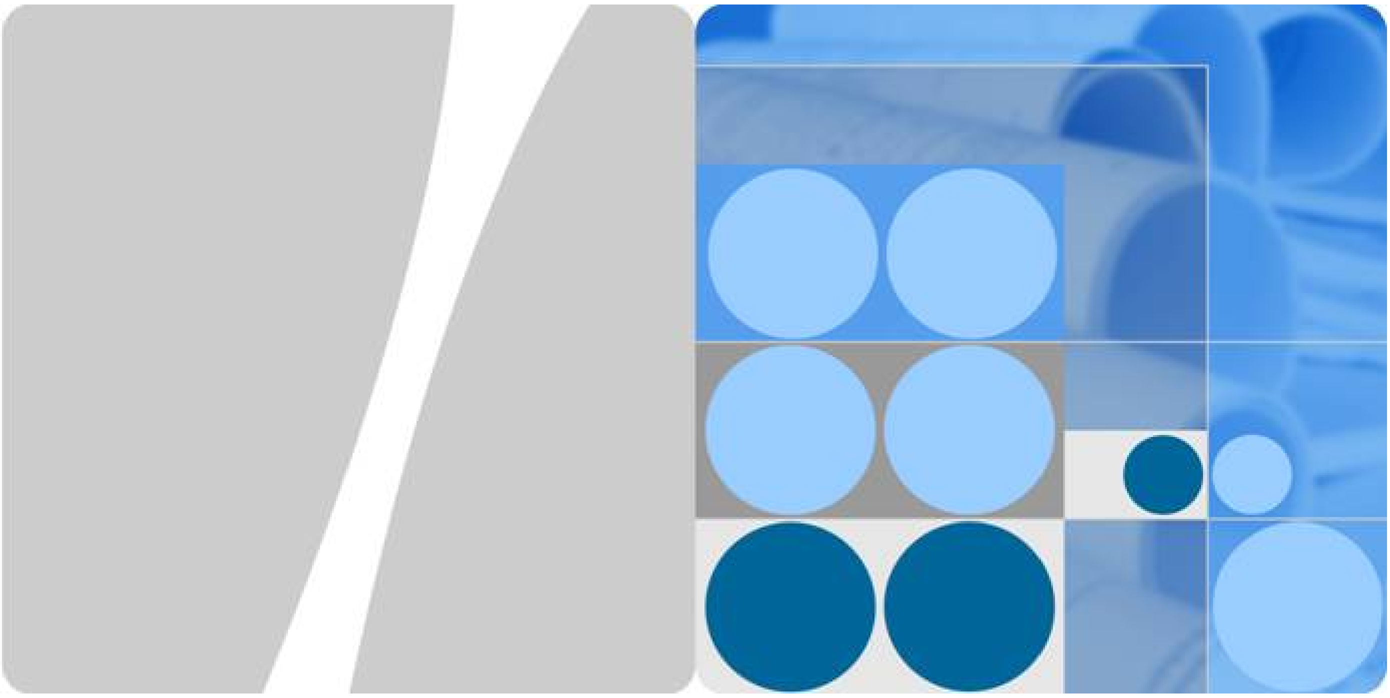


Quidway S5700 Series Ethernet Switches

V100R006C01

Product Description

Issue 01

Date 2011-10-26

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Intended Audience

This document describes the positioning, characteristics, architecture, link features, service features, application scenarios, operation and maintenance functions, and technical specifications of the S5700.

This document helps you understand the characteristics and features of the S5700.

This document is intended for:

- Network planning engineers
- Hardware installation engineers
- Commissioning engineers
- Data configuration engineers
- On-site maintenance engineers
- Network monitoring engineers
- System maintenance engineers

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
⚠ DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injuries.
⚠ WARNING	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injuries.
⚠ CAUTION	Indicates a potentially hazardous situation that, if not avoided, could cause device damage, data loss, and performance degradation, or unexpected results.
🔑 TIP	Indicates a tip that may help you solve a problem or save you time.

Symbol	Description
🕮 NOTE	Provides additional information to emphasize or supplement important points of the main text.

Command Conventions

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italic*.
[ ]	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 items are grouped in brackets and separated by vertical bars. One item is selected or no item 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 items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.
&<1-n>	The parameter before the & sign can be repeated 1 to n times.
#	A line starting with the # sign is comments.

Change History

Updates between document issues are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Changes in Issue 01 (2011-10-26)

This is the first release.

Contents

1 Product Positioning and Characteristics

About This Chapter

1.1 Product Positioning

⚠ **CAUTION**

The Quidway S5700 Series series Ethernet switches are class A products. The switches that are operating may cause radio interference. Customers need to take prevention measures.

The Quidway S5700 Series series Ethernet switches (hereinafter referred to as the S5700) provide the access, aggregation, and data transport functions. They are developed by Huawei to meet the requirements for reliable access and high-quality transmission of multiple services on the enterprise network.

Positioned for the access layer or aggregation layer of the enterprise network, the S5700 provides large capacity, high port density, and cost-effective packet forwarding capabilities. In addition, the S5700 provides multi-service access capabilities, excellent extensibility, quality of service (QoS) guarantee, powerful multicast replication, and carrier-class security, and can be used to build ring topologies of high reliability.

The switches are classified into SI switches, EI switches and HI switches. The EI switches provide more powerful, multicast, and reliability functions than SI switches.The HI switches provide MPLS, LDP than SI and EI.

NOTE

The S5700-6TP-LI-AC does not support hardware-based forwarding for Layer 3 services.

1.2 Product Characteristics

1.2.1 Flexible Networking Capability

The S5700 provides 10/100/1000Base-T Ethernet electrical interfaces, 100/1000Base-X Ethernet optical interfaces, and 10GE optical interfaces. It supports multiple interface types such as access, trunk, and hybrid.

The S5700 provides swappable Small Form-Factor Pluggable (SFP) optical modules for optical fiber connections.For the 10GE optical fiber connections, the S5700 provides 10 Gigabit Small Form Factor Pluggable (XFP) and Small Form-Factor Pluggable Plus (SFP+) optical modules. The length of optical fibers can be selected according to the transmission distance.

The S5700 can be used to construct a tree, star, or ring Ethernet network. For the ring Ethernet, the S5700 supports the Spanning Tree Protocol (STP) and RRPP to prevent loops and provide rapid switchover.

1.2.2 Network-Level QoS Guarantee

The S5700 provides comprehensive QoS mechanisms. It can intelligently identify services and classify traffic according to Layer 2 to Layer 4 information in the Open System Interconnection (OSI) model. Then, it provides various polices such as access traffic filter, traffic policing, and queue scheduling to provide differentiated services.

1.2.3 High Extensibility

Based on the Huawei proprietary Versatile Routing Platform (VRP), the S5700 provides high-speed switching and various service features by integrating network management technologies.

The S5700 provides a versatile slot that supports various interface cards to meet the requirements for service expansion.

NOTE

The interface cards are not available on S5700-24TP-SI-AC, S5700-24TP-SI-DC, S5700-24TP-PWR-SI, S5700-48TP-SI-AC, S5700-48TP-SI-DC, S5700-6TP-LI-AC and S5700-48TP-PWR-SI.

1.2.4 Comprehensive Security Measures

The S5700 guarantees the security of network devices and data transmission. It provides the following security measures to protect the network against attacks initiated by malicious users:

- Packet filtering based on MAC addresses
- Various ACL policies
- Mechanism of searching the forwarding table based on VLAN IDs and MAC addresses
- Traffic suppression

In addition, the S5700 provides the following functions to ensure secure login of users:

- Providing login passwords and password encryption for login users
- Protecting commands through users levels and command levels
- Locking the configuration terminal through a certain command to prevent illegal use of the device
- Displaying confirm or prompt information for important commands that affect system performance

The S5700 provides the Automatic Laser Shutdown (ALS) function. That is, when the fiber is broken, the S5700 stops transmitting laser. This protects users against the laser.

1.2.5 Convenient Operation and Maintenance

In addition to collecting traffic statistics based on interfaces and VLANs, the S5700 provides fault detection and location tools such as ping and traceroute on an IP network. It can also work with the Huawei U2000 network management system (NMS) to implement performance monitoring, alarm report, and fast fault location.

Through the U2000, you can configure and manage the S5700, for example, manage interfaces, VLANs, multicast services, software upgrading, and configuration files. The U2000 supports various personalized configuration modes such as end-to-end configuration, batch configuration, and configuration wizard. In addition, it provides default configuration templates for management functions.

The S5700 supports the Huawei Group Management Protocol (HGMP). Through HGMP, an S5700 can manage multiple Layer 2 switches by automatically collecting topology information and using a uniform management channel.

1.2.6 Energy-Saving Design

The S5700 adopts the following measures to save energy:

- Low noise fans that can adjust the speed automatically are used, thus reducing noises in the system and power consumption of fans
- The chip switches to the power saving mode when no connected device is detected on a service interface, that is, the interface is idle.
- It uses highly-integrated and energy-saving chips produced through advanced processing techniques. With the help of the intelligent device management system, the chips not only improve system performance but also greatly reduce power consumption of the entire system.

1.2.7 Advanced Lightning Protection Technologies

The S5700 adopts the Huawei patented lightning protection technologies to protect the equipment. The lightning protection technologies reduce the probability of damages caused by lightning and increase the safety factor by 30 times, thus greatly improving the device reliability.

1.2.8 Convenient PoE Power Supply

The S5700 has the PoE function. It provides centralized power supply for the attached IP phone, wireless access point (AP), portable device charger, POS machine, camera, and data collector through twisted pairs.

The PoE function of the S5700 complies with IEEE 802.3af and IEEE 802.3at. The S5700 can provide power for the devices of different vendors remotely. In IEEE 802.3at, the maximum power supply capability is 30 W. This capability ensures adequate power for IP video phone, dualband WiFi AP, IP camera, multi-function STB11, and RFID and simplifies the network.

The S5700 has the ability to control power supply based on time range, thus effectively managing network devices, reducing power consumption, and lowering the OPEX.

2 Product Architecture

About This Chapter

2.1 Introduction

The S5700 series adopt the integrated hardware platform and have the front-access structure. The hardware consists of the chassis, power supply, fan, SCU, and interface card for upstream services. The width of the S5700 complies with the industry standards, and the S5700 can be installed in an IEC 297 cabinet or an ETSI cabinet.

The S5700 series include the S5700C and S5700TP.

The S5700C switches include S5700-28C-EI, S5700-28C-EI-24S, S5700-52C-EI, S5700-28C-PWR-EI, S5700-52C-PWR-EI, S5700-28C-SI S5700-28C-HI, S5700-28C-HI-24S and S5700-52C-SI.

The S5700TP switches include S5700-24TP-SI-AC,S5700-24TP-SI-DC, S5700-48TP-SI-AC, S5700-48TP-SI-DC, S5700-48TP-PWR-SI, S5700-6TP-LI-AC and S5700-48TP-PWR-SI.

2.2 Device Structure

This section describes the structure of the S5700.

The S5700 Ethernet switches adopt an integrated hardware platform. An S5700 consists of the chassis, power supply unit, fan, switch control unit (SCU), and interface subcard. The width of an S5700 complies with industry standards, and the S5700 can be installed in an IEC297 cabinet or an ETSI cabinet.

The S5700 switches include S5700C and S5700TP.

NOTE

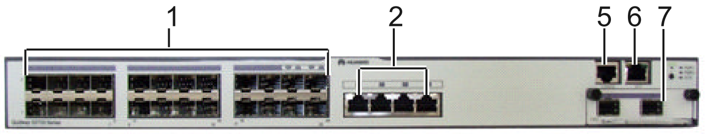
The S5700 is 1 U (1 U = 44.45 mm) high.

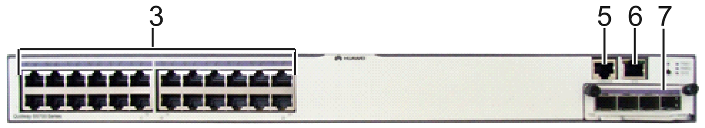
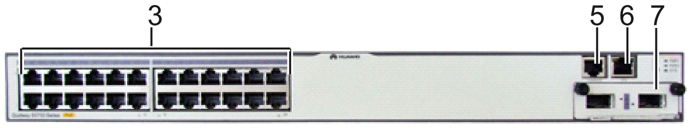
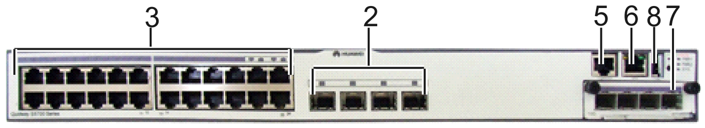
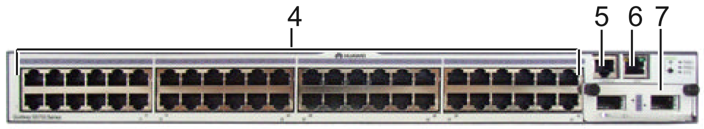
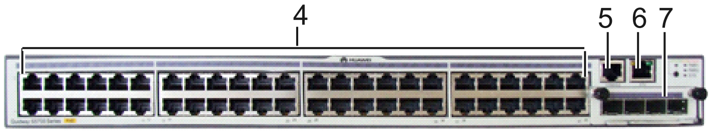
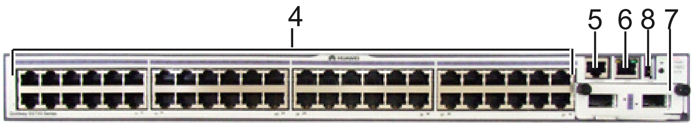
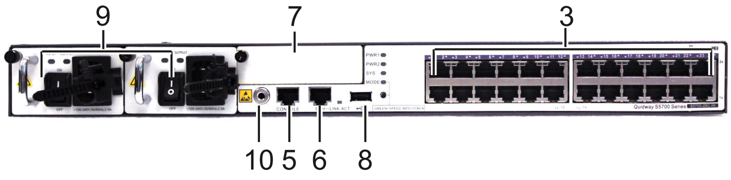
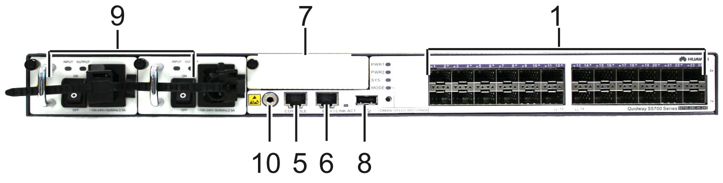
- The dimensions of S5700-24TP-SI-AC, S5700-24TP-SI-DC, S5700-28C-HI or S5700-28C-HI-24S are 442.0 mm x 220.0 mm x 43.6 mm (width x depth x height).
- The dimensions of S5700-6TP-LI-AC are 250.0 mm × 180.0 mm × 43.6 mm (width x depth x height).
- The dimensions of an S5700 switch except S5700-24TP-SI-AC, S5700-24TP-SI-DC, S5700-28C-HI, S5700-28C-HI-24S and S5700-6TP-LI-AC are 442.0 mm x 420.0 mm x 43.6 mm (width x depth x height).

S5700C Appearances

Table 2-1 shows the front views of S5700C.

Table 2-1 S5700C front views

Model	Image
S5700-28C-EI-24S	

Model	Image
S5700-28C-EI	
S5700-28C-PWR-EI	
S5700-28C-SI	
S5700-52C-EI	
S5700-52C-PWR-EI	
S5700-52C-SI	
S5700-28C-HI	
S5700-28C-HI-24S	

1. Twenty-four 100/1000BASE-X Ethernet optical interfaces	2. Four GE combo interfaces (10/100/1000BASE-T+100/1000BASE-X, used together with the last four Ethernet interfaces)	3. Twenty-four 10/100/1000BASE-T Ethernet interfaces	4. Forty-eight 10/100/1000BASE-T Ethernet interfaces
5. One console interface	6. One management interface	7. Front subcard slot	8. One USB interface
9. Power supply unit slot	10. ESD jack		

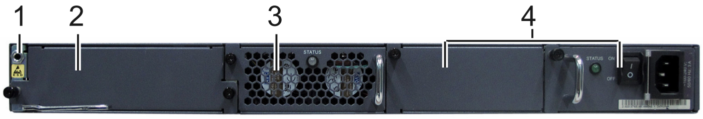
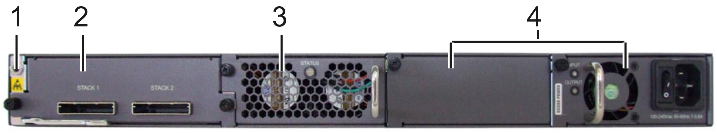
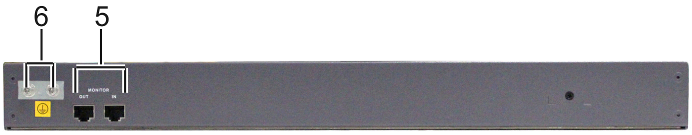
NOTE

By default, a combo interface works in the auto mode. In the auto mode, if the electrical interface is connected to a network cable first, the combo interface works as an electrical interface to transmit data; if the optical interface is connected to a fiber first, the combo interface works as an optical interface to transmit data.

S5700-28C-EI-24S support 1000BASE-T Copper SFP Transceiver.

Table 2-2 shows the rear views of S5700C.

Table 2-2 S5700C rear views

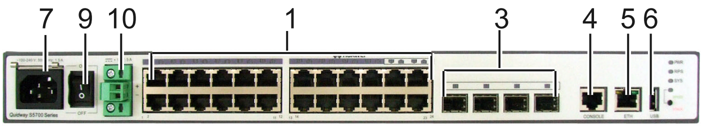
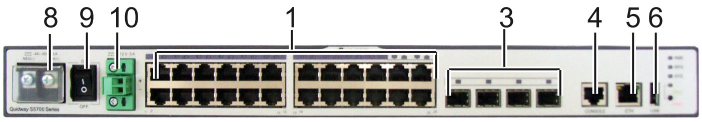
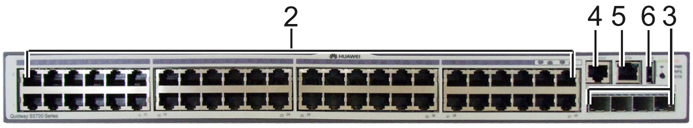
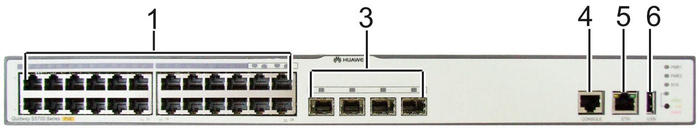
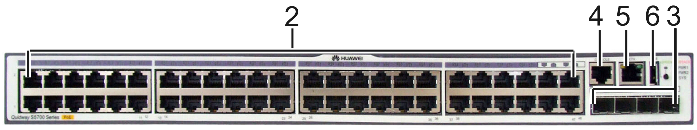
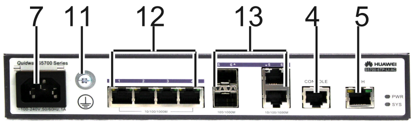
Model	Image
S5700-28C-EI-24S S5700-28C-EI S5700-28C-SI S5700-52C-EI S5700-52C-SI	
S5700-28C-PWR-EI S5700-52C-PWR-EI	
S5700-28C-HI S5700-28C-HI-24S	

1. ESD jack	2. Rear subcard slot	3. Fan module	4. Power supply unit slot
5. Two monitor interfaces	6. Two ground screws		

S5700TP Appearances

Table 2-3 shows the front views of S5700TP.

Table 2-3 S5700TP front views

Model	Image
S5700-24TP-SI-AC	
S5700-24TP-SI-DC	
S5700-48TP-SI-AC S5700-48TP-SI-DC	
S5700-24TP-PWR-SI	
S5700-48TP-PWR-SI	
S5700-6TP-LI-AC	

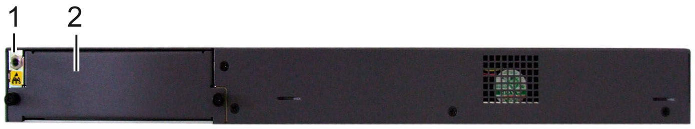
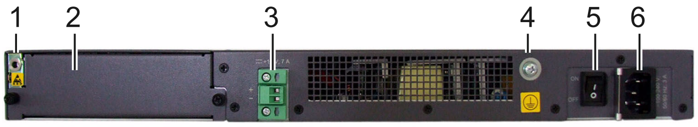
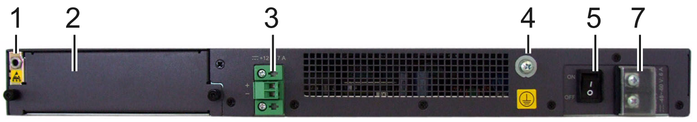
1. Twenty-four 10/100/1000BASE-T Ethernet interfaces	2. Forty-eight 10/100/1000BASE-T Ethernet interfaces	3. Four GE combo interfaces (10/100/1000BASE-T+100/1000BASE-X, used together with the last four Ethernet interfaces)	4. One console interface
5. One management interface	6. One USB interface	7. AC jack	8. DC jack
9. Switch	10. RPS power jack	11. Ground screw	12. Four 10/100/1000BASE-T Ethernet interfaces
13. Two 1000M combo interfaces (10/100/1000BASE-T+100/1000BASE-X)			

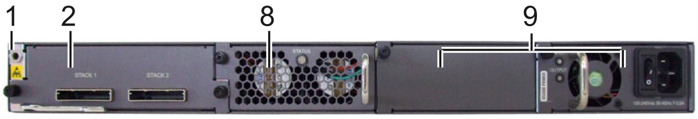
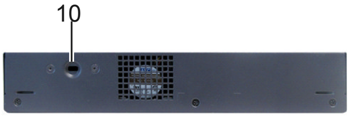
NOTE

By default, a combo interface works in the auto mode. In the auto mode, if the electrical interface is connected to a network cable first, the combo interface works as an electrical interface to transmit data; if the optical interface is connected to a fiber first, the combo interface works as an optical interface to transmit data.

Table 2-4 shows the rear views of S5700TP.

Table 2-4 S5700TP rear views

Model	Image
S5700-24TP-SI-AC S5700-24TP-SI-DC	
S5700-48TP-SI-AC	
S5700-48TP-SI-DC	

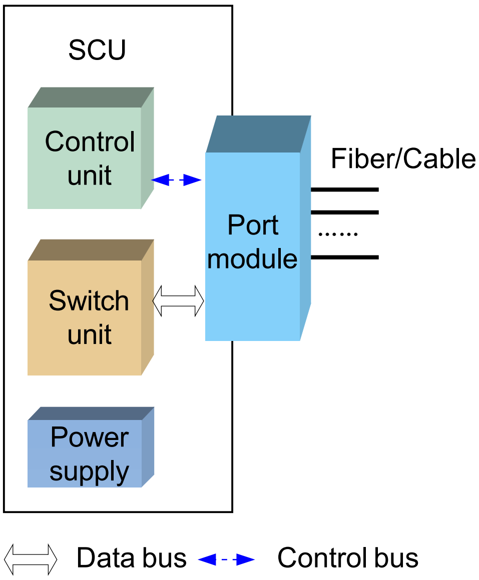
Model	Image
S5700-24TP-PWR-SI S5700-48TP-PWR-SI	
S5700-6TP-LI-AC	

1. ESD jack	2. Rear subcard slot	3. RPS power jack	4. Ground screw	5. Switch
6. AC jack	7. DC jack	8. Fan module	9. Power supply unit slot	10. Security lock

2.3 Hardware Modules

Figure 2-1 shows the logical structure of hardware modules of the S5700.

Figure 2-1 Logical structure of hardware modules of the S5700



Hardware modules of the S5700 refer to the interface card, SCU, power supply, and fan.

2.3.1 SCU

The SCU is fixed on the S5700. Each S5700 has one SCU.

The SCU is responsible for packet switching and device management. It integrates multiple functional modules, namely, the main control module, switching module, and interface module.

Main Control Module

The main control module implements the following functions:

- Processing protocols
- Functioning as an agent of the user to manage the system and monitor the system performance according to instructions of the user, and report the running status of the device to the user
- Monitoring and maintaining the interface module and switching module on the SCU.

Switching Module

The switching module, also called the switching fabric, is responsible for packet exchange, multicast replication, QoS scheduling, and access control on the interface module of the SCU.

The switching module adopts high performance ASIC chips to implement line-speed forwarding and fast switching of data with different priorities.

Interface Module

The interface module provides Ethernet interfaces for accessing Ethernet services.

2.3.2 Power Supply

The S5700 can use either the DC power supply or the AC power supply. But the switches with PoE can only use the AC power supply.

Table 2-5 Power supply

Device Name	AC	DC	1:1 Backup power supplies
S5700-28C-EI	Y	Y	Y
S5700-28C-EI-24S	Y	Y	Y
S5700-52C-EI	Y	Y	Y
S5700-24TP-SI-AC	Y	N	N
S5700-24TP-PWR-SI	Y	N	Y
S5700-48TP-SI-DC	N	Y	N
S5700-48TP-PWR-SI	Y	N	Y
S5700-28C-PWR-EI	Y	N	Y
S5700-52C-PWR-EI	Y	N	Y
S5700-28C-SI	Y	Y	Y
S5700-52C-SI	Y	Y	Y

Device Name	AC	DC	1:1 Backup power supplies
S5700-28C-HI	Y	Y	Y
S5700-28C-HI-24S	Y	Y	Y
S5700-6TP-LI-AC	Y	N	N

The S5700-24TP-SI-DC and S5700-48TP-SI-DC support the RPS DC power supply.

2.3.3 Fan

The fans can work in the intelligent mode or forcible mode.

In the intelligent mode, the fans start to operate only when the environment temperature exceeds a specified value.

The S5700-24TP-SI-AC, S5700-24TP-SI-DC, S5700-48TP-SI-AC, S5700-48TP-SI-DC support the intelligent mode.

S5700-28C-HI, S5700-28C-HI-24S, S5700-6TP-LI-AC support the forcible mode.

The S5700-24TP-PWR-SI, S5700-48TP-PWR-SI, S5700-28C-SI, S5700-52C-SI, S5700-28C-PWR-EI, S5700-52C-PWR-EI, S5700-28C-EI, S5700-52C-EI, and S5700-28C-EI-24S support the hot pluggable fans. The fan module can be replaced on site and maintained in service.

2.3.4 Interface Card

The S5700C series switches support the interface card for upstream services. The interface card improves the networking flexibility, and provides the cost-effective and personalized solutions to customers.

Except S5700-28C-HI, S5700-28C-HI-24S and S5700-6TP-LI-AC, the S5700 series switches support the stack card.The S5700 series switches support the stack card. Multiple switches can be connected through stack cards to form a logical device. This function facilitates network expansion, saves investment, reduces management costs, and improves network reliability.

NOTE

The interface cards of the S5700C, except S5700-28C-HI and S5700-28C-HI-24S are not hot swappable.

2.4 Software Architecture

The S5700 runs on the latest VRP version 5 (VRPv5) to provide various features. VRPv5 consists of the following parts:

- System service plane

  This plane provides task and memory management, timer, software loading and patching on the basis of the operating system. In addition, it enhances modular technology to facilitate system upgrade and customization.

- General control plane

  This plane is the core of the VRP data communication platform, providing link management, IP protocol stack, and routing protocol processing, and implementing the security and QoS functions. It is used to control the data forwarding plane and implement functions of the device.

- Data forwarding plane

  This plane forwards data under the control of the general control plane. The VRPv5 supports data forwarding based on software and hardware.

- Service control plane

  This plane controls and manages services based on users or interfaces. It implements the authentication, authorization, and accounting for users through DHCP Option 82 and implements authentication for access interfaces through IEEE 802.1x.

- System management plane

  This plane provides a graphic user interface and manages the input and output information for network management and maintenance.

3 Link Features

About This Chapter

3.1 Ethernet Features

3.1.1 Link Aggregation

Link aggregation is a function that binds multiple physical interfaces on one device or multiple devices into a logical interface (such as an Eth-Trunk). This logical interface is also called a load balancing group or a link aggregation group.

After multiple physical interfaces are bound into a logical interface, the S5700 load balances the traffic passing through the logical interface among the member interfaces. When a member interface fails, the traffic on this interface is shared by the other member interfaces without interrupting services. When the faulty interface recovers, the traffic is balanced among all interfaces again.

Currently, the S5700 implements link aggregation between XGE interfaces, GE interfaces or FE interfaces. Load balancing can be implemented based on the following information:

- Source MAC address
- Destination MAC address
- Source MAC address and destination MAC address
- Source IP address
- Destination IP address
- Source IP address and destination IP address

Using the link aggregation technology, you can increase the bandwidth and improve link reliability without upgrading the hardware, thus saving costs.

3.1.2 Flow Control on an Interface

Flow control on an interface is a method of congestion management. It applies to all types of flows. The S5700 implements flow control on an interface by using the hardware backpressure mechanism. When an interface works in full duplex mode, the S5700 implements flow control complying with IEEE 802.3x. When the interface works in half duplex mode, the S5700 implements flow control through the backpressure mechanism.

When congestion occurs, the S5700 sends continuous Pause frames to the upstream device, requesting it to stop sending data for a specified period of time. When the upstream device receives the pause frames, it reduces the volume of traffic sent from its outbound interface. Flow control on an interface does not identify flow types.

3.1.3 Traffic Suppression

Traffic suppression limits the number of unknown unicast packets, multicast packets, and broadcast packets within a proper range to ensure network efficiency.

The S5700 can suppress the packets based on interfaces. When traffic suppression is enabled on an interface, the interface monitors received unknown unicast packets, multicast packets, and broadcast packets to check whether their traffic exceeds the threshold. If traffic exceeds the threshold, the S5700 discards excessive packets to keep the traffic volume within the limit and thus services on the network run normally.

The S5700 can also control the percentage of unknown unicast packets, multicast packets, and broadcast packets on an interface.

3.1.4 VLAN

A local area network (LAN) can be divided into several logical LANs. Each logical LAN is a broadcast domain, which is called a virtual LAN (VLAN). To put it simply, devices on a LAN are logically grouped into different LAN segments, irrespective of their physical locations. In this manner, VLANs isolate broadcast domains on a LAN.

Methods to Define VLANs

A physical LAN can be divided into several VLANs, and several physical LANs can be grouped into a VLAN. Devices on a VLAN belong to the same broadcast domain and can communicate with each other. Different VLANs are isolated from each other, so devices on different VLANs cannot communicate with each other.

The S5700 supports the following methods to define VLANs:

- Based on interfaces

  After an interface is added to a VLAN, packets received by the interface are sent on the VLAN.

- Based on MAC addresses

  VLAN members are defined according to source MAC addresses of packets. When an interface of the S5700 receives a packet, the S5700 determines the VLAN ID of the packet according to the source MAC address of the packet and sends the packet on the corresponding VLAN.

- Based on protocols

  The S5700 determines the VLAN ID of a received packet according to the protocol (or protocol suite) and encapsulation format of the packet.

- Based on IP subnets

  VLAN members are defined according to the source IP addresses and the subnet masks of packets. When an interface of the S5700 receives a packet, the S5700 determines the VLAN ID of the packet according to the source IP address of the packet and sends the packet on the corresponding VLAN.

- Based on policies

  VLAN members are defined according to the MAC+IP or MAC+IP+port binding policy. When an interface of the S5700 receives a packet, the S5700 determines the VLAN ID of the packet according to the binding policy and sends the packet on the corresponding VLAN.

VLAN Aggregation

To implement communication between VLANs on the S5700, you need to configure VLANIF interfaces and assign an IP address to each VLANIF interfaces. Therefore, this wastes IP addresses when there are many VLANs. VLAN aggregation can solve this problem.

VLAN aggregation means that multiple VLANs are aggregated into a super-VLAN. The VLANs that form the super-VLAN is called sub-VLANs.

MUX VLAN

The MUX VLAN function is used to isolate Layer 2 traffic between the interfaces of a VLAN. For example, on an intranet, a user interface can communicate with a server interface, but the user interfaces cannot communicate with each other.

This function involves a MUX VLAN and several subordinate VLANs. Subordinate VLANs are classified into subordinate group VLANs and subordinate separate VLANs. Ports on subordinate VLANs can communicate with ports on the MUX VLAN. Ports on a subordinate group VLAN can communicate with each other but cannot communicate with ports on other subordinate group VLANs. Ports on a subordinate separate VLAN cannot communicate with each other.

DHCP Policy VLAN

After DHCP policy VLANs are configured on the S5700, VLANs are allocated to hosts connected to interfaces of the S5700 based on IP addresses of hosts. When a host is connected to an interface of the S5700, the host cannot be added to a VLAN because it has not obtained a valid IP address. The DHCP policy VLAN function enables new hosts to obtain valid IP addresses and be added to corresponding VLANs based on obtained IP addresses.

The S5700 supports the following DHCP policy VLAN functions:

- Generic DHCP policy VLAN
- DHCP policy VLAN based on MAC addresses
- DHCP policy VLAN based on interfaces

Voice VLAN

A voice VLAN is used to transmit voice data flows. You can create a voice VLAN and add the interface connected to the voice device to the voice VLAN. Then voice data flows can be transmitted on the voice VLAN.

You can apply special QoS configuration to the voice data packets transmitted on the voice VLAN so that voice data packets are transmitted with high priority. The quality of the voice service is ensured.

VLAN Mapping

VLAN mapping means that the S5700 replaces the outer VLAN tags of data frames to the specified VLAN tags according to the preset VLAN mapping table so that services are transmitted according to the network planning of the carrier.

The S5700 supports the mapping from one or more customer VLAN IDs (C-VLANs) to a service VLAN ID (S-VLAN).

NOTE

- C-VLAN is the VLAN that a user-side interface belongs to. It identifies a user or a type of users.
- An S-VLAN is a VLAN defined on the public network by the carrier. The S-VLAN ID identifies a service.

VLAN Switching

VLAN switching is a forwarding technology based on VLAN tags. A static forwarding path must be configured on switching nodes on a network to implement VLAN switching. After receiving packets from certain VLANs, a switch forwards them to corresponding interfaces according to the VLAN switching table without searching the MAC address table. This improves the forwarding efficiency and security, and prevents MAC address attacks and broadcast storms.

The S5700 implements the following functions through VLAN switching:

- Adding an outer VLAN tag to packets (stack-vlan)
- Translating VLAN tags between interfaces (switch-vlan)

3.1.5 QinQ

The 802.1Q-in-802.1Q (QinQ) protocol is a Layer 2 tunneling protocol based on the IEEE 802.1Q. A frame transmitted on the public network has double 802.1Q tags. One tag identifies the public network and the other identifies the private network.

Usually, carriers define VLANs on the public network, and users define VLANs on their own private networks. Therefore, different private networks may use the same VLAN ID. Through the QinQ function, the S5700 adds public VLAN tags to the packets from private networks. Then the private VLAN tag becomes the inner VLAN tag. In this way, packets from user networks are transmitted transparently on the public network, and thus user networks are separated from the public network.

Currently, the S5700 supports basic QinQ and selective QinQ.

- Basic QinQ

  Basic QinQ is implemented based on interfaces. All the frames that reach the public network through an interface are tagged with the same public VLAN ID.
- Selective QinQ

  Selective QinQ extends the basic QinQ function. It enables an interface to determine the outer VLAN tag according to the private VLAN tag so that packets from different private networks are transmitted through different paths. Thus different services can be identified and service deployment is easier. For example, voice data packets from different VLANs are tagged with the same outer tag to obtain the same QoS level; common data services are tagged with another VLAN tag to obtain different QoS level.

3.1.6 GVRP

GVRP is a protocol used for dynamic registration and deregistration of VLANs. GVRP maintains the dynamic VLAN registration information in a switch and propagates the registration information to other switches on the network through GARP.

GVRP enables switches on the network to dynamically maintain and update VLANs. With GVRP, you do not need to expend time to analyze the topology and manage configurations. You can adjust the VLAN deployment on the entire network by configuring only a few devices.

The S5700 supports GARP and GVRP. Through GVRP, the S5700 can send VLAN declaration to other devices and dynamically create VLANs after receiving VLAN registration information from other devices.

3.2 STP/RSTP/MSTP

3.2.1 STP and RSTP

The Spanning Tree Protocol (STP) and the Rapid Spanning Tree Protocol (RSTP) are link-layer management protocols and are mainly applied to LANs to prevent loops. STP blocks redundant links and trims a network into a tree topology free from loops. RSTP enhances STP. It provides fast transition of interfaces status to speed up network convergence.

STP and RSTP prevent broadcast storms caused by loops and provides backup links for data forwarding.

3.2.2 MSTP

The Multiple Spanning Tree Protocol (MSTP) is developed based on STP and RSTP. MSTP divides a network into multiple regions. Based on VLAN tags, each region has several spanning trees that are independent of each other. As a result, the entire network is trimmed to a tree topology that is free from loops. Broadcast storms are thus prevented on the network.

MSTP associates VLANs with spanning trees so that packets of different VLANs are transmitted along different spanning trees. This speeds up network convergence and implements load balancing.

Different from STP and RSTP, MSTP provides multiple backup links to implement load balancing among VLANs.

3.2.3 MSTP Protection

BPDU Protection

The S5700 provides Bridge Protocol Data Unit (BPDU) protection when MSTP is enabled. When BPDU protection is enabled, the S5700 shuts down the edge port that receives a protocol BPDU instead of turning the edge port into a non-edge port. In this case, the spanning tree is not recalculated, and thus network flapping is prevented.

Root Protection

The S5700 provides root protection when MSTP is enabled. It retains the role of the root switch by maintaining the role of the designated port as follows:

When the designated port enabled with root protection receives a BPDU of higher priority, the port does not change to a non-designated port. Instead, it turns to the Listening state and stops forwarding packets. If the port does not receive protocol BPDUs of higher priority for a long time, it restores the Forwarding state. This prevents network flapping.

Loop Protection

After loop protection is enabled on the S5700, it sets the root port to the Blocking state if the root port does not receive protocol BPDUs from the upstream device. If the port receives protocol BPDUs again, it becomes the root port and changes to the Forwarding state. If no protocol BPDU is received, the port remains in the Blocking state and does not forward packets. In this way, loops are prevented on the network.

3.2.4 Partitioned STP and BPDU Tunnel

Partitioned STP

To improve the reliability of links on the enterprise network, the S5700 can be dual-homed to the upstream Ethernet. In addition, MSTP needs to run on the whole enterprise network to prevent loops. The traditional MSTP networks are not divided. In this case, the convergence speed of an MSTP network is low because the network is large. As a result, the forwarding capability of the network is degraded.

By using the partitioned STP technology, the S5700 logically allocates a VLAN for each partitioned STP network. The tagged BPDUs can be forwarded only within the VLAN that the tag belongs to. Partitioned STP allows BPDUs to be transmitted within a certain range. This prevents loops and speeds up convergence.

BPDU Tunnel

On a partitioned STP network, the S5700 considers the tagged BPDUs as common Layer 2 frames. That is, the S5700 forwards the BPDUs within the VLAN to which the tag belongs rather than sending them to the MSTP module. After the BPDU tunnel is configured, the devices on the MAN do not participate in the topology calculation of the partitioned STP network. Thus, the convergence speed of the network is improved.

To implement the BPDU tunnel function, the access device at the edge of the MAN must be configured with MSTP Snooping. If the forwarding path is changed because of the topology change on the partitioned STP network, the device can detect the topology change, and then notify other devices on the network of the topology change. In this way, the packets are forwarded according to the new topology.

3.3 RRPP

The Rapid Ring Protection Protocol (RRPP) is a link layer protocol applied to the Ethernet ring. It can prevent the broadcast storm caused by the loops in the Ethernet ring. The topology convergence speed on the network running RRPP is much faster than that on the network running other protocols such as STP. This is because the RRPP packets are forwarded through hardware.

In addition, the RRPP ring supports link bundle, which is widely used on the high-bandwidth ring networks.

3.3.1 RRPP Ring Network Composition

An RRPP domain consists of a group of S5700s with the same domain ID and control VLAN ID. An RRPP domain consists of the following elements:

- A physical RRPP ring maps a ring-shaped Ethernet topology. An RRPP domain is composed of multiple rings connected with each other. One of them is the primary ring and the others are subrings.
- An RRPP domain can be configured with a main control VLAN and a sub control VLAN. The main control VLAN transmits packets of the primary ring; the sub control VLAN transmits packets of subrings.
- A control VLAN transmits only RRPP packets; a data VLAN transmits only data packets.
- The master node initiates the polling and determines how to handle topology changes.
- The transit node monitors the status of its directly connected RRPP links. When the link status changes, the transit node notifies the master node. The master node then decides how to handle the change.

3.3.2 How Does RRPP Work

The master node on a ring has a primary interface and a secondary interface. The primary interface on the master node periodically transmits hello messages. If the secondary interface on the master node receives the hello messages, it indicates that the path is a closed ring, and the master node blocks the secondary interface. This prevents loops on the network.

If the secondary interface on the master node fails to receive a hello message in a certain period, it indicates that the link on the ring is faulty, and the master node opens the secondary interface.

3.3.3 Various Topologies

Single RRPP Ring

There is only one Ethernet ring on a network and only one RRPP domain exists. In this case, the network can respond to topology changes quickly. The fast convergence of the RRPP ring is thus performed and Layer 2 and Layer 3 services can be quickly switched.

Tangent RRPP Rings

There are two or more Ethernet rings on a network and only one public node exits between each pair of rings. The rings belong to different RRPP domains.

This networking is suitable for large-scale networks that need to be managed in different domains. When one ring is faulty or recovers, other domains are not affected. The convergence process of the RRPP ring in the local domain is the same as the convergence process of a sing RRPP ring.

Intersecting RRPP Rings

There are two or more Ethernet rings on a network and two public nodes exit between each pair of rings. The rings belong to the same RRPP domain. One ring is the primary ring, and the others are the subrings.

The protocol packets on a subring are transmitted through the channel between the two interfaces connecting the primary ring and the subring. The primary ring can be considered as a node on the subring. This networking is applicable to the convergence of a dual-homing network. Through this networking, the upstream links are backed up.

Connecting RRPP Network with Other Networks

When an RRPP ring is adjacent to an Ethernet ring enabled with STP, only the tangent rings are supported, but the intersecting rings are not supported. This prevents the conflict between RRPP and STP if both of them calculate the interface status.

3.4 Smart Link

Smart Link is a flexible link backup mechanism, which provides an effective and reliable solution for dual-homed networking. Compared with STP, Smart Link provides faster convergence speed. On a dual-homed network, the configuration of Smart Link is simpler than the configuration of RRPP.

Smart Link implements fast protective switchover when the active link fails on the dual-homed network. In normal situations, there is an active link and a standby link in the two upstream links. That is, one upstream interface is in Forwarding state, and the other is in Block state. When the active link fails, the Smart Link group quickly switches traffic to the standby link.

Smart Link provides manual switchover and automatic switchover. When a link is faulty, the Smart Link group sends Flush packets to neighboring devices, requesting the devices to update their MAC tables and ARP tables.

When multiple devices at different layers are connected for convergence, Monitor Link that adopts the interface association mechanism monitors upstream links. This improves the backup function of Smart Link. When an upstream link is faulty, Monitor Link blocks the downstream interface. After the upstream link recovers, the downstream interface is opened. This switches traffic between different paths for transmission.

3.5 SEP

The Smart Ethernet Protection (SEP) protocol is a ring network protocol applied to the link layer of an Ethernet network. The SEP protocol works on the basis of SEP segments. An SEP segment consists of a group of switching devices that are configured with the same SEP segment ID and control VLAN ID.

Most metropolitan area networks (MANs) and enterprise intranets adopt the ring networking to ensure high reliability. The services, however, are affected if any node on the ring fails. Generally, a ring network adopts the Resilient Packet Ring (RPR) or Ethernet ring technology. The costs of the RPR technology are high because it requires special hardware components. The Ethernet ring is improved and its costs are low; therefore, more and more MANs and enterprise intranets adopt the Ethernet ring.

Huawei originates the SEP protocol, which achieves the protective switchover on the open ring and closed ring and displays the uncertain blocked points or ring network topology. Compared with other Ethernet ring technologies, SEP has the following advantages:

- It can run on a network together with STP, RSTP, MSTP, and RRPP.
- It solves the problem of unidirectional traffic.
- Unidirectional traffic may cause unidirectional broadcast storms on the network. The SEP protocol can prevent unidirectional broadcast storms because it can detect the unidirectional traffic effectively.
- It supports the display of network topology. The network topology is displayed on the basis of SEP segments.
- When the devices of other vendors are used on the network, the SEP can also prevent loops, but does not need to be configured on these devices.

3.6 Interface Security

Interface security is a security mechanism to control the access to a network. It checks whether the source MAC addresses of data frames received on an interface are valid. When detecting packets with invalid source MAC addresses, it takes certain actions to protect the interface.

After security protection is enabled on an interface, the S5700 considers the following types of MAC addresses valid:

- Static MAC addresses that are manually configured
- Dynamic or static MAC addresses in the DHCP snooping table
- Dynamic MAC addresses that are learned before the number of learned MAC addresses reaches the limit

When the interface receives frames with invalid source MAC addresses, the S5700 triggers the interface security function to discard the frames or generates an alarm according to the configuration.

3.7 Link Detection

Link detection includes loopback detection and virtual cable test (VCT). They provide users with two means to detect link faults on LANs.

- Loopback detection is used to check whether loops exist on a LAN. The S-switch sends specific packets to detect loopback on the entire LAN.
- VCT is mainly used to estimate the length of a network cable and locate the failure point of the cable. The S-switch simulates radar to detect cable faults and locate the failure points on the basis of a single link.

4 Service Features

About This Chapter

4.1 IPv4 Forwarding

4.1.1 IPv4 Features

The S5700 supports the following IPv4 features:

- TCP/IP protocol stack, including ICMP, IP, TCP, UDP, socket (TCP/UDP/Raw IP), and ARP
- Static DNS and specified DNS server
- FTP server/client, TFTP client, and SSH
- Ping, tracert, and Network Quality Analysis (NQA): NQA can detect the status of ICMP, TCP, UDP, DHCP, FTP, HTTP and SNMP services and test the response time of various services
- DHCP Server, DHCP Relay, DHCP Client, and DHCP Snooping
- BFD, including BFD for OSPF, BFD for ISIS, BFD for BGP, and BFD for PIM

📖 **NOTE**

The BFD functions arenot available on S5700SI.

The DHCP Server, DHCP Relay and BFD functions are not available on S5700-6TP-LI-AC.

4.1.2 Unicast Routing Features

📖 **NOTE**

The static routes, RIP and RIPng are available on S5700SI. But the other routing protocols and routing policy are not available.

Only the static routes are available on S5700-6TP-LI-AC. All of the routing protocols and routing policy are not available.

The S5700 supports the following unicast routing features:

- IPv4 unicast forwarding at line speed through bottom-layer ASIC chips
- IPv4 routing protocols, including RIP v1/v2, OSPF, IS-IS, and BGPv4
- Virtual Routing Forwarding (VRF)
- Static routes that are manually configured by the administrator, which simplify network configurations and improve network performance
- Selection of the optimal route through the perfect routing policy

4.1.3 Multicast Routing Features

📖 **NOTE**

The multicast routing features are not available on S5700SI and S5700-6TP-LI-AC.

The S5700 supports the multicast function. This saves network bandwidth and reduces network load. The S5700 also guarantees QoS of multicast traffic and forwards multicast traffic at line speed. It supports the following multicast routing features:

- IPv4 multicast forwarding at line speed through the bottom-layer ASIC chips
- Multicast protocols, including IGMP, PIM-SM, PIM-DM, MSDP, and MBGP

- ASM and SSM
- Anycast RP: Multiple RPs can exist in a domain and they are configured as MSDP peers. A multicast source can register with the nearest RP, and the receiver can also choose the nearest RP and join the shared tree of the RP. In this manner, load balancing is carried out among the RPs. When an RP fails, its previously registered sources and receivers choose another nearest RP. This implements the backup of RPs.
- Multicast static routes
- Routing policy used for receiving, importing, and advertising multicast routes. When forwarding IP multicast packets, the S5700 can filter and forward the packets based on policies.
- PIM BFD
- RPF check

4.2 IPv6

NOTE

The OSPFv3 and VRRP6 are not available on S5700SI switches.

S5700-6TP-LI-AC switches support IPv6 protocol stack only.

The S5700 provides the IPv6 host function, which protects the investment of customers and prevents repeat investment during network upgrade.

The IPv6 functions supported by the S5700 include:

- IPv6 protocol stack
- Unicast routing protocols: RIPng and OSPFv3
- VRRP6
- IPv4/IPv6 transition technologies

4.3 Routing Protocol

The S5700 supports the following unicast routing features:

NOTE

The static routes, RIP and RIPng are available on S5700SI. But the other routing protocols and routing policy are not available.

Only the static routes are available on S5700-6TP-LI-AC. All of the routing protocols and routing policy are not available.

- Static routes that are manually configured by the administrator, which simplify network configurations and improve network performance
- IPv4 routing protocols:
  - Open Shortest Path First version 2 (OSPFv2)
  - Intermediate System-to-Intermediate System (IS-IS)
  - Border Gateway Protocol version 4 (BGPv4)
  - Routing Information Protocol (RIP)
- IPv6 routing protocols:

  - OSPFv3
  - RIPng
- Selection of the optimal route through the perfect routing policy

4.4 Multicast

The Internet Group Management Protocol (IGMP) is a protocol used to manage IP multicast members in the TCP/IP suite. It sets up and maintains the member relationship between IP hosts and their directly connected multicast routers.

4.4.1 IGMP Snooping

Located between hosts and a multicast router, the S5700 supports static multicast forwarding entries and generates a dynamic Layer 2 multicast forwarding table with multicast groups, VLANs, and outbound interfaces by listening to IGMP messages.

When the S5700 receives a multicast packet, it forwards the packet only to the members on the VLAN corresponding to the multicast group. The multicast packet is transmitted in multicast mode on the VLAN according to the Layer 2 forwarding table. This saves bandwidth and enhances the security of information transfer.

4.4.2 IGMP Proxy

IGMP proxy is deployed on the switch that is located between the router and hosts. Then the switch serves as an agent server. The switch terminates IGMP protocol packets sent by hosts to the router and responds to the IGMP Query messages for the hosts. In addition, the switch processes IGMP protocol packets sent by the router and the hosts. In this manner, the forwarding entries for Layer 2 multicast are created.

4.4.3 Prompt Leave of Multicast Member Interfaces

When a multicast member leaves a multicast group, the host sends an IGMP Leave message. When an interface on the S5700 is connected to only one host, the S5700 deletes the multicast forwarding entry of the interface immediately after receiving the IGMP Leave message. This saves bandwidth and system resources and implements fast switching of services.

4.4.4 Multicast Traffic Control

Unknown multicast packets refer to the multicast packets that do not have forwarding entries in the multicast forwarding table. When receiving unknown multicast packets, the S5700 discards the packets or broadcasts them on the VLAN that the inbound interface belongs to.

The S5700 can also control inbound multicast traffic volume by limiting the percentage or rate (in pps) of multicast packets on an Ethernet interface.

4.4.5 Inter-VLAN Multicast Replication

Inter-VLAN multicast replication means that an MVLAN aggregates multicast flows and replicates the flows to different user VLANs.

The S5700 forwards multicast packets through the multicast VLAN, and then replicates the packets based on the L2 multicast forwarding entries. Then, the S5700 sends these packets to different MVLANs. user VLAN multicast replication transmits multicast data in different VLANs. It facilitates the management and control of multicast flows and saves bandwidth.

4.4.6 Controllable Multicast

Multicast protocols do not provide user authentication. Therefore, a user can join or leave a multicast group freely. The multicast source does not know when a user joins or leaves a multicast group, so the number of users receiving multicast traffic on a network in a certain period is unknown. Therefore, the carrier cannot perform accounting for the users. The controllable multicast technology is introduced to solve these problems. Users have to pass authentication before receiving multicast traffic. Furthermore, only authorized multicast traffic can be received by users. Users who pass authentication are allowed to preview unauthorized multicast traffic and can receive multicast traffic in specified periods within a day. Controllable multicast does not apply to static multicast.

4.5 QoS

The S5700 provides the class-based QoS mechanism and supports the 802.1p priority. It provides guarantee of low end-to-end delay, jitter, and high bandwidth.

The S5700 classifies traffic according to certain rules and then performs corresponding actions on the packets such as priority re-marking, traffic policing, congestion management, congestion avoidance, and rate limit on the interface. In this way, value-added services such as NGN services, IPTV, and broadband access are provided with better network service.

4.5.1 Traffic Classification

Traffic classification is a function of identifying the packets of a certain type by matching information in the packet header. For example, the 802.1p priority of the packets sent by the Operating Support System (OSS) and NMS is set to 7; the 802.1p priority of VoIP packets is set to 6; the 802.1p priority of BTV packets and VOD packets is set to 5 or 4; the 802.1p priority of packets sent by VPN users is set to 3, 2, or 1 according to the level of VPN users; the 802.1p priority of packets of the Internet access service is set to 0. Then the packets can be classified based on their 802.1p priorities.

The S5700 adopts a hardware classifier to guarantee line-speed transmission of services data on interfaces.

Simple Traffic Classification

On the S5700SI and S5700EI, you can perform simple traffic classification for packets according to the mapping between priorities of packets and Per-Hop Behaviors (PHBs). If packets come from an upstream device, the S5700SI and S5700EI maps priorities of the packets to PHBs and colors. On the S5700SI and S5700EI, congestion management is performed for packets according to PHBs of packets and congestion avoidance is performed for packets according to colors of packets. The downstream device provides QoS services according to the priorities of packets.

On the S5700HI and S5700-6TP-LI-AC, you can perform simple traffic classification for packets according to the mapping between priorities of packets and Per-Hop Behaviors (PHBs) defined in a Differentiated Services (DiffServ) domain. If packets come from an upstream device, the S5700HI and S5700-6TP-LI-AC binds a DiffServ domain to the incoming interface. In the DiffServ domain, the S5700HI and S5700-6TP-LI-AC maps priorities of the packets to PHBs and colors. On the S5700HI and S5700-6TP-LI-AC, congestion management is performed for packets according to PHBs of packets and congestion avoidance is performed for packets according to colors of packets. If packets are sent to a downstream device, the S5700HI and

S5700-6TP-LI-AC binds a DiffServ domain to the outgoing interface. In the DiffServ domain, the S5700HI and S5700-6TP-LI-AC maps PHBs and colors of the packets to priorities. Then, the downstream device provides QoS services according to the priorities of packets.

Simple traffic classification is based on:

- DiffServ Code Point (DSCP) priority of IP packets
- 802.1p priority of VLAN packets

Complex Traffic Classification

You can perform complex traffic classification according to Layer 2 or Layer 3 information in packets or through access control lists (ACLs). Then, you can bind a traffic classifier to a traffic behavior to process packets matching the traffic classifier.

The traffic behavior adopted is related to the current phase of packets and the current load of a network. For example, when packets enter an S5700, the S5700 performs traffic policing and access control for the packets according to the committed information rate (CIR); when packets exit an S5700, the S5700 shapes the traffic of packets and re-marks the priorities of packets.

Complex traffic classification is based on:

- 802.1p priority of VLAN packets
- VLAN ID of packets
- Double tags in VLAN packets

  NOTE

  The S5700SI does not support complex traffic classification according to double tags in VLAN packets.
- Incoming or outgoing interface

  NOTE

  The S5700SI does not support complex traffic classification according to the outbound interface.
- IP priority of IP packets
- DSCP priority of IP packets
- SYN Flag field in Transmission Control Protocol (TCP) packets
- Source MAC address
- Destination MAC address
- Protocol type field encapsulated in Layer 2 packets
- Layer 3 protocol type
- IP quintuple

4.5.2 Access Control and Re-marking

After traffic classification, the S5700 performs access control on the packets, that is, permits or denies the packets. Then, the S5700 re-marks the following fields in the packets:

- 802.1p field, that is, the PRI field in a VLAN tag
- DSCP field
- Precedence field of IP packets
- Local precedence

- VLAN ID, that is, the outer VLAN ID or inner VLAN ID of QinQ packets
- Destination MAC addresses

4.5.3 Traffic Policing

The S5700 uses the token bucket algorithm to control the Committed Access Rate (CAR) of network traffic.

The S5700 controls the rate of traffic by adjusting the rate of placing tokens. Each token equals a forwarding rate of 64 kbit/s. The S5700 "punishes" the excessive traffic to limit the incoming traffic within a proper range and to protect the network resources.

4.5.4 Congestion Management

The S5700 manages traffic congestion through queue scheduling. Each outbound interface on the S5700 is configured with eight queues. After traffic classification, packets are sent to the corresponding queues based on their priorities.

The S5700 provides the following queue scheduling policies:

- Priority Queuing(PQ)
- Weight Round Robin(WRR)
- Deficit Round Robin(DRR)
- PQ + WRR
- PQ + DRR

4.5.5 Congestion Avoidance

Congestion avoidance is a flow control technology that relieves overload on a network by adjusting the network traffic. By monitoring the network resources in use, such as queues and memory buffers, the S5700 automatically discards packets when congestion occurs or tends to aggravate.

S5700SI and S5700EI

The S5700EI adopts the Simple Random Early Detection (SRED) technology to avoid congestion. After traffic classification, the S5700EI marks packets with two types of drop precedence. Packets with low request for QoS are marked with high drop precedence, and the other packets are regarded as normal packets. Based on the drop precedence of the packets, the S5700EI can discard packets to adjust the rate of the outbound traffic sent from its interfaces.

The SRED is not available on S5700SI. S5700SI adopts tail drop to avoid congestion.

4.5.6 Rate Limit on an Interface

Rate limit on an interface is used to adjust the rate of traffic on an outbound interface or inbound interface to prevent burst traffic. The S5700 uses the token bucket and a buffer to limit the traffic rate on an outbound interface, implementing traffic shaping. When the rate of packets exceeds the rate limit, the S5700 buffers excessive packets and sends them when the traffic rate falls below the limit. In this manner, the transmission rate is smoothed.

4.5.7 Two-Rate-Three-Color

The S5700 controls traffic according to the result of traffic classification and discards the excessive packets. The S5700 supports two-rate-three-color. You can set the following parameters on the S5700:

- Committed Information Rate (CIR), which is the allowed rate at which traffic can pass through
- Committed Burst Size (CBS), which is the maximum size of traffic that can pass through
- Peak Information Rate (PIR), which is the peak rate at which traffic can pass through
- Peak Burst Size (PBS), which is the peak size of traffic that can pass through

In addition, the S5700 can mark packets red, green, or yellow according to traffic volume, and map behaviors to the colors, such as forwarding or discarding the packets. The S5700 can also re-mark packets.

4.5.8 Aggregate CAR

NOTE

Aggregate CAR is not available on S5700HI and S5700-6TP-LI-AC.

Aggregate CAR is the CAR applied to multiple interfaces to implement traffic policing for service flows on the interfaces. The sum of rate limits on the interfaces must be equal to or smaller than the aggregate CAR.

4.6 Security

The S5700 guarantees both device security and service security.

4.6.1 Device Security

Hierarchical Command Protection

When a user logs in to the S5700 from an Ethernet interface through Telnet, the S5700 authenticates the user to ensure security. The user can configure and maintain the S5700 only after passing the authentication.

The S5700 adopts a hierarchical protection mode for commands. Commands are classified into the visit level, monitoring level, configuration level, and management level, with their levels in ascending order. Login users are also classified into four levels, corresponding to the four levels of commands. After logging in to the S5700, a user can run only the commands at the same or lower level. This mode effectively controls the user authority.

The S5700 extends command levels and user levels to 16 levels so that users are managed more refinedly.

Remote SSH Login

The S5700 supports the Secure Shell (SSH). On an insecure network, SSH provides powerful security guarantee and authentication for login users and can defend against various attacks.

Encrypted Authentication Through SNMPv3

The S5700 supports encrypted authentication through SNMPv3. When S5700 is managed by an NMS workstation through SNMP, it adopts the encrypted authentication mode in user-based security mode (USM) to ensure security.

AAA

The S5700 supports the Authentication, Authorization, and Accounting (AAA). Using AAA and hierarchical command protection, the S5700 can authenticate and authorize login users. In addition, it can authenticate the NMS administrator. AAA effectively prevents unauthorized users from logging in to the S5700.

The S5700 supports authentication methods such as local authentication, RADIUS authentication, and HWTACAS+ authentication.

CPU Channel Protection

The S5700 can filter the protocol packets and management packets sent to the CPU based on the protocol ID, interface, and combination of interface and VLAN. This protects the CPU channels against Denial of Service (DoS) attacks.

Limit of MAC Address Learning on Interfaces

You can set the maximum number of MAC addresses learned by an interface on the S5700 to prevent hackers from initiating source MAC address attack from the interface. This ensures that the MAC address entries of the S5700 will not be used up.

4.6.2 Service Security

VLAN

The S5700 supports the division of a LAN into multiple VLANs. Devices on different VLANs cannot communicate with each other. This isolates broadcast domains and improves service security.

Blackhole MAC Address Entry

The S5700 supports blackhole MAC address entries. When receiving a packet, the S5700 compares the source or destination MAC address of the packet with its MAC address entries. If the source or destination MAC address of packet is the same as a blackhole MAC address, the S5700 discards the packet.

When detecting attacking packets from a MAC address, you can set a blackhole MAC address entry on the S5700 to filter out the packets with the MAC address.

MAC Table Searching Based on VLAN+MAC

The S5700 supports MAC table searching based on VLANs and MAC addresses to improve interface security. You can add static MAC address entries in the MAC table to map specific MAC addresses to interfaces. In this way, specific devices are bound to interfaces so that hackers cannot attack the S5700 by using fake MAC addresses.

Port Isolation

Port isolation prevents ports on the same S5700 from sending Layer 2 packets to each other. The S5700 supports unidirectional and bidirectional port isolation. Port isolation ensures security of user networks and helps to construct low-cost intelligent community networks. Port isolation also limits unnecessary broadcast packets and thus increases network throughput.

Packet Filtering

Packet filtering is used to filter out invalid or unwanted packets.

The S5700 filters packets based on user-defined rules. For example, it filters packets by checking the MAC address, IP address, port number, and VLAN ID of packets. Packet filtering does not check the session status or analyze the data. By filtering packets, the S5700 can effectively control the packets passing through it.

4.6.3 Security Authentication

The 802.1x protocol is a port-based network access control protocol. It authenticates and controls access devices on a LAN based on interfaces. A user device can access resources on the LAN only after it passes the authentication on the access interface.

MAC address-based authentication controls the network access authority of a user based on the access interface and MAC address of the user. The user does not need to install any authentication client software. After detecting the MAC address of the user for the first time, the device starts authenticating the user. During the authentication, the user does not need to enter the user name or password.

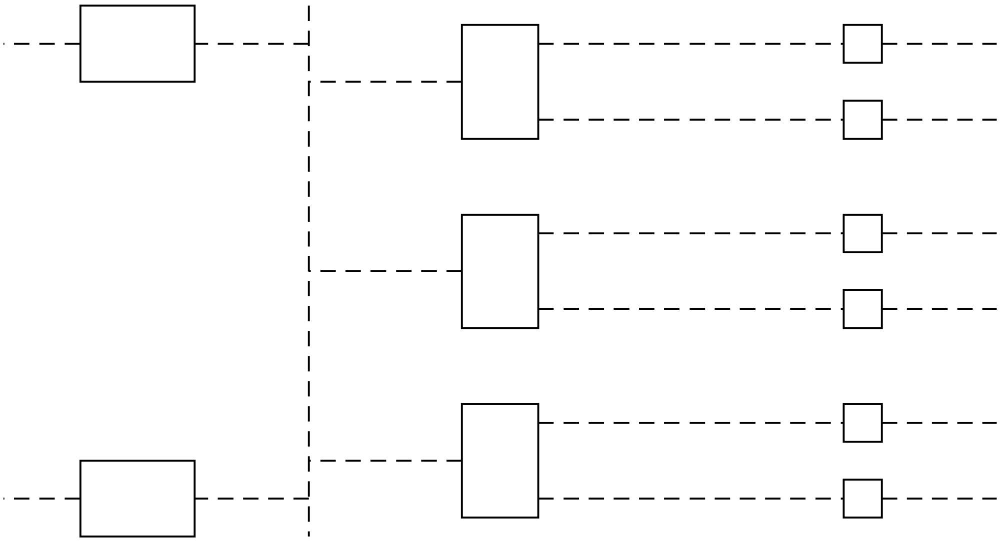
4.7 MAC-Forced Forwarding

The access layer provides network connections between the user-side hosts and the enterprise-side access routers (ARs), especially the reliable connections between the hosts with the Internet or other IP networks.

The access layer can be divided into the user network and convergence network. The user network is connected to the access node (AN) through a subscriber line, which is a physical line and usually called "the first mile."

The subscriber line is then connected to the convergence network through the AN. In this manner, the AN is the border between the subscriber line and the convergence network. User traffic is centralized and aggregated on the convergence network, which is usually called "the second mile." For details, see **Figure 4-1**.

Figure 4-1 Connections at the access layer



At the access layer, the enterprise has the following requirements:

- In order that the enterprise uses the AR to perform secure filtering, policy scheduling, and accounting for the traffic, the ARs need to perform Layer 3 forwarding for the traffic of different user hosts in different networks. The ARs, however, cannot forward packets through Layer 2 switching.
- The efficiency of address assignment needs to be improved to save IPv4 addresses. The effectiveness of address assignment needs to be improved if an address is assigned from a large address pool rather than a small and independent network segment to the host.

To implement user isolation at the access layer and meet the preceding requirements of the enterprise, the MAC-Forced Forwarding (MFF) protocol is introduced.

MFF is a security protocol that isolates the user hosts accessing the same device. When MFF is running, its security program applies to any shared access media, bringing no extra problems to these networks.

In addition to Layer 2 isolation, the AN that runs MFF discards any upstream broadcast packets except for DHCP packets and ARP request packets. The AN discards DHCP response packets received through the subscriber line and limits the rate of DHCP broadcast packets.

The AN that runs MFF must track the IPv4 addresses allocated to the subscriber line. This is to discard the upstream traffic with the fake IPv4 source addresses.

4.8 DHCP

NOTE

The DHCP Server and DHCP Relay are not available on S5700-6TP-LI-AC switches.

DHCP Client and DHCP Server

DHCP adopts the client/server mode, that is, the DHCP client sends request messages to the DHCP server. Then, the DHCP server returns the reply messages according to the address pool policy.

The DHCP server assigns an IP address to the client by using an address pool. When the client sends a DHCP request to the server, the DHCP server selects a proper address pool, finds an idle IP address from the pool, and delivers the IP address along with other related parameters, such as the gateway address, the DNS address and the address lease, to the client.

To dynamically allocate IP addresses to clients, you need to first configure the address pool range on the DHCP server. Currently, an address pool can be configured with only one address range and the address range is determined by the mask length.

DHCP Snooping

The S5700 can be deployed between the DHCP server and the DHCP client and it monitors the DHCP messages between the DHCP server and the DHCP client. The S5700 creates the IP +MAC+PORT+VLAN binding table according to the monitoring result to filter out invalid packets.

The S5700 also supports Option 82.

- After receiving a Request message from the DHCP client, the S5700 appends the Option 82 field to the Request message. The DHCP server enforces the IP address allocation policy according to the Option 82 field.
- The DHCP server appends the Option 82 field to a Response message. The S5700 analyzes the Option 82 field, determines a forwarding interface, removes the Option 82 field, and then forwards the message to a user.

Option 82 can be implemented in two modes on the S5700, Option 82 insert and Option 82 rebuild.

The S5700HI can be configured to discard DHCP packets with multi-layer Option 82 fields.

The Option 82 field contains the user circuit IDs. The user circuit IDs include user device name, outer VLAN ID, inner VLAN ID and port number etc. This can effectively prevent attackers from modifying the DHCP messages.

DHCP Relay

The DHCP client and the DHCP server send broadcast packets during the allocation of IP addresses. Therefore, DHCP can be applied only when the DHCP client and DHCP server are in the same subnet. It is a waste of resource to deploy a DHCP server in each network segment.

The DHCP relay is introduced to solve this problem. Through DHCP relay, a DHCP client in a subnet can communicate with the DHCP server in another subnet and finally obtains an IP address. In this manner, the DHCP clients on different network segments can use the same DHCP server. This reduces costs and achieves centralized management.

4.9 Network-Level HA

4.9.1 MSTP Protective Switchover

The S5700 supports MSTP to eliminate broadcast storms on a network and provide redundant links for data transmission.

The S5700 provides the root protection function. To retain the role of the root device, you need to set the role of a designated interface to remain unchanged when the interface receives a BPDU with higher priority. This prevents incorrect change of the network topology.

The S5700 provides the loop protection function. If the root interface cannot receive any BPDU from the upstream device, the root interface enters the blocking state and stops forwarding packets. At the same time, no new root interface is elected. This prevents loops on the network.

4.9.2 RRPP Rapid Protective Switchover

An RRPP ring is applied to the protected dual-homed networks. The RRPP ring can be deployed between CEs and UPEs, or between UPEs and NPEs.

An RRPP ring is composed of a master node and multiple transit nodes that are connected to each other. The master node periodically sends out protocol packets from the primary interface to monitor the link status. If the link fails, the master node can enable the secondary interface to realize self-healing.

If a single-point failure occurs on the ring, the RRPP can enable the backup link as soon as possible and the link among nodes can recover quickly.

4.9.3 Smart Link Dual-Homing Protection

The S5700 is dual-homed to an upstream device through the Smart Link technology. The downstream links of the S5700 form a Monitor Link group. The layer-by-layer connection of convergence implements association between Smart Link and Monitor Link. When no upstream links exist, the S5700 disables the downstream interface and switches traffic between different paths through the interface association mechanism.

4.9.4 Ethernet OAM

Conforming to IEEE 802.3ah, the S5700 supports the point-to-point Ethernet fault management to detect faults in the first mile of the directly connected link on the user side of the Ethernet. At present, the S5700 supports the following functions defined in IEEE 802.3ah:

- OAM discovery
- Link monitoring
- Fault notification
- Remote loopback

The S5700 provides end-to-end Ethernet OAM complying with IEEE 802.1ag to detect connectivity faults on a network. The S5700 supports end-to-end connectivity fault detection, fault notification, fault verification, and fault location.

The S5700 provides the performance management function. Performance management is used to measure the packet loss ratio, delay, and jitter during packet transmission, and collect statistics on various types of packets. Performance management is performed at the user access points. By using performance management tools, a carrier can monitor the network running status and locate faults through the network management system. The carrier can then check whether the forwarding capacity of the network complies with the Service Level Agreement (SLA) signed with users.

Ethernet OAM improves management and maintenance capabilities on the Ethernet and guarantees a stable network.

The S5700-28C-HI, S5700-28C-HI-24S, and S5700-6TP-LI-AC support high-performance IEEE 802.1ag based on hardware.

4.10 LLDP

The S5700 supports the Link Layer Discovery Protocol (LLDP) that conforms to IEEE 802.1ab. LLDP is a link layer protocol used for interconnected devices to obtain the connection information of each other.

Using LLDP, the local NMS can obtain the link layer information of all devices on the local network and details about the network topology. Thus the NMS can manage a larger area on the network.

The LLDP-enabled interfaces on the S5700 periodically notify the neighbors of its own status. If the status of an interface changes, the interface sends status update messages to the directly connected neighboring device. The neighboring device stores the status update message in the standard SNMP MIB. Then the NMS can obtain the link layer information of the network from the MIB to calculate the topology of the entire network.

4.11 NQA

With the development of value-added services, users and carriers demand increasingly high QoS. After voice over IP and video over IP services are launched, carriers and users all tend to sign Service Level Agreements (SLAs). To show whether the committed bandwidth meets users' requirement, network carriers need to know the network performance in time according to statistical parameters such as the delay, jitter, and packet loss ratio on network devices.

The S5700 supports Network Quality Analysis (NQA). NQA tests the performance of different protocols running on a network so that carriers can collect the network performance indexes of networks in real time, such as the total delay of the Hypertext Transfer Protocol (HTTP) service, delay in the Transmission Control Protocol (TCP) connection, file transmission speed, and delay in File Transfer Protocol (FTP) connection. By controlling these indexes, carriers can provide network services of different levels and charge services differently. NQA is also an effective tool for diagnosing and locating faults on a network.

4.12 Cluster Management

The Huawei Group Management Protocol (HGMP) is a Huawei proprietary protocol used to manage multiple S5700s or other switches through one S5700. In HGMP implementation, the Neighbor Discovery Protocol (NDP) is used to collect information about directly connected neighbors including the device type, software version, hardware version, connected interface, and member ID. The Network Topology Discovery Protocol (NTDP) is used to collect topology information.

As defined in HGMP, a management domain (namely a cluster) consists of a command switch and multiple member switches. The S5700 can function as a command switch or a member switch.

- Member switch

A member switch is managed by the command switch. Member switches are usually Layer 2 switches and do not need public IP addresses. When the S5700 functions as a member switch, it is managed by a high-end device.

- Command switch

  The command switch functions as the proxy of the external network management station or server to manage the member switches of a cluster. It has a public IP address and can manage other switches.

In actual application, the S5700 usually functions as a command switch to manage a large number of member switches on a residential network in a centralized manner.

- Automatically detects new remote devices and adds them to the cluster.
- Collects and maintains the network topology information from the member switches in the cluster.
- Provides methods of batch configurations and upgrade for member switches in the cluster.

HGMP saves IP addresses by managing devices in a cluster.

4.13 Stacking

NOTE

The S5700-28C-HI, S5700-28C-HI-24S, and S5700-6TP-LI-AC do not support stacking.

Stacking means that the switches located in the same place are connected through the stacking cable or high-speed uplink interfaces, and thus the switches form a reliable switch group. In a switch group, the S5700s are connected through the stack interfaces. Through stacking, the user can manage and maintain the switches uniformly; therefore, the stacking reduces the maintenance cost of the user.

The stacked switches have three roles:

- Master switch

  A stack has only one master switch. The master switch manages the entire stack system by assigning stack IDs to member switches, collecting information about the stack topology, and notifying all the member switches of the information.

- Backup switch

  As the backup of the master switch, the backup switch becomes the master if the master switch is faulty and takes over the work of the master switch.

- Slave switch

  A slave switch only processes service traffic on the network and is managed by the master switch.

4.14 Web Server

Users can manage network devices through the GUI provided by the Web Server. This reduces requirements for junior maintenance personnel.

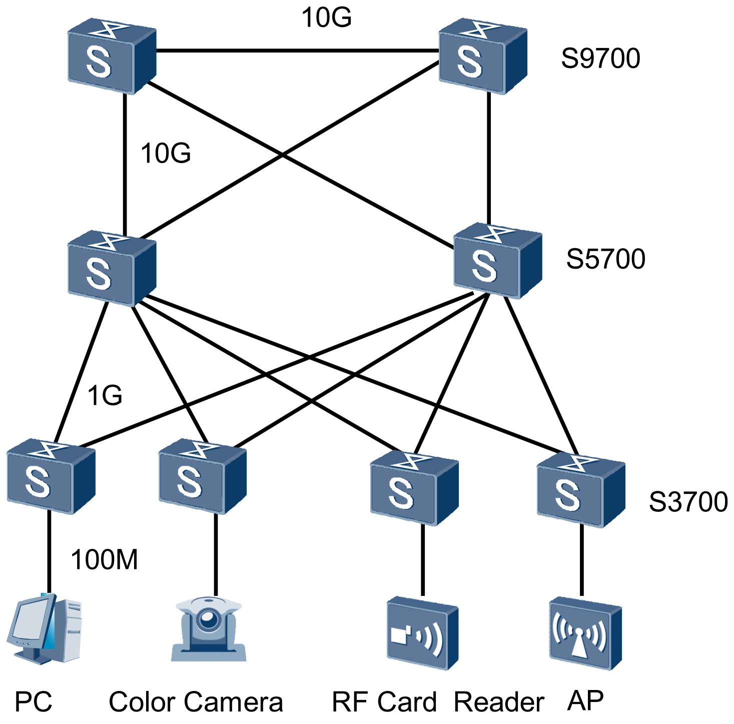
5 Networking and Applications

About This Chapter

5.1 Aggregation Device of Enterprise Network or Campus Network

On the enterprise network or campus network shown in **Figure 5-1**, the S5700s connect to access switches using 1000 Mbit/s interfaces, and connect to core switches S5700s using 10 Gbit/s optical interfaces or 10 Gbit/s electrical interfaces. The network provides 10 Gbit/s rate for the backbone layer and 100 Mbit/s access rate for terminals. This solution provides high bandwidth and meets multi-service requirements.

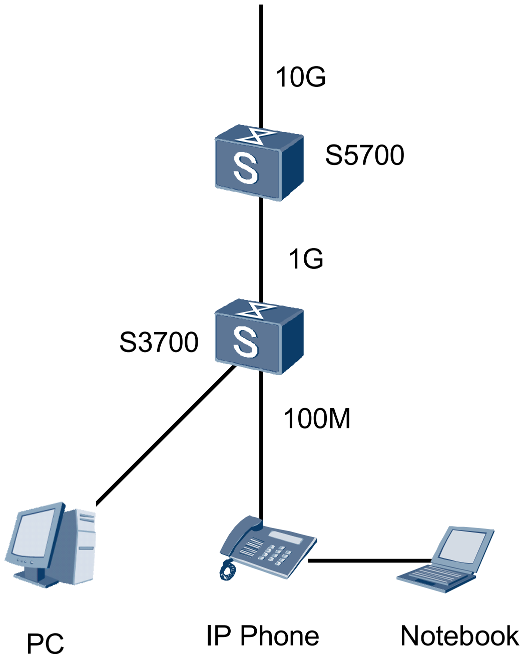
Figure 5-1 Aggregation device of enterprise network or campus network



5.2 Desktop Aggregation

As shown in **Figure 5-2**, the S5700 provides the functions such as PoE, voice VLAN and NAC. The S5700 can be used for desktop access and provides 1000 Mbit/s access rate.

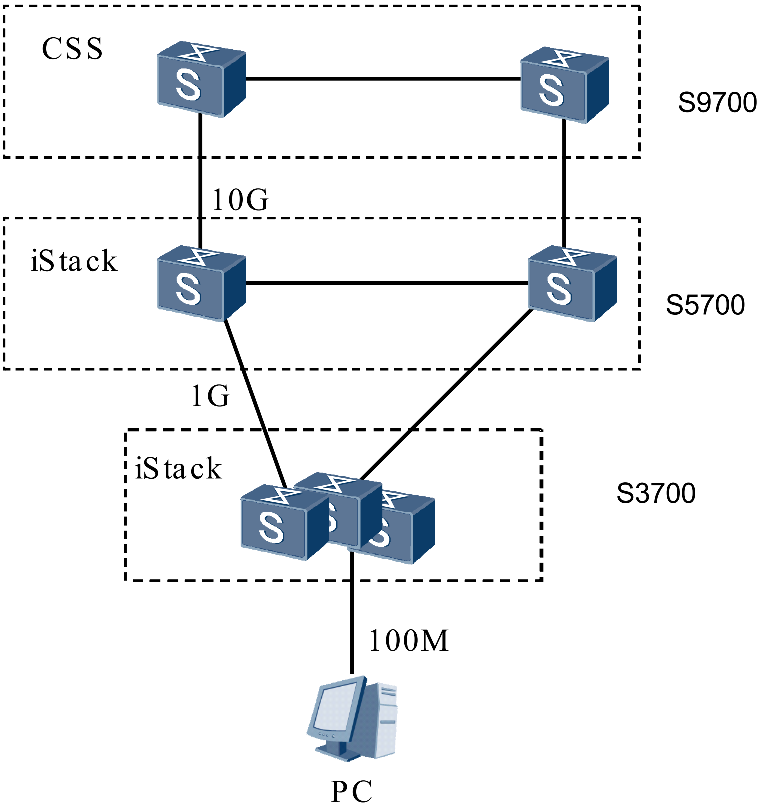
Figure 5-2 Desktop aggregation



5.3 iStack

As shown in **Figure 5-3**, iStack improves performance and reliability of the access layer and aggregation layer. The S5700s use the iStack technology to form a stack system, implementing the distributed forwarding structure and fast fault recovery. The stack system increases the number of user interfaces and improves packet processing capability. The iStack-enabled S5700s can be managed in a uniform manner to facilitate network management and maintenance.

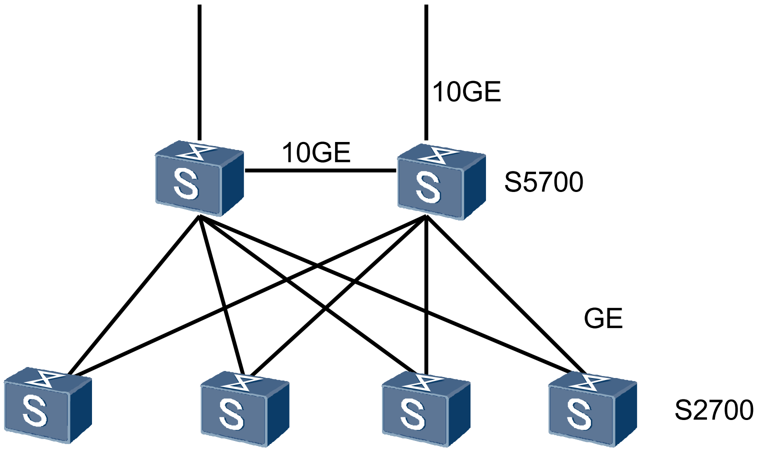
Figure 5-3 iStack



5.4 Core Device for Small Enterprise Network

As shown in **Figure 5-4**, the S5700s functioning as core switches on the small-sized enterprise network have powerful aggregation and routing capabilities.

Figure 5-4 Core device for small-sized enterprise network



6 Maintenance and Network Management System

About This Chapter

6.1 Maintenance and Management

6.1.1 Various Configuration Methods

Configuration Modes

The S5700 supports the following configuration and management modes:

- Command line

  A user connects to the console port of the S5700 through the console terminal, and then configures various functions and sets parameters in the command line interface (CLI).

- Network management station

  A user configures and manages the S5700 through the SNMP protocol.

- HGMP

  A user logs in to the S5700 to manage Layer 2 switches or other S5700s in the same cluster based on HGMP.

Login Modes

The S5700 provides a console port. A user can connect to the console port through the serial port on a console terminal, and then configure the S5700 locally or remotely.

In addition, the user can telnet to the service interface of the S5700 for configuration and management.

The S5700 supports multiple authentication modes, including non-authentication, local authentication, and AAA.

6.1.2 Monitoring and Maintenance

Hardware Monitoring

The S5700 provides the following hardware monitoring functions:

- Provides the re-detection function to prevent incorrect detection because of instant interference.
- Checks version matching automatically when the system is running.
- Sends the Dying gasp trap to the upper-layer device before power-off.

Device Management and Maintenance

The S5700 provides various management and maintenance functions:

- Provides flexible online help for the command line in Chinese or English.
- Provides hierarchical commands and user authority management.
- Provides an information center to uniformly manage logs, traps, and debugging information and redirects information as required.

- Provides the electronic labels. A user can view the basic information about the SCU and optical modules through the CLI, and back up the information to an external server through FTP.
- Supports the display of the software version, module status, ambient temperature, CPU usage, and memory usage.

6.1.3 Diagnosis and Debugging

Ping and TraceRoute

On traditional IP networks, the S5700 provides the following tools to check network connectivity:

- Ping
- TraceRoute

These tools are used to test network connectivity and record transmission paths of packets to assist fault location.

Debugging

The S5700 provides various debugging commands for each software feature. Each debugging command supports multiple parameters and can be flexibly controlled. The debugging commands display the detailed information about processes, packet receiving and sending, and error check during the running of a feature.

Black Box

The S5700 provides the black box function to record information on the feature modules, tasks, and events. In addition, the black box records the final results, process status, and function calling track to facilitate fault location.

VCT

A user can run the VCT commands on the switch. According to Time Domain Reflectometry (TDR) theory, an interface can receive the reflected signal after transmitting the test signal. Then the user can know the cable status according to the characteristics of the reflected signal.

Mirroring

The S5700 supports interface- or flow-based mirroring.

- Port mirroring

  The incoming traffic, outgoing traffic, or both incoming and outgoing traffic at an observed interface is completely copied to an observing interface.
- Flow mirroring

  The traffic at an observed interface is completely copied to an observing interface.

By connecting a monitoring host to an observing interface on the S5700, a network administrator can easily observe the packets that pass through the S5700 in real time. The mirroring result serves as a basis for traffic detection, fault location, and data analysis.

6.1.4 Software Upgrade and In-Service Patching

Software Upgrade

The S5700 can detect the integrity and validity of the system software before the upgrade and provides various methods of upgrading the software:

- Local upgrade

  When the S5700 is powered on, the software can be loaded and upgraded through the BootROM menu.
- Remote in-service upgrade

  When the S5700 runs normally, it can download the software through FTP or TFTP. The new software is run when the S5700 is restarted. This realizes the remote seamless software upgrade.

The S5700 supports rollback to the previous version in case of upgrade failure.

In-Service Patching

The S5700 supports in-service patching to protect services from being affected when a patch is installed. The software can be restored to the earlier version, and the device data before and after in-service patching is recorded.

6.1.5 Hardware Fault Handling

The S5700 supports automatic and manual intervention when a hardware fault occurs, for example, a chip on a board fails. The maintenance personnel can locate a hardware fault and handle it quickly to shorten service interruption.

6.2 U2000 Network Management System

The S5700 uses the Huawei U2000 as a centralized NMS. The U2000 supports a multi-language graphical user interface (GUI) for convenient and visualized operations. The U2000 also provides northbound interfaces for connecting to a third-party NMS so that it can work with other NMSs of carriers.

6.2.1 Network Management Modes

The NMS can manage the S5700 in two modes: inband and outband.

Inband Management

In inband management mode, the network management information is transmitted through the service channel of the S5700, and no additional communications network is required between the NMS and the S5700. The network administrator simply needs to connect the NMS to the adjacent network devices and set the SNMP parameters.

The inband management mode features flexible networking and does not rely on geographical locations. In addition, it guarantees the channel security better than the outbound management mode. However, the network management information consumes bandwidth of the service channel. And if the service channel fails, the NMS cannot manage the S5700 remotely.

Outband Management

In outbound management mode, an independent network needs to be set up between the S5700 and the NMS so that the network management information is separated from the service information.

This mode ensures reliable transmission of the network management information and the NMS can still manage the S5700 when the service channel fails. However, the independent NMS network is limited by geographical locations.

6.2.2 U2000

The U2000 can display the software version, and save and restore configuration files and VRP mapping programs. The U2000 also supports in-service patching for the S5700 through CLI.

The U2000 provides the following functions.

Resource Management

The U2000 provides resource management to help you easily manage network resources including devices, boards, interfaces, and links on a large and complicated network. Through the U2000, you can query and manage resources of the S5700 and locate abnormal resources on the network.

View Management

The U2000 provides a unified topology view of all devices on a network to help you obtain network information directly and conveniently. The U2000 provides a powerful topology management function. You can browse device information in the system topology view, protocol topology view, and user-defined view. In addition, the U2000 provides friendly interfaces for operation and maintenance of the network and devices.

The protocol topology views include the HGMP view and Ethernet view, which cover the topologies of various networking modes and network layers of the S5700. These views support automatic topology discovery to reflect changes of the network topology and device status in real time.

Configuration Management

Configuration management is used to configure the S5700 and it supports management of devices, interfaces, VLANs, Layer 2 features, software upgrade, and configuration files. the U2000 provides personalized configuration modes such as end-to-end configuration, batch configuration, and configuration wizard, and provides default configuration templates.

Fault Management

Fault management is an important and commonly used management method for maintaining networks. Through the GUI, you can query and monitor the running status and faults of the S5700 in real time, filter faults, locate faults, confirm faults, and analyze faults. The U2000 can generate alarm sounds or display alarms on the alarm panel. It can be connected to an alarm box for convenient routine maintenance.

Performance Management

The U2000 can collect performance data, monitor the device performance, and analyze the collected data. It provides various reports and charts about device performance. In addition, the

U2000 can display the CPU usage, memory usage, and device ports. The U2000 collects statistics about device load and user access so that you can know the QoS of the network and thus assess and adjust network resource configuration in time.

Performance management serves resource management, and performance data is displayed on the GUI in iWeb mode.

Security Management

The U2000 provides various measures for security management. Users are authenticated uniformly on the U2000 and their operation authority is configured based on the minimum granularity principle. The U2000 authenticates users strictly to ensure system security. It also provides detailed operation logs for you to query and analyze user operations.

Security management supports user management, access control, user group management, and operation management.

6.3 iTec

The S5700 supports the U2000 and iTec network management systems. The iTec network management system manages the enterprise networks.

iTec has the following features:

- Managing devices of other vendors: It manages the devices of other vendors.
- Managing services specifically: It analyzes network flows and focuses on core services.
- Managing IT and IP devices: It manages application software, IT devices (such as servers and printers), and network devices.
- User-oriented operating and maintenance system: It ensures the security for desktop access and performs authentication, authorization, and accounting (AAA) on network access users.
- Secondary development platform: It provides a secondary development platform for customizing the network management functions.
- Northbound integration: It can work with the upper-layer OSS system.

7 System Technical Specifications

About This Chapter

7.1 Physical Specifications

Table 7-1 Physical specifications

Item	Description
Dimensions (width x depth x height)	● S5700-24TP-SI-AC: 442.0 mm x 220.0 mm x 43.6 mm ● S5700-24TP-SI-DC: 442.0 mm x 220.0 mm x 43.6 mm ● S5700-28C-EI-24S: 442.0 mm x 420.0 mm x 43.6 mm ● S5700-28C-EI: 442.0 mm x 420.0 mm x 43.6 mm ● S5700-28C-PWR-EI: 442.0 mm x 420.0 mm x 43.6 mm ● S5700-28C-SI: 442.0 mm x 420.0 mm x 43.6 mm ● S5700-52C-EI: 442.0 mm x 420.0 mm x 43.6 mm ● S5700-52C-PWR-EI: 442.0 mm x 420.0 mm x 43.6 mm ● S5700-52C-SI: 442.0 mm x 420.0 mm x 43.6 mm ● S5700-48TP-SI-AC: 442.0 mm x 420.0 mm x 43.6 mm ● S5700-48TP-SI-DC: 442.0 mm x 420.0 mm x 43.6 mm ● S5700-24TP-PWR-SI: 442.0 mm x 420.0 mm x 43.6 mm ● S5700-48TP-PWR-SI: 442.0 mm x 420.0 mm x 43.6 mm ● S5700-28C-HI: 442.0mm×220.0mm×43.6mm ● S5700-28C-HI-24S: 442.0mm×220.0mm×43.6mm ● S5700-6TP-LI-AC: 250.0mm×180.0mm×43.6mm

Item		Description
Maximum power (full configuration)		● S5700-28C-EI: 60W ● S5700-52C-EI: 88W ● S5700-28C-EI-24S: 63W ● S5700-28C-SI: 56W ● S5700-52C-SI: 78W ● S5700-24TP-SI-AC: 40W ● S5700-24TP-SI-DC: 40W ● S5700-48TP-SI-AC: 64W ● S5700-48TP-SI-DC: 64W ● S5700-24TP-PWR-SI: 455 W (Dissipated power: 85 W, PoE: 370 W) ● S5700-48TP-PWR-SI: 907 W (Dissipated power: 167 W, PoE: 740 W) ● S5700-28C-PWR-EI: 842 W (Dissipated power: 102 W, PoE: 740 W) ● S5700-52C-PWR-EI: 930 W (Dissipated power: 190 W, PoE: 740 W) ● S5700-28C-HI: 89W ● S5700-28C-HI-24S: 91.6W ● S5700-6TP-LI-AC: 30W
Weight	Full configuration	⩽ 8.5 kg
	Empty chassis	⩽ 5 kg
DC input voltage	Rated voltage	–48V DC to –60V DC
	Maximum voltage	–36V DC to –72V DC
AC input voltage	Rated voltage	100V AC to 240V AC
	Maximum voltage	90V AC to 264V AC
Temperature	operating temperature	S5300SI, S5300EI: 0°C to 50°C S5700-6TP-LI-AC: -5°C to 55°C (Altitude: 0 m to 2000 m); S5700HI: -5°C to 55°C (Altitude: 0 m to 1800 m) **NOTE** ● For S5700HI, if using 40km SFP+ optical module, the operating temperature of S5700HI is between -5°C and 45° C.
	Storage temperature	-40°C to 70°C
Relative humidity		10%RH to 90%RH

Item	Description
Altitude	S5706TP-LI-AC: 0 m to 2000 m S5700SI\S5700EI: 0 m to 2000 m S5700HI: 0 m to 4000 m

7.2 Optical Module Attributes

Table 7-2 Attributes of the SFP (FE) optical module

Attribute	Specification
Transmission distance	2 km
Center wavelength	1310 nm
Transmitting power	-19.0 dBm to -14.0 dBm
Receiver sensitivity	-30.0 dBm
Overload power	-14.0 dBm
Extinction ratio	10 dB
Type of the optical connector	LC
Fiber type	Single mode

Table 7-3 Attributes of the ESFP (FE) optical module

Attribute	Specification				
Transmission distance	15 km	15 km (single-mode bidirectional fiber)	15 km (single-mode bidirectional fiber)	40 km	80 km
Center wavelength	1310 nm	Sending: 1310 nm Receiving: 1550 nm	Sending: 1550 nm Receiving: 1310 nm	1310 nm	1550 nm

Attribute	Specification				
Transmitting power	-15.0 dBm to -8.0 dBm	-15.0 dBm to -8.0 dBm	-15.0 dBm to -8.0 dBm	-5.0 dBm to 0 dBm	-5.0 dBm to 0 dBm
Receiver sensitivity	-31.0 dBm	-32.0 dBm	-32.0 dBm	-34.0 dBm	-34.0 dBm
Overload power	-8.0 dBm	-8.0 dBm	-8.0 dBm	-10.0 dBm	-10.0 dBm
Extinction ratio	8.2 dB	8.5 dB	8.5 dB	10.0 dB	10.0 dB
Type of the optical connector	LC	LC/PC	LC/PC	LC	LC
Fiber type	Single mode	Single mode	Single mode	Single mode	Single mode

Table 7-4 Attributes of the ESFP (GE) optical module

Attribute	Specification							
Transmission distance	0.5 km	10 km	10 km (single-mode bidirectional fiber)	10 km (single-mode bidirectional fiber)	40 km	40 km	80 km	100 km
Center wavelength	850 nm	1310 nm	Sending: 1310 nm Receiving: 1490 nm	Sending: 1490 nm Receiving: 1310 nm	1550 nm	1310 nm	1550 nm	1550 nm
Transmitting power	-9.5 dBm to -2.5 dBm	-9.0 dBm to -3.0 dBm	-9.0 dBm to -3.0 dBm	-9.0 dBm to -3.0 dBm	-5.0 dBm to 0 dBm	-5.0 dBm to 0 dBm	-2.0 dBm to 5.0 dBm	0 dBm to 5.0 dBm
Receiver sensitivity	-17.0 dBm	-20.0 dBm	-19.5 dBm	-19.5 dBm	-22.0 dBm	-22.0 dBm	-22.0 dBm	-30.0 dBm
Overload power	0 dBm	-3.0 dBm	-3.0 dBm	-3.0 dBm	-3.0 dBm	-3.0 dBm	-3.0 dBm	-9.0 dBm
Extinction ratio	9.0 dB	9.0 dB	6.0 dB	6.0 dB	8.5 dB	9.0 dB	9.0 dB	8.0 dB

Attribute	Specification							
Type of the optical connector	LC	LC	LC	LC	LC	LC	LC	LC
Fiber type	Multi-mode	Single mode	Single mode	Single mode	Single mode	Single mode	Single mode	Single mode

Table 7-5 Attributes of the ESFP (CWDM) optical module

Attribute	Specification							
Transmission distance	80 km	80 km	80 km	80 km	80 km	80 km	80 km	80 km
Center wavelength	1571 nm	1591 nm	1551 nm	1511 nm	1611 nm	1491 nm	1531 nm	1471 nm
Transmitting power	0 dBm to 5.0 dBm	0 dBm to 5.0 dBm	0 dBm to 5.0 dBm	0 dBm to 5.0 dBm	0 dBm to 5.0 dBm	0 dBm to 5.0 dBm	0 dBm to 5.0 dBm	0 dBm to 5.0 dBm
Receiver sensitivity	-28.0 dBm	-28.0 dBm	-28.0 dBm	-28.0 dBm	-28.0 dBm	-28.0 dBm	-28.0 dBm	-28.0 dBm
Overload power	-9.0 dBm	-9.0 dBm	-9.0 dBm	-9.0 dBm	-9.0 dBm	-9.0 dBm	-9.0 dBm	-9.0 dBm
Extinction ratio	8.5 dB	8.5 dB	8.5 dB	8.5 dB	8.5 dB	8.5 dB	8.5 dB	8.5 dB
Type of the optical connector	LC	LC	LC	LC	LC	LC	LC	LC
Fiber type	Single mode							

Table 7-6 SFP+ optical module (10GE) attributes

Item	Description			
Transmission distance	0.22 km	0.3 km	10 km	40 km
Center wavelength	1310 nm	850 nm	1310 nm	1550 nm
Transmitting power	-6.5 dBm to -0.5 dBm	-7.3 dBm to -1.0 dBm	-8.2 dBm to 0.5 dBm	-4.7 dBm to 4.0 dBm
Receiver sensitivity	-6.5 dBm	-11.1 dBm	-12.6 dBm	-14.1 dBm
Overload power	1.5 dBm	-1.0 dBm	0.5 dBm	-1.0 dBm
Extinction ratio	-3.5 dB	3.0 dB	3.5 dB	
Connector type	LC			
Fiber type	Multi-mode		Single-mode	

Table 7-7 Attributes of optical/electrical modules

Attribute	Description
Connector	RJ45
Standards compliance	IEEE802.3z
Frame format	Ethernet_II, Ethernet_SAP, or Ethernet_SNAP
Network protocol	IP

7.3 System Configuration

Table 7-8 System configuration

Item	Parameter
Processor	S5700C-EI: 533 MHz S5700C-SI: 800 MHz S5700TP-SI: 800 MHz S5700C-HI: 1GHz S5700-6TP-LI-AC: 1GHz

Item	Parameter
Switching capacity	● S5700-24TP: 48 Gbit/s ● S5700-28C-SI/EI/HI: 128 Gbit/s ● S5700-48TP: 96 Gbit/s ● S5700-52C-SI/EI: 176 Gbit/s ● S5700-6TP-LI-AC: 12Gbit/s
Packet forwarding capacity	● S5700-24TP: 35.71 Mpps ● S5700-28C-SI/EI/HI: 95.2 Mpps ● S5700-48TP: 71.42 Mpps ● S5700-52C-SI/EI: 130.94 Mpps ● S5700-6TP-LI-AC: 8.9Mpps
DDR memory	512M for S5700C-HI and S5700-6TP-LI-AC, and 256 MB for others
Flash Memory	64M for S5700C-HI and S5700-6TP-LI-AC, and 32 MB for others

7.4 List of Software Features

Table 7-9 List of software features supported

Attribute		Description
Ethernet features	Ethernet	● Operating modes, including full duplex, half duplex, and auto-negotiation ● Operating rates of an Ethernet interface, including 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, 10 Gbit/s, and auto-negotiation ● Flow control on interfaces ● Jumbo frames ● Link aggregation ● Load balancing among the links of a trunk ● Interface isolation and forwarding restriction on interfaces ● Suppression of broadcast storms
	VLAN	● Access modes of access, trunk, hybrid, and QinQ ● Default VLAN ● VLAN mapping. ● Selective QinQ ● Voice VLAN ● VLAN switching ● DHCP policy VLAN

Attribute		Description
	MAC	● Automatic learning and aging of MAC addresses ● Static, dynamic, and blackhole MAC address entries ● Packet filtering based on source MAC addresses ● Limitation on MAC address learning on interfaces
	ARP	● Static and dynamic ARP entries ● ARP on a VLAN ● Aging of ARP entries
	SmartLink	● SmartLink ● SmartLink multi-instance ● MonitorLink
	LLDP	LLDP
	NAC	NAC
	VCT	VCT
Ethernet loop protection	MSTP	● STP ● RSTP ● MSTP ● BPDU protection, Root protection, and loop protection ● Partitioned STP and BPDU tunnels
	RRPP	● RRPP protective switchover ● Single RRPP ring, tangent RRPP rings, and intersecting RRPP rings ● Hybrid networking of RRPP rings and other ring networks
IPv4/IPv6 forwarding	IPv4 features	● ARP/RARP ● ARP proxy ● Auto-detection
	Unicast routing	● Static routes ● RIP-1/RIP-2 ● OSPF ● BGP ● IS-IS ● Routing policies and policy-based routes ● uRPF check ● VRF ● DHCP Client/Server/Relay ● DHCP snooping

Attribute		Description
	Multicast routing	● IGMPv1/v2/v3 ● PIM-DM ● PIM-SM ● PIM-SSM ● MBGP ● MSDP ● Multicast routing policy ● RPF
	IPv6 features	● IPv6 protocol stack ● IPv6 unicast routing protocols: RIPng and OSPFv3 ● VRRP6 ● SNMP IPv6 ● IPv4/IPv6 transition technologies
MPLS	Basic MPLS functions	● LDP ● Two-layer MPLS labels ● 802.1p-MPLS EXP mapping
	VLL	SVC/Martini/CCC VLL
Device reliability	BFD	● Basic BFD functions ● BFD for OSPF ● BFD for IS-IS ● BFD for BGP ● BFD for PIM
	Others	VRRP
Layer 2 multicast	Layer 2 multicast	● IGMP snooping ● IGMP proxy ● Prompt leave ● Multicast traffic control ● Inter-VLAN multicast replication ● Controllable multicast
Ethernet OAM	EFM OAM	● Neighbor discovery ● Link monitoring ● Fault notification ● Remote loopback

Attribute		Description
	CFM OAM	● CCM check ● MAC Ping ● MAC Trace ● Hardware-based CCM check (only supported by 5700-28C-HI, 5700-28C-HI-24S, and S5700-6TP-LI-AC)
	Y.1731	● Jitter and latency measurement ● Hardware-based CCM check (only supported by 5700-28C-HI, 5700-28C-HI-24S, and S5700-6TP-LI-AC)
QoS	Traffic classification	● Traffic classification based on the combination of the L2 protocol header, IP quintuple, outgoing interface, and 802.1p field ● Traffic classification based on the C-VID and C-PRI of QinQ packets
	Traffic behaviors	● Access control after traffic classification ● Traffic policing based on traffic classification ● Re-marking based on traffic classification ● Class-based packet queuing ● Combination of traffic classification and traffic behaviors
	Queue scheduling	● PQ ● DRR ● PQ+DRR ● WRR ● PQ+WRR
	Congestion avoidance	● S5700SI and S5700EI: SRED ● S5700HI and S5700-6TP-LI-AC: WRED
	Rate limit on outbound interfaces	Rate limit on outbound interfaces
Configuration and maintenance	Terminal service	● Configurations through command lines ● Help information in English and Chinese ● Login through console and Telnet terminals ● Information exchange between terminals through the send function
	File system	● File system ● Directory and file management ● File upload and download through FTP or TFTP

Attribute		Description
	Debugging and maintenance	● Centralized management of logs, alarms, and debugging information ● Electronic label ● User operation logs ● Detailed debugging information for diagnosing network faults ● Network test tools such as traceroute and ping commands ● Interface mirroring and flow mirroring
	Version upgrade	● Software loading on the entire equipment and online software loading ● Online upgrade of the BootROM ● In-service patching
Security and managem ent	System security	● Hierarchical command line protection to prevent unauthorized users from accessing the S5700 ● SSH v2.0 ● RADIUS authentication and HWTACACS authentication ● ACL filtering ● DHCP packet filtering (with Option 82) ● Defense against control packet attacks ● Defense against attacks of source address spoofing, LAND, SYN flood (TCP SYN), smurf, ping flood (ICMP echo), Teardrop, and Ping of Death
	Network management	● Ping and traceroute ● SNMPv1/v2c/v3 ● Standard MIB ● RMON
	Cluster management	● HGMPv2 ● S5700 functioning as the command switch ● S5700 functioning as the member switch ● S5700 joining cluster automatically ● Member switches using private IP addresses ● Logging in to the member switch through Telnet