# Table of Contents

1 **Product Overview** .................................................................................................................. 1-1  
  Preface .............................................................................................................................. 1-1  
  System Features .................................................................................................................. 1-2  
  Service Features .................................................................................................................. 1-3  

2 **Hardware Description** ......................................................................................................... 2-1  
  H3C S5120-20P-SI .................................................................................................................. 2-1  
    Front Panel .......................................................................................................................... 2-1  
    Rear Panel .......................................................................................................................... 2-1  
    Power Supply System ......................................................................................................... 2-1  
    Cooling System .................................................................................................................. 2-1  
  H3C S5120-28P-SI .................................................................................................................. 2-2  
    Front Panel .......................................................................................................................... 2-2  
    Rear Panel .......................................................................................................................... 2-2  
    Power Supply System ......................................................................................................... 2-2  
    Cooling System .................................................................................................................. 2-2  
  H3C S5120-52P-SI .................................................................................................................. 2-3  
    Front Panel .......................................................................................................................... 2-3  
    Rear Panel .......................................................................................................................... 2-3  
    Power Supply System ......................................................................................................... 2-3  
    Cooling System .................................................................................................................. 2-3  
  H3C S5120-28P-PWR-SI ......................................................................................................... 2-4  
    Front Panel .......................................................................................................................... 2-4  
    Rear Panel .......................................................................................................................... 2-4  
    Power Supply System ......................................................................................................... 2-4  
    Cooling System .................................................................................................................. 2-4  
  H3C S5120-28P-HPWR-SI ...................................................................................................... 2-5  
    Front Panel .......................................................................................................................... 2-5  
    Rear Panel .......................................................................................................................... 2-5  
    Power Supply System ......................................................................................................... 2-5  
    Cooling System .................................................................................................................. 2-6  
  LEDs ........................................................................................................................................ 2-6  
    Power LED ............................................................................................................................ 2-6  
    RPS Status LED .................................................................................................................. 2-6  
    Port Mode LED ................................................................................................................... 2-6  
    10/100/1000Base-T auto-sensing Ethernet port status LEDs .............................................. 2-7  
    1000Base-X SFP interface status LEDs ............................................................................. 2-8  

3 **Software Features** .................................................................................................................. 3-1  
  Basic Features ...................................................................................................................... 3-1  
  Link Aggregation ................................................................................................................... 3-1  
  Flow Control ......................................................................................................................... 3-1  
  Broadcast Storm Control ....................................................................................................... 3-1  
  VLAN .................................................................................................................................... 3-2
6 Guide to Purchase

Purchasing the S5120SI Series

Purchasing SFP Modules
# Product Overview

## Preface

The H3C S5120SI Series Ethernet Switches (hereinafter referred to as the S5120SI series) are Layer 2 Gigabit Ethernet switches developed by Hangzhou H3C Technology Co., Ltd. They are intelligent manageable switches designed for network environments where high performance, high-density port distribution, and easy installation are required.

With 10/100/1000 Mbps Ethernet interfaces, the S5120SI series are mainly deployed at the access layer in enterprise networks requiring Gigabit to the Desktop (GTG) application and at the distribution layer in metropolitan-area networks (MANs). In the latter deployment, the S5120SI series provide GE electrical interfaces for user access or low-end switch convergence in the downlink direction. Whereas, in the uplink direction, they are aggregated to large-capacity Layer 3 switches or switches at the exchange office through their GE interfaces.

Table 1-1 lists the models in the S5120SI series:

<table>
<thead>
<tr>
<th>Model</th>
<th>Power supply unit</th>
<th>Number of service ports</th>
<th>Ports</th>
<th>Console port</th>
</tr>
</thead>
<tbody>
<tr>
<td>S5120-20P-SI</td>
<td>AC-input</td>
<td>20</td>
<td>16 × 10/100/1000Base-T autosensing Ethernet ports + 4 GE SFP interfaces</td>
<td>1</td>
</tr>
<tr>
<td>S5120-28P-SI</td>
<td>AC-input</td>
<td>28</td>
<td>24 × 10/100/1000Base-T autosensing Ethernet ports + 4 GE SFP interfaces</td>
<td>1</td>
</tr>
<tr>
<td>S5120-52P-SI</td>
<td>AC-input</td>
<td>52</td>
<td>48 × 10/100/1000Base-T autosensing Ethernet ports + 4 GE SFP interfaces</td>
<td>1</td>
</tr>
<tr>
<td>S5120-28P-PWR-SI</td>
<td>AC-input</td>
<td>28</td>
<td>24 × 10/100/1000Base-T autosensing Ethernet ports + 4 GE SFP interfaces</td>
<td>1</td>
</tr>
<tr>
<td>S5120-28P-HPWR-SI</td>
<td>AC-input DC-input</td>
<td>28</td>
<td>24 × 10/100/1000Base-T autosensing Ethernet ports + 4 GE SFP interfaces</td>
<td>1</td>
</tr>
</tbody>
</table>

The feature-rich S5210SI series support the following services:

- Broadband Internet access
- Gigabit access of small- to medium-sized enterprise networks
- Multimedia services, such as VOD
- Delay-sensitive voice services, such as VoIP
- Multicast audio and video services

The S5120SI series deliver these features:
- Full-Gigabit access ports
- Support for jumbo frames
- 802.1X
- LACP
- 4K VLANs
- 8K MAC addresses and support for blackhole MAC addresses
- Port-based automatic mapping of Layer 2 and Layer 3 priority levels
- Port mirroring
- Traffic redirecting
- Port isolation
- Access control lists (ACLs)
- Line rate
- Supplying power to PDs from Ethernet interfaces

System Features

Table 1-2 The H3C S5120SI series system specifications (1)

<table>
<thead>
<tr>
<th>Item</th>
<th>H3C S5120-20P-SI</th>
<th>H3C S5120-28P-SI</th>
<th>H3C S5120-52P-SI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical dimensions (H × W × D)</td>
<td>43.6 × 440 × 160 mm (1.72 × 17.32 × 6.30 in.)</td>
<td>43.6 × 440 × 160 mm (1.72 × 17.32 × 6.30 in.)</td>
<td>43.6 × 440 × 260 mm (1.72 × 17.32 × 10.24 in.)</td>
</tr>
<tr>
<td>Weight</td>
<td>≤ 3 kg (6.61 lb)</td>
<td>≤ 3 kg (6.61 lb)</td>
<td>≤ 5 kg (11.02 lb)</td>
</tr>
<tr>
<td>Console port</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Service ports</td>
<td>16 × 10/100/1000Base-T autosensing Ethernet ports + 4 GE SFP interfaces</td>
<td>24 × 10/100/1000Base-T autosensing Ethernet ports + 4 GE SFP interfaces</td>
<td>48 × 10/100/1000Base-T autosensing Ethernet ports + 4 GE SFP interfaces</td>
</tr>
<tr>
<td>Input voltage</td>
<td>AC:</td>
<td>Rated voltage range: 100 VAC to 240 VAC, 50 Hz or 60 Hz</td>
<td>Maximum voltage range: 90 VAC to 264 VAC, 47 Hz or 63 H</td>
</tr>
<tr>
<td>Maximum power consumption</td>
<td>25.1 W</td>
<td>31.5 W</td>
<td>59.8 W</td>
</tr>
<tr>
<td>Operating temperature</td>
<td>0°C to 45°C (32°F to 113°F)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating humidity (noncondensing)</td>
<td>10% to 90%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1-3 The H3C S5120SI series system specifications (2)

<table>
<thead>
<tr>
<th>Item</th>
<th>H3C S5120-28P-PWR-SI</th>
<th>H3C S5120-28P-HPWR-SI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical dimensions (H × W × D)</td>
<td>43.6 × 440 × 420 mm (1.72× 17.32 ×16.54 in.)</td>
<td>43.6 × 440 × 420 mm (1.72× 17.32 ×16.54 in.)</td>
</tr>
<tr>
<td>Weight</td>
<td>≤ 7 kg (15.43 lb)</td>
<td>≤ 7 kg (15.43 lb)</td>
</tr>
<tr>
<td>Console port</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
## Service Features

The software design of the S5120SI series is based on H3C's proprietary COMWARE platform. Table 1-3 summarizes the service features of the S5120SI series.

### Table 1-4 Service features of the S5120SI series

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Wire speed</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L2 switching</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switching capacity</td>
<td>40 Gbps</td>
<td>56 Gbps</td>
<td></td>
<td></td>
<td>104 Gbps</td>
</tr>
<tr>
<td>(Full duplex)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Packet forwarding rate</td>
<td>29.8 Mpps</td>
<td>41.7 Mpps</td>
<td></td>
<td></td>
<td>77.4 Mpps</td>
</tr>
<tr>
<td><strong>Link aggregation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Support dynamic aggregation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>of Gigabit Ethernet (GE) ports</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Dynamic link aggregation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>through Link Aggregation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control Protocol (LACP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Support manual link</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>aggregation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Support up to (total number</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>of ports/2) link aggregation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>groups, each supporting up</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>to eight GE ports</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Flow control</strong></td>
<td>IEEE 802.3x flow control and back pressure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jumbo Frame</td>
<td>Supports maximum frame size of 10 KB</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>--------------</td>
<td>--------------</td>
<td>------------------</td>
<td>-------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>MAC address table</td>
<td>8K MAC addresses</td>
<td>1K static MAC addresses</td>
<td>Blackhole MAC addresses</td>
<td>MAC address learning limit on a port</td>
<td></td>
</tr>
<tr>
<td>VLAN</td>
<td>Port-based VLANs (4094 VLANs)</td>
<td>Voice VLAN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ARP</td>
<td>256 entries</td>
<td>64 static entries</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN virtual interface</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP</td>
<td>DHCP Client</td>
<td>DHCP Snooping</td>
<td>DHCP Relay</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Broadcast/multicast/unicast storm control</td>
<td>Storm control based on port rate percentage</td>
<td>PPS-based storm control</td>
<td>bps-based storm control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MSTP</td>
<td>STP/RSTP/MSTP protocol</td>
<td>Support 4 spanning tree instances</td>
<td>Support STP Root Protection</td>
<td>Support BPDU Protection</td>
<td></td>
</tr>
<tr>
<td>QoS/ACL</td>
<td>Support 802.1p/DSCP precedence marking</td>
<td>Support four queues per port</td>
<td>Support SP, SDWRR, and SP+SDWRR queue scheduling algorithms</td>
<td>Support port-based line rate, with a minimum of 64-kbps granularity</td>
<td>Support flow-based traffic redirecting</td>
</tr>
<tr>
<td>Mirroring</td>
<td>Support port mirroring</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security features</td>
<td>Support hierarchical management and password protection of users</td>
<td>Support AAA authentication</td>
<td>Support RADIUS authentication</td>
<td>Support port isolation</td>
<td>Support 802.1X</td>
</tr>
<tr>
<td>802.1X</td>
<td>Up to 1024 users under a single port</td>
<td>Support port-based and MAC address–based authentication</td>
<td>Support Guest VLAN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loading and upgrade</td>
<td>Support loading and upgrade through XModem protocol</td>
<td>Support loading and upgrade through file transfer protocol (FTP)</td>
<td>Support loading and upgrade through trivial file transfer protocol (TFTP)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>--------------</td>
<td>--------------</td>
<td>------------------</td>
<td>-------------------</td>
<td>--------------</td>
</tr>
</tbody>
</table>
| **Management** | · Support configuration through CLI
· Support remote configuration through Telnet
· Support configuration through Console port
· Support Simple Network Management Protocol (SNMP)
· Support Remote Monitoring (RMON) alarm, event and history recording
· Support DM NMS
· Support Web NMS
· Support system log
· Support hierarchical alarms
· Support HW Group Management Protocol (HGMP) V2
· Support NTP
· Support power, fan, and temperature alarms | | | | |
| **Maintenance** | · Support debugging information output
· Support packet internet groper (ping) and Tracert
· Support remote maintenance through Telnet
· Support virtual cable test | | | | |


2 Hardware Description

H3C S5120-20P-SI

Front Panel

Figure 2-1 H3C S5120-20P-SI front panel

(1) 10/100/1000Base-T auto-sensing Ethernet port
(2) Port status LED
(3) Power LED (Power)
(4) Console port
(5) 1000Base-X SFP interface

Rear Panel

Figure 2-2 H3C S5120-20P-SI rear panel

(1) AC receptacle
(2) Grounding screw

Power Supply System

AC power input:
Rated voltage range: 100 VAC to 240 VAC, 50 Hz or 60 Hz
Input voltage range: 90 VAC to 264 VAC, 47 Hz or 63 Hz

Cooling System

The H3C S5120-20P-SI is equipped with one fan for heat dissipation
H3C S5120-28P-SI

Front Panel

Figure 2-3 H3C S5120-28P-SI front panel

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>10/100/1000Base-T auto-sensing Ethernet port</td>
<td>(2) Port status LED</td>
</tr>
<tr>
<td>(3)</td>
<td>Power LED (Power)</td>
<td>(4) Console port</td>
</tr>
<tr>
<td>(5)</td>
<td>1000Base-X SFP interface</td>
<td></td>
</tr>
</tbody>
</table>

Rear Panel

Figure 2-4 H3C S5120-28P-SI rear panel

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>AC receptacle</td>
</tr>
<tr>
<td>(2)</td>
<td>Grounding screw</td>
</tr>
</tbody>
</table>

Power Supply System

AC power input:
Rated voltage range: 100 VAC to 240 VAC, 50 Hz or 60 Hz
Input voltage range: 90 VAC to 264 VAC, 47 Hz or 63 Hz

Cooling System

The H3C S5120-28P-SI is equipped with one fan for heat dissipation.
H3C S5120-52P-SI

Front Panel

Figure 2-5 H3C S5120-52P-SI front panel

(1) 10/100/1000Base-T auto-sensing Ethernet port
(2) 10/100/1000Base-T auto-sensing Ethernet port status LED
(3) Console port
(4) Power LED (Power)
(5) 1000Base-X SFP interface
(6) 1000Base-X SFP interface status LED

Rear Panel

Figure 2-6 H3C S5120-52P-SI rear panel

(1) AC receptacle
(2) Grounding screw

Power Supply System

AC power input:
Rated voltage range: 100 VAC to 240 VAC, 50 Hz or 60 Hz
Input voltage range: 90 VAC to 264 VAC, 47 Hz or 63 Hz

Cooling System

The H3C S5120-52P-SI is equipped with one fan for heat dissipation.
H3C S5120-28P-PWR-SI

Front Panel

Figure 2-7 H3C S5120-28P-PWR-SI front panel

1. 10/100/1000Base-T auto-sensing Ethernet port
2. Port status LED mode switching button
3. Port status LED
4. Power LED (Power)
5. Port mode LED
6. Console port Port
7. 1000Base-X SFP interface

Rear Panel

Figure 2-8 H3C S5120-28P-PWR-SI rear panel

1. AC receptacle
2. Grounding screw

Power Supply System

AC power input:
Rated voltage range: 100 VAC to 240 VAC, 50 Hz or 60 Hz
Input voltage range: 90 VAC to 264 VAC, 47 Hz or 63 Hz

Cooling System

The H3C S5120-28P-PWR-SI is equipped with three fans for heat dissipation.
H3C S5120-28P-HPWR-SI

Front Panel

**Figure 2-9** H3C S5120-28P-HPWR-SI front panel

<table>
<thead>
<tr>
<th>(1)</th>
<th>(2)</th>
<th>(3)</th>
<th>(4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/100/1000Base-T auto-sensing Ethernet port</td>
<td>Port status LED mode switching button</td>
<td>RPS status LED (RPS)</td>
<td>Port status LED</td>
</tr>
<tr>
<td>(5)</td>
<td>(6)</td>
<td>(7)</td>
<td>(8)</td>
</tr>
<tr>
<td>Power LED (Power)</td>
<td>Port mode LED</td>
<td>Console port</td>
<td>Port 1000Base-X SFP interface</td>
</tr>
</tbody>
</table>

Rear Panel

**Figure 2-10** H3C S5120-28P-HPWR-SI rear panel

<table>
<thead>
<tr>
<th>(1)</th>
<th>(2)</th>
<th>(3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Screw hole of the plug</td>
<td>AC receptacle</td>
<td>Grounding screw</td>
</tr>
<tr>
<td>(4)</td>
<td>(5)</td>
<td></td>
</tr>
<tr>
<td>DC power receptacle</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Power Supply System

H3C S5120-28P-HPWR-SI can adopt AC power input, or DC power input, or both to provide backup

- **AC power input:**
  - Rated voltage range: 100 VAC to 240 VAC, 50 Hz or 60 Hz
  - Input voltage range: 90 VAC to 264 VAC, 47 Hz or 63 Hz

- **DC power input**
  - Rated voltage range: –52 VDC to –55 VDC

---

**Caution**

Only the RPS recommended by H3C can be used for the H3C S5120-28P-HPWR-SI. The –48 VDC power supply in the equipment room cannot be used directly. Otherwise, the device may be damaged.
Cooling System

The H3C S5120-28P-HPWR-SI is equipped with six fans for heat dissipation.

LEDs

On the front panel of an S5120SI series switch, there is the Power LED, status LEDs of the 10/100/1000Base-T autosensing Ethernet ports, and status LEDs of the 1000Base-X SFP interfaces.

Power LED

The power LED indicates the operation status of the switch.

<table>
<thead>
<tr>
<th>LED</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>Solid green</td>
<td>The switch functions normally.</td>
</tr>
<tr>
<td></td>
<td>Blinking green (1 Hz)</td>
<td>The system is performing power-on self test (POST) or downloading software.</td>
</tr>
<tr>
<td></td>
<td>Blinking green (3 Hz)</td>
<td>The POST has failed or another fatal error has been detected.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>The switch has been powered off.</td>
</tr>
</tbody>
</table>

RPS Status LED

The S5120-28P-HPWR-SI provides an RPS status LED on its front panel, indicating the working status of the RPS of the switch.

<table>
<thead>
<tr>
<th>LED</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPS</td>
<td>Solid green</td>
<td>The RPS DC input is normal.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>The RPS unit is not connected or the RPS DC input is abnormal.</td>
</tr>
</tbody>
</table>

Port Mode LED

The port mode LED on the S5120-28P-PWR-SI/S5120-28P-HPWR-SI can display the working status of a port for you to obtain more device information. You can use the port mode switching button to change the status of the port mode LED.

<table>
<thead>
<tr>
<th>LED</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Solid green</td>
<td>Indicates port rate.</td>
</tr>
<tr>
<td></td>
<td>Blinking green (1 Hz)</td>
<td>Indicates port PoE power supply.</td>
</tr>
</tbody>
</table>
### 10/100/1000Base-T auto-sensing Ethernet port status LEDs

#### Table 2-4 10/100/1000Base-T auto-sensing Ethernet port LEDs description

<table>
<thead>
<tr>
<th>Switch model</th>
<th>Port mode LED</th>
<th>Ethernet port status LED</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>S5120-20P-SI</td>
<td>—</td>
<td>Green On</td>
<td>The port operates at a rate of 1000 Mbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fast blinking</td>
<td>Data is being transmitted or received at 1000 Mbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off</td>
<td>The port is not up or does not operate at 1000 Mbps</td>
</tr>
<tr>
<td>S5120-28P-SI</td>
<td>—</td>
<td>Yellow On</td>
<td>The port operates at a rate of 10/100 Mbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fast blinking</td>
<td>Data is being transmitted or received at 10/100 Mbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Blinking (3 Hz)</td>
<td>The POST has failed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off</td>
<td>The port is not up or does not operate at 10/100 Mbps</td>
</tr>
<tr>
<td>S5120-52P-SI</td>
<td>—</td>
<td>Solid green (rate mode)</td>
<td>The port operates at a rate of 1000 Mbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fast blinking green</td>
<td>Data is transmitted or received at a rate of 1000 Mbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Solid yellow</td>
<td>The port operates at a rate of 10/100 Mbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fast blinking yellow</td>
<td>Data is transmitted or received at a rate of 10/100 Mbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off</td>
<td>The port is not up or the POST has failed</td>
</tr>
<tr>
<td>S5120-28P-PWR-SI</td>
<td>Solid green (rate mode)</td>
<td>On</td>
<td>The port operates at a rate of 1000 Mbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fast blinking</td>
<td>Data is transmitted or received at a rate of 1000 Mbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off</td>
<td>The port is not up or does not operate at 1000 Mbps</td>
</tr>
<tr>
<td>S5120-28P-HPWR-SI</td>
<td>Solid green (rate mode)</td>
<td>On</td>
<td>The port operates at a rate of 10/100 Mbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fast blinking</td>
<td>Data is transmitted or received at a rate of 10/100 Mbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Blinking (3 Hz)</td>
<td>The POST has failed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off</td>
<td>The port is not up or does not operate at 10/100 Mbps</td>
</tr>
<tr>
<td></td>
<td>Blinking Green</td>
<td>On</td>
<td>PoE power supply is normal.</td>
</tr>
</tbody>
</table>
### 1000Base-X SFP interface status LEDs

#### Table 2-5 1000Base-X SFP interface status LEDs description

<table>
<thead>
<tr>
<th>LED</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solid green</td>
<td>The port operates at a rate of 1000 Mbps</td>
</tr>
<tr>
<td></td>
<td>The port is transmitting data at 1000 Mbps</td>
</tr>
<tr>
<td>Blinking green</td>
<td>The LED is fast blinking when data is being received on the port.</td>
</tr>
<tr>
<td>Off</td>
<td>No link is present on the port</td>
</tr>
</tbody>
</table>
Software Features

Basic Features

Link Aggregation

The link aggregation function is used for the connection between Ethernet switches or between the switches and high-speed servers. It is a simple and cheap way to expand the bandwidth of a switch port and balance the traffic among all the ports in a link aggregation. Moreover, it enhances the connection reliability.

With link aggregation, several Ethernet ports on a switch are bundled together and are considered one logical port inside the switch. The switch automatically balances the traffic among the ports in the aggregation and increases the bandwidth of the ports. If the link on a port in the aggregation fails, the traffic on it is distributed among other ports without interrupting the normal service. After the port recovers, the traffic is automatically distributed again so that the port can share the load with others.

The S5120SI series support manual link aggregation and dynamic link aggregation through Link Aggregation Control Protocol (LACP).

Flow Control

Flow control is a congestion management method on a switch. With flow control enabled on the two ports of a link, the receiving port notifies the sending port to stop packet sending for a certain period when congestion occurs. As incoming traffic is reduced, packet loss is avoided.

Ethernet ports of the S5120SI series support full-duplex flow control (IEEE 802.3x-compliant) and half-duplex back pressure. With full-duplex flow control, a port notifies the peer end to stop sending packets by sending pause frames. Comparatively, with half-duplex back pressure, a port notifies the peer end to stop packet sending by sending Jam signals.

Broadcast Storm Control

The broadcast storm control function suppresses the propagation of unknown unicast packets, multicast packets, and broadcast packets in a network, thus limiting their impact on the operating efficiency of the network.

For the S5120SI series, the broadcast storm control function is configured on ports. After storm control is enabled on a port, you can monitor the unknown unicast traffic, multicast traffic, and the broadcast traffic received on it. When the traffic exceeds the specified bandwidth limit, the switch drops the excessive traffic to reduce the traffic ratio to a rational range, so as to guarantee the normal operation of network services.

The S5120SI series allows you to set a limit on broadcast/multicast/unknown unicast traffic on a port as a percentage of total port bandwidth or a traffic rate in pps or in bps. Of them, the bps-level control delivers more accurate bandwidth control.
**VLAN**

Virtual local area network (VLAN) is a technology that implements virtual workgroups by assigning the devices in a LAN into network segments logically rather than physically. VLAN standard is described in IEEE 802.1Q protocol standard, which is issued in 1999.

You can use VLAN to divide a LAN into multiple broadcast domains known as virtual LANs, namely, VLANs, the computers in each of which are correlated in a certain way. As VLANs are implemented logically rather than physically, the computers in the same VLAN do not necessarily reside on the same physical LAN segment; instead, they can belong to different physical LAN network segments.

On a switch, the port-based VLAN are supported.

VLAN offers the benefit that the broadcast and unicast traffic inside a VLAN are not forwarded to other VLANs, thereby helping implement network traffic control, save equipment investment, streamline network management, and enhance network security.

The H3C S5120SI series support the following types of VLAN.

**Port-based VLAN**

In a port-based VLAN, VLAN members are defined based on the Ethernet switch ports. You can add specific ports to the same VLAN, through which the hosts connecting to these can communicate with each other. This is the simplest way of creating a VLAN. An S5120SI Ethernet switch supports up to 4,094 port-based VLANs.

**VLAN Trunk**

The VLAN trunk function is used for the connections between switches. A VLAN trunk is a point-to-point link between two switches. The ports of the two switches across a VLAN trunk are called trunk ports. Multiple VLANs can be carried over the same trunk port.

The implementation principle is as follows: On a trunk port, messages of different VLANs are differentiated through different 802.1Q tags. In this way, interconnections among all VLANs are enabled networkwide.

**Management VLAN**

The management VLAN feature can isolate management packets from common data packets to reduce security risks and enhance management reliability. The management VLAN is configurable and usually specified in the network planning phase. The default management VLAN is VLAN 1.

Cluster management requires that a cluster must be established in the management VLAN. For a Layer 2 switch, the only VLAN interface must also be created on the management VLAN.

Therefore, the management VLAN must be set before establishing a cluster or creating a VLAN interface.

For a cluster, you only need to configure the management VLAN on the command switch. The configuration will be synchronized to all discovered switches after the cluster is established.
Network Protocol Features

ARP

Address resolution protocol (ARP) dynamically maps IP addresses to specific MAC addresses. Upon being enabled, ARP carries out the address resolution without manual intervention.

The S5120SI series switches support the following extended ARP and attack defense implementations:

Gratuitous ARP

Gratuitous ARP enables a device to test whether or not IP address conflicts exist between itself and other devices in the network by sending ARP requests. Since both the source and destination IP addresses of a gratuitous ARP request packet are set to the local IP address, an IP address conflict exists if a host responds to the ARP request.

A gratuitous ARP request is also used to update the corresponding MAC address entries maintained by other devices. A switch updates the corresponding MAC address entry if the IP address contained in a received ARP request packet matches the MAC address entry. As an ARP request packet is broadcast across the network, all the MAC address entries matching the ARP request packet are updated.

ARP Attack Defense

ARP attacks and viruses are threatening LAN security. H3C S5120SI Series Ethernet Switches can provide ARP attack defense to prevent such attacks.

In normal cases, a Layer 2 access device broadcasts an ARP request within a VLAN, and forwards ARP responses at Layer 2. If an attacker sends an ARP request with the source being the IP address of another client, the corresponding ARP entry maintained by the gateway or other clients is modified. Consequently, the attacker will receive the packets sent to the client.

The ARP detection feature allows only the ARP packets of legal clients to be forwarded.

ARP Detection consists of two functions: user validity check and ARP packet validity check.

- User validity check: With this feature enabled, the device compares the source IP and MAC addresses of an ARP packet received from the VLAN against the DHCP snooping entries, 802.1X security entries, or static IP-to-MAC binding entries.
- ARP packet validity check: With this feature enabled, the device filters out invalid ARP packets received on ARP untrusted ports. You can base ARP packet validity check on the source MAC address, destination MAC address or IP address. ARP packet validity check does not apply to packets received on ARP trusted ports.

DHCP

DHCP Relay

A routing switch operating as a DHCP relay can relay messages between a DHCP server and a client, making it possible for a DHCP server in a subnet to provide DHCP service to the hosts in another subnet. With DHCP Relay, a network manager needs not to set DHCP server for every subnet, thereby reducing DHCP server costs.

DHCP Client

On a contemporary large-sized and complex network, some computers are mobile and the available IP addresses are far from adequate comparing with the fast-growing number of computers. To address the
issue, the dynamic host configuration protocol (DHCP) was introduced. DHCP works in the client/server model, where the DHCP client requests the DHCP server for configuration information dynamically, and upon the receipt of the request the DHCP server returns the configuration information (IP address for example) based on the adopted policy.

**DHCP Snooping**

The DHCP snooping function enables the acquisition of user IP addresses and MAC addresses by listening to DHCP broadcast packets. It can be used to improve network security and prevent unauthorized accesses. Additionally, with the DHCP snooping function employed, ports are classified into trusted ports and untrusted ports. Ports with DHCP servers attached are trusted ports; and those with hosts attached are untrusted ports. The DHCP_ACK and DHCP_OFF packets received through untrusted are discarded, through which illegal DHCP servers can be prevented.

**NTP**

Clock synchronization among devices becomes important given increasingly complex network topologies. The network time protocol (NTP) is a TCP/IP protocol that advertises accurate time on the entire network.

NTP provides consistency guarantee for the following applications:

- When increment backup is performed between a backup server and a client, it ensures the clock between the two systems be synchronous.
- When multiple systems are used to deal with complex events, it ensures the correct order of these events.
- It ensures the normal performance of the Remote Procedure Call (RPC) between systems.
- It provides time information about such operations as system login of users and file modification for application programs.

**Multicast Features**

**IGMP Snooping**

Internet group management protocol snooping (IGMP Snooping) operates on Layer 2 Ethernet switches. It provides a mechanism to manage and control multicast groups.

IGMP snooping runs on the link layer. It checks the information carried in the IGMP packets exchanged between hosts and routers. On the detection of an IGMP host report message, the switch adds the host to the corresponding multicast table. And on the detection of an IGMP Leave message, the switch removes the corresponding multicast entry from the multicast table. By continuously listening to IGMP packets, a switch creates and maintains a Layer 2 MAC multicast address table, through which the switch forwards the multicast packets transmitted by the routers.

When IGMP Snooping is not enabled, multicast packets are broadcast on Layer 2. While when IGMP Snooping is enabled, the packets are multicast instead of being broadcast on Layer 2.
Figure 3-1 IGMP Snooping

<table>
<thead>
<tr>
<th>Multicast packet transmission without IGMP Snooping</th>
<th>Multicast packet transmission when IGMP Snooping runs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host A Receiver</td>
<td>Host A Receiver</td>
</tr>
<tr>
<td>Host C Receiver</td>
<td>Host C Receiver</td>
</tr>
</tbody>
</table>

**STP/RSTP/MSTP**

**STP/RSTP**

Spanning tree protocol (STP)/rapid spanning tree protocol (RSTP) prunes a loop L2 switching network into a loop-free tree (all data on the L2 switching network must travel along the spanning tree), thereby avoiding network broadcast storms caused by network loops and providing redundant links for data forwarding.

Basically, STP/RSTP is used to generate a "tree" whose root is a switch called root bridge. Which switch is to be selected as root bridge is based on their settings (such as switch priority and MAC address), but there should be only one root bridge at any time. From the root bridge, a tree stretches through the switches. A non-root switch forwards data to the root through its root port and to the connected network segment through its designated port. A root periodically transmits configuration BPDUs, while a non-root switch receives and forwards them. If a switch receives configuration BPDUs from two or more ports, it assumes that there is a loop in the network. To eliminate the loop, the switch selects one of the ports as the root port and blocks others. When a port receives no configuration BPDUs for a long time, the switch considers that the configuration of this port has timed out and the network topology may have changed. Then, it recalculates the network topology and generates a new tree.

RSTP is an STP enhancement that significantly shortens the time for the network topology to stabilize.

**MSTP**

Multiple spanning tree protocol (MSTP) is compatible with STP and RSTP. STP cannot transit fast. Even on the point-to-point link or the edge port, it has to take an interval twice as long as forward delay before the network converges.

RSTP can converge fast. However, like STP, RSTP has this drawback: All the network bridges in a VLAN share a spanning tree and the redundant links cannot be blocked by VLAN, with all the packets in the VLAN forwarded along a spanning tree.
MSTP makes up for the drawback of STP and RSTP. It makes the network converge fast and enables the traffic of different VLANs to be distributed along their respective paths, which provides a better load sharing mechanism for the redundant links.

MSTP associates VLAN with spanning tree by using a VLAN mapping table; that is, a table showing the correspondence relationship between VLANs and spanning tree. Meanwhile, MSTP divides a switched network into several domains. In each domain, multiple independent STPs are generated. MSTP prunes a loop network to a loop-free network so as to avoid packet propagation and endless loop. It also provides multiple redundant paths for load balancing of VLAN data in the process of data forwarding.

**STP Protection**

**BPDU guard**

For access layer devices, the access ports are usually connected directly with the user terminals (such as PCs) or file servers. In this case, the access ports are configured as edge ports to allow fast migration of these ports. When these ports receive configuration messages (BPDUs), the system will automatically set these ports as non-edge ports and recalculate the spanning tree. This will cause flapping of the network topology. Under normal conditions, these ports should not receive STP BPDUs. If someone forges BPDUs maliciously to attack the switch, network flapping will occur. The BPDU guard function protects the system against such attacks.

**Root guard**

The root bridge and backup switches in a spanning tree must reside in the same domain. This is especially true for the root bridge and backup switches of a common and internal spanning tree (CIST). This is because the root bridge and backup switches of a CIST are normally placed in a high-bandwidth core domain. However, due to misconfiguration or a malicious network attack, a legal root bridge in the network may receive a BPDU that has a higher priority. This turns the current root bridge into a non-root switch, causing a wrong change in the network topology. Such illegal change leads the traffic that would otherwise pass through a high-speed link to follow a lower-speed link, causing network congestion. The root guard function prevents this from occurring.

**Loop guard**

A switch can keep track of the states of the root port and blocked ports by continuously receiving the BPDUs sent by upstream switches. However, these ports may be unable to receive the BPDUs sent by upstream switches due to link congestion or unidirectional links. In this case, the switch reelects a root port, the original root port turns into a designated port, and blocked ports go into the forwarding state. This causes loops in the switched network. The loop guard function prevents such loops. With the loop guard function enabled, the role of the root port remains unchanged and blocked ports remains in the Discarding state without forwarding any packet. This prevents loops in the network.

**TC-BPDU attack prevention**

Upon receiving a TC-BPDU, the switch deletes MAC address entries and ARP entries. If someone forges TC-BPDUs to attack the switch maliciously, the switch will receive excessive TC-BPDUs in a short time. Frequent packet deletion places a heavy burden on the switch and compromises network stability.

After TC-BPDU attack prevention is enabled, the switch deletes the received TC-BPDUs only once within a specific timer (usually 10 seconds) and monitors whether any TC-BPDU is received during that
timer. If any TC-BPDUs are received within the timer, the switch deletes the TC-BPDUs again after the timer times out. This saves the switch from deleting MAC address entries and ARP entries frequently.

**QACL**

Quality of service (QoS) provides network services of different types and grades selected by users, from the top service quality to normal service quality networkwide to accommodate to various demands. An access control list (ACL) is used primarily to identify traffic flows. In order to filter data packets, a series of match rules must be configured on the network device to identify the packets to be filtered. After the specific packets are identified, and based on the predefined policy, the network device can permit/prohibit the corresponding packets to pass.

**Traffic Classification**

Traffic classification is to classify packets according to the packet filtering keywords configured by the user. Various types of user-defined service processing can be implemented on the classified packets.

In traffic classification, rules are defined to discriminate packets that conform to certain characteristics. The classification rules can be very simple. For example, traffic flows with different priority characteristics can be discriminated according to the differentiated services codepoint (DSCP) in the packet header. They can also be quite complicated. For example, packets can be classified according to combinations of information involving the data link layer, network layer and transport layer -- such as MAC address, IP protocol type, source host/network segment address, destination host/network segment address, and even application port number.

**Priority Mapping Tables**

On a switch, every packet to be forwarded is assigned a set of service parameters that define its QoS guarantee. The service parameters provided by the S5120SI series include DSCP precedence, 802.1p priority, and local precedence.

The S5120 series support two priority mapping tables: DSCP to service parameters and 802.1p to service parameters.

**DSCP to service parameters mapping table**

This mapping table is used by the switch to assign service parameters according to the DSCP precedence of packets. The switch maps a DSCP precedence value to an 802.1p priority value, a DSCP precedence value, and a local precedence value.

**802.1p to service parameters mapping table**

This mapping table is used by the switch to assign service parameters according to the 802.1p priority of packets. The switch maps an 802.1p priority value to a new 802.1p priority value, a DSCP precedence value, and a local precedence value.

**Priority Trust Mode**

An S5210 switch assigns a set of service parameters to an incoming packet by:

- Mapping its DSCP precedence to a set of service parameters
- Mapping its 802.1p priority to a set of service parameters
- Adopting the default service parameters of the port
You can choose to use, that is, trust the priority of the port or a type of priority carried in the packet for mapping.

**Trusting port priority**

In this mode, the switch uses the 802.1p priority of the receiving port rather than the one carried in the incoming packet to look up the 802.1p to service parameters mapping table for target service parameter settings for the packet. In addition, the switch modifies the original 802.1p priority of the packet to the target one.

The 802.1p priority of the port is configurable at the command line.

**Trusting the 802.1p priority of packets**

In this mode, the switch uses the 802.1p priority (if any) of the incoming packet to look up the 802.1p to service parameters mapping table for target service parameters, and replaces the original 802.1p priority and DSCP precedence values of the packet with the target ones at the outgoing port.

For packets without 802.1p precedence, the port priority is trusted.

**Trusting the DSCP precedence of packets**

In this mode, the switch uses the DSCP precedence (if any) of the incoming packet to look up the DSCP to service parameters mapping table for target service parameters, and replaces the original 802.1p priority and DSCP precedence values of the packet with the target ones at the outgoing port.

For non-IP packets, the port priority is trusted.

**Line Rate**

The line rate features limits traffic rate per port. It limits the total rate of incoming and outgoing packets of a port.

The S5120SI series support configuring line rate for incoming packets and outgoing packets respectively on a port.

**Traffic Redirection**

Based on traffic classification, the S5120SI series can redirect the identified packets. The traffic redirection function enables you to re-specify the output port of packet forwarding and bypass the Bridge mechanism, with the destination port determined by the traffic redirection function.

**Port Mirroring**

Port mirroring is used for monitoring packets on a specific port.

This function copies the data packets on the specified port to the monitoring port to facilitate network tests and troubleshooting.

The S5120SI series support inbound and outbound port mirroring.

**Queue Scheduling**

Queue scheduling applies to the situation where multiple forwarded packets compete for the resources. The S5120SI series support four queue scheduling algorithms: strict priority (SP), weighted round robin (WRR) and SP+WRR. The following sections describe these algorithms briefly:
SP queue-scheduling algorithm

Figure 3-2 Diagram for SP queuing

SP queue-scheduling algorithm is specially designed for critical service applications. An important feature of critical services is that they demand preferential service in congestion in order to reduce the response delay. A port provides four queues, that is, queue 3, queue 2, queue 1, and queue 0, in the descending priority order.

In queue scheduling, SP sends packets in the queue with higher priority strictly following the priority order from high to low. When the queue with higher priority is empty, packets in the queue with lower priority are sent. You can put critical service packets into the queues with higher priority and put non-critical service (such as e-mail) packets into the queues with lower priority. In this case, critical service packets are sent preferentially and non-critical service packets are sent when critical service groups are not sent.

The disadvantage of SP queue is that: if there are packets in the queues with higher priority for a long time in congestion, the packets in the queues with lower priority will be “starved” because they are not served.

SDWRR queue scheduling algorithm

SDWRR queue scheduling is an enhanced WRR queue scheduling algorithm. Compared with WRR, SDWRR further reduces scheduling delay and smoothes jitter for lower priority queues while guaranteeing minimum bandwidth for each queue. Suppose the weights of queue 1 and queue 0 are configured as 5 and 3 respectively. According to WRR and SDWRR scheduling, the queue scheduling sequences are as follows:

<table>
<thead>
<tr>
<th>Queue scheduling algorithm</th>
<th>Queue scheduling sequence</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>WRR</td>
<td>0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1</td>
<td>0 represents the packets identical to one weight in queue 0.</td>
</tr>
<tr>
<td>SDWRR</td>
<td>0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0</td>
<td>1 represents the packets identical to one weight in queue 1.</td>
</tr>
</tbody>
</table>

As the scheduling sequences show, WRR dequeues the number of packets identical to weight 3 from queue 1 only after the number of packets identical to weight 5 are dequeued from queue 0. If there is a
wide difference between the weight values of two queues, great delay and jitter will result for the lower-weight queue.

SDWRR addresses the problem by scheduling the two queues in turn in such a way that packets identical to one weight are dequeued from queue 0 first and then from queue 1. The procedure is repeated until the scheduling for one queue is over. Then, SDWRR schedules the queue with remaining weights to dequeue the number of packets identical to the remaining weights.

An S5120SI switch supports two SDWRR scheduling groups. You can assign queues to either of these two SDWRR groups. The inter-group scheduling algorithm is SP.

**SP+SDWRR queue scheduling algorithm**

The S5120SI series support SP+SDWRR mixed queue scheduling, with which SP scheduling is used between SP scheduling queues and the two SDWRR scheduling groups. The priority of an SDWRR scheduling group is determined by the lowest-priority queue in the group. You can configure an SP+SDWRR mixed queue scheduling scheme properly to guarantee critical services the minimum delay with SP and fair sharing of remaining bandwidth for other services with SDWRR.

**Centralized Management Features**

**HGMP**

Through cluster management, the network administrator can configure and troubleshoot multiple switches through a single public network IP address of a primary switch. In each cluster, there is a master switch called a command switch. The rest of the switches serve as member switches. A member switch is typically not configured with an IP address. The command switch and member switches form a cluster. In a cluster the switches have different roles based on different roles and functions. You can specify switch roles. The roles can be switched based on certain rules.

Switch roles in a cluster include command switch, member switch, and candidate switch.

1) Command switch: the switch configured with a public network IP address. A management command is sent to the command switch and the command switch processes this command. If the destination is a member switch, the management command will be forwarded to the command switch.

2) Member switch: a member in a cluster. The member switch is managed through the proxy of the command switch. Typically no public network IP address is set for the member switch.

3) Candidate switch: Candidate switches are cluster-capable devices that have not yet been added to a cluster.

**Security Features**

The popularity of network applications, especially in some sensitive occasions (e-commerce for example), highlights the issue of network security.

The S5120SI series have been designed based on full consideration of customers’ demands, so as to provide full-range network solutions.

With respect to terminal access control and user access control, the S5120SI series provide the following network security features:

- Hierarchical user management and password protection
- MAC address black hole
- MAC address learning limit
- Binding of MAC addresses to ports
- Supports SSH 2.0
- IEEE 802.1X compliant access user authentication
- Supports local and RADIUS authentication modes
- Supports port isolation

With respect to filtering and authenticating Ethernet frames and packets from the upper layers, the S5120SI series support:

- ACL, with which information is filtered at layers 2 through 4 (such as based on port, by source/destination MAC address, by source/destination IP address, or by the type of upper layer protocol).
- Encrypted authentication of SNMPv3

**Terminal Access User Classification**

The S5120SI series protect command lines in a hierarchical way by dividing the command lines into four levels: visitor, monitor, operator, and administrator. Commensurate with the command division, login users are classified into four levels. A login user can use only the commands equal to or lower than its level.

**SSH**

When users log in to the Ethernet switch from an insecure network, Secure Shell (SSH) offers security information protection and powerful authentication function to safeguard the Ethernet switch from attacks, such as IP address spoofing and plain text cipher interception. An Ethernet switch can accept multiple SSH customer connections at the same time. The SSH client allows users to connect to the Ethernet switches and UNIX mainframes that support SSH servers.

The S5120SI series Ethernet switches support SSH2.0.

**Port Isolation**

Port isolation means isolating ports of the same switch so that Layer 2 and Layer 3 packet forwarding cannot be implemented between these ports. This prevents visiting between the ports, effectively controls unnecessary broadcasting and increases the network throughput.

**IEEE 802.1X Authentication**

IEEE 802.1X is virtually a port-based network access control protocol. As "port-based network access control" implies, the NAS on a LAN authenticates and controls the connected customer premises equipment (CPE) at the port level. If the CPE connected to a port passes authentication, it is allowed to access the LAN resources. Otherwise, it is rejected just like its physical link is disconnected.

In implementing 802.1X, the Ethernet switches not only support the port-based access authentication, but also extends and optimizes it by:

- Allowing a physical port to be connected to several terminals.
- Supporting access control (that is user authentication) based on MAC address in addition to port.

This greatly enhances the security, operability and manageability of the system.

Note that, although 802.1X provides an implementation scheme for user authentication, the protocol itself is not enough to implement the scheme. The NAS administrators, however, can use RADIUS or local authentication to complete the user authentication with 802.1X.
MAC Address Learning Limit

MAC address learning limit: limits the number of MAC addresses learned by an Ethernet switch port. The number ranges from 0 to 8k. Static MAC addresses added on the port are not affected.

MAC Address Black Hole

On an S5120SI series switch, you can enable the black hole function and configure a black hole list. When the switch receives a packet with a source or destination MAC address in the black hole, it drops the packet.

AAA, RADIUS

The S5120SI series support user authentication locally or with RADIUS servers.

AAA

AAA is the abbreviation of Authentication, Authorization and Accounting. It provides a uniform framework to configure the security functions including authentication, authorization, and accounting. Actually, it offers a way to control the network security, which can be implemented with RADIUS.

AAA performs the following services:

- Authentication: Authenticates if the user can access the network sever.
- Authorization: Authorizes the user with specified services.
- Accounting: Tracks the network resources consumed by users.

RADIUS

RADIUS is a distributed system in the client/server model. It can fend off invalid users and is often used in a network environment where both high security and remote user access are desired. For example, it can be used to manage the access based on 802.1X.

RADIUS is based on the client/server model where user authentication always involves a device that can provide the proxy function, such as NAS. Between the RADIUS client and server, the exchanged messages are authenticated using a shared key and user passwords are sent encrypted over the network. The security is thus ensured.
Simple and Flexible Maintenance System

System Configuration

The S5120SI series can be configured through the command line interface (CLI), NMS, or Web.

- In the CLI approach, you can configure the S5120SI series locally through the console port, or configure it remotely through modem dialup or Telnet. As for Telnet, both Telnet server and Telnet client are supported.
- In the NMS approach, you can configure the S5120SI series through an SNMP-based NMS.
- In the Web approach, you can configure the models in the S5120SI series that support the Web-based network management.

System Maintenance

The S5120SI series provide diverse management and maintenance functions:

- LEDs are available on the switches and optional modules, indicating the board running status.
- Remote maintenance through Telnet
- Hierarchical management of user authorities and operation logs, as well as online help function
- Hierarchical alarm management and alarm filtering
- System status query, version query, debugging and tracing functions, to monitor system running status

System Test and Diagnosis

The S5120SI series provide means for system software and hardware fault detection and diagnosis. The tools such as ping and tracert are available for you to test network connectivity and trace packet transmission paths on line and hence address faults.

Software Upgrade

The S5120SI series provide multiple approaches to software upgrade, and support remote upgrade and rollback to the previous version after upgrade.

The S5120SI series support software upgrade methods:

- Software upgrade through a serial port by using the XModem protocol.
- Software upgrade through an Ethernet port through TFTP or FTP.
- Software upgrade through the Web-based NMS through HTTP.

H3C Device Management System

The S5120SI series support H3C Device Manager for centralized management. The H3C Device Manager uses multilingual graphic interfaces and is easy to operate. The H3C Device Manager
provides topology management, configuration management, fault management, security management, and performance management.

**Topology Management**

The H3C Device Manager helps you learn your network in the most direct and convenient way by providing a network-wide device topology view. The H3C Device Manager delivers powerful topology management. It provides physical topology view, logical topology view, and customized views, offering a unified network-wide equipment view. It also provides user-friendly interfaces for network/equipment operation and maintenance. The H3C Device Manager supports automatic topology discovery, reflecting the real-time changes in network topology and equipment status.

**Configuration Management**

With the H3C Device Manager, you can configure and manage the S5120SI series Ethernet switches, such as querying/enabling/disabling ports, querying/resetting/loading boards, and querying port parameters/VLAN configurations.

**Fault Management**

Fault management is the most important and common management approach during the network operation and maintenance. In the graphic interfaces, you can implement equipment running/fault status query, real-time monitoring, fault filtering/locating/check/analysis. The system provides audio prompt and graphical displays on the alarm card. Additionally, it can be connected to the alarm box and therefore facilitates routine maintenance.

**Performance Management**

The H3C Device Manager can collect and analyze performance data, monitor performance, and provide graphical performance reports in different forms. You can thus learn the information on equipment load and access traffic, track network service quality, and allocate network resources based on your network evaluation.

**Security Management**

The H3C Device Manager provides many security measures to strictly authenticate the user’s operations and ensure the system security. It offers detailed operation log for later query and analysis.

**Web-Based Network Management**

Web-based network management allows you to manage and maintain a switch through Web. In the implementation of Web-based network management, the switch provides a built-in Web server and runs a Web-based network management program on the homepage at the IP address of the management VLAN. The PC users connected to the Ethernet ports on the switch can access and use, through a browser, the program on the homepage to manage the switch. Figure 4-1 shows the Web-based network operating environment:
Figure 4-1 Web-based network management operating environment
The S5120SI series are GigabitEthernet switches. They are designed as distribution and access devices for small- and medium-sized enterprise networks. An S5120SI switch provides 16, 24, or 48 autosensing downstream GE interfaces, and thus can be used in networking flexibly. For example, the S5120SI series can be used for Gigabit to the Desktop (GTTD) access in enterprise networks and connecting data center server clusters. Several typical networking applications are presented in this section.

**Distribution Layer Switches**

In medium- and large-sized enterprises or campus networks, the S5120SI series Ethernet switches can serve as distribution layer switches that provide high-performance and large-capacity switching service.

**Figure 5-1** Application of the S5120SI series at the distribution layer of enterprise networks/campus networks
Access Switches

The S5120SI series can serve as access switches to provide large access bandwidth and high port density.

**Figure 5-2** Application of the S5120SI series at the access layer
Guide to Purchase

To meet varied customer needs, the S5120SI series can be delivered to your order. You can purchase the S5120SI series and optional interface modules as needed.

Purchasing the S5120SI Series

When you order the S5120SI series, take the following points into account.

Network requirements

- Location and function of the switch in your network
- Desired processing and access capabilities in both directions
- Desired scalability (in case of network capacity expansion)
- Transmission distance of the switch in the network

Table 6-1 List of the S5120SI series and corresponding power supply systems

<table>
<thead>
<tr>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>S5120-20P-SI (AC power supply, input voltage 100VAC to 240 VAC, 50/60 Hz)</td>
<td></td>
</tr>
<tr>
<td>S5120-28P-SI (AC power supply, input voltage 100VAC to 240 VAC, 50/60 Hz)</td>
<td></td>
</tr>
<tr>
<td>S5120-52P-SI (AC power supply, input voltage 100VAC to 240 VAC, 50/60 Hz)</td>
<td></td>
</tr>
<tr>
<td>S5120-28P-PWR-SI (AC power supply, input voltage 100VAC to 240 VAC, 50/60 Hz)</td>
<td></td>
</tr>
<tr>
<td>S5120-28P-HPWR-SI (AC/DC power supply, input voltage 100VAC to 240 VAC, 50/60 Hz)</td>
<td>input voltage –52 VDC to –55 VDC</td>
</tr>
</tbody>
</table>

Purchasing SFP Modules

Table 6-2 List of SFP modules

<table>
<thead>
<tr>
<th>Transceiver type</th>
<th>Transceiver</th>
<th>Central wavelength</th>
<th>Connector</th>
<th>Fiber</th>
<th>Max transmission distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>GE SFP transceiver</td>
<td>SFP-GE-SX-MM850-A</td>
<td>850 nm</td>
<td>LC</td>
<td>50/125 μm multimode optical fiber</td>
<td>550 m (0.34 miles)</td>
</tr>
<tr>
<td></td>
<td>SFP-GE-LX-SM1310-A</td>
<td>1310 nm</td>
<td>LC</td>
<td>62.5/125 μm multimode optical fiber</td>
<td>275 m (0.17 miles)</td>
</tr>
<tr>
<td></td>
<td>SFP-GE-LH40-SM1310</td>
<td>1310 nm</td>
<td>LC</td>
<td>9/125 μm single mode optical fiber</td>
<td>40 km (24.86 miles)</td>
</tr>
<tr>
<td></td>
<td>SFP-GE-LH40-SM1550</td>
<td>1550 nm</td>
<td>LC</td>
<td></td>
<td>40 km (24.86 miles)</td>
</tr>
<tr>
<td>Transceiver type</td>
<td>Transceiver</td>
<td>Central wavelength</td>
<td>Connector</td>
<td>Fiber</td>
<td>Max transmission distance</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------</td>
<td>--------------------</td>
<td>-----------</td>
<td>--------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td></td>
<td>SFP-GE-LH70-SM1550</td>
<td></td>
<td></td>
<td></td>
<td>70 km (43.50 miles)</td>
</tr>
<tr>
<td></td>
<td>SFP-GE-LX-SM1310-BIDI</td>
<td>TX: 1310 RX: 1490</td>
<td>LC</td>
<td>9/125 µm single mode optical fiber</td>
<td>10 km (6.21 miles)</td>
</tr>
<tr>
<td></td>
<td>SFP-GE-LX-SM1490-BIDI</td>
<td>TX: 1490 RX: 1310</td>
<td></td>
<td>9/125 µm single mode optical fiber</td>
<td>10 km (6.21 miles)</td>
</tr>
<tr>
<td></td>
<td>SFP-GE-T</td>
<td>—</td>
<td>RJ-45</td>
<td>Twisted pair cable</td>
<td>100 m (0.08 miles)</td>
</tr>
</tbody>
</table>