. The patches are in the IDLE state after execution of this command.

## Examples

```
# Delete patch 3 and all the patches before patch 3 on the device with member ID being 1.
```

```
<Sysname> system-view
[Sysname] patch delete 3 slot 1
```

## patch install

### Syntax

```
patch install patch-location
undo patch install
```

### View

System view

### Default Level

3: Manage level

### Parameters

*patch-location*: A string consisting of 1 to 64 characters. About the 3Com Switch 4800G, the location is "flash:".

### Description

Use the **patch install** command to install all the patches in one step.

Use the **undo patch install** to remove the patches.

After you execute the **patch install** command, a message "Do you want to continue running patches after reboot? [Y/N]:" is displayed.

- Entering **y** or **Y**: All the specified patches are installed, and turn to the RUNNING state from IDLE. This equals execution of the commands **patch location**, **patch load**, **patch active**, and **patch run**. The patches remain RUNNING after system reboot.
- Entering **n** or **N**: All the specified patches are installed and turn to the ACTIVE state from IDLE. This equals execution of the commands **patch location**, **patch load** and **patch active**. The patches turn to the DEACTIVE state after system reboot.

Note that:

- Before executing the command, save the patch files to root directories of the member devices' storage media.
- The **patch install** command changes the patch file location specified with the **patch location** command to the directory specified by the *patch-file* argument of the **patch install** command. For example, if you execute the **patch location xxx** command and then the **patch install yyy** command, the patch file location automatically changes from xxx to yyy.

### Examples

```
# Install the patches located on the flash.
```

```
<Sysname> system-view
[Sysname] patch-install flash:
Patches will be installed. Continue? [Y/N]:y
Do you want to run patches after reboot? [Y/N]:y
Installing patches...
Installation completed, and patches will continue to run after reboot.
```

[ Sysname ]

## patch load

### Syntax

```
patch load slot slot-number
```

### View

System view

### Default Level

3: Manage level

### Parameters

**slot** *slot-number*: Specifies a member device by its member ID. The value range of this argument varies with the device model and can be displayed through the **display irf** command.

### Description

Use the **patch load** command to load the patch file on the storage medium.

Before using the command, save the patch files to the root directories of the member devices' storage media.

### Examples

# Load the patch files for the device with member ID being 1.

```
<Sysname> system-view  
[Sysname] patch load slot 1
```

## patch location

### Syntax

```
patch location patch-location
```

### View

System view

### Default Level

3: Manage level

### Parameters

*patch-location*: Specifies the patch file location. It is a string consisting of 1 to 64 characters. About the 3Com Switch 4800G, the location is "flash:".

### Description

Use the **patch location** command to configure the patch file location.

By default, the patch file location is **flash:**.

Note that the **patch install** command changes the patch file location specified with the **patch location** command to the directory specified by the *patch-location* argument of the **patch install** command. For

example, if you execute the **patch location xxx** command and then the **patch install yyy** command, the patch file location automatically changes from xxx to yyy.

## Examples

# Configure the root directory of the flash as the patch file location.

```
<Sysname> system-view  
[Sysname] patch location flash:
```

## patch run

### Syntax

```
patch run patch-number [ slot slot-number ]
```

### View

System view

### Default Level

3: Manage level

### Parameters

*patch-number*: Sequence number of a patch. The valid values of this argument depend on the patch file used.

**slot** *slot-number*: Specifies a member device by its member ID. The value range of this argument varies with the device model and can be displayed through the **display irf** command.

### Description

Use the **patch run** command to confirm the running of the specified patch and all the ACTIVE patches before the specified patch number.

With the **slot** keyword specified, the command confirms the running state of all the qualified patches on a member device. If the keyword is not specified, the command confirms the running state of all the qualified patches on all the member devices.

This command is applicable to patches in the ACTIVE state only.

If the running of a patch is confirmed, after the system reboots, the patch will still be effective.

## Examples

# Confirm the running of patch 3 and all the ACTIVE patches before patch 3 on the device with member ID being 1.

```
<Sysname> system-view  
[Sysname] patch run 3 slot 1
```

# Table of Contents

<b>1 Cluster Management Configuration Commands</b> .....	<b>1-1</b>
NDP Configuration Commands.....	1-1
display ndp .....	1-1
ndp enable.....	1-4
ndp timer aging.....	1-5
ndp timer hello.....	1-6
reset ndp statistics.....	1-6
NTDP Configuration Commands .....	1-7
display ntdp .....	1-7
display ntdp device-list .....	1-8
display ntdp single-device mac-address .....	1-10
ntdp enable.....	1-11
ntdp explore.....	1-11
ntdp hop.....	1-12
ntdp timer.....	1-12
ntdp timer hop-delay.....	1-13
ntdp timer port-delay.....	1-14
Cluster Configuration Commands.....	1-14
add-member .....	1-14
administrator-address.....	1-15
auto-build.....	1-16
black-list add-mac.....	1-17
black-list delete-mac.....	1-18
build .....	1-18
cluster .....	1-19
cluster enable .....	1-20
cluster switch-to.....	1-21
cluster-local-user .....	1-21
cluster-mac .....	1-22
cluster-mac syn-interval.....	1-23
cluster-snmp-agent community .....	1-23
cluster-snmp-agent group v3.....	1-24
cluster-snmp-agent mib-view included .....	1-25
cluster-snmp-agent usm-user v3.....	1-26
delete-member .....	1-27
display cluster .....	1-28
display cluster base-topology .....	1-29
display cluster black-list.....	1-31
display cluster candidates .....	1-32
display cluster current-topology.....	1-33
display cluster members.....	1-35
ftp-server .....	1-38
holdtime .....	1-39

ip-pool.....	1-40
logging-host.....	1-40
management-vlan.....	1-41
management-vlan synchronization enable.....	1-42
nm-interface vlan-interface.....	1-43
reboot member.....	1-43
snmp-host.....	1-44
tftp-server.....	1-44
timer.....	1-45
topology accept.....	1-46
topology restore-from.....	1-47
topology save-to.....	1-47

# 1 Cluster Management Configuration Commands

---

## NDP Configuration Commands

### display ndp

#### Syntax

```
display ndp [ interface interface-list ]
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

**interface** *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [ **to** *interface-type interface-number* ] } & <1-10>, where, *interface-type* is port type and *interface-number* is port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument.

#### Description

Use the **display ndp** command to display NDP configuration information, which includes the interval to send NDP packets, the time for the receiving device to hold NDP information and the information about the neighbors of all ports.

#### Examples

# Display NDP configuration information.

```
<Sysname> display ndp
Neighbor Discovery Protocol is enabled.
Neighbor Discovery Protocol Ver: 1, Hello Timer: 60(s), Aging Timer: 180(s)
Interface: GigabitEthernet1/0/1
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/2
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/3
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/4
    Status: Enabled, Pkts Snd: 28440, Pkts Rvd: 27347, Pkts Err: 0
```

Neighbor 1: Aging Time: 122(s)  
MAC Address : 000f-e200-2579  
Host Name : Sysname  
Port Name : GigabitEthernet1/0/4  
Software Ver: ESS 2200  
Device Name : 3Com Switch 4800G 48-Port  
Port Duplex : AUTO  
Product Ver : Switch 4800G 24-Port-ESS2201  
BootROM Ver : 505

Interface: GigabitEthernet1/0/5  
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/6  
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/7  
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/8  
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/9  
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/10  
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/11  
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/12  
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/13  
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/14  
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/15  
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/16  
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/17

```

Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/18
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/19
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/20
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/21
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/22
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/23
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/24
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitGigabitEthernet1/0/1
Status: Enabled, Pkts Snd: 28438, Pkts Rvd: 54160, Pkts Err: 0
Neighbor 1: Aging Time: 176(s)
  MAC Address : 000f-cbb8-9528
  Host Name   : Sysname
  Port Name   : GigabitGigabitEthernet1/0/2
  Software Ver: V100R002B01D011SP1
  Device Name : Sysname S5648P
  Port Duplex : AUTO
  Product Ver : 005

Interface: GigabitGigabitEthernet1/0/2
Status: Enabled, Pkts Snd: 1, Pkts Rvd: 1, Pkts Err: 0

```

**Table 1-1 display ndp command output description**

Field	Description
Neighbor Discovery Protocol is enabled	NDP is enabled globally on the current device.
Neighbor Discovery Protocol Ver	Version of NDP
Hello Timer	Interval to send NDP packets
Aging Timer	The time for the receiving device to hold NDP information
Interface	A specified port

Field	Description
Status	NDP state of a port
Pkts Snd	Number of the NDP packets sent through the port
Pkts Rvd	Number of the NDP packets received on the port
Pkts Err	Number of the error NDP packets received
Neighbor 1: Aging Time	Aging time of the NDP information of a neighbor device
MAC Address	MAC address of a neighbor device
Host Name	Host name of a neighbor device
Port Name	Port name of a neighbor device
Software Ver	Software version of the neighbor device
Device Name	Device name of a neighbor device
Port Duplex	Port duplex mode of a neighbor device
Product Ver	Product version of a neighbor device
BootROM Ver	Boot ROM version of a neighbor device

## ndp enable

### Syntax

In Ethernet interface view or Layer 2 aggregate interface view:

**ndp enable**

**undo ndp enable**

In system view:

**ndp enable** [ **interface** *interface-list* ]

**undo ndp enable** [ **interface** *interface-list* ]

### View

System view, Ethernet interface view, Layer 2 aggregate interface view

### Default Level

2: System level

### Parameters

**interface** *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type* *interface-number* [ **to** *interface-type* *interface-number* ] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument.

### Description

Use the **ndp enable** command to enable NDP.

Use the **undo ndp enable** command to disable this feature.

By default, NDP is enabled globally and also on all ports.

Note that:

- When being executed in system view, the **ndp enable** command enables NDP globally if you do not specify the **interface** keyword; if you specify the **interface** keyword, the command enables NDP for the specified Ethernet port(s).
- When being executed in interface view, this command enables NDP for the current port only.
- Configured in Layer 2 aggregate interface view, the configuration will not take effect on the member ports of the aggregation group that corresponds to the aggregate interface; configured on a member port of an aggregation group, the configuration will take effect only after the member port quit the aggregation group. For description of aggregation configurations, refer to *Link Aggregation Configuration* in the *Access Volume*.

## Examples

# Enable NDP globally.

```
<Sysname> system-view
[Sysname] ndp enable
```

# Enable NDP for port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ndp enable
```

## ndp timer aging

### Syntax

```
ndp timer aging aging-time
undo ndp timer aging
```

### View

System view

### Default Level

2: System level

### Parameters

*aging-time*: Time for a device to keep the NDP packets it receives, in the range 5 to 255 seconds.

### Description

Use the **ndp timer aging** command to specify the time that a device should keep the NDP packets it received from the adjacent device.

Use the **undo timer aging** command to restore the default.

By default, the time that a receiving device should keep the NDP packets is 180 seconds.

Note that the time for the receiving device to hold NDP packets cannot be shorter than the interval to send NDP packets; otherwise, the NDP table may become instable.

Related commands: **ndp timer hello**.

## Examples

```
# Configure the time that a receiving device should keep the NDP packets as 60 seconds.
```

```
<Sysname> system-view  
[Sysname] ndp timer aging 60
```

## ndp timer hello

### Syntax

```
ndp timer hello hello-time  
undo ndp timer hello
```

### View

System view

### Default Level

2: System level

### Parameters

*hello-time*: Interval to send NDP packets, in the range 5 to 254 seconds.

### Description

Use the **ndp timer hello** command to set the interval to send NDP packets.

Use the **undo ndp timer hello** command to restore the default.

By default, the interval to send NDP packets is 60 seconds.

Note that the interval for sending NDP packets cannot be longer than the time for the receiving device to hold NDP packets; otherwise, the NDP table may become instable.

Related commands: **ndp timer aging**.

## Examples

```
# Set the interval to send NDP packets to 80 seconds.
```

```
<Sysname> system-view  
[Sysname] ndp timer hello 80
```

## reset ndp statistics

### Syntax

```
reset ndp statistics [ interface interface-list ]
```

### View

User view

### Default Level

2: System level

## Parameters

**interface** *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [ **to** *interface-type interface-number* ] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument.

## Description

Use the **reset ndp statistics** command to clear NDP statistics.

If no **interface** *interface-list* is specified, NDP statistics of all ports are cleared; otherwise, NDP statistics of a specified port are cleared.

## Examples

```
# Clear NDP statistics of all ports.  
<Sysname> reset ndp statistics
```

# NTDP Configuration Commands

## display ntdp

### Syntax

```
display ntdp
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display ntdp** command to display NTDP configuration information.

### Examples

```
# Display the global NTDP information.  
<Sysname> display ntdp  
NTDP is running.  
Hops      : 4  
Timer     : 1 min(disable)  
Hop Delay : 100 ms  
Port Delay: 10 ms  
Last collection total time: 92ms
```

**Table 1-2 display ntdp command output description**

Field	Description
NTDP is running	NTDP is enabled globally on the local device.
Hops	Hop count for topology collection
Timer	Interval to collect topology information (after the cluster is created)
disable	Indicates the device is not a management device and unable to perform periodical topology collection
Hop Delay	Delay time for the device to forward topology collection requests
Port Delay	Delay time for a topology-collection request to be forwarded through a port
Last collection total time	Time cost during the last collection

## display ntdp device-list

### Syntax

```
display ntdp device-list [ verbose ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**verbose:** Displays the detailed device information.

### Description

Use the **display ntdp device-list** command to display the device information collected through NTDP.

Note that the information displayed may not be that of the latest device if you do not execute the **ntdp explore** command before using this command.

### Examples

```
# Display the device list collected through NTDP.
```

```
<Sysname> display ntdp device-list
```

```
MAC                HOP  IP                Device
000f-e200-3133     2                    Switch 4200G
000f-e20f-c415     2    31.31.31.5/24     Switch 4200G
000f-e200-2579     1                    Switch 4200G
000f-e200-1751     0    31.31.31.1/24     Switch 4200G
00e0-fd00-0043     2                    Sysname S3528P
000f-e200-3199     3                    Switch 4200G
```

**Table 1-3 display ntdp device-list command output description**

Field	Description
MAC	MAC address of a device
HOP	Hops to the collecting device
IP	IP address and mask length of the management VLAN interface on the device
Device	Device name

# Display the detailed device information collected through NTDP.

```
<aabbcc_0.3Com> display ntdp device-list verbose
```

```

Hostname   : 3Com
MAC        : 000f-e200-1400
Hop        : 0
Device     : 3Com Switch 4800G 24-Port
IP         : 192.168.1.5/24
Version    :
3Com Corporation
Switch 4800G 24-Port Software Version 5.20 ESS 2201
Copyright (c) 2004-2008 3Com Corp. and its licensors. All rights reserved.
Switch 4800G 24-Port uptime is 0 week, 0 day, 0 hour, 46 minutes

```

**Table 1-4 display ntdp device-list verbose command output description**

Field	Description
Hostname	System name of the device
MAC	MAC address of the device
Hop	Hops from the current device to the device that collect topology information
Device	Device name
IP	IP address and subnet mask length of the management VLAN interface on the device
Version	Version information
Cluster	Role of the device in the cluster
Cluster : Member switch of cluster aabbcc	The device is a member device of the cluster <b>aabbcc</b> .
Administrator MAC	MAC address of the management device
Administrator switch of cluster aabbcc	The device is the management device of the cluster <b>aabbcc</b> .
Peer MAC	MAC address of a neighbor device
Peer Port ID	Name of the peer port connected to the local port
Native Port ID	Name of the local port to which a neighbor device is connected
Speed	Speed of the local port to which a neighbor device is connected

Field	Description
Duplex	Duplex mode of the local port to which a neighbor device is connected

## display ntdp single-device mac-address

### Syntax

**display ntdp single-device mac-address** *mac-address*

### View

Any view

### Default Level

1: Monitor level

### Parameters

*mac-address*: MAC address of the device, in the format of H-H-H.

### Description

Use the **display ntdp single-device mac-address** command to view the detailed NTDP information of a specified device.

### Examples

# Display the detailed NTDP information of the device with a MAC address of 000f-e200-5111.

```
<Sysname> display ntdp single-device mac-address 000f-e200-5111

Hostname   : aaa_1.42-com2
MAC        : 000f-e200-5111
Hop         : 1
Device     : Switch 4800G 24-Port
IP         : 16.168.1.2/24
Version    :
3Com Corporation
Switch 4800G 24-Port Software Version 5.20 ESS 2201
Copyright (c) 2004-2008 3Com Corp. and its licensors. All rights reserved.
Switch 4800G 24-Port uptime is 0 week, 0 day, 0 hour, 46 minutes
Cluster    : Member switch of cluster aaa , Administrator MAC: 000f-e200-5175

Peer MAC      Peer Port ID      Native Port ID      Speed Duplex
000f-e200-5175 GigabitEthernet1/0/1  GigabitEthernet1/0/1  100 FULL
000f-e200-5175 GigabitEthernet1/0/5  GigabitEthernet1/0/7  100 FULL
```

Refer to [Table 1-4](#) for the description of the above prompt information.

## ntdp enable

### Syntax

```
ntdp enable
undo ntdp enable
```

### View

System view, Ethernet interface view, Layer 2 aggregate interface view

### Default Level

2: System level

### Parameters

None

### Description

Use the **ntdp enable** command to enable NTDP.

Use the **undo ntdp enable** command to disable NTDP.

By default, NTDP is enabled globally and on all ports.

Note that:

- Execution of the command in system view enables the global NTDP; execution of the command in interface view enables NTDP of the current port.
- Configured in Layer 2 aggregate interface view, the configuration will not take effect on the member ports of the aggregation group that corresponds to the aggregate interface; configured on a member port of an aggregation group, the configuration will take effect only after the member port quit the aggregation group. For description of aggregation configurations, refer to *Link Aggregation Configuration* in the *Access Volume*.

### Examples

```
# Enable NTDP globally.
```

```
<Sysname> system-view
[Sysname] ntdp enable
```

```
# Enable NTDP for port GigabitEthernet 1/0/1.
```

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ntdp enable
```

## ntdp explore

### Syntax

```
ntdp explore
```

### View

User view

### Default Level

2: System level

### Parameters

None

### Description

Use the **ntdp explore** command to start topology information collection manually.

### Examples

```
# Start the topology information collection.
```

```
<Sysname> ntdp explore
```

## ntdp hop

### Syntax

```
ntdp hop hop-value
```

```
undo ntdp hop
```

### View

System view

### Default Level

2: System level

### Parameters

*hop-value*: Maximum hop for collecting topology information, in the range 1 to 16.

### Description

Use the **ntdp hop** command to set maximum hop for collecting topology information.

Use the **undo ntdp hop** command to restore the default.

By default, the value is 3.

Note that this command is only applicable to the topology-collecting device. A bigger number of hops requires more memory of the topology-collecting device.

### Examples

```
# Set the hop count for topology information collection to 5.
```

```
<Sysname> system-view
```

```
[Sysname] ntdp hop 5
```

## ntdp timer

### Syntax

```
ntdp timer interval-time
```

```
undo ntdp timer
```

## View

System view

## Default Level

2: System level

## Parameters

*interval-time*: Interval (in minutes) to collect topology information, in the range 0 to 65,535. The value 0 means not to collect topology information.

## Description

Use the **ntdp timer** command to configure the interval to collect topology information.

Use the **undo ntdp timer** command to restore the default.

By default, the interval to collect topology information is 1 minute.

Note that the management device can start to collect the topology information only after the cluster is set up.

## Examples

# Set the interval to collect the topology information to 30 minutes.

```
<Sysname> system-view  
[Sysname] ntdp timer 30
```

## ntdp timer hop-delay

### Syntax

```
ntdp timer hop-delay time  
undo ntdp timer hop-delay
```

### View

System view

### Default Level

2: System level

### Parameters

*time*: Delay time (in milliseconds) for a device receiving topology-collection requests to forward them through its first port. This argument ranges from 1 to 1,000.

### Description

Use the **ntdp timer hop-delay** command to set the delay time for the device to forward topology-collection requests through the first port.

Use the **undo ntdp timer hop-delay** command to restore the default delay time, which is 200 ms.

## Examples

# Set the delay time for the device to forward topology-collection requests through the first port to 300 ms.

```
<Sysname> system-view
[Sysname] ntdp timer hop-delay 300
```

## ntdp timer port-delay

### Syntax

```
ntdp timer port-delay time
undo ntdp timer port-delay
```

### View

System view

### Default Level

2: System level

### Parameters

*time*: Delay time (in milliseconds) for a device to forward a topology-collection request through its successive ports, in the range 1 to 100.

### Description

Use the **ntdp timer port-delay** command to set the delay time for a device to forward a received topology-collection request through its successive ports.

Use the **undo ntdp timer port-delay** command to restore the default delay time, or 20 ms.

## Examples

# Set the delay time for the device to forward topology-collection requests through the successive ports to 40 ms.

```
<Sysname> system-view
[Sysname] ntdp timer port-delay 40
```

## Cluster Configuration Commands

### add-member

#### Syntax

```
add-member [ member-number ] mac-address mac-address [ password password ]
```

#### View

Cluster view

#### Default Level

2: System level

## Parameters

*member-number*: Member number assigned to the candidate device to be added to a cluster, ranging from 1 to 31.

*mac-address*: MAC address of the candidate device (in hexadecimal form of H-H-H).

*password*: Password of the candidate device, a string of 1 to 16 characters. The password is required when you add a candidate device to a cluster. However, this argument is not needed if the candidate device is not configured with a super password.

## Description

Use the **add-member** command to add a candidate device to a cluster.

Note that:

- You must add a cluster member through the management device.
- When adding a member device to a cluster, you need not assign a number to the device. The management device will automatically assign a usable number to the newly added member device.
- After a candidate device joins the cluster, its level 3 password is replaced by the super password of the management device in cipher text.

## Examples

# Add a candidate device to the cluster, setting the member number to 6. (Assume that the MAC address and user password of the candidate device are 000f-e200-35E7 and 123456 respectively.)

```
<aabbcc_0.Sysname> system-view
[aabbcc_0.Sysname] cluster
[aabbcc_0.Sysname-cluster] add-member 6 mac-address 000f-e200-35e7 password 123456
```

## administrator-address

### Syntax

**administrator-address** *mac-address* **name** *cluster-name*

**undo administrator-address**

### View

Cluster view

### Default Level

2: System level

## Parameters

*mac-address*: MAC address of the management device (in hexadecimal form of H-H-H).

*cluster-name*: Name of an existing cluster, a string of 1 to 8 characters, which can only be letters, numbers, subtraction sign (-), and underline (\_).

## Description

Use the **administrator-address** command to add a candidate device to a cluster.

Use the **undo administrator-address** command to remove a member device from the cluster.

By default, a device belongs to no cluster.

Note that:

- The **administrator-address** command is applicable on candidate devices only, while the **undo administrator-address** command is applicable on member devices only.
- You are recommended to use the **delete-member** command on the management device to remove a cluster member from a cluster.

## Examples

# Remove a member device from the cluster.

```
<aabbcc_1.Sysname> system-view
[aabbcc_1.Sysname] cluster
[aabbcc_1.Sysname-cluster] undo administrator-address
```

## auto-build

### Syntax

**auto-build [ recover ]**

### View

Cluster view

### Default Level

2: System level

### Parameters

**recover**: Automatically reestablishes communication with all the member devices.

### Description

Use the **auto-build** command to establish a cluster automatically.

Note that:

- This command can be executed on a candidate device or the management device.
- If you execute this command on a candidate device, you will be required to enter the cluster name to build a cluster. Then the system will collect candidates and add the collected candidates into the cluster automatically.
- If you execute this command on the management device, the system will collect candidates directly and add them into the cluster automatically.
- The **recover** keyword is used to recover a cluster. Using the **auto-build recover** command, you can find the members that are currently not in the member list and add them to the cluster again.
- Ensure that NTDP is enabled, because it is the basis of candidate and member collection. The collection range is also decided through NTDP. You can use the **ntdp hop** command in system view to modify the collection range.
- If a member is configured with a super password different from the super password of the management device, it cannot be added to the cluster automatically.

## Examples

# Establish a cluster automatically.

```
<Sysname> system-view
```

```

[Sysname] cluster
[Sysname-cluster] auto-build
There is no base topology, if set up from local flash file?(Y/N)
y
  Begin get base topology file from local flash.....
  Get file error, can not finish base topology recover

Please input cluster name:aabbcc
Collecting candidate list, please wait...

#Jul 22 14:35:18:841 2006 Sysname CLST/5/Cluster_Trap:
OID:1.3.6.1.4.1.2011.6.7.1.0.3: member 0.0.0.0.0.224.252.0.0.0 role change, NTDP
Index:0.0.0.0.0.0.224.252.0.0.0, Role:1
Candidate list:

Name                               Hops  MAC Address      Device

Processing...please wait
Cluster auto-build Finish!
0 member(s) added successfully.

```

## black-list add-mac

### Syntax

**black-list add-mac** *mac-address*

### View

Cluster view

### Default Level

2: System level

### Parameters

*mac-address*: MAC address of the device to be added into the blacklist, in the form of H-H-H.

### Description

Use the **black-list add-mac** command to add a device to the blacklist.

Note that this command can be executed on the management device only.

### Examples

# Add a device with the MAC address of 0ec0-fc00-0001 to the blacklist.

```

<aabbcc_0.Sysname> system-view
[aabbcc_0.Sysname] cluster
[aabbcc_0.Sysname-cluster] black-list add-mac 0ec0-fc00-0001

```

## black-list delete-mac

### Syntax

```
black-list delete-mac { all | mac-address }
```

### View

Cluster view

### Default Level

2: System level

### Parameters

**all**: Deletes all devices from the blacklist.

*mac-address*: MAC address of the device to be deleted from the blacklist, in the form of H-H-H.

### Description

Use the **black-list delete-mac** command to delete a device from the blacklist.

Note that this command can be executed on the management device only.

### Examples

# Delete a device with the MAC address of 0EC0-FC00-0001 from the blacklist.

```
<aabbcc_0.Sysname> system-view  
[aabbcc_0.Sysname] cluster  
[aabbcc_0.Sysname-cluster] black-list delete-mac 0ec0-fc00-0001
```

# Delete all devices in the blacklist.

```
[aabbcc_0.Sysname-cluster] black-list delete-mac all
```

## build

### Syntax

```
build name
```

```
undo build
```

### View

Cluster view

### Default Level

2: System level

### Parameters

*name*: Cluster name, a string of 1 to 8 characters, which can only be letters, numbers, subtraction sign (-), and underline (\_).

### Description

Use the **build** command to configure the current device as the management device and specify a name for it.

Use the **undo build** command to configure the current management device as a candidate device.  
By default, the device is not a management device.

Note that:

- When executing this command, you will be asked whether to create a standard topology map or not.
- This command can only be applied to devices that are capable of being a management device and are not members of other clusters. The command takes no effect if you execute the command on a device which is already a member of another cluster. If you execute this command on a management device, you will replace the cluster name with the one you specify.
- The member number of the management device is 0.

## Examples

# Configure the current device as a management device and specify the cluster name as **aabbcc**.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] build aabbcc
[Sysname-cluster] ip-pool 172.16.0.1 255.255.255.248
Restore topology from local flash file,for there is no base topology.
(Please confirm in 30 seconds, default No). (Y/N)
Y
  Begin get base topology file from local flash.....
  Get file error, can not finish base topology recover

#Sep 18 19:56:03:804 2006 Sysname IFNET/4/INTERFACE UPDOWN:
  Trap 1.3.6.1.6.3.1.1.5.4: Interface 3276899 is Up, ifAdminStatus is 1, ifOperSt
atus is 1
#Sep 18 19:56:03:804 2006 Sysname CLST/4/Cluster_Trap:
OID:1.3.6.1.4.1.2011.6.7.1.0.3: member 0.0.0.0.0.224.252.0.29.0 role change, NTD
PIndex:0.0.0.0.0.224.252.0.29.0, Role:1
%Sep 18 19:56:03:804 2006 Sysname IFNET/4/UPDOWN:
  Line protocol on the interface Vlan-interface100 is UP
[aabbcc_0.Sysname-cluster]
%Sep 18 19:56:18:782 2006 Sysname CLST/4/LOG:
Member 000f-e200-1e00 is joined in cluster aabbcc.
[aabbcc_0.Sysname-cluster]
```

## cluster

### Syntax

```
cluster
```

### View

```
System view
```

### Default Level

```
2: System level
```

## Parameters

None

## Description

Use the **cluster** command to enter cluster view.

## Examples

```
# Enter cluster view
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster]
```

## cluster enable

### Syntax

```
cluster enable
undo cluster enable
```

### View

System view

### Default Level

2: System level

## Parameters

None

## Description

Use the **cluster enable** command to enable the cluster function.

Use the **undo cluster enable** command to disable the cluster function.

By default, the cluster function is enabled.

Note that:

- When you execute the **undo cluster enable** command on a management device, you remove the cluster and its members, and the device stops operating as a management device.
- When you execute the **undo cluster enable** command on a member device, you disable the cluster function on the device, and the device leaves the cluster.
- When you execute the **undo cluster enable** command on a device that belongs to no cluster, you disable the cluster function on the device.

## Examples

```
# Enable the cluster function.
<Sysname> system-view
[Sysname] cluster enable
```

## cluster switch-to

### Syntax

```
cluster switch-to { member-number | mac-address mac-address | administrator | sysname member-sysname }
```

### View

User view

### Default Level

0: Visit level

### Parameters

*member-number*: Number of a member device in a cluster, in the range 1 to 31.

**mac-address** *mac-address*: MAC address of a member device, in the format of H-H-H.

**administrator**: Switches from a member device to the management device.

**sysname** *member-sysname*: System name of a member device, a string of 1 to 32 characters.

### Description

Use the **cluster switch-to** command to switch between the management device and member devices.

### Examples

# Switch from the operation interface of the management device to that of the member device numbered 6 and then switch back to the operation interface of the management device.

```
<aaa_0.Sysname> cluster switch-to 6
<aaa_6.Sysname> quit
<aaa_0.Sysname>
```

# Enter the member device numbered 5 with the system name of **switcha**.

```
<aaa_0.Sysname> cluster switch-to sysname switcha
SN      Device          MAC Address      Status Name
 5      Switch 4200G        000f-e200-5101  UP      test_5.switch
 6      Switch 4200G        000f-e200-5102  UP      test_6.switch
      press SN number to switch to the device, other number will quit the command: 5
<aaa_5.switcha>
```

## cluster-local-user

### Syntax

```
cluster-local-user username password { cipher | simple } password
```

```
undo cluster-local-user username
```

### View

Cluster view

### Default Level

1: Monitor level

## Parameters

**cipher**: Indicates that the password is in cipher text.

**simple**: Indicates that the password is in plain text.

*username*: Username used for logging onto the devices within a cluster through Web, a string of 1 to 55 characters.

*password*: Password used for logging onto the devices within a cluster through Web. This password is a string of 1 to 63 characters when the **simple** keyword is specified, and can be in either plain text or cipher text when the **cipher** keyword is specified. A plain text password must be a string of 1 to 63 characters. The cipher text password must have a fixed length of 24 or 88 characters. The password is case sensitive.

## Description

Use the **cluster-local-user** command to configure Web user accounts in batches.

Use the **undo cluster-local-user** command to remove the configuration.

Note that the command can be configured once on the management device only.

## Examples

# Configure Web user accounts for the devices within a cluster, with username being **abc**, password being 123456 and displayed in plain text.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-local-user abc password simple 123456
```

## cluster-mac

### Syntax

**cluster-mac** *mac-address*

**undo cluster-mac**

### View

Cluster view

### Default Level

2: System level

## Parameters

*mac-address*: Multicast MAC address (in hexadecimal in the format of H-H-H), which can be 0180-c200-0000, 0180-c200-000a, 0180-c200-0020 through 0180-c200-002f, or 010f-e200-0002.

## Description

Use the **cluster-mac** command to configure the destination MAC address for cluster management protocol packets.

Use the **undo cluster-mac** command to restore the default.

By default, the destination MAC address is 0180-c200-000a.

Note that this command can be executed on the management device only.

## Examples

```
# Set the multicast MAC address of the cluster management protocol packets to 0180-c200-0000.
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] cluster-mac 0180-c200-0000
```

## cluster-mac syn-interval

### Syntax

```
cluster-mac syn-interval interval-time
```

### View

Cluster view

### Default Level

2: System level

### Parameters

*interval-time*: Interval (in minutes) to send broadcast packets, in the range 0 to 30. If the interval is set to 0, the management device does not send broadcast packets to the member devices.

### Description

Use the **cluster-mac syn-interval** command to set the interval for a management device to send MAC address negotiation broadcast packets for cluster management.

By default, the interval is set to one minute.

Note that this command can be executed on the management device only.

## Examples

```
# Set the interval for the management device to send MAC address negotiation broadcast packets for cluster management to two minutes.
```

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] cluster-mac syn-interval 2
```

## cluster-snmp-agent community

### Syntax

```
cluster-snmp-agent community { read | write } community-name [ mib-view view-name ]
undo cluster-snmp-agent community community-name
```

### View

Cluster view

## Default Level

1: Monitor level

## Parameters

**read:** Indicates to allow the community's read-only access to MIB objects. The community with read-only authority can only query the device information.

**write:** Indicates to allow the community's read-write access to MIB objects. The community with read-write authority can configure the device information.

*community-name:* Community name, a string of 1 to 26 characters.

*view-name:* MIB view name, a string of 1 to 32 characters.

## Description

Use the **cluster-snmp-agent community** command to configure an SNMP community shared by a cluster and set its access authority.

Use the **undo cluster-snmp-agent community** command to remove a specified community name.

Note that:

- The command used to configure the SNMP community with read or read-only authority can only be executed once on the management device. This configuration will be synchronized to the member devices in the whitelist, which is equal to configuring multiple member devices at one time.
- SNMP community name will be retained if a cluster is dismissed or a member device is removed from the whitelist.
- If the same community name as the current one has been configured on a member device, the current community name will replace the original one.

## Examples

# Configure the SNMP community name shared by a cluster as **comaccess** and allow the community's read-only access to MIB objects.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-snmp-agent community read comaccess
```

# Configure the SNMP community name shared by a cluster as **comaccesswr** and allow the community's read-write access to MIB objects.

```
[aaa_0.Sysname-cluster] cluster-snmp-agent community write comaccesswr
```

## cluster-snmp-agent group v3

### Syntax

```
cluster-snmp-agent group v3 group-name [ authentication | privacy ] [ read-view read-view ]
[ write-view write-view ] [ notify-view notify-view ]
```

```
undo cluster-snmp-agent group v3 group-name [ authentication | privacy ]
```

### View

Cluster view

## Default Level

1: Monitor level

## Parameters

*group-name*: Group name, a string of 1 to 32 characters.

**authentication**: Specifies to authenticate a packet but not to encrypt it.

**privacy**: Specifies to authenticate and encrypt a packet.

*read-view*: Read-only view name, a string of 1 to 32 characters.

*write-view*: Read-write view name, a string of 1 to 32 characters.

*notify-view*: View name in which Trap messages can be sent, a string of 1 to 32 characters.

## Description

Use the **cluster-snmp-agent group** command to configure the SNMPv3 group shared by a cluster and set its access rights.

Use the **undo cluster-snmp-agent group** command to remove the SNMPv3 group shared by a cluster.

Note that:

- The command can be executed once on the management device only. This configuration will be synchronized to the member devices in the whitelist, which is equal to configuring multiple member devices at one time.
- SNMPv3 group name will be retained if a cluster is dismissed or a member device is deleted from the whitelist.
- If the same group name as the current one has been configured on a member device, the current group name will replace the original one.

## Examples

# Create an SNMP group **snmpgroup**.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-snmp-agent group v3 snmpgroup
```

## cluster-snmp-agent mib-view included

### Syntax

**cluster-snmp-agent mib-view included** *view-name oid-tree*

**undo cluster-snmp-agent mib-view** *view-name*

### View

Cluster view

## Default Level

1: Monitor level

## Parameters

*view-name*: MIB view name, a string of 1 to 32 characters.

*oid-tree*: MIB subtree, a string of 1 to 255 characters, which can only be a variable OID string or variable name string. OID is composed of a series of integers, indicating where a node is in the MIB tree. It can uniquely identify an object in a MIB.

## Description

Use the **cluster-snmp-agent mib-view included** command to create or update the MIB view information shared by a cluster.

Use the **undo cluster-snmp-agent mib-view** command to delete the MIB view information shared by a cluster.

By default, the MIB view name shared by a cluster is ViewDefault, in which the cluster can access ISO subtree.

Note that:

- This command can be executed once on the management device only. This configuration will be synchronized to member devices on the whitelist, which is equal to configuring multiple member devices at one time.
- The MIB view will be retained if a cluster is dismissed or a member device is deleted from the whitelist.
- If the same view name as the current one has been configured on a member device, the current view will replace the original one on the member device.

## Examples

# Create a view including all objects of **mib2**.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-snmp-agent mib-view included mib2 1.3.6.1.2.1
```

## cluster-snmp-agent usm-user v3

### Syntax

**cluster-snmp-agent usm-user v3** *user-name group-name* [ **authentication-mode** { **md5** | **sha** } *auth-password* ] [ **privacy-mode** **des56** *priv-password* ]

**undo cluster-snmp-agent usm-user v3** *user-name group-name*

### View

Cluster view

### Default Level

1: Monitor level

### Parameters

*user-name*: User name, a string of 1 to 32 characters.

*group-name*: Group name, a string of 1 to 32 characters.

**authentication-mode**: Specifies the security level to be authentication needed.

**md5**: Specifies the authentication protocol to be HMAC-MD5-96.

**sha**: Specifies the authentication protocol to be HMAC-SHA-96.

*auth-password*: Authentication password, a string of 1 to 16 characters if in plain text; it can only be a string of 24 characters if in cipher text.

**privacy-mode**: Specifies the security level to be encrypted.

**des56**: Specifies the encryption protocol to be DES (data encryption standard).

*priv-password*: Encryption password, a string of 1 to 16 characters in plain text; it can only be a string of 24 characters in cipher text.

## Description

Use the **cluster-snmp-agent usm-user v3** command to add a new user to the SNMP v3 group shared by a cluster.

Use the **undo cluster-snmp-agent usm-user v3** command to delete the SNMP v3 group user shared by the cluster.

Note that:

- The command can be executed once on the management device only. This configuration will be synchronized to member devices on the whitelist, which is equal to configuring multiple member devices at one time.
- SNMPv3 group user will be retained if a cluster is dismissed or a member device is deleted from the whitelist.
- If the same username as the current one has been configured on a member device, the current username will replace the original one on the member device.

## Examples

# Add a user **wang** to the SNMP group **snmpgroup**, set the security level to authentication-needed and specify the authentication protocol as HMAC-MD5-96 and authentication password as **pass**.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-snmp-agent usm-user v3 wang snmpgroup authentication-mode
md5 pass
```

## delete-member

### Syntax

```
delete-member member-number [ to-black-list ]
```

### View

Cluster view

### Default Level

2: System level

### Parameters

*member-number*: Number of a member device in a cluster, in the range 1 to 31.

**to-black-list**: Adds the device removed from a cluster to the blacklist to prevent it from being added to the cluster.

## Description

Use the **delete-member** command to remove a member device from the cluster.

Note that you should perform the operation to remove a member device from a cluster on the management device only.

## Examples

# Remove the member device numbered 2 from the cluster.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] delete-member 2
```

# Remove the member device numbered 3 from the cluster, and add it to the blacklist.

```
[aaa_0.Sysname-cluster] delete-member 3 to-black-list
```

## display cluster

### Syntax

**display cluster**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

## Description

Use the **display cluster** command to display the state and statistics of the cluster to which the current device belongs.

Note that this command can be executed on the management device and member devices only.

## Examples

# Display cluster information on the management device.

```
<aaa_0.Sysname> display cluster
Cluster name:"aaa"
Role:Administrator
Management-vlan:100
Handshake timer:10 sec
Handshake hold-time:60 sec
IP-Pool:1.1.1.1/16
cluster-mac:0180-c200-000a
No logging host configured
No SNMP host configured
```

```
No FTP server configured
No TFTP server configured
```

```
2 member(s) in the cluster, and 0 of them down.
```

#### # Display cluster information on a member device.

```
<aaa_1.Sysname> display cluster
Cluster name:"aaa"
Role:Member
Member number:1
Management-vlan:100
cluster-mac:0180-c200-000a
Handshake timer:10 sec
Handshake hold-time:60 sec

Administrator device IP address:1.1.1.1
Administrator device mac address:000f-e200-1d00
Administrator status:Up
```

**Table 1-5 display cluster** command output description

Field	Description
Cluster name	Name of the cluster
Role	Role of the switch in the cluster, Administrator means the current device is a management device and Member means the current device is a member device.
Member number	Member number of the switch in the cluster
Management-vlan	Management VLAN of the cluster
Handshake timer	Interval to send handshake packets
Handshake hold-time	Value of handshake timer
IP-Pool	Private IP addresses of the member devices in the cluster
cluster-mac	Multicast MAC address of cluster management packets
Administrator device IP address	IP address of the management device
Administrator device mac address	MAC address of the management device
Administrator status	State of the management device

## display cluster base-topology

### Syntax

```
display cluster base-topology [ mac-address mac-address | member-id member-number ]
```

### View

Any view

## Default Level

2: System level

## Parameters

*mac-address*: Specifies a device by its MAC address. The system will display the standard topology with the device as the root.

*member-number*: Specifies a device by its number. The system will display the standard topology with the device as the root.

## Description

Use the **display cluster topology** command to display the standard topology of a cluster.

You can create a standard topology map when executing the **build** or **auto-build** command, or you can use the **topology accept** command to save the current topology map as the standard topology map.

Note that this command can be executed on the management device only.

## Examples

# Display the standard topology of a cluster.

```
<aaa_0.Sysname> display cluster base-topology
```

```
-----  
      (PeerPort) ConnectFlag (NativePort) [SysName:DeviceMac]  
-----  
[aaa_0.Sysname:000f-e200-1400]  
|  
|  |-- (P_4/1) <--> (P_1/7) [Sysname:000f-e200-3333]  
|  |  
|  |  |-- (P_1/7) <--> (P_4/1) [aaa_3.Sysname:000f-e200-0000]  
|  |  |  
|  |  |  |-- (P_4/1) <--> (P_4/1) [aaa_0.Sysname:000f-e200-1400]  
|  |  |  |  
|  |  |  |  |-- (P_4/1) <--> (P_1/9) [Sysname:000f-e200-4800]  
|  |  |  |  |  
|  |  |  |  |  L-- (P_4/1) <--> (P_1/11) [Sysname:000f-e200-7000]  
|  |  |  |  |  |  
|  |  |  |  |  |  |-- (P_1/7) <--> (P_1/9) [Sysname:000f-e200-4800]  
|  |  |  |  |  |  |  
|  |  |  |  |  |  |  |-- (P_1/9) <--> (P_4/1) [aaa_0.3Com:000f-e200-1400]  
|  |  |  |  |  |  |  |  
|  |  |  |  |  |  |  |  L-- (P_1/9) <--> (P_1/11) [Sysname:000f-e200-7000]  
|  |  |  |  |  |  |  |  |  
|  |  |  |  |  |  |  |  |  L-- (P_1/7) <--> (P_1/11) [Sysname:000f-e200-7000]  
|  |  |  |  |  |  |  |  |  |  
|  |  |  |  |  |  |  |  |  |  |-- (P_1/3) <--> (P_1/2) [aaa_2.Sysname:00e0-fd00-4800]  
|  |  |  |  |  |  |  |  |  |  |  
|  |  |  |  |  |  |  |  |  |  |  |-- (P_1/10) <--> (P_4/1) [Sysname:000f-e205-4300]  
|  |  |  |  |  |  |  |  |  |  |  |  
|  |  |  |  |  |  |  |  |  |  |  |  |-- (P_1/11) <--> (P_4/1) [aaa_0.Sysname:000f-e200-1400]
```



Note that this command can be executed on the management device only.

## Examples

# View the current blacklist of the cluster.

```
<aaa_0.Sysname> display cluster black-list
  Device ID          Access Device ID      Access port
  000f-e200-0010    000f-e200-3550      GigabitEthernet1/0/1
```

**Table 1-7** display cluster black-list command output description

Field	Description
Device ID	ID of the blacklist device, indicated by its MAC address.
Access Device ID	ID of the device connected to the blacklist device, indicated by its MAC address.
Access port	Port connected to the blacklist device.

## display cluster candidates

### Syntax

```
display cluster candidates [ mac-address mac-address | verbose ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**mac-address** *mac-address*: Specifies the MAC address of a candidate device, in the format of H-H-H.

**verbose**: Displays the detailed information about a candidate device.

### Description

Use the **display cluster candidates** command to display the information about the candidate devices of a cluster.

Note that the command can be executed on the management device only.

## Examples

# Display the information about all the candidate devices.

```
<aaa_0.Sysname> display cluster candidates
  MAC          HOP  IP          Device
  000f-e200-3199  3           Switch 4200G
  000f-cbb8-9528  1   31.31.31.56/24  Switch 4200G
```

**Table 1-8 display cluster candidates** command output description

Field	Description
MAC	MAC address of a candidate device
HOP	Hops from a candidate device to the management device
IP	IP address of a candidate device
Device	Platform information of a device

# Display the information about a specified candidate device.

```
<aaa_0.Sysname> display cluster candidates mac-address 000f-e261-c4c0
Hostname   : LSW1
MAC        : 000f-e261-c4c0
Hop        : 1
Device     : Sysname Switch 4200G
IP         : 1.5.6.9/16
```

# Display the detailed information about all the candidate devices.

```
<aaa_0.Sysname> display cluster candidates verbose
Hostname   : 3100_4
MAC        : 000f-e200-3199
Hop        : 3
Device     : Switch 4200G
IP         :

Hostname   : Sysname
MAC        : 000f-cbb8-9528
Hop        : 1
Device     : Switch 4200G
IP         : 31.31.31.56/24
```

**Table 1-9 display cluster candidates verbose** command output description

Field	Description
Hostname	Name of a candidate device
MAC	MAC address of a candidate device
Hop	Hops from a candidate device to the management device
IP	IP address of a candidate device
Device	Platform information of a candidate device

## display cluster current-topology

### Syntax

```
display cluster current-topology [ mac-address mac-address [ to-mac-address mac-address ] |
member-id member-number [ to-member-id member-number ] ]
```

## View

Any view

## Default Level

2: System level

## Parameters

*member-number*: Number of the devices in a cluster (including the management device and member devices).

*mac-address*: MAC addresses of the devices in a cluster (including the management device and member devices).

## Description

Use the **display cluster current-topology** command to display the current topology information of the cluster.

- If you specify both the **mac-address** *mac-address* and **to-mac-address** *mac-address* arguments, the topology information of the devices that are in a cluster and form the connection between two specified devices is displayed.
- If you specify both the **member-id** *member-number* and **to-member-id** *member-number* arguments, the topology information of the devices that are in a cluster and form the connection between two specified devices is displayed.
- If you specify only the **mac-address** *mac-address* or **member-id** *member-number* argument, the topology information of all the devices in a cluster is displayed, with a specified device as the root node.

Note that this command can be executed on the management device only.

## Examples

# Display the information of the current topology of a cluster.

```
<aaa_0.Sysname> display cluster current-topology
-----
      (PeerPort) ConnectFlag (NativePort) [SysName:DeviceMac]
-----
ConnectFlag:
  <--> normal connect      ---> odd connect      **** in blacklist
  ???? lost device        +??? new device      -||- STP discarding
-----
[aaa_0.Sysname:000f-e200-7016]
|
L- (P_1/12) +??? (P_1/8) [Sysname:000f-e200-7000]
|
| - (P_1/11) +??? (P_1/9) [Sysname:000f-e200-4800]
| |
| | - (P_1/9) +??? (P_4/1) [aaa_2.Sysname:000f-e200-0000]
| |
| | L- (P_1/9) +??? (P_1/7) [Sysname:000f-e200-3333]
|
```

```

|- (P_1/11)++++ (P_4/1) [bbb_2.3Com:000f-e200-0000]
|
|
|   L- (P_4/1)++++ (P_1/7) [Sysname:000f-e200-3333]
|
|
L- (P_1/11)++++ (P_1/7) [Sysname:000f-e200-3333]

```

**Table 1-10** display cluster current-topology command output description

Field	Description
PeerPort	Peer port
ConnectFlag	Connection flag
NativePort	Local port
SysName:DeviceMac	System name of the device
<--> normal connect	Indicates a normal connection between the device and the management device
---> odd connect	Indicates a unidirectional connection between the device and the management device
**** in blacklist	Indicates the device is in the blacklist
???? lost device	Indicates a lost connection between the device and the management device
++++ new device	Indicates this is a new device, whose identity is to be recognized by the administrator
-  - STP discarding	STP is blocked



#### Note

A new device in the topology information is identified based on the standard topology. After you add a device into a cluster, if you do not use the **topology accept** command to confirm the current topology and save it as the standard topology, this device is still regarded as a new device.

## display cluster members

### Syntax

```
display cluster members [ member-number | verbose ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

*member-number*: Number of the member device, in the range 0 to 31.

**verbose:** Displays the detailed information about all the devices in a cluster.

## Description

Use the **display cluster members** command to display the information about cluster members.

Note that this command can be executed on the management device only.

## Examples

# Display the information about all the devices in a cluster.

```
<aaa_0.Sysname> display cluster members
SN   Device           MAC Address      Status Name
0    Switch 4200G      000f-e200-1751  Admin 123_0.3100_1
2    Switch 4200G      000f-e200-3199  Up     123_2.3100_4
3    Sysname S3628P    00e0-fd00-0043  Up     123_3.S3528P
4    Switch 4200G      00f-e200-2579  Up     123_4.3100_2
5    Switch 4200G      000f-e20f-c415  Up     123_5.3100_5
```

**Table 1-11 display cluster members** command output description

Field	Description
SN	Member number
Device	Device type
MAC Address	MAC address of a device
Status	State of a device: <ul style="list-style-type: none"><li>• <i>up</i>: The member device which is up</li><li>• <i>down</i>: The member which is down</li><li>• <i>deleting</i>: The member which is being deleted</li><li>• <i>admin</i>: The management device</li></ul>
Name	Name of a device

# Display the detailed information about the management device and all member devices.

```
<aaa_0.Sysname> display cluster members verbose
Member number:0
Name:aaa_0.3Com
Device:3Com Switch 4800G 24-Port
MAC Address:000f-e200-1400
Member status:Admin
Hops to administrator device:0
IP:
Version:
3Com Corporation
Switch 4800G 24-Port Software Version 5.20 ESS 2201
Copyright (c) 2004-2008 3Com Corp. and its licensors. All rights reserved.
Switch 4800G 24-Port uptime is 0 week, 0 day, 0 hour, 46 minutes

Member number:1
Name:aaa_1.3Com
```

Device:3Com Switch 4800G 48-Port  
MAC Address:000f-e200-7016  
Member status:Up  
Hops to administrator device:2  
IP: 192.168.100.245/24  
Version:  
3Com Corporation  
Switch 4800G 48-Port Software Version 5.20 ESS 2201  
Copyright (c) 2004-2008 3Com Corp. and its licensors. All rights reserved.  
Switch 4800G 48-Port uptime is 0 week, 0 day, 0 hour, 46 minutes

Member number:2  
Name:aaa\_2.3Com  
Device:3Com Switch 4800G 24-Port  
MAC Address:000f-e200-4800  
Member status:Up  
Hops to administrator device:2  
IP:  
Version:  
3Com Corporation  
Switch 4800G 24-Port Software Version 5.20 ESS 2201  
Copyright (c) 2004-2008 3Com Corp. and its licensors. All rights reserved.  
Switch 4800G 24-Port uptime is 0 week, 0 day, 0 hour, 46 minutes

Member number:3  
Name:aaa\_3.3Com  
Device:3Com Switch 4800G 24-Port  
MAC Address:000f-e200-0000  
Member status:Up  
Hops to administrator device:1  
IP:  
Version:  
3Com Corporation  
Switch 4800G 24-Port Software Version 5.20 ESS 2201  
Copyright (c) 2004-2008 3Com Corp. and its licensors. All rights reserved.  
Switch 4800G 24-Port uptime is 0 week, 0 day, 0 hour, 46 minutes

**Table 1-12** display cluster members verbose command output description

Field	Description
Member number	Device member number
Name	Name of a member device, composed of the cluster name and the host name of the member device, in the format of cluster.name.hostname When the management device type is not consistent with the member device type, if a user modifies the cluster name on the management device continuously, the cluster name may appear twice in the cluster member name, for example, "clustername.clustername.hostname". This abnormal case can restore in a period of time.
Device	Device type
MAC Address	MAC address of a device
Member status	State of a device
Hops to administrator device	Hops from the current device to the management device
IP	IP address of a device
Version	Software version of the current device

## ftp-server

### Syntax

```
ftp-server ip-address [ user-name username password { simple | cipher } password ]  
undo ftp-server
```

### View

Cluster view

### Default Level

3: Manage level

### Parameters

*ip-address*: IP address of the FTP server.

*username*: Username used to log onto the FTP server, a string of 1 to 32 characters.

**simple**: Indicates that the password is in plain text.

**cipher**: Indicates that the password is in cipher text.

*password*: Password used to log onto the FTP server. This password must be in plain text when the **simple** keyword is specified, and can be in either plain text or cipher text when the **cipher** keyword is specified. A plain text password must be a string of no more than 16 characters, such as "aabbcc". The cipher text password must have a fixed length of 24 characters, such as \_(TT8F]Y\5SQ=^Q`MAF4<1!!.

### Description

Use the **ftp-server** command to configure a public FTP server (by setting its IP address, username, and password) on the management device for the member devices in the cluster.

Use the **undo ftp-server** command to remove the FTP server configured for the member devices in the cluster.

By default, a cluster is not configured with a public FTP server.

Note that the command can be executed on the management device only.

## Examples

# Set the IP address, username and password of an FTP server shared by the cluster on the management device to be 1.0.0.9, **ftp**, and in plain text respectively.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] ftp-server 1.0.0.9 user-name ftp password simple ftp
```

## holdtime

### Syntax

**holdtime** *seconds*

**undo holdtime**

### View

Cluster view

### Default Level

2: System level

### Parameters

*seconds*: Holdtime in seconds, in the range 1 to 255.

### Description

Use the **holdtime** command to configure the holdtime of a device.

Use the **undo holdtime** command to restore the default.

By default, the holdtime of a device is 60 seconds.

Note that this command can be executed on the management device only. The configuration is valid on all member devices in a cluster.

## Examples

# Set the holdtime to 30 seconds.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] holdtime 30
```

## ip-pool

### Syntax

```
ip-pool administrator-ip-address { mask | mask-length }  
undo ip-pool
```

### View

Cluster view

### Default Level

2: System level

### Parameters

*administrator-ip-address*: Private IP address of the management device in a cluster.

*mask* | *mask-length*: Mask of the IP address pool of a cluster. It is an integer or in dotted decimal notation. When it is an integer, it ranges from 1 to 30. A network address can be obtained by ANDing this mask with *administrator-ip-address*. The private IP addresses of all member devices in a cluster belong to this network segment.

### Description

Use the **ip-pool** command to configure a private IP address range for cluster members.

Use the **undo ip-pool** command to remove the IP address range configuration.

By default, no private IP address range is configured for cluster members.

Note that:

- You must configure the IP address range on the management device only and before establishing a cluster. If a cluster has already been established, you are not allowed to change the IP address range.
- For a cluster to work normally, the IP addresses of the VLAN interfaces of the management device and member devices must not be in the same network segment as that of the cluster address pool.

### Examples

```
# Configure the IP address range of a cluster.
```

```
<Sysname> system-view  
[Sysname] cluster  
[Sysname-cluster] ip-pool 10.200.0.1 20
```

## logging-host

### Syntax

```
logging-host ip-address  
undo logging-host
```

### View

Cluster view

## Default Level

2: System level

## Parameters

*ip-address*: IP address of the logging host.

## Description

Use the **logging-host** command to configure a logging host shared by a cluster.

Use the **undo logging-host** command to remove the logging host configuration.

By default, no logging host is configured for a cluster.

Note that:

- This command can be executed on the management device only.
- You have to execute the **info-center loghost** command in system view first for the logging host you configured to take effect.

For related configuration, refer to the **info-center loghost** command in *Information Center Commands* in the *System Volume*.

## Examples

```
# Configure the IP address of the logging host shared by a cluster on the management device as 10.10.10.9.
```

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] logging-host 10.10.10.9
```

## management-vlan

### Syntax

```
management-vlan vlan-id
```

```
undo management-vlan
```

### View

System view

### Default Level

2: System level

### Parameters

*vlan-id*: ID of the management VLAN, in the range 1 to 4094.

### Description

Use the **management-vlan** command to specify the management VLAN.

Use the **undo management-vlan** command to restore the default.

By default, VLAN 1 is the management VLAN.

Note that:

- The management VLAN must be specified before a cluster is created. Once a member device is added to a cluster, the management VLAN configuration cannot be modified. To modify the management VLAN for a device belonging to a cluster, you need to cancel the cluster-related configurations on the device, specify the desired VLAN to be the management VLAN, and then re-create the cluster.
- For the purpose of security, you are not recommended to configure the management VLAN as the default VLAN ID of the port connecting the management device and the member devices.
- Only when the default VLAN ID of all cascade ports and the port connecting the management device and the member device is the management VLAN, can the packets in the management VLAN packets be passed without a tag. Otherwise, you must configure the packets from a management VLAN to pass these ports. For the configuration procedure, refer to *VLAN Configuration* in the *Access Volume*.

## Examples

```
# Specify VLAN 2 as the management VLAN.
```

```
<Sysname> system-view  
[Sysname] management-vlan 2
```

## management-vlan synchronization enable

### Syntax

```
management-vlan synchronization enable  
undo management-vlan synchronization enable
```

### View

Cluster view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **management-vlan synchronization enable** command to enable the management VLAN auto-negotiation function.

Use the **undo management-vlan synchronization enable** command to disable the management VLAN auto-negotiation function.

By default, the management VLAN auto-negotiation function is disabled.

## Examples

```
# Enable the management VLAN auto-negotiation function on the management device.
```

```
<aaa_0.Sysname> system-view  
[aaa_0.Sysname] cluster  
[aaa_0.Sysname-cluster] management-vlan synchronization enable
```

## nm-interface vlan-interface

### Syntax

```
nm-interface vlan-interface vlan-interface-id
```

### View

Cluster view

### Default Level

2: System level

### Parameters

*vlan-interface-id*: ID of the VLAN interface. The value range is the same as that of the existing VLAN interface ID.

### Description

Use the **nm-interface vlan-interface** command to configure the VLAN interface of the access management device (including FTP/TFTP server, management host and log host) as the network management interface of the management device.

### Examples

```
# Configure VLAN-interface 2 as the network management interface.
```

```
<aaa_0.Sysname> system-view  
[aaa_0.Sysname] cluster  
[aaa_0.Sysname-cluster] nm-interface vlan-interface 2
```

## reboot member

### Syntax

```
reboot member { member-number | mac-address mac-address } [ eraseflash ]
```

### View

Cluster view

### Default Level

2: System level

### Parameters

*member-number*: Number of the member device, in the range 1 to 31.

**mac-address** *mac-address*: MAC address of the member device to be rebooted, in the format of H-H-H.

**eraseflash**: Deletes the configuration file when the member device reboots.

### Description

Use the **reboot member** command to reboot a specified member device on the management device.

## Examples

```
# Reboot the member device numbered 2.
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] reboot member 2
```

## snmp-host

### Syntax

```
snmp-host ip-address [ community-string read string1 write string2 ]
undo snmp-host
```

### View

Cluster view

### Default Level

3: Manage level

### Parameters

*ip-address*: IP address of an SNMP host.

*string1*: Community name of read-only access, a string of 1 to 26 characters.

*string2*: Community name of read-write access, a string of 1 to 26 characters.

### Description

Use the **snmp-host** command to configure a shared SNMP host for a cluster.

Use the **undo snmp-host** command to cancel the SNMP host configuration.

By default, no SNMP host is configured for a cluster.

Note that this command can be executed on the management device only.

## Examples

```
# Configure a shared SNMP host for the cluster on the management device.
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] snmp-host 1.0.0.9 community-string read 123 write 456
```

## tftp-server

### Syntax

```
tftp-server ip-address
undo tftp-server
```

## View

Cluster view

## Default Level

2: System level

## Parameters

*ip-address*: IP address of a TFTP server.

## Description

Use the **tftp-server** command to configure a shared TFTP server for a cluster.

Use the **undo tftp-server** command to cancel the TFTP server of the cluster.

By default, no TFTP server is configured.

Note that this command can be executed on the management device only.

## Examples

# Configure a shared TFTP server on the management device as 1.0.0.9.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] tftp-server 1.0.0.9
```

## timer

### Syntax

**timer** *interval-time*

**undo timer**

### View

Cluster view

### Default Level

2: System level

### Parameters

*interval-time*: Interval (in seconds) to send handshake packets. This argument ranges from 1 to 255.

### Description

Use the **timer** command to set the interval to send handshake packets.

Use the **undo timer** command to restore the default.

By default, the interval to send handshake packets is 10 seconds.

Note that this command can be executed on the management device only and is valid for all member devices in a cluster.

## Examples

```
# Configure the interval to send handshake packets as 3 seconds.
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] timer 3
```

## topology accept

### Syntax

```
topology accept { all [ save-to { ftp-server | local-flash } ] | mac-address mac-address | member-id member-number }
```

```
undo topology accept { all | mac-address mac-address | member-id member-number }
```

### View

Cluster view

### Default Level

2: System level

### Parameters

**all**: Accepts the current cluster topology information as the standard topology information.

**mac-address** *mac-address*: Specifies a device by its MAC address. The device will be accepted to join the standard topology of the cluster.

**member-id** *member-number*: Specifies a device by its member number. The device will be accepted to join the standard topology of the cluster. The *member-number* argument is in the range 0 to 31.

**save-to**: Confirms the current topology as the standard topology, and backs up the standard topology on the FTP server or local flash in a file named “topology.top”.

### Description

Use the **topology accept** command to confirm the current topology information and save it as the standard topology.

Use the **undo topology accept** to delete the standard topology information.

Note that:

- This command can be executed on the management device only.
- The file used to save standard topology on the FTP server or the local flash is named “topology.top”, which includes both the information of blacklist and whitelist. A blacklist contains the devices that are prohibited to be added to a cluster. A whitelist contains devices that can be added to a cluster.

## Examples

```
# Take the current topology as the standard topology.
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
```

```
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] topology accept all
```

## topology restore-from

### Syntax

```
topology restore-from { ftp-server | local-flash }
```

### View

Cluster view

### Default Level

2: System level

### Parameters

**ftp-server:** Restores the standard topology information from the FTP server.

**local-flash:** Restores the standard topology information from the local flash.

### Description

Use the **topology restore-from** command to restore the standard topology information from the FTP server or the local flash in case the cluster topology information is incorrect.

Note that:

- This command can be executed on the management device only.
- If the stored standard topology is not correct, the device cannot be aware of it. Therefore, you must ensure that the standard topology is correct.

### Examples

```
# Restore the standard topology.
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] topology restore-from local-flash
```

## topology save-to

### Syntax

```
topology save-to { ftp-server | local-flash }
```

### View

Cluster view

### Default Level

2: System level

## Parameters

**ftp-server:** Saves the standard topology information to the FTP server.

**local-flash:** Saves the standard topology information to the local flash.

## Description

Use the **topology save-to** command to save the standard topology information to the FTP server or the local flash.

Note that:

- The file used to save standard topology on the FTP server or the local flash is named “topology.top”, which includes both the information of blacklist and whitelist. A blacklist contains the devices that are prohibited to be added to a cluster. A whitelist contains devices that can be added to a cluster.
- This command can be executed on the management device only.

## Examples

# Save the standard topology information to the local flash.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] topology save-to local-flash
```

# Table of Contents

<b>1 IRF Stack Configuration Commands</b> .....	<b>1-1</b>
IRF Stack Configuration Commands .....	1-1
display irf .....	1-1
display irf configuration .....	1-2
display irf topology .....	1-3
display switchover state .....	1-5
irf auto-update enable .....	1-6
irf link-delay .....	1-7
irf mac-address persistent .....	1-8
irf member priority .....	1-9
irf member renumber .....	1-10
irf member irf-port .....	1-11
irf switch-to .....	1-12

# 1 IRF Stack Configuration Commands

---

## IRF Stack Configuration Commands

### display irf

#### Syntax

display irf

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

None

#### Description

Use the **display irf** command to display the information of the current Intelligent Resilient Framework (IRF) stack, which has the device you are working on as its stack member.

The command displays the information of stack members, and the information of the devices that are joining in this stack.

#### Examples

# Display the information of the current IRF stack.

```
<Sysname> display irf
```

Switch	Role	Priority	CPU-MAC
1	Slave	13	000f-e2b8-1f84
2	Slave	1	000f-e220-2122
*3	Master	20	000f-e2b8-1a82
+4	SlaveWait	1	000f-e2c8-1b82
5	Loading	1	000f-e2c8-1c82

-----  
\* indicates the device is the master.

+ indicates the device through which the user logs in.

The Bridge MAC of the IRF is : 000f-e2b8-1a61

Auto upgrade : yes

Mac persistent : 6 min

**Table 1-1 display irf command output description**

Field	Description
Switch	Member ID. <ul style="list-style-type: none"><li>• The ID with * indicates that the device is the master;</li><li>• The ID with + indicates that it is the device through which the user logs in to the stack.</li></ul>
Role	The role of a member in the stack, which may take the following values: <ul style="list-style-type: none"><li>• Slave</li><li>• Master</li><li>• SlaveWait</li><li>• Loading</li></ul>
CPU-MAC	CPU MAC address of the device
Auto upgrade	Whether the auto upgrade of configuration files is enabled: <ul style="list-style-type: none"><li>• yes: Enabled</li><li>• no: Disabled</li></ul>
Mac persistent	Whether the stack bridge MAC address preservation is enabled: <ul style="list-style-type: none"><li>• yes: Enabled</li><li>• no: Disabled</li></ul>

## display irf configuration

### Syntax

**display irf configuration**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display irf configuration** command to display the pre-configurations of stack members in the current IRF stack.

The pre-configuration takes effect after the reboot of the device. The command displays the member ID, logical stack port, and physical stack port information.

### Examples

# Display the pre-configurations of all the stack members in the current stack.

```
<Sysname> display irf configuration
MemberID  NewID  IRF-Port1  IRF-Port2
  1         5      1,2        3,4
  2         2      1,2        3
 *3         3      1          3
```

```
+4      4      1      disable
```

---

\* indicates the device is the master.

+ indicates the device through which the user logs in.

**Table 1-2 display irf configuration command output description**

Field	Description
MemberID	Member ID <ul style="list-style-type: none"> <li>The ID with * indicates that the device is the master;</li> <li>The ID with + indicates that it is the device through which the users logs in to the stack.</li> </ul>
NewID	The member ID configured for a device after its reboot
IRF-Port1	The physical stack port number corresponding to logical stack port 1 of a device after its reboot. (If it displayed in the format of <b>x</b> , it indicates that logical stack port 1 is bound to physical stack port x; if it is displayed in the format of <b>x,y</b> , it indicates that logical stack port 1 is aggregated by physical stack ports x and y; if it is displayed as <b>disable</b> , it indicates that logical stack port 1 is not enabled.)
IRF-Port2	The physical stack port number corresponding to logical stack port 2 of a device after its reboot. (If it displayed in the format of <b>x</b> , it indicates that logical stack port 2 is bound to physical stack port x; if it is displayed in the format of <b>x,y</b> , it indicates that logical stack port 2 is aggregated by physical stack ports x and y; if it is displayed as <b>disable</b> , it indicates that logical stack port 2 is not enabled.)

## display irf topology

### Syntax

```
display irf topology
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display irf topology** command to display the topology information of the current IRF stack. The command displays all the topology information learned by the current device.

### Examples

```
# Display the topology information of the current IRF stack.
```

```
<Sysname> display irf topology
Topology Info
```

---

Switch	Link	IRF-Port1		IRF-Port2			Belong To
		member	neighbor	Link	member	neighbor	
1	DOWN	1,2	--	UP	3,4	2	000f-cbb8-1a82
2	UP	1,2	1	UP	3	3	000f-cbb8-1a82
*+3	UP	1	2	DIS	--	--	000f-cbb8-1a82

\* indicates the device is the master.

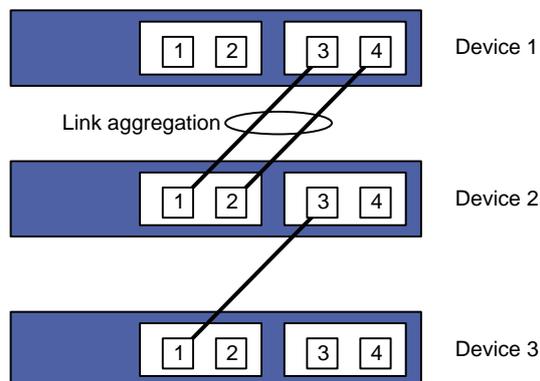
+ indicates the device through which the user logs in.

The above information indicates following:

- On device 1, logical stack port 1 is aggregated from physical stack ports 1 and 2, and it is down; logical stack port 2 is aggregated from physical stack ports 3 and 4, and it is up.
- On device 2, logical stack port 1 is aggregated from physical stack ports 1 and 2, and it is up; logical stack port 2 corresponds to physical stack port 3, and it is up.
- On device 3, logical stack port 1 corresponds to physical stack port 1, and it is up; stack is disabled on logical stack port 2.
- Logical stack port 1 of device 1 does not connect with any other device; logical stack port 2 of device 1 connects to logical stack port 1 of device 2; logical stack port 2 connects to logical stack port 1 of device 3; logical stack port 2 of device 3 does not connect with any other device.
- All the three devices belong to one IRF stack. The bridge MAC address of the master is 000f-cbb8-1a82.

Network topology view is as shown in [Figure 1-1](#):

**Figure 1-1** Network topology view



**Table 1-3** display irf topology command output description

Field	Description
Switch	Member ID <ul style="list-style-type: none"> <li>• The ID with * indicates that the device is the master;</li> <li>• The ID with + indicates that it is the device through which the users logs in to the stack.</li> </ul>
IRF-Port 1	Information of logical stack port 1, including link (link state), member (corresponding physical port), and neighbor.
IRF-Port 2	Information of logical stack port 2, including link, member, and neighbor.
BelongTo	The IRF stack that the device belongs to, represented by the stack CPU MAC address.

Field	Description
Link	Link state of the logical stack port: <ul style="list-style-type: none"> <li>• UP</li> <li>• DOWN</li> <li>• ISOLATE: The corresponding physical stack port is isolated because it cannot meet the requirement of the stack. The reason may be that the physical stack port connects to a non-Switch 4800G device, or the logical stack port of the peer end is not connected according to the port serial numbers.</li> <li>• TIMEOUT: The port does not receive any Hello packet from the peer end after the expected time, that is, the Hello packet sent to the port times out.</li> <li>• DIS: The stack port is not enabled.</li> </ul>
member	The corresponding physical port(s) of the logical stack port. If the logical stack port is disabled, -- will be displayed.
neighbor	The device ID that connects with this logical stack port If the logical stack port does not connect with any device, -- will be displayed.

## display switchover state

### Syntax

```
display switchover state [ slot slot-id ]
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**slot slot-id**: ID of the stack member. With this argument, the command displays the master/slave switchover state of the specified stack member. Without this argument, the command displays the master/slave switchover state of the stack master.

### Description

Use the **display switchover state** command to display the master/slave switchover states of stack members.

A stack functions like a logical distributed device with multiple standby switching and routing processing units (SRPUs). The master is like the active SRPU, and the slaves are like the standby SRPUs. A stack system uses member ID to uniquely identify a member device, whereas a distributed device uses slot ID to uniquely identify a board. Therefore, in the displayed information of this command, a member device is also identified by the slot ID, which is equal to the member ID.

### Examples

```
# Display the master/slave switchover states of the master.
```

```
<Sysname> display switchover state
```

```

Master HA State to Slot [1]: Slave is absent.
Master HA State to Slot [2]: Slave is absent.
Master HA State to Slot [4]: Waiting batch backup request from slave.
Master HA State to Slot [5]: Slave is absent.
Master HA State to Slot [6]: Realtime backup to slave.
Master HA State to Slot [7]: Realtime backup to slave.
Master HA State to Slot [8]: Slave is absent.
Master HA State to Slot [9]: Slave is absent.

```

The above information indicates the following:

- Slaves 1, 2, 5, 8, and 9 are absent, which means that these devices are not in use
- The master is waiting for the batch backup request from slave 4
- Slaves 6 and 7 are performing real time backup

**Table 1-4 display switchover state** command output description for the master

Field	Description
Master HA State to Slot <i>slot-id</i>	Indicates that this output information is generated by the master. Describes the master/slave switchover states between the master and the slave whose <i>slot-id</i> represents its member ID.
Data smooth	The master and the slave are smoothing data.

# Display the master/slave switchover state of slave 6.

```

<Sysname> display switchover state slot 6
Slave HA State: Receiving realtime data.

```

The above information indicates that slave 6 is receiving real time backup data.

**Table 1-5 display switchover state** command output description for a slave

Field	Description
Slave HA State	Indicates that this output information is generated by a slave. Describes the master/slave switchover state of the slave.
Waiting	The slave is ready, and is waiting to enter the batch backup state.

## irf auto-update enable

### Syntax

```

irf auto-update enable
undo irf auto-update enable

```

### View

System view

### Default Level

3: Manage level

## Parameters

None

## Description

Use the **irf auto-update enable** command to enable the auto update of boot files in an IRF stack.

Use the **undo irf auto-update enable** command to disable this function.

This function is enabled by default.

Note the following:

- Before adding a device into an IRF stack, ensure that the device and the stack master have the same software version
- After loading the master's boot file automatically, a slave configures the file as the boot file for the next boot and reboots automatically.
- Because system boot file occupies large memory space, to make the auto upgrade succeed, ensure that there is enough space on the storage media of the slave.
- If the downloaded boot file and the local file have duplicate filenames, the local file is overwritten. To avoid this, check the names of local files and make sure whether you need to save the one with the same filename or back it up before downloading the boot file.

## Examples

```
# Enable auto upgrade of boot files in an IRF stack.
```

```
<Sysname> system-view
```

```
[Sysname] irf auto-update enable
```

## irf link-delay

### Syntax

```
irf link-delay interval
```

```
undo irf link-delay
```

### View

System view

### Default Level

3: Manage level

### Parameters

*Interval*: Time interval in milliseconds for the link layer to report a link-down event of a stack, in the range 200 to 2000.

### Description

Use the **irf link-delay** command to set the delay time for the link layer to report a link-down state event of a stack.

Use the **undo irf link-delay** command to restore the default.

This function is disabled by default.

## Examples

```
# Set the delay time for the link layer to report a link-down event of the current stack to 300 milliseconds.
<Sysname> system-view
[Sysname] irf link-delay 300
```

## irf mac-address persistent

### Syntax

```
irf mac-address persistent { timer | always }
undo irf mac-address persistent
```

### View

System view

### Default Level

3: Manage level

### Parameters

**timer**: Stack bridge MAC address preservation mode, with this keyword, the stack bridge MAC address will be preserved for 6 minutes after the master leaves.

**always**: Stack bridge MAC address preservation mode, with this keyword, the stack bridge MAC address will be preserved permanently.

### Description

Use the **irf mac-address persistent** command to configure the preservation time of stack bridge MAC address.

Use the **undo irf mac-address persistent** command to configure the stack not to preserve the stack bridge MAC address as soon as the master leaves.

By default, stack bridge MAC address is preserved for 6 minutes.

- Preserve for six minutes: After the master leaves, the bridge MAC address will not change within six minutes. If the master does not come back after six minutes, the stack system will use the bridge MAC address of the newly elected master as that of the stack.
- Preserve permanently: No matter the master leaves the stack or not, the stack bridge MAC address remains unchanged.
- Not preserved: As soon as the master leaves, the system will use the bridge MAC address of the newly elected master as that of the stack.

## Examples

```
# Configure the stack bridge MAC address to be preserved permanently.
<Sysname> system-view
[Sysname] irf mac-address persistent always
```

## irf member priority

### Syntax

```
irf member member-id priority priority
```

```
undo irf member member-id priority
```

### View

System view

### Default Level

3: Manage level

### Parameters

*member-id*: ID of the stack member, in the range 1 to 9. With this argument, you can specify a priority for another stack member on this device. You can view the member IDs and current priorities of stack members by using the **display irf** command.

*priority*: Priority value, in the range 1 to 32.

### Description

Use the **irf member priority** command to specify a priority for a stack member.

Use the **undo irf member priority** command to restore the default.

By default, the priority of a stack member is 1.

The greater the priority value, the higher the priority. A member with a higher priority is more likely to be a master, and more likely to preserve its ID in a member ID collision.

Note the following:

- You can specify a priority for a member of the current IRF stack only.
- The setting of priority takes effect right after your configuration.

### Examples

# Specify a priority for the local device.

```
<Sysname> display irf
```

Switch	Role	Priority	CPU-MAC
1	Slave	13	000f-e2b8-1f84
2	Slave	1	000f-e220-2122
*3	Master	20	000f-e2b8-1a82
+4	SlaveWait	1	000f-e2c8-1b82
5	Loading	1	000f-e2c8-1c82

-----  
\* indicates the device is the master.

+ indicates the device through which the user logs in.

The Bridge MAC of the IRF is : 000f-e2b8-1a67

Auto upgrade : yes

Mac persistent : 6 min

The above information indicates that the member ID of the local device is 4, and you can specify a priority for the local device by providing its member ID.

```
<Sysname> system-view
[Sysname] irf member 4 priority 16

# Specify a priority for member 2 in the current stack.

<Sysname> system-view
[Sysname] irf member 2 priotiry 32
```

## irf member renumber

### Syntax

```
irf member member-id renumber new-member-id
undo irf member member-id renumber
```

### View

System view

### Default Level

3: Manage level

### Parameters

*member-id*: ID of the stack member, in the range 1 to 9. With this argument, you can modify a member ID of another stack member on this device. You can view the member IDs of in a stack by using the **display irf** command.

*new-member-id*: New ID of the stack member, in the range 1 to 9.

### Description

Use the **irf member renumber** command to set a member ID for a device.

Use the **undo irf member renumber** command to cancel the configuration.

By default, the member ID of a stack member is 1.

Note the following:

- The above setting takes effect after the reboot of the device.
- In an IRF stack, member IDs are not only used to identify devices, but also used to identify the port configurations on different member devices in the configuration file. Therefore, modifying a member ID may cause device configuration changes or even losses, so modify member ID with caution. For example, three members (of same device model) with the member IDs of 1, 2 and 3 are connected to a stack port. Suppose that each member has several ports: change the member ID of device 2 to 3, change that of device 3 to 2, reboot both devices, and add them into the stack again. Then device 2 will use the original port configurations of device 3, and device 3 will use those of device 2.
- When the newly added device and another member have duplicated member IDs, the existing member can preserve its ID, and the system will automatically assign the smallest unused member ID to the new member.

### Examples

```
# Set the member ID of the local device (the current member ID is 1) to 3.
```

```
<Sysname> system-view
```

```
[Sysname] irf member 1 renumber 3
```

Warning: Renumbering the switch number may result in configuration change or loss.

```
Continue?[Y/N]:Y
```

## irf member irf-port

### Syntax

```
irf member member-id irf-port irf-port-id port port-list
```

```
undo irf member member-id irf-port irf-port-id
```

### View

System view

### Default Level

3: Manage level

### Parameters

*member-id*: ID of the stack member, in the range 1 to 9. With this argument, you can configure the stack ports of another stack member on this device. You can view the member IDs of in stack by using the **display irf** command.

*irf-port-id*: ID of an enabled logical stack port, the value can be either 1 (the left port) or 2 (the right port).

*port-list*: Physical stack port list. The *port-list* is in the format of { *port* }&<1-4>, where

- *port* indicates the port ID. The physical stack ports are numbered according to their physical locations on the rear panel of the Switch 4800G series. With the rear panel facing you, the physical stack ports are numbered successively from left to right: ports on the interface module in slot 1 are numbered 1 and 2, and ports on the interface module in slot 2 are numbered 3 and 4.
- &<1-4> indicates that you can specify one to four ports at one time. When multiple ports are specified, they aggregate together to form a stack port. On the Switch 4800G series, only the physical stack ports that are on the same interface module can be aggregated together.



#### Note

For the correspondence between a logical stack port and physical stack port, refer to the related part in *IRF Stack Configuration*.

---

### Description

Use the **irf member irf-port** command to bind the physical stack port(s) to a logical stack port of a device, and enable IRF stack on the logical stack port simultaneously.

Use the **undo irf member irf-port** command to disable IRF stack on a logical stack port. If this logical stack port is aggregated from multiple physical stack ports, the aggregated physical ports are disaggregated.

Note the following:

- The above configuration takes effect after the reboot of the device.

- A logical stack port should be enabled first before it can connect to other devices to form a stack.

## Examples

# Bind physical stack port 1 to logical stack port 1, and enable logical stack port 1 of the local device.

```
<Sysname> system-view
[Sysname] irf member 1 irf-port 1 port 1
```

# Bind physical stack ports 3 and 4 to logical stack port 2 of member 3, and enable IRF stack on the logical stack port.

```
<Sysname> system-view
[Sysname] stack member 3 stack-port 2 port 3 4
```

## irf switch-to

### Syntax

**irf switch-to** *member-id*

### View

User view

### Default Level

3: Manage level

### Parameters

*member-id*: ID of the stack member. The *member-id* argument in this command cannot be the member ID of the master. You can view the member IDs of in a stack by using the **display irf** command.

### Description

Use the **irf switch-to** command to redirect to the specified slave device, so that you can access the slave device directly.

When you access an IRF stack, you actually log in to the master device. The console of the master is displayed as the operation interface of the access terminal. After you execute this command, you are redirected to the specified slave device, which is equal to log in to the slave directly. The operation interface of the access terminal switches from the console of the master to that of the slave, and the system enters the user view of the slave. You will see that the command prompt changes to the following format: `<Sysname-member ID>`, for example, `<Sysname-Slave#2>`.

After this command is executed, the instructions that you input at the terminal will be forwarded to the specified slave, without being processed by the local device. Currently, you can execute the following commands on a slave:

- **display**
- **quit**
- **return**
- **system-view**
- **debugging**
- **terminal debugging**
- **terminal trapping**
- **terminal logging**

The console of the master will not time out and will not output any information. You can return to the console of the master by pressing the **Ctrl+K** keys, or execute the **quit** or **return** command. The master is therefore reactivated and is ready for outputting information.

### Examples

# Redirect to member 2.

```
<Sysname> irf switch-to 2
```

```
<Sysname-Slave#2>
```

# Table of Contents

<b>1 IPC Configuration Commands .....</b>	<b>1-1</b>
IPC Configuration Commands .....	1-1
display ipc channel .....	1-1
display ipc link .....	1-2
display ipc multicast-group .....	1-3
display ipc node.....	1-4
display ipc packet .....	1-4
display ipc performance.....	1-5
display ipc queue.....	1-7
ipc performance enable .....	1-8
reset ipc performance.....	1-9

# 1 IPC Configuration Commands

---



- The **display** commands in this document display information of active nodes only.
  - For a centralized device, “local node” refers to a local device; for a distributed device, “local node” refers to the active main control board.
- 

## IPC Configuration Commands

### display ipc channel

#### Syntax

```
display ipc channel { node node-id | self-node }
```

#### View

Any view

#### Default Level

1: Monitor level

#### Parameters

**node** *node-id*: Displays channel information of the specified node, where *node-id* represents the number of the specified node, in the range of 0 to 9.

**self-node**: Displays the channel information of the local node.

#### Description

Use the **display ipc channel** command to display the channel information of the specified node.

#### Examples

```
# Display channel information of node 6.
```

```
<Sysname> display ipc channel node 6
```

```
ChannelID      Description
```

```
-----  
14             Prehistorical channel, NO.2
```

```
15             Prehistorical channel, NO.6
```

```
16             Prehistorical channel, NO.7
```

```
19             Prehistorical channel, NO.1
```

```
25             Prehistorical channel, NO.4
```

26	Prehistorical channel, NO.8
27	FIB4
32	Prehistorical channel, NO.3
33	Prehistorical channel, NO.11
34	Prehistorical channel, NO.9
35	IPC test channel
37	Prehistorical channel, NO.12
43	Prehistorical channel, NO.14
45	Prehistorical channel, NO.5
53	Prehistorical channel, NO.13
62	Prehistorical channel, NO.10

**Table 1-1 display ipc channel command output description**

Field	Description
ChannelID	Channel number, which has been predefined and assigned by the system. One channel number corresponds to one module. The <b>display ipc channel</b> command displays the numbers of the current active modules.
Description	Description information, which is generated by the internal software of the device, is used to describe the functions of a channel. For example, "FIB4" indicates that the channel is used for Layer 3 fast forwarding; "Prehistorical channel, NO.2" indicates that no description is defined for the channel, and the channel is the second channel established.

## display ipc link

### Syntax

```
display ipc link { node node-id | self-node }
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**node** *node-id*: Displays the link information of the specified node, where *node-id* represents the number of the specified node, in the range of 0 to 9.

**self-node**: Displays the link status information of the local node.

### Description

Use the **display ipc link** command to display the link status information of the specified node.

### Examples

```
# Display link status information of the local node.
```

```
<Sysname> display ipc link self-node
```

```
Dst-NodeID          LinkStatus
```

```
-----
```

1	UP
2	DOWN

The above prompt information indicates that:

- A connection exists between the local node and node 1, and the connection is up;
- A connection exists between the local node and node 2, and the connection is down.

**Table 1-2 display ipc link command output description**

Field	Description
Dst-NodeID	Number of the peer node
LinkStatus	Link status, which may take the following values: UP: A connection is established. DOWN: A connection is terminated.

## display ipc multicast-group

### Syntax

```
display ipc multicast-group { node node-id | self-node }
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**node** *node-id*: Displays the multicast group information of the specified node, where *node-id* represents the number of the specified node, in the range of 0 to 9.

**self-node**: Displays the multicast group information of the local node.

### Description

Use the **display ipc multicast-group** command to display the multicast group information of the specified node.

### Examples

# Display the multicast group information of node 6.

```
<Sysname> display ipc multicast-group node 6
```

```
GroupID      Status      ChannelID
-----
8            INUSE      12
```

**Table 1-3 display ipc group** command output description

Field	Description
GroupID	Multicast group ID
Status	Link status, which may take the following values: INUSE: The multicast group is in use. DELETE: The multicast group is to be deleted.
ChannelID	Channel number

## display ipc node

### Syntax

**display ipc node**

### View

Any view

### Default Level

1: Monitor level

### Parameters

None

### Description

Use the **display ipc node** command to display node information.

### Examples

# Display node information of the device.

```
<Sysname> display ipc node
```

```
Self node ID: 6
```

```
Current active node ID: 2,3,6,8
```

**Table 1-4 display ipc node** command output description

Field	Description
Self node ID	Number of the local node
Current active node ID	List of the current active nodes

## display ipc packet

### Syntax

**display ipc packet { node *node-id* | self-node }**

### View

Any view

## Default Level

1: Monitor level

## Parameters

**node** *node-id*: Displays the packet statistics information of the specified node, where *node-id* represents the number of the specified node, in the range of 0 to 9.

**self-node**: Displays the packet statistics information of the local node.

## Description

Use the **display ipc packet** command to display the packet statistics information of the specified node.

## Examples

# Display the packet statistics information of the local node.

```
<Sysname> display ipc packet self-node
```

```
ChannelID Sent-fragments Sent-packets Received-fragments Received-packets
```

```
-----
```

11	828	810	819	810
13	0	0	0	0
14	5	3	5	5
15	0	0	0	0
16	0	0	0	0
17	50	50	37	35
19	0	0	0	0

**Table 1-5 display ipc packet** command output description

Field	Description
ChannelID	Channel number
Sent-fragments	Number of fragments sent
Sent-packets	Number of packets sent (whether a packet is fragmented depends on the interface MTU. If the number of bytes the packet is larger than the MTU, the packet is fragmented; if smaller than or equal to the MTU, the packet is sent.)
Received-fragments	Number of fragments successfully received
Received-packets	Number of packets successfully received (if fragments are received on an interface, the system reassembles the fragments and sends a complete packet to the upper layer software.)

## display ipc performance

### Syntax

```
display ipc performance { node node-id | self-node } [ channel channel-id ]
```

### View

Any view

## Default Level

1: Monitor level

## Parameters

**node** *node-id*: Displays the IPC performance statistics information of the specified node, where *node-id* represents the number of the specified node, in the range of 0 to 9.

**self-node**: Displays the IPC performance statistics information of the local node.

**channel** *channel-id*: Displays the IPC performance statistics information of the specified channel, where *channel-id* represents the channel number, in the range of 0 to 159.

## Description

Use the **display ipc performance** command to display IPC performance statistics information.

If IPC performance statistics is enabled, the command displays the current IPC performance statistics; if IPC performance statistics is disabled, the command displays the IPC performance statistics at the time when IPC performance statistics is disabled.

Related commands: **ipc performance enable**.

## Examples

# Display IPC performance statistics information of node 6.

```
<Sysname> display ipc performance node 6
Peak: Peak rate (pps)
10Sec: Average rate in the last 10 seconds (pps)
1Min: Average rate in the last 1 minute (pps)
5Min: Average rate in the last 5 minutes (pps)
Total-Data: Total number of data (packets)

Statistics for packets sent successfully:
Peak          10Sec          1Min          5Min          Total-Data
-----
1              1              1              0              80
Statistics for packets recieved successfully:
Peak          10Sec          1Min          5Min          Total-Data
-----
1              1              1              0              82
Statistics for packets acknowledged:
Peak          10Sec          1Min          5Min          Total-Data
-----
1              1              1              0              78
```

**Table 1-6 display ipc performance** command output description

Field	Description
Peak	Peak rate (average rate is counted every 10 seconds, the greatest value of which is taken as the peak rate), in pps
10Sec	Average rate in the past 10 seconds, in pps
1Min	Average rate in the past 1 minute, in pps

Field	Description
5Min	Average rate in the past 5 minutes, in pps
Total-Data	Total amount of data collected from the time when IPC performance statistics was enabled to the time when this command is executed

## display ipc queue

### Syntax

```
display ipc queue { node node-id | self-node }
```

### View

Any view

### Default Level

1: Monitor level

### Parameters

**node** *node-id*: Displays the sending queue information of the specified node, where *node-id* represents the number of the specified node, in the range of 0 to 9.

**self-node**: Displays the sending queue information of the local node.

### Description

Use the **display ipc queue** command to display the sending queue information of the specified node.

### Examples

# Display the sending queue information of the local node.

```
<Sysname> display ipc queue self-node
QueueType  QueueID  Dst-NodeID  Length  FullTimes  Packet
-----
UNICAST    0         0            4096    0          0
UNICAST    1         0            4096    0          0
UNICAST    2         0            4096    0          0
UNICAST    3         0            4096    0          0
UNICAST    0         1            4096    0          0
UNICAST    1         1            4096    0          0
UNICAST    2         1            4096    0          0
UNICAST    3         1            4096    0          0
MULTICAST  0         --           4096    0          0
MULTICAST  1         --           4096    0          0
MULTICAST  2         --           512     0          0
MULTICAST  3         --           512     0          0
MULTICAST  4         --           512     0          0
MULTICAST  5         --           512     0          0
MIXCAST    0         --           2048    0          0
MIXCAST    1         --           2048    0          0
```

**Table 1-7 display ipc queue** command output description

Field	Description
QueueType	Queue type, including: UNICAST: unicast queue MULTICAST: multicast (including broadcast) queue MIXCAST: mixcast queue, which can accommodate unicasts, multicasts and broadcasts
QueueID	Queue number
Dst-NodeID	Peer node number. If no peer node exists, the field is displayed as "--".
Length	Queue length (namely, number of packets that can be cached)
FullTimes	Times that the queue is full
Packet	Total number of packets in the queue

## ipc performance enable

### Syntax

```
ipc performance enable { node node-id | self-node } [ channel channel-id ]  
undo ipc performance enable [ node node-id | self-node ] [ channel channel-id ]
```

### View

User view

### Default Level

1: Monitor level

### Parameters

**node** *node-id*: Enables IPC performance statistics of the specified node, where *node-id* represents the number of the specified node, in the range of 0 to 9.

**self-node**: Enables IPC performance statistics of the local node.

**channel** *channel-id*: Enables IPC performance statistics information of the specified channel, where *channel-id* represents the channel number, in the range of 0 to 159.

### Description

Use the **ipc performance enable** command to enable IPC performance statistics. Use the **undo ipc performance** command to disable IPC performance statistics.

By default, IPC performance statistics is disabled.

When IPC performance statistics is disabled, the statistics data does not change. In this case, if you execute the **display ipc performance** command, the statistics data at the time when ICP performance statistics was disabled.

### Examples

```
# Enable IPC performance statistics of node 6 on channel 18.
```

```
<Sysname> ipc performance enable node 6 channel 18
```

## reset ipc performance

### Syntax

```
reset ipc performance [ node node-id | self-node ] [ channel channel-id ]
```

### View

User view

### Default Level

1: Monitor level

### Parameters

**node** *node-id*: Clears the IPC performance statistics information of the specified node, where *node-id* represents the number of the specified node, in the range of 0 to 9.

**self-node**: Clears the IPC performance statistics information of the local node.

**channel** *channel-id*: Clears the IPC performance statistics information of the specified channel, where *channel-id* represents the channel number, in the range of 0 to 159.

### Description

Use the **reset ipc performance** command to clear IPC performance statistics information.

After this command is executed, the corresponding statistics information will be cleared.

### Examples

# Clear IPC performance statistics information of node **6** on channel **18**.

```
<Sysname> reset ipc performance node 6 channel 18
```