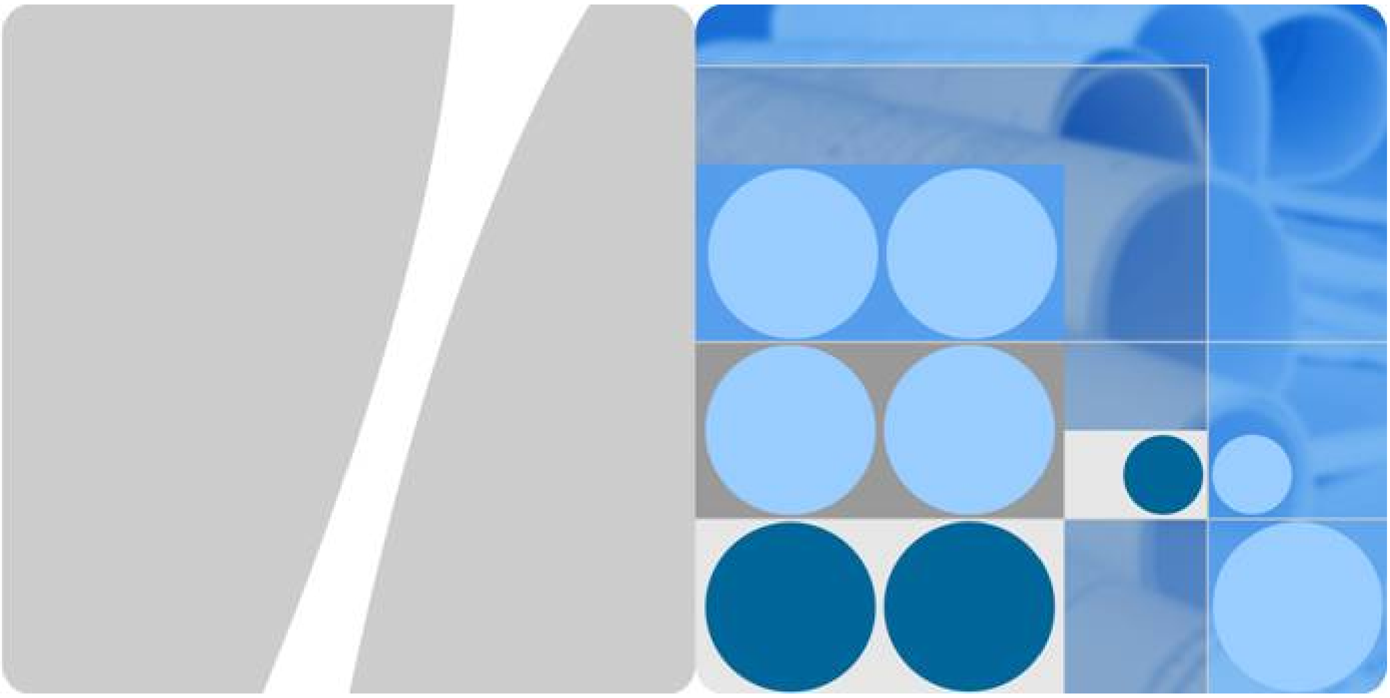


S9700 Core Routing Switch

V200R002C00

Product Description

Issue 01

Date 2012-12-08

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 a 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://enterprise.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 S9700.

This document helps you understand the characteristics and features of the S9700.

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.

Change History

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

Changes in Issue 01 (2012-12-08)

Initial commercial release.

Contents

1 Product Overview

About This Chapter

This section describes the features and position of the S9700 series switches.

1.1 System Overview

The S9700 Core Routing Switch (S9700 for short) is high-end switches designed for next-generation campus networks and data centers to provide service aggregation. Based on Huawei Versatile Routing Platform (VRP), the S9700 provides high L2/L3 switching capabilities and integrates diversified services such as MPLS VPN, hardware IPV6, desktop cloud, video conferencing, wireless access. In addition, the S9700 also provides a variety of reliability technologies including in-service software upgrade, non-stop forwarding, hardware OAM/BFD, and ring network protection. These technologies improve customers' network efficiency and maximize the normal operation time, which reduce customers' total cost of ownership (TCO).

The S9700 comes in three different models: S9703, S9706, and S9712. The S9703 supports a maximum of three line processing units (LPUs); the S9706 supports a maximum of six LPUs; the S9712 supports a maximum of 12 LPUs.

NOTE

The release in Russia does not provide IPSec VPN.

1.2 Product Characteristics

Advanced Architecture to Ensure Industry-Leading Performance

The S9700 core routing switch (S9700 for short) is designed for a 100G platform and provides a maximum of 3.84 Tbit/s switching capacity, which can be expanded to 5.12 Tbit/s or 7.68 Tbit/s to support high-density GE/10GE line-speed forwarding. The S9700 supports:

- Line cards that have the highest densities in the industry, such as 8*40GE and 40*10GE line cards.
- A maximum of 96*40GE ports or 480*10GE ports, bringing enterprise campus networks and data centers into the era of the all-10GE core network.
- The 100G Ethernet standard to meet future requirements from bandwidth-intensive applications (such as multimedia conferencing and data access), eliminating the trouble of frequent upgrading.

Innovative CSS Technology

The S9700 switches can form a cluster switch system (CSS) using service ports on LPUs. CSS technology virtualizes multiple physical switches into one logical device that has higher reliability, flexibility and is easier to manage.

- High reliability: Through hot backup of routes, all control plane and data plane information is backed up and forwarded continuously at Layer 3, which significantly improves device reliability and performance.
- Flexibility: Service ports can be used as stack ports so that stack members can be connected through optical fibers. This expands the stacking distance substantially.
- Easy management: The member switches in a stack are managed using the same IP address, which simplifies device management and topology management, improves operation efficiency, and reduces maintenance costs.

Carrier-grade Reliability

All the key components of the S9700 (including MPUs, power modules, and fans) use a redundant design, and all modules are hot swappable to ensure stable network operation. In addition, the S9700 provides the following functions to enhance network reliability:

- Hardware-based BFD for protocols such as static routing, RIP, OSPF, BGP, ISIS, VRRP, PIM, and MPLS, which can detect link failures in a minimum of 3.3 ms.
- Hardware-based Ethernet OAM, including comprehensive IEEE 802.3ah, 802.1ag, and ITU-Y. 1731 implementations. Hardware-based Ethernet OAM can collect accurate network parameters, such as transmission latency and jitter, to help customers monitor network operating status in real time and to realize quick detection, location, and switching when a network fault occurs.
- Graceful restart to realize nonstop forwarding and ensure reliable and high-speed operation of the entire network.

Multi-Service Switching Platform

The S9700 uses a multi-service routing and switching platform and can provide wireless, voice, video, and data services. It helps enterprises build a highly available, low-latency, and multi-service network through the following functions:

- Distributed Layer 2 and Layer 3 MPLS VPN functions, including Multiprotocol Label Switching (MPLS), virtual private LAN service (VPLS), hierarchical VPLS (HVPLS), and virtual leased line (VLL), providing secure access for enterprise VPN users.
- Layer 2 and Layer 3 multicast protocols, including Protocol Independent Multicast Sparse Mode (PIM SM), PIM Dense Mode (DM), Multicast Listener Discovery (MLD), and Internet Group Management Protocol (IGMP) snooping. These multicast protocols ensure high-quality HD video surveillance and video conferencing services.
- Multiple routing protocols. The S9700 can provide routes for small, medium, and even super large enterprises. In addition, it supports IPv6, enabling enterprise networks to seamlessly migrate to IPv6.

Integrated AC Card to Provide Wireless Access

The S9700 wireless AC card supports radio frequency (RF) management and allows APs to automatically select their radio channels and power. When signals of different APs conflict, APs can adjust their power and channels. The received signal strength indicator (RSSI) and signal-to-noise ratio (SNR) are updated in real time so that the AC can know the radio environment of each wireless user. The RF management function helps improve network availability. The AC card supports 802.1x authentication, MAC address authentication, Portal authentication, and WLAN authentication and privacy infrastructure (WAPI), providing access authentication for terminals of different types and security levels.

Powerful Network Traffic Analysis

The S9700 supports NetStream and V5/V8/V9 packet formats. The NetStream feature supports aggregation traffic template, real-time traffic sampling, dynamic report generation traffic attribute analysis, and traffic exception alarms. The S9700 sends traffic statistics logs to master and backup servers simultaneously to avoid data loss. The NetStream function helps monitor operating status and traffic model on the entire network. It also provides fault pre-detection, effective fault rectification, fast problem handling, as well as security monitoring, to help customers optimize network structure and adjust service deployment.

Excellent Security Design

The S9700 can use an integrated firewall card to provide virtual firewall and NAT multi-instance functions, allowing multiple VPN customers to share the same firewall. The firewall card uses application-specific packet filter (ASPF) to check and filter application-layer packets based on complex rules. The S9700 provides the following functions:

- Comprehensive network admission control (NAC) solutions for enterprise networks: The S9700 supports MAC address authentication, portal authentication, 802.1x authentication, and DHCP snooping-triggered authentication. These authentication methods ensure security of various access modes such as dumb terminal access, mobile access, and centralized IP address allocation.
- Two-level CPU protection mechanism: The S9700 supports 1K CPU hardware queues, separates the data plane from the control plane. This helps defend against DoS attacks and unauthorized access, and prevents control plane overloading.

High-Performance IPv6 Service Support

Both the hardware platform and software platform of the S9700 support IPv6. The S9700 has earned the IPv6 Ready Phase 2 (Gold) designation. The S9700 helps in seamless migration to IPv6 through the following features:

- IPv6 unicast routing protocols, including static routing, RIPng, OSPFv3, IS-ISv6, and BGP4+
- IPv6 multicast protocols, including MLD v1/v2, MLD snooping, PIM-SM/DMv6, and PIM-SSMv6
- Various IPv4-to-IPv6 technologies to ensure seamlessly migration from IPv4 to IPv6, including IPv6 manual tunnel, 6-to-4 tunnel, Intra-site Automatic Tunnel Addressing Protocol (ISATAP) tunnel, Generic Routing Encapsulation (GRE) tunnel, and IPv4-compatible automatic tunnel

Innovative Energy Saving Design

The S9700 uses a left-to-rear airflow design to improve heat dissipation efficiency. In addition, it uses a variable current chip to dynamically adjust the power according to traffic, reducing power consumption of a chassis by 11%. The S9700 adopts the following energy-saving technologies:

- Port sleeping: Idle ports enter the sleeping state to reduce power consumption.
- Intelligent fan-speed adjustment: Fans are grouped into multiple zones and their fan speed in each zone is adjusted individually based on service loads. This technology lowers power consumption, reduces noises, and extends the service life of fans.
- Energy Efficient Ethernet (IEEE 802.3az): Transceivers on line cards can quickly transition to the lower power idle state to reduce power consumption when no traffic is being transmitted.

2 Architecture

About This Chapter

This section describes the appearance, hardware structure and software architecture of the S9700

2.1 S9700 Series System Structure

This section describes the appearance and component layout.

The S9700 uses a distributed hardware architecture, consisting of the following components:

- Chassis
- Backplane
- Power module
- Fan frame
- Switch Routing Unit (SRU) or Main Control Unit (MCU)
- Line Processing Unit (LPU)
- Central Management Unit (CMU)

The S9700 can be installed in either the International Electrotechnical Commission (IEC) 297 cabinet or a European Telecommunications Standards Institute (ETSI) cabinet.

NOTE

- The SRU and CMU are applicable only to the S9712 and S9706.
- The MCU is applicable only to the S9703.

2.1.1 S9703

Appearance

The S9703 chassis is 4 U high (1 U = 44.45 mm). When the chassis has no cable divider installed, the dimensions are 442 mm x 476 mm x 175 mm (W x D x H). When the chassis has cable dividers installed, the dimensions are 442 mm x 585 mm x 175 mm (W x D x H). **Figure 2-1** and **Figure 2-2** show the appearance of the S9703 chassis.

Figure 2-1 Appearance of the S9703 chassis (front view)

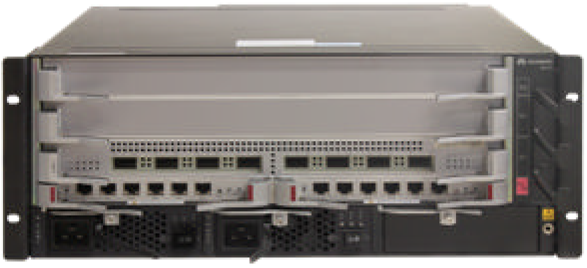
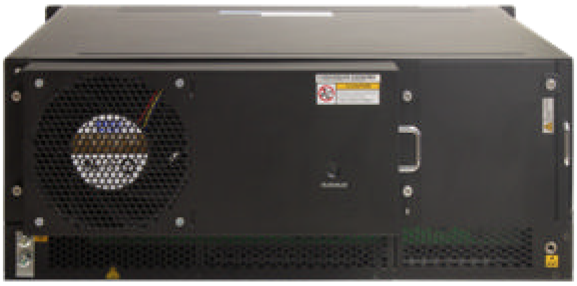


Figure 2-2 Appearance of the S9703 chassis (rear view)



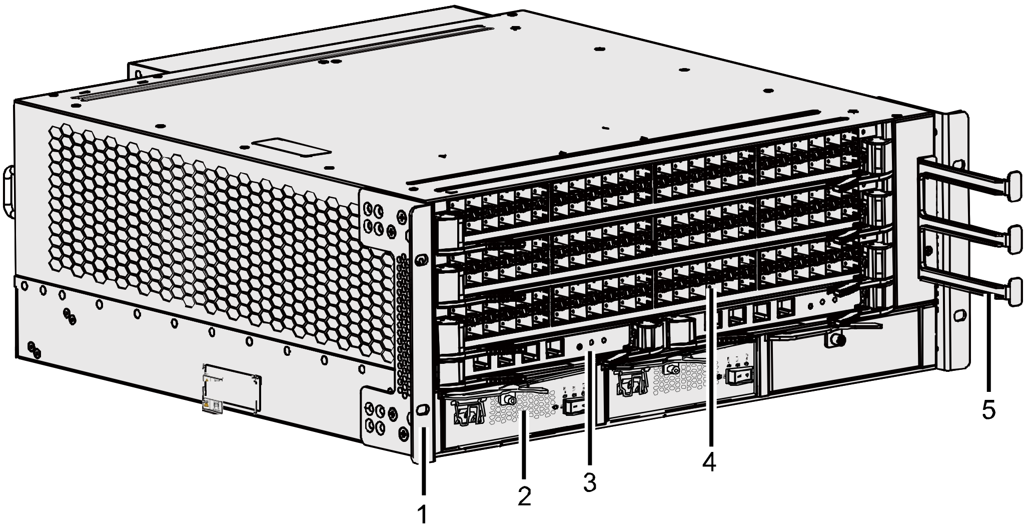
NOTE

- The S9703 uses either an FCC chassis or a common chassis.

Structure

Figure 2-3 and Figure 2-4 show the structure of the S9703 chassis.

Figure 2-3 Structure of the S9703 chassis (front view)



1. Rack-mounting ear

NOTE

It is used to secure the chassis in a rack.

2. System power module

3. MCU

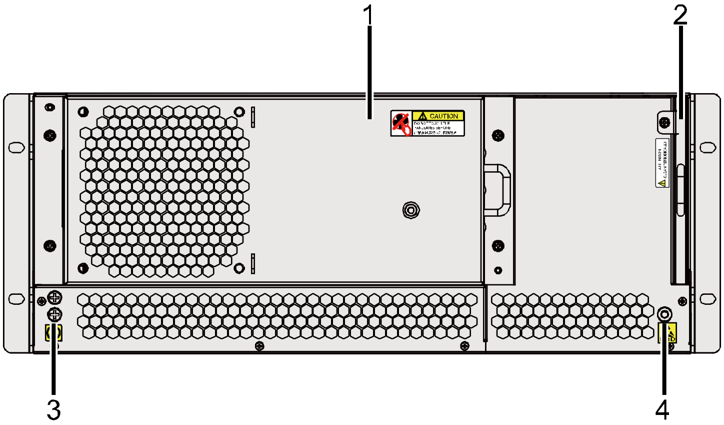
4. LPU

5. Cable divider

NOTE

It is used to arrange cables.

Figure 2-4 Structure of the S9703 chassis (rear view)



1. Fan module

NOTE

Each chassis is configured with only one fan module. For details about the fan module, see S9700 Fan Module.

2. Air filter

NOTE

It prevents dust from entering the chassis.

3. Ground screw

NOTE

It is used to ground the chassis.

4. ESD jack

NOTE

An ESD wrist strap can be inserted into this ESD jack.

ESD preventive measures take effect only when the chassis is properly grounded.

2.1.2 S9706

Appearance

The S9706 chassis is 10 U high (1 U = 44.45 mm). When the chassis has no cable divider installed, the dimensions are 442 mm x 476 mm x 441.7 mm (W x D x H). When the chassis has cable dividers installed, the dimensions are 442 mm x 585 mm x 441.7 mm (W x D x H). **Figure 2-5** and **Figure 2-6** show the appearance of the S9706 chassis.

Figure 2-5 Appearance of the S9706 chassis (front view)

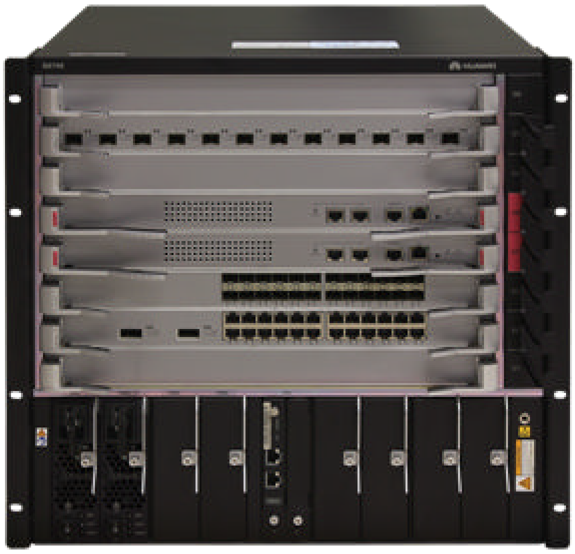
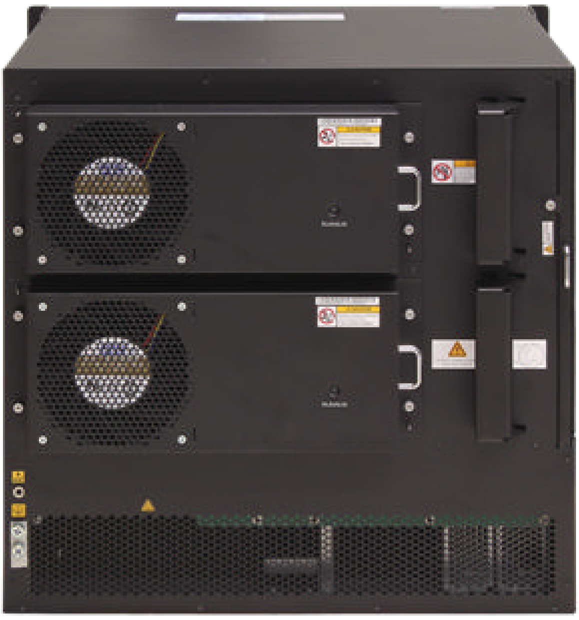


Figure 2-6 Appearance of the S9706 chassis (rear view)



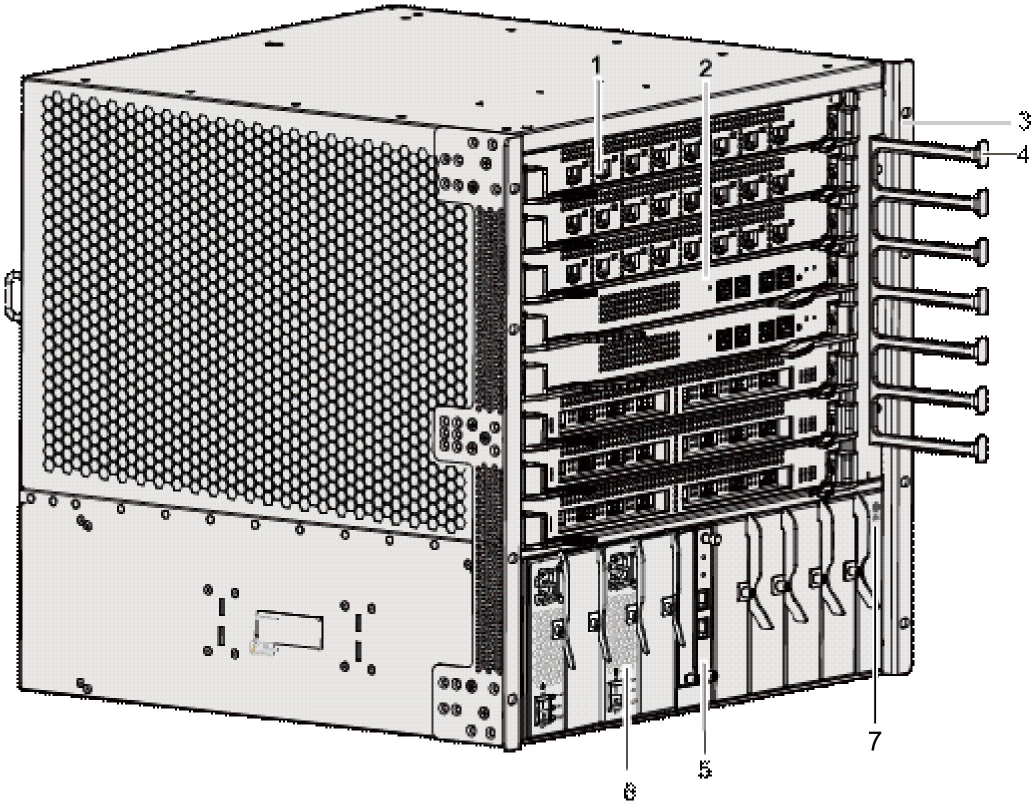
NOTE

- The S9706 uses either an FCC chassis or a common chassis.

Structure

Figure 2-7 and Figure 2-8 show the structure of the S9706 chassis.

Figure 2-7 Structure of the S9706 chassis (front view)



1. LPU

2. SRU

3. Rack-mounting ear

NOTE

It is used to secure the chassis in a rack.

4. Cable divider

NOTE

It is used to arrange cables.

5. CMU

6. System power module

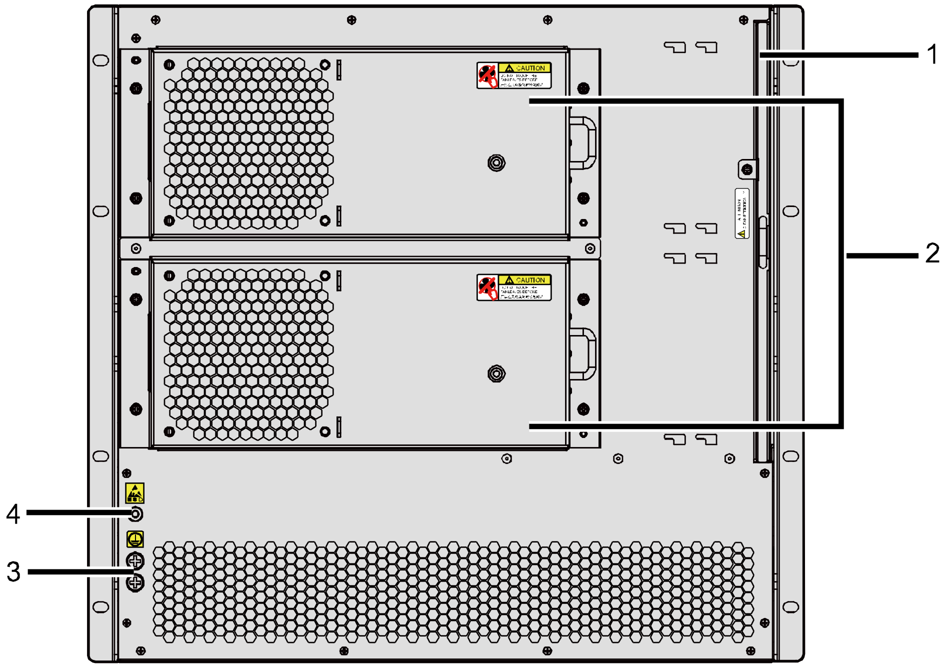
7. ESD jack

NOTE

An ESD wrist strap can be inserted into this ESD jack.

ESD preventive measures take effect only when the chassis is properly grounded.

Figure 2-8 Structure of the S9706 chassis (rear view)



1. Air filter

NOTE

It prevents dust from entering the chassis.

2. Fan module

NOTE

Each chassis is configured with two fan modules. For details about the fan modules, see S9700 Fan Module.

3. Dual-OT ground screw

NOTE

It is used to ground the chassis.

4. ESD jack

NOTE

An ESD wrist strap can be inserted into this ESD jack.

ESD preventive measures take effect only when the chassis is properly grounded.

2.1.3 S9712

Appearance

The S9712 chassis is 15 U high (1 U = 44.45 mm). When the chassis has no cable divider installed, the dimensions are 442 mm x 476 mm x 663.95 mm (W x D x H). When the chassis has cable dividers installed, the dimensions are 442 mm x 585 mm x 663.95 mm (W x D x H). **Figure 2-9** and **Figure 2-10** show the appearance of the S9712 chassis.

Figure 2-9 Appearance of the S9712 chassis (front view)

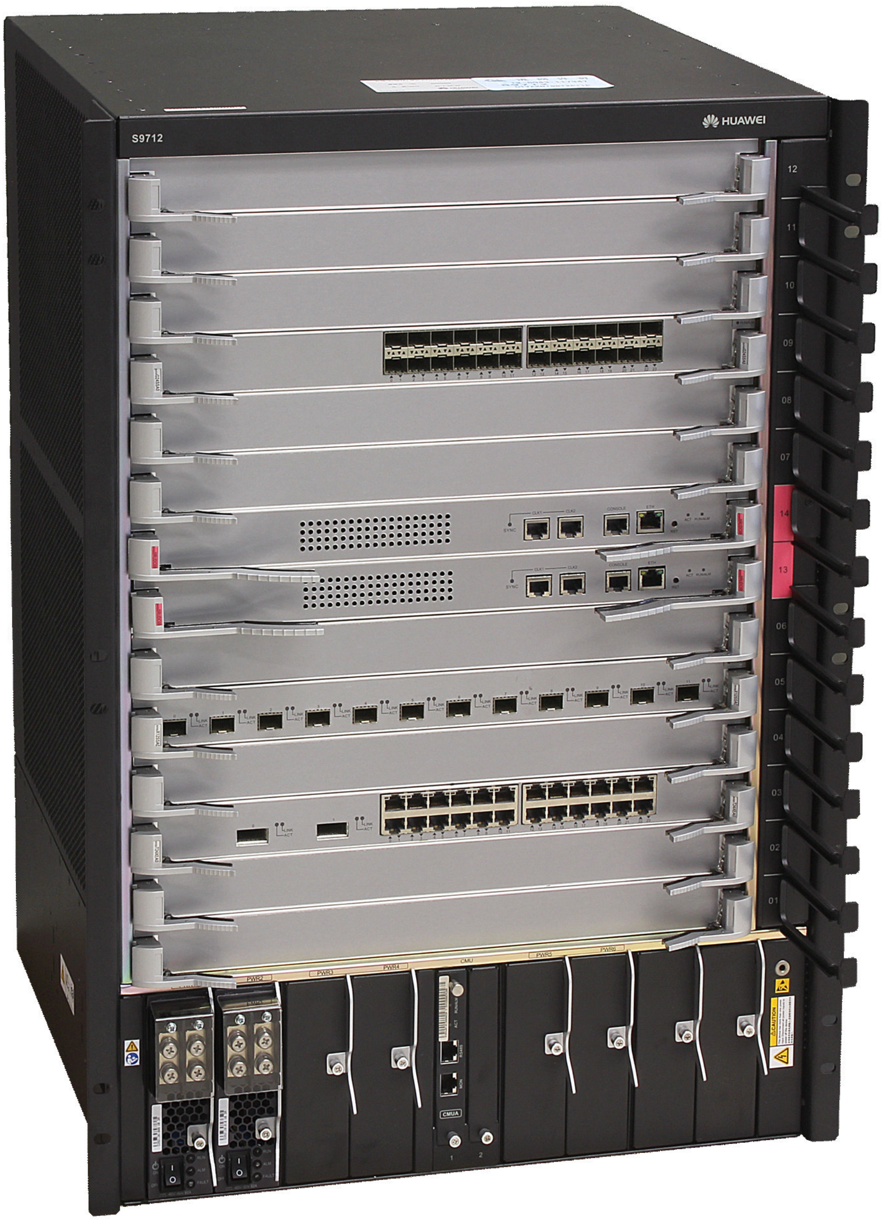
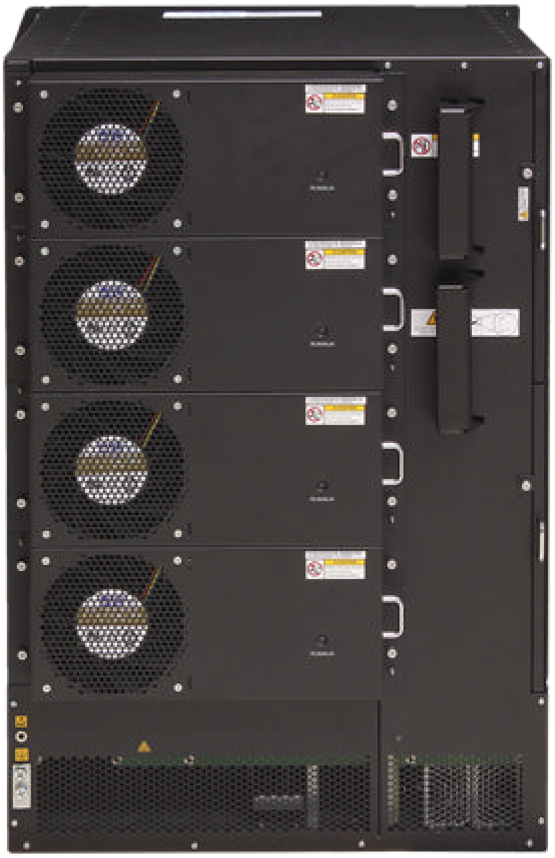


Figure 2-10 Appearance of the S9712 chassis (rear view)



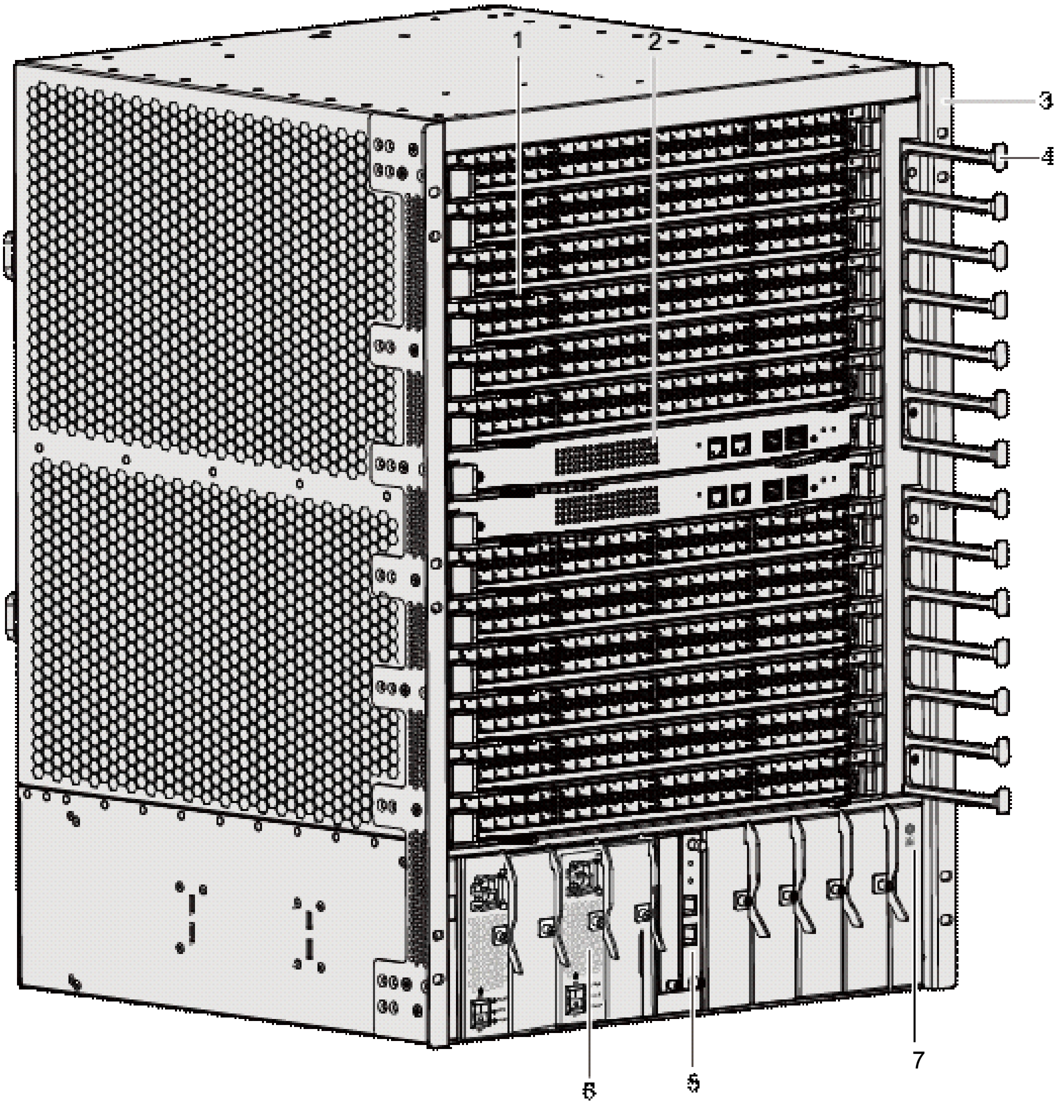
NOTE

- The S9712 uses either an FCC chassis or a common chassis.

Structure

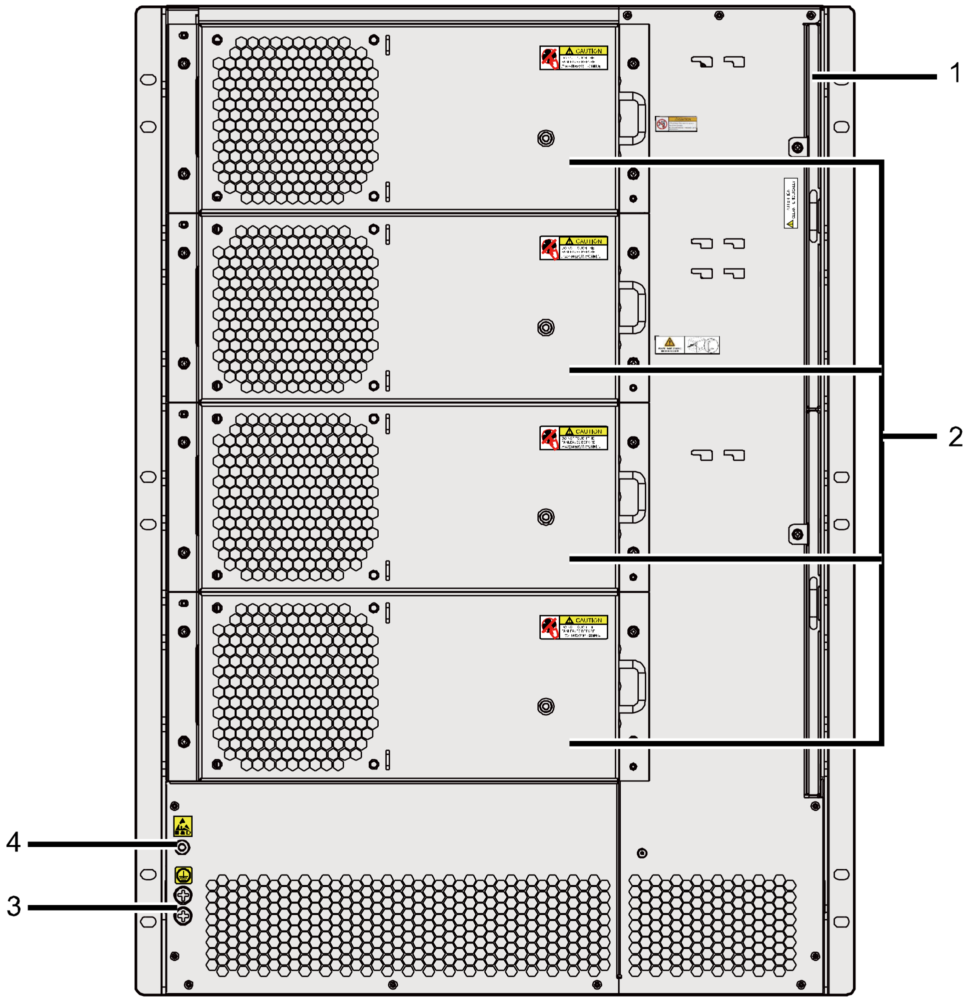
Figure 2-11 and **Figure 2-12** show the structure of the S9712 chassis.

Figure 2-11 Structure of the S9712 chassis (front view)



1. LPU	2. SRU	3. Rack-mounting ear **NOTE** It is used to secure the chassis in a rack.
4. Cable divider **NOTE** It is used to arrange cables.	5. CMU	6. System power module
7. ESD jack **NOTE** An ESD wrist strap can be inserted into this ESD jack. ESD preventive measures take effect only when the chassis is properly grounded.		

Figure 2-12 Structure of the S9712 chassis (rear view)



1. Air filter

NOTE

It prevents dust from entering the chassis.

2. Fan module

NOTE

Each chassis is configured with four fan modules. For details about the fan modules, see S9700 Fan Module.

3. Dual-OT ground screw

NOTE

It is used to ground the chassis.

4. ESD jack

NOTE

An ESD wrist strap can be inserted into this ESD jack.

ESD preventive measures take effect only when the chassis is properly grounded.

2.2 Hardware Layout

This section describes the hardware structure, including the backplane, MCU, SRU, LPU, CMU of the S9700.

Figure 2-13 shows the hardware structure of the S9703.

Figure 2-13 Hardware layout of the S9703

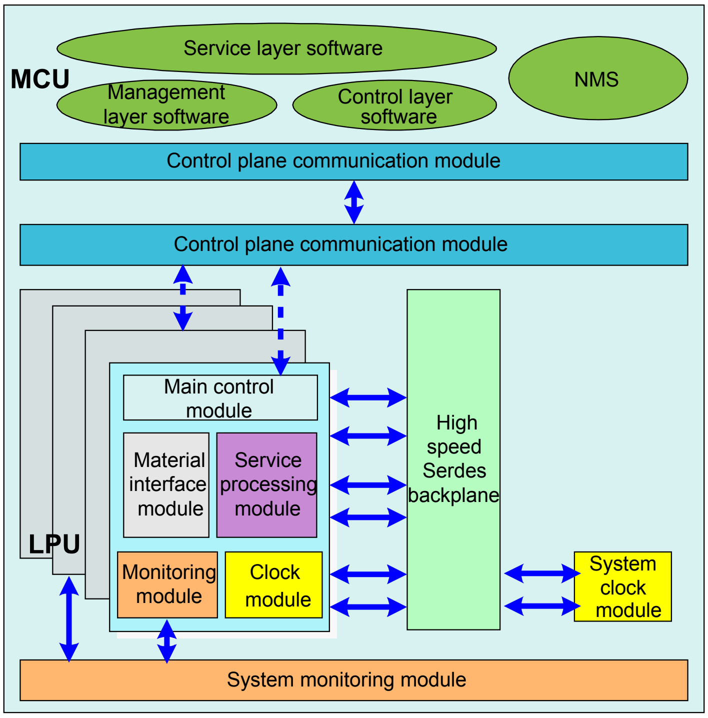
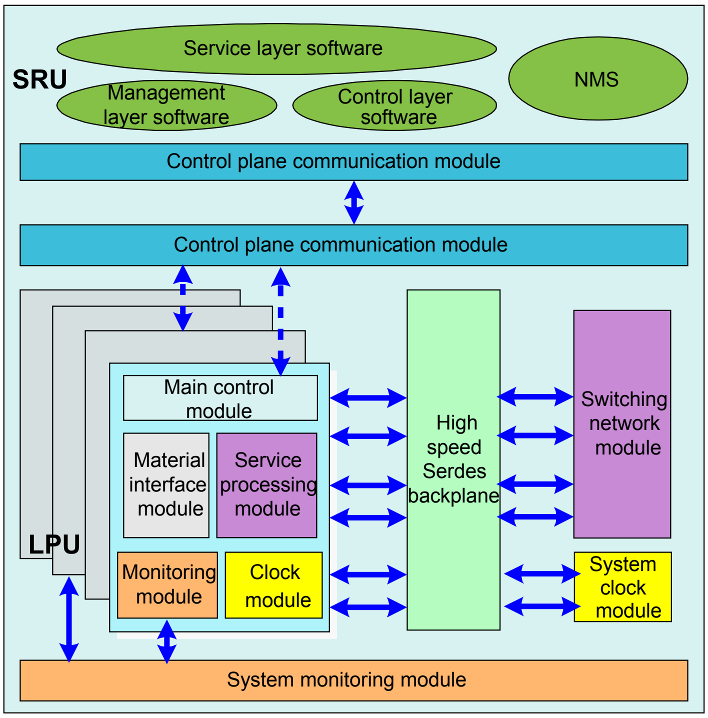

Service layer software
MCU
Management layer software
Control layer software
NMS
Control plane communication module
Control plane communication module
Main control module
Material interface module
Service processing module
LPU
Monitoring module
Clock module
High speed Serdes backplane
System clock module
System monitoring module

Figure 2-14 shows the hardware structure of the S9706 and S9712.

Figure 2-14 Hardware structure of the S9706 and S9712


Service layer software
SRU
Management layer software
Control layer software
NMS
Control plane communication module
Control plane communication module
Main control module
Material interface module
Service processing module
LPU
Monitoring module
Clock module
High speed Serdes backplane
Switching network module
System clock module
System monitoring module

2.2.1 Backplane

The S9700 is designed with a passive backplane composed of control buses, management buses, and clock buses that interact between the SRU, MCU and other communication components.

Each S9700 backplane provides two control unit slots. The S9703's backplane provides 3 LPU slots, the S9706's backplane provides 6 LPU slots, and the S9712's backplane provides 12 LPU slots.

2.2.2 SRU

The SRU is the control board of S9706 and S9712. The SRU integrates multiple functional modules such as a data switching module, main control module,OAM, Compact Flash (CF) module, and system monitoring module. The SRU can be expanded to include a clock module.As the core of system control and data switching, the SRU switches data, and controls and monitors the system.

The control units on the two SRUs support 1+1 hot backup, and the data switching units on the two SRUs support load balancing.

The S9700's SRU has the following functions:

- Forwards data on the data plane.
- Processes protocols including STP, MPLS, and various routing protocols.
- Monitors components.
- Manages the system and monitors system performance according to the user's instruction, and provides users with feedback on the system's running status.

Table 2-1 SRU switching capabilities

SRU	Service Switching Capability	FCC Available
EH1D2SRUDC00	1.92 Tbit/s	No
EH1D2SRUDC01	1.92 Tbit/s	Yes

2.2.3 MCU

The MCU is the control board of S9703. The MCU integrates the main control module, CF module, system monitoring module and clock module.

The S9700's MCU has the following functions:

- Processes protocols including STP, MPLS, and various routing protocols.
- Monitors components, collects running data of each component periodically, and generates control information based on the running status of the components, for example, checking whether the boards are available and controlling the running of the switching fabric.
- Manages the system and monitors system performance according to the user's instruction, and provides users with feedback on the system's running status.

2.2.4 CMU

The CMU is the monitoring board applied to the S9706 and S9712. The CMU monitors and manages the power modules, fan modules.

The CMU helps monitor and manage the system and facilitates energy savings and emissions reduction.

2.2.5 LPU

A Line Processing Unit (LPU) processes packets and provides service interfaces. The following table lists the LPUs supported by the S9700.

NOTE

LPUs of the S9700 are classified into S series, E series, F series, and B series Ethernet interface cards, and POS interface cards:

- The S series LPUs are SA cards, for example, 24-port 100/1000M Ethernet optical interface card (**SA**, SFP)-32K MAC.
- E series LPUs include EA, EC, and ED cards, for example, 48-port 100M Ethernet optical interface card (**EA**, SFP)-32K MAC.
- F series LPUs include FA and FC cards, for example, 48-port 1000M Ethernet electrical interface card (**FA**, RJ45)-32K MAC.
- B series LPUs are BC cards, for example, 48-port 100/1000M Ethernet optical interface card (**BC**, SFP)-128K MAC.
- A POS card consists of a WAN card and a P4CF, P4HF, or P1UF subcard.

Table 2-2 Ethernet interface cards

Card Name	Description	FCC Compliance
EH1D2F48SEA0	48-port 100M Ethernet optical interface card (EA, SFP)-32K MAC	Yes
EH1D2F48SEC0	48-port 100M Ethernet optical interface card (EC, SFP)-128K MAC	Yes
EH1D2F48TEA0	48-port 10/100M Ethernet electrical interface card (EA, RJ45)-32K MAC	Yes
EH1D2F48TEC0	48-port 10/100M Ethernet electrical interface card (EC, RJ45)-128K MAC	Yes
EH1D2F48TFA0	48-port 10/100M Ethernet electrical interface card (FA, RJ45)-32K MAC	Yes
EH1D2G48SEA0	48-port 100/1000M Ethernet optical interface card (EA, SFP)-32K MAC	Yes
EH1D2G48SEC0	48-port 100/1000M Ethernet optical interface card (EC, SFP)-128K MAC	Yes
EH1D2G48SED0	48-port 100/1000M Ethernet optical interface card (ED, SFP)-512K MAC	Yes

Card Name	Description	FCC Compliance
EH1D2G48SFA0	48-port 100/1000M Ethernet optical interface card (FA, SFP)-32K MAC	Yes
EH1D2G48TEA0	48-port 10/100/1000M Ethernet electrical interface card (EA, RJ45)-32K MAC	Yes
EH1D2G48TEC0	48-port 10/100/1000M Ethernet electrical interface card (EC, RJ45)-128K MAC	Yes
EH1D2G48TED0	48-port 10/100/1000M Ethernet electrical interface card (ED, RJ45)-512K MAC	Yes
EH1D2G48TFA0	48-port 10/100/1000M Ethernet electrical interface card (FA, RJ45)-32K MAC	Yes
EH1D2T36SEA0	12-port 100/1000M optical and 36-port 10/100/1000M electrical interface card (EA, RJ45/SFP)-32K MAC	Yes
EH1D2X04XEA0	4-port 10G Ethernet optical interface card (EA, XFP)-32K MAC	No
EH1D2X04XEC0	4-port 10G Ethernet optical interface card (EC, XFP)-128K MAC	No
EH1D2X04XED0	4-port 10G Ethernet optical interface card (ED, XFP)-512K MAC	No
EH1D2X02XEA0	2-port 10G Ethernet optical interface card (EA, XFP)-32K MAC	No
EH1D2X02XEC0	2-port 10G Ethernet optical interface card (EC, XFP)-128K MAC	No
EH1D2S24CEA0	24-port 100/1000M Ethernet optical and 8-port 10/100/1000M combo electrical interface card (EA, SFP/RJ45)-32K MAC	Yes
EH1D2G24SSA0	24-port 100/1000M Ethernet optical interface card (SA, SFP)-32K MAC	Yes
EH1D2G24SEC0	24-port 100/1000M Ethernet optical interface card (EC, SFP)-128K MAC	Yes
EH1D2G24SED0	24-port 100/1000M Ethernet optical interface card (ED, SFP)-512K MAC	Yes
EH1D2S24CSA0	24-port 100/1000M Ethernet optical and 8-port 10/100/1000M combo electrical interface card (SA, SFP/RJ45)-32K MAC	Yes
EH1D2X12SSA0	12-port 10G Ethernet optical interface card (SA, SFP+)-32K MAC	No

Card Name	Description	FCC Compliance
EH1D2T24XEA0	24-port 10/100/1000M Ethernet electrical and 2-port 10G Ethernet optical interface card (EA, RJ45/XFP)-32K MAC	Yes
EH1D2S24XEA0	24-port 100/1000M Ethernet optical and 2-port 10G Ethernet optical interface card (EA, SFP/XFP)-32K MAC	Yes
EH1D2S24XEC0	24-port 100/1000M Ethernet optical and 2-port 10G Ethernet optical interface card (EC, SFP/XFP)-128K MAC	Yes
EH1D2G48SBC0	48-port 100/1000M Ethernet optical interface card (BC, SFP)-128K MAC	Yes
EH1D2G48TBC0	48-port 10/100/1000M Ethernet electrical interface card (BC, RJ45)-128K MAC	Yes
EH1D2G24TFA0	24-port 10/100/1000M Ethernet electrical interface card (FA, RJ45)-32K MAC	Yes
EH1D2X40SFC0	40-port 10G Ethernet optical interface card (FC, SFP+)-128K MAC	No
EH1D2X40SFC1	40-port 10G Ethernet optical interface card (FC, SFP+)-128K MAC	Yes
EH1D2X16SFC0	16-port 10G Ethernet optical interface card (FC, SFP+)-128K MAC	No
EH1D2X16SFC1	16-port 10G Ethernet optical interface card (FC, SFP+)-128K MAC	Yes
EH1D2X08SED4	8-port 10G Ethernet optical interface card (ED, SFP+)-512K MAC	No
EH1D2X08SED5	8-port 10G Ethernet optical interface card (ED, SFP+)-512K MAC	Yes
EH1D2L02QFC0	2-port 40G Ethernet optical interface card (FC, QSFP+)-128K MAC	Yes
EH1D2L08QFC0	8-port 40G Ethernet optical interface card (FC, QSFP+)-128K MAC	Yes

Table 2-3 POS interface cards

Card Name	Description	FCC Compliance
EH1D2WM00000	WAN card	Yes
P4CF	4-port OC-3c/STM-1c POS-SFP subcard (installed on a WAN card)	Yes
P4HF	4-port OC-12c/STM-4c POS-SFP subcard (installed on a WAN card)	Yes
P1UF	1-port OC-48c/STM-16c POS-SFP subcard (installed on a WAN card)	Yes

NOTE

- SFP refers to a Small Form-Factor Pluggable optical module.
- XFP refers to a 10 Gigabit Small Form-Factor Pluggable optical module.
- SFP+ refers to a 10 Gigabit Small Form-Factor Pluggable optical transceiver, with a smaller caliber than an XFP optical module.
- QSFP+ refers to a Quad Small Form-Factor Pluggable Plus optical module (40G).
- An optical interface works at 1000 Mbit/s by default and cannot work at 100 Mbit/s through negotiation. To use an optical interface work as a 100M interface, manually set the interface speed to 100 Mbit/s.
- Use FCC-certified cards in FCC-certified chassis.

2.2.6 SPU

The Service Process Unit (SPU) is the value-added service card, which does not provide service interfaces.

The SPU used on the S9700 series switches is referred to as the Value Added service Multi-core Processor (VAMPA), where "A" represents the version. It supports the following functions:

- Firewall
- NAT
- Integrated NetStream
- Load balancing
- IPSec VPN

  NOTE

  The release in Russia does not provide IPSec VPN.
- WLAN AC

Table 2-4 SPU

Name	Description
VAMPA	Processes value-added services.

2.2.7 OSP

OSP: Open Service Platform. It does not provide service interfaces.

The Open Service Platform Unit supports mainstream operating systems including Windows Vista, Windows 7, Windows Server 2008, Windows Server 2008 R2, and VMWare ESX and third-party applications. Customers can integrate new features or conduct secondary development on the Open Service Platform Unit.

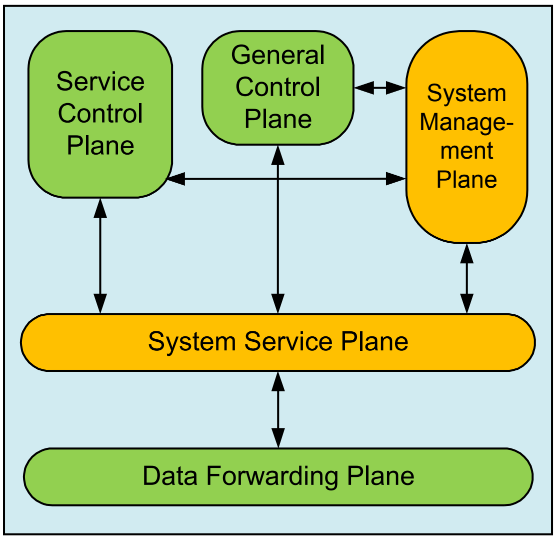
Table 2-5 OSP

Name	Description	FCC Compliance
EH1D2PS 00P00	Open service platform (OSP) card	Yes

2.3 Software Architecture

The S9700 runs on the latest VRP version 5 (VRPv5) to provide various features. VRPv5 consists of the following parts:

Figure 2-15 Software architecture



- 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 Service Features

About This Chapter

This section describes the major service functions of the S9700, including IP features,MPLS, MPLS L2VPN, MPLS L3VPN, QoS, Ethernet, Ethernet OAM, NAC, multicast, reliability, LLDP, security, clock, Web network management, firewall/NAT, load balancing, IPSec VPN, NetStream, and WLAN AC.

NOTE

The release in Russia does not provide IPSec VPN.

3.10 MPLS & VPN

3.1 Ethernet

This section describes the basics of VLAN mapping, selective QinQ, and Layer 2 Protocol Transparent Transmission.

3.1.1 VLAN Aggregation

As network technologies develop, a greater number of network addresses are required to handle the growing number of applications and devices. To deal with network address insufficiencies, VLAN aggregation is used to conserve IP addresses.

In VLAN aggregation, a super VLAN is associated with multiple sub-VLANs. A super VLAN does not contain physical interfaces, but can be configured with a VLANIF interface. A sub-VLAN can contain physical interfaces, but cannot be configured with a VLANIF interface. All sub-VLAN interfaces use the VLANIF interface address of the super VLAN. The subnet IDs, subnet gateway addresses, and subnet broadcast addresses can be conserved. Different broadcast domains use the addresses of the same subnet; therefore, addressing becomes flexible and IP addresses are conserved. In addition to keeping each sub-VLAN as an independent broadcast domain, VLAN aggregation uses fewer IP addresses than a common VLAN.

3.1.2 VLAN Mapping

VLAN mapping refers to setting up of a mapping table on the S9700 that dictates how the Customer VLAN (C-VLAN) interacts with the Service VLAN (S-VLAN). One or multiple C-VLAN IDs can be mapped to a S-VLAN ID.

📖 NOTE

- C-VLANs are the VLANs on the port at the user side. They take effect locally and identify a user or a class of users.
- S-VLANs are designated by the ISP at the network side. They take effect globally and identify a type of service.

The S9700 supports VLAN mapping of a single VLAN tag in the following modes, provided the user side interface has been specified:

- 1:1 VLAN mapping

  Maps a C-VLAN tag to the S-VLAN tag.
- N:1 VLAN mapping

  Maps multiple C-VLAN tags to the S-VLAN tag.

The S9700 also supports double-tagged VLAN mappings.

- 2:2 VLAN mapping

  The S9700 can map user side double-tagged packets to network side double-tagged packets. Additionally, the S9700 can replace both the outer and inner tags of a packet.
- 2 to 1 VLAN mapping

  The S9700 maps the user side outer and inner VLAN tags to the network side outer VLAN tag. It can also change the network side outer VLAN tag, but leave the network-side inner VLAN tag unchanged.

In addition, the S9700 supports the CoS-based VLAN mapping. It can map multiple C-VLAN tags to the same S-VLAN tag according to the CoS.

3.1.3 Selective QinQ

Selective QinQ expands the VLAN tag space, enabling the S9700 to flexibly select outer S-VLAN tags based on the received packets' C-VLAN tags. In this way, various user services can travel along different paths, improving service deployment. The selective QinQ feature can be applied to both inbound and outbound interfaces, making networking more flexible.

The S9700 can add a different outer S-VLAN tag based on the VLAN ID of the packets' VLAN tags on the port.

The QinQ-enabled port learns MAC addresses from packets' outer VLAN tags, and then forwards the upstream packets and downstream packets according to the packets' destination MAC addresses.

The S9700's powerful hardware implements selective QinQ using traffic classification based on ACLs, permitting the S9700 to flexibly add S-VLAN tags or modify C-VLAN tags.

3.1.4 Layer 2 Protocol Transparent Transmission

Layer 2 protocol transparent transmission is a Layer 2 tunneling technology that transparently transmits Layer 2 protocol packets from private networks over VLAN VPNs on an ISP network. With this technology, private networks in different areas can calculate a spanning tree. The spanning trees of private networks and ISP network are independent from each other, and therefore the network convergence speed is improved.

After Layer 2 protocol transparent transmission is enabled, the S9700 dose not send tagged Layer 2 protocol packets to the CPU. Instead, it forwards these packets in matching VLANs as common Layer 2 data frames or encapsulates them in MPLS packets to forward them on an MPLS network.

Bridge protocol data unis (BPDUs) are commonly used Layer 2 protocol packets. Layer 2 protocol transparent transmission provides a BPDU tunnel to transmit BPDUs so that private networks and the ISP network do not interfere with each other.

3.2 IP Features

This section describes the IP features supported by the S9700.

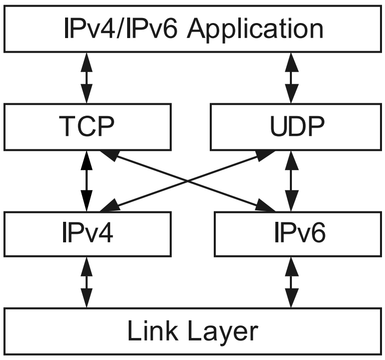
NOTE

To implement IPv6, apply for and purchase the relevant license from the local Huawei vendor.

3.2.1 IPv4/IPv6 Protocol Stack

The IPv4/IPv6 protocol stack can communicate with many other protocols and the IPv4/IPv6 implementation is simple. **Figure 3-1** shows the IPv4/IPv6 protocol stack structure.

Figure 3-1 IPv4/IPv6 protocol stack structure



3.2.2 IPv4 Features

The S9700 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 client/server and TFTP client
- DHCP relay agent and DHCP server
- Ping, tracert, and NQA: NQA can detect the status of ICMP, TCP, UDP, DHCP, FTP, HTTP and SNMP services and test the response time of various services.

  NOTE

  To implement NQA, apply for and purchase the relevant license from the local Huawei vendor.
- IP policy-based routing: specifies next hop based on packet attributes without searching the routing table.

3.2.3 IPv6 Features

The S9700 supports the following IPv6 features:

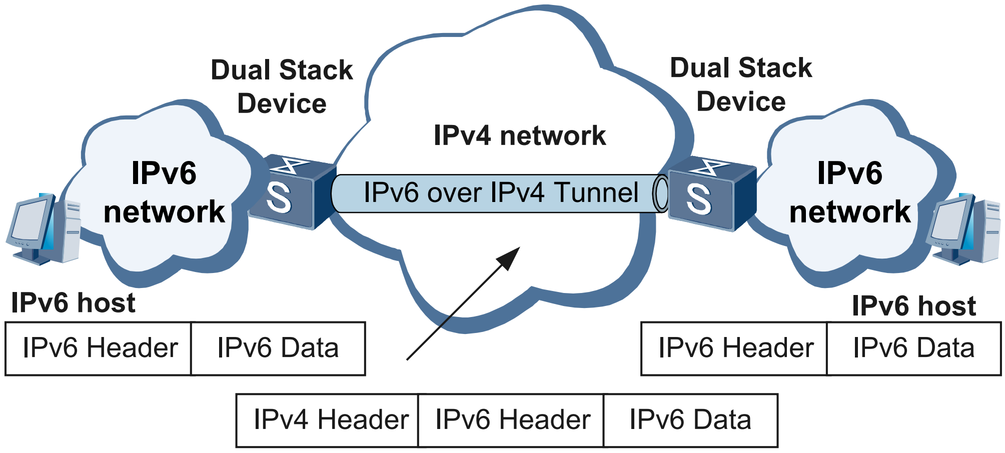
- IPv6 Neighbor Discovery (ND)
- Path MTU Discovery (PMTU)
- TCP6, ping IPv6, tracert IPv6, socket IPv6, UDP6 and RawIP6
- TFTP IPv6 Client
- IPv6 policy-based routing
- DHCPv6 snooping and MLDv1/v2 snooping
- Neighbor Discovery (ND) snooping

3.2.4 IPv4/IPv6 Transition Technologies

IPv6 over IPv4 Tunnel

As shown in **Figure 3-2**, the IPv6 over IPv4 tunnel technology is used during the transition from an IPv4 network to an IPv6 network.

Figure 3-2 Network diagram of an IPv6 over IPv4 tunnel



The S9700 supports the following IPv6 over IPv4 tunnels:

- IPv6 manual tunnel

  An IPv6 manual tunnel is created manually on routers at both ends of a tunnel by statically configuring the source and destination IPv4 addresses. The tunnel is a permanent link that connects two IPv6 domains through an IPv4 backbone network. It is a fixed channel for two edge routers to communicate with each other and can be used by isolated IPv6 sites to communicate with each other.

- 6to4 tunnel

  A 6to4 tunnel can connect multiple isolated IPv6 sites to an IPv6 network through an IPv4 network.

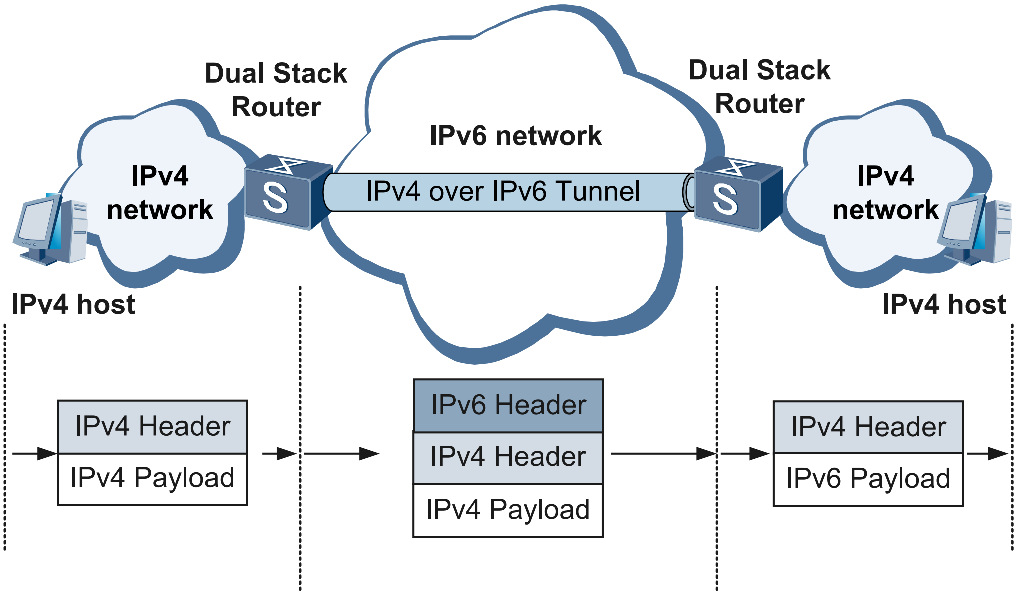
  Compared with a manual tunnel, a 6to4 tunnel can be a P2MP connection, whereas a manual tunnel is a P2P connection. Routers using a 6to4 tunnel are not configured in pairs. Similar to routers on an automatic tunnel, a router on a 6to4 tunnel can search for the other end of the tunnel. However, since a 6to4 tunnel uses a special IPv6 address, called a 6to4 address, it is not necessary to specify an IPv4-compatible IPv6 address for a 6to4 tunnel.

IPv4 over IPv6 Tunnel

During the later stage of an IPv4 to IPv6 network transition, a large number of IPv6 networks are deployed; therefore, there may be isolated IPv4 sites. Connecting these isolated sites using dedicated lines can be very costly, so, instead, a tunnel connecting isolated IPv4 sites can be created on an IPv6 network. This is similar to deploying a VPN on an IP network using tunnel technology. The tunnel connecting isolated IPv4 sites on an IPv6 network is called an IPv4 over IPv6 tunnel.

To set up IPv4 over IPv6 tunnels, the IPv4/IPv6 dual stack needs to be enabled on the routers at the edges of the IPv6 network and the IPv4 network.

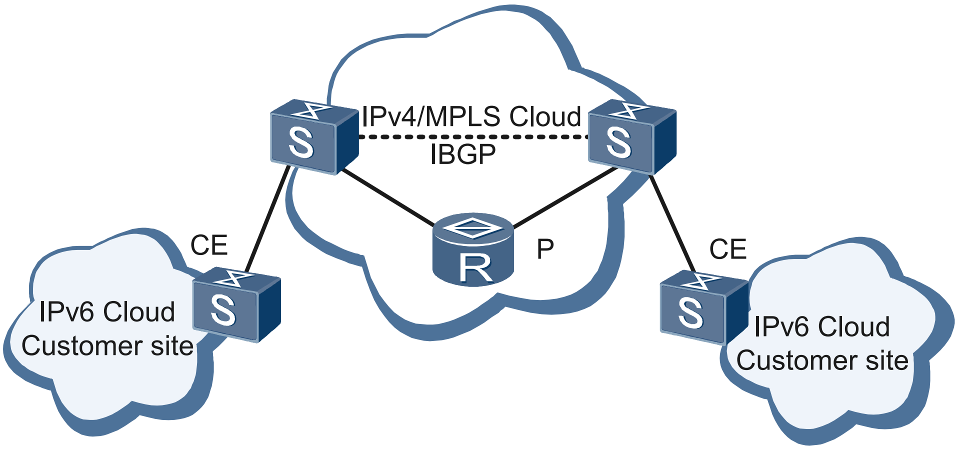
Figure 3-3 Network diagram of an IPv4 over IPv6 tunnel



6PE

An IPv6 Provider Edge (6PE) router facilitates communication between isolated IPv6 CE routers over an IPv4 network. **Figure 3-4** illustrates a simple 6PE network topology. The ISP can use the IPv4 backbone network to provide services for IPv6 networks with widely distributed users.

Figure 3-4 Network diagram of a basic 6PE network



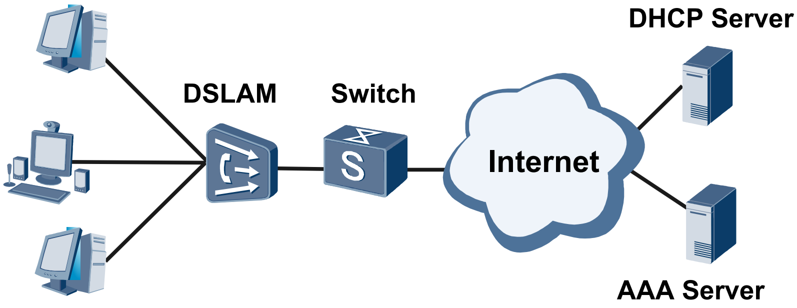
The 6PE router labels IPv6 routing information and advertises the information onto the ISP's IPv4 backbone network through Internal Border Gateway Protocol (IBGP) sessions. IPv6 packets are labeled before entering the tunnels on the backbone network. The tunnels can be MPLS LSPs.

3.2.5 IP Session

This section describes the IP session feature supported by the S9700.

As shown in **Figure 3-5**, Switch represents the S9700.

Figure 3-5 Networking diagram of an IP session



The S9700 can assign IP addresses to terminate and authenticate IP sessions.

An STB or VoIP terminal sends a DHCP Request message to which the S9700 either directly assigns an IP address to the terminal or relays the message to the DHCP server requesting an IP address. Before assigning an IP address, the S9700 sends the VLAN (QinQ) information or DHCP Relay Agent information to the AAA server to authenticate the terminal. If the authentication is successful, the S9700 assigns an IP address to that terminal.

The S9700 can perform scheduling on different types of services or encapsulate service traffic into different VPNs to separate services.

3.3 Multicast

This section describes the basics of IGMP snooping, multicast flow control, controllable multicast, multicast VLAN, and multicast replication.

The S9700 supports multicast features including IGMP snooping, IGMP proxy, static multicast, multicast across VLANs.

3.3.1 Multicast Routing Protocol

The S9700 supports the following multicast routing protocols:

- Internet Group Management Protocol (IGMP), Protocol Independent Multicast-Dense Mode (PIM-DM), Protocol Independent Multicast-Sparse Mode (PIM-SM), Multicast Source Discovery Protocol (MSDP), and Multi-protocol Border Gateway Protocol (MBGP).
- Protocol Independent Multicast- Source-Specific Multicast (PIM-SSM): When a multicast source is specified, a host can join the multicast source directly, without registering with the Rendezvous Point (RP).
- Anycast RP: Multiple RPs can exist in a domain 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 RP's shared tree. When an RP expires, the multicast source and receiver

registered on that RP choose another nearby RP to register and join, sharing the load across RPs.

- IPv6 multicast routing protocols: PIM-IPv6-DM, PIM-IPv6-SM, and PIM-IPv6-SSM.
- Multicast Listener Discovery (MLD): MLD is used to set up and maintain the groups' member relationships between hosts and their directly connected multicast routers. MLD functions and is implemented the same way as IGMP. MLD has the following versions:
  - MLDv1

    MLDv1 is defined in RFC 2710 and derived from IGMPv2. MLDv1 supports the Any-Source Multicast (ASM) model.
  - MLDv2

    MLDv2 is defined in RFC 3810 and derived from IGMPv3. MLDv2 supports the ASM. With the help of SSM mapping, MLDv2 can support the Source-Specific Multicast (SSM) model.

When the multicast routing module receives, imports, and advertises multicast routes, the S9700 can filter the routes based on routing policies. When forwarding IP multicast packets, the S9700 can filter and forward packets based on these policies.

3.3.2 IGMP Snooping and MLD Snooping

Located between the host and the multicast router, the S9700 can statically configure multicast forwarding entries. In addition, the S9700 maintains the multicast group, the VLAN ID mapping and outbound ports by listening to passing IGMP/MLD messages. The S9700 dynamically sets up a Layer 2 forwarding table for multicast packets.

When the S9700 receives a multicast packet, it only forwards the packet to the VLAN members of that multicast group. Based on the Layer 2 forwarding table, the packet is multicast while in the VLAN. This reduces the number of packets transmitted over the network to save network bandwidth, and improves information security.

Prompt Leaving of Ports

When one of the S9700's ports are attached to only one host, the S9700 directly deletes that port's corresponding multicast forwarding entry as long as it receives an IGMP/MLD Leave message from the host through that port. After that, the S9700 does not forward IGMP/MLD Query messages to that port, saving bandwidth and system resources while ensuring prompt switchover of services.

Multicast Querier

On a Layer 2 network, the S9700 can act as querier for the following multicast functions:

- Run queries.
- Establish multicast forwarding tables on Layer 2 networks.

Multicast Packet Suppression

If the S9700 receives a Report packet or Leave packet from users within a short period of time, the S9700 checks whether the same Report packet or Leave packet has been received during the suppression period. The S9700 then decides whether to send the packets to the router, reducing the number of IGMP/MLD packets handled by the router.

Controllable Multicast

The S9700 can control VLAN users multicast group access by configuring ACL, facilitating controllable multicast communication.

Multicast Call Admission Control (CAC)

Multicast CAC is mainly used to control the number and bandwidth of IPTV channels used in the Layer 2 IPTV multicast scheme, preventing users from requesting additional channels or bandwidth to ensure high service quality for all users.

3.3.3 Static Multicast

A user host receives multicast traffic through a DSLAM. For example, the Set Top Box (STB) receives video programs from Broadband Television (BTV). The S9700 can be deployed between multiple DSLAMs and an upstream multicast router. If IGMP/MLD is not enabled for some VLANs on the S9700, the S9700 sets up a multicast member relationship statically and sets up multicast forwarding entries for those VLANs as required.

Each DSLAM supports controllable multicast and can directly control the addition, deletion, and switching of channels from the STB. The S9700 is not involved in IGMP/MLD packet transmission; thus the delay generated by images and voices when the number of users switch channels is greatly reduced.

3.3.4 Multicast VLAN and Multicast Replication

Multicast VLAN is used to converge and forward the multicast packets from different VLANs. Users join a multicast VLAN when they need multicast packets. The multicast VLAN copies multicast packets to different user VLANs, carrying out multicast duplication across VLANs. The S9700 can copy up to 127 copies of multicast packets of different VLANs to each port.

The S9700 forwards multicast packets through the multicast VLAN, and copies the packets based on the multicast entries. The S9700 then sends these packets to different users' VLANs. Using the multicast VLAN technique, the S9700 can converge the multicast packets from all user VLANs into one or several VLANs.

Multicast VLAN enables the S9700 to send unicast packets and multicast packets through different VLANs, helping to manage and control multicast traffic and conserve the bandwidth resources.

3.4 QoS

This section describes the basics of QoS supported by the S9700.

3.4.1 Hierarchical Traffic Policing

The S9700 supports two-level traffic policing, namely, traffic policing based on users and traffic policing based on user groups. It supports bandwidth multiplexing of users and user groups.

Traffic policing is used to monitor service traffic matching traffic classifier rules on an inbound interface, allowing the interface to be adapted to available network resources such as bandwidth. Traffic policing limits the rate of traffic on the inbound interface, allowing the S9700 to monitor incoming traffic. If the rate is too high, the S9700 chooses to discard packets or reset packet priorities.

The S9700 supports the two-rate-three-color marker and one-rate-two-color marker, guaranteeing granular bandwidth management.

3.4.2 Flow Control

Flow control is used for congestion management. When a network cannot provide the committed or negotiated performance specifications, such as rate, congestion occurs.

In this case, an Ethernet switch sends pause frames to its peer to inform the peer to stop sending data for a while. This helps decrease the volume of traffic on the network. When flow control is enabled on a port, it applies to all traffic on the port.

3.4.3 Re-marking

With re-marking, the S9700 applies service parameters to packets that match certain ACL rules. Re-marking is implemented as follows:

- The S9700 applies self-defined service parameters to packets.
- The S9700 applies service parameters as defined by the mapping table according to packets' Differentiated Services Code Point (DSCP).
- The S9700 applies service parameters as defined by the mapping table according to DSCP defined by users.
- Users assign service parameters to packets.

3.4.4 Queue Scheduling

When an Ethernet switch forwards multiple packets, these packets may compete for resources. The S9700 uses the following queue scheduling algorithms to address this problem:

- Strict Priority (SP)
- Weighted Round Robin (WRR)
- SP + WRR
- Deficit Round Robin (DRR)
- SP + DRR

Outgoing packets on Ethernet switch ports are forwarded differently as decided by the preceding algorithms.

3.4.5 Congestion Avoidance

When congestion occurs, a switch immediately discards certain packets to release queue resources. The switch also schedules packets into queues other than those experiencing delay to help alleviate congestion.

The S9700 supports the Weighted Random Early Detection (WRED) algorithm. WRED monitors packets in each queue and compares the queue length to its lower packet drop threshold. Based on this, the S9700 processes packets in queues in the following ways when congestion occurs.

- When a queue is shorter than the lower threshold, the device does not discard packets.
- When the queue length is between the lower threshold and the upper threshold, WRED begins to discard packets randomly.

- When the queue is longer than the upper threshold, the device discards all incoming packets.

3.4.6 Traffic Shaping

Traffic shaping controls the outgoing packet transmission rate, ensuring packets are transmitted at an even rate. Traffic shaping is applied to downstream traffic to make its transmission rate the same as that provided by downstream devices. This prevents packets from being discarded and traffic congestion. The difference between traffic shaping and traffic policing is that traffic shaping is used to buffer packets that exceed the set rate limit and then transmit packets at an even rate; traffic policing is used to discard packets that exceed the set rate limit. In traffic shaping, packets are delayed for transmission. In traffic policing, however, no delay is added for packets.

The S9700 shapes traffic for all interfaces and CoSs. Different types of traffic shaping can be implemented using different parameters.

3.5 Reliability

This section describes the basics of link aggregation, BFD, and HA at the equipment level.

3.5.1 Link Aggregation

The S9700 can manually bind multiple ports to an Eth-Trunk interface. The S9700 also supports link aggregation in static mode. That is, the administrator can set up an aggregation group and add member links, and the Link Aggregation Control Protocol (LACP) will maintain the aggregated link.

When one of the links fail, traffic is balanced among the other links without interruption. The S9700 can aggregate links on different LPUs, improving service reliability.

3.5.2 DLDP

The S9700 supports Device Link Detection Protocol (DLDP). DLDP monitors the link status of optical fibers or copper twisted-pair cables. If a unidirectional link exists, DLDP automatically shuts down or notifies users to manually shut down the port on the unidirectional link as required, preventing network faults.

3.5.3 RRPP and Multi-Instance Technology

To reduce the impact of network scaling on convergence time, Huawei has developed Rapid Ring Protection Protocol (RRPP), a data link layer protocol used exclusively in Ethernet ring networks.

When an Ethernet ring network is complete, RRPP can prevent broadcast storms caused by data loops. When a link is disconnected, RRPP helps quickly enable the standby link and then restore communication between nodes on the ring network.

Compared with other Ethernet ring technologies, RRPP boasts the following features:

- Convergence time is unrelated to the number of nodes on a ring network. Thus, RRPP can be applied to a network with a great diameter.
- RRPP can prevent broadcast storms caused by loops when an Ethernet ring network is complete.

- On an Ethernet ring network, when a link is down, a backup link immediately starts up to resume normal communication between nodes.

On intersecting RRPP rings, when the topology of a ring changes, topology flapping will not occur on adjacent rings, improving data transmission reliability.

RRPP multi-instance technology applies to ring Ethernet networks, in which different RRPP instances are applied to different C-VLANs so they may carry out independent topology calculations and convergence. In addition, multi-instance technology optimizes networks and simplifies the configurations of complex topologies containing multiple intersecting rings or multiple rings in multiple domains.

3.5.4 Smart Link and Multi-Instance Technology

Dual-homing networking is one of the most commonly used forms of networking. In most cases, STP is enabled to implement link backup; however, STP cannot meet quick convergence requirements.

Thus, Smart Link was developed to provide link backup and fast switching between active and standby link traffic, ensuring fast link convergence. In a dual-homing network, when the active link fails, the device automatically switches traffic to the standby link. In this manner, the redundant link is blocked and link backup is assured.

Smart Link features are as follows:

- Dedicated to dual-homing networks
- Down to sub-second convergence time
- Easy to configure and operate

In Smart Link multi-instance, a Smart Link group is configured with multiple instances and each instance is configured with a VLAN range. Commands are used to configure some instances to transmit packets through standby links. Thus the VLANs transmit packets through different paths to implement load balancing.

3.5.5 Ethernet OAM

The S9700 supports Ethernet OAM, including fault management and performance management.

Point-to-Point Ethernet Fault Management

Ethernet fault management detects network connectivity by sending detection packets periodically or through manual triggering, which is similar to implementation of the Bidirectional Forwarding Detection (BFD). OAM also provides methods similar to the ping and Traceroute on IP networks to locate faults on an Ethernet network. The fault management mechanism can trigger a protective switchover, with service interruption less than 50 ms.

IEEE 802.3ah, put forward by the Ethernet in the First Mile Alliance (AFMA), defines capability discovery, link performance monitoring, fault detection and alarm, and loop detection. It also detects faults on a direct Ethernet link, especially on a user access link. 802.3ah is a slow protocol and the interval for sending detection packets is 1 second.

Conforming to IEEE 802.3ah, the S9700 supports the point-to-point Ethernet fault management. It can detect faults in the last mile of a direct link on the user side. Currently, the S9700 supports automatic neighbor discovery, link fault monitoring, remote fault notification, and remote loopback configuration defined in IEEE 802.3ah.

End-to-End Ethernet Fault Management

IEEE 802.1ag applies to bridges (VLAN-aware) on the virtual bridging network to provide fault detection, verification, and isolation. It can detect a fault within 50 ms. The fault management mechanism can trigger a protective switchover, with service interruption less than 50 ms. 802.1ag provides the following fault management functions to ensure normal packet forwarding.

- Fault detection, that is, continuity check (CC) function
- Fault verification through loopback packets
- Fault location and isolation (Traceroute)
- Fault notification and alarm suppression through alarm indication signal (AIS) and remote defect indicator (RDI). The AIS is not supported currently.

Conforming to IEEE 802.1ag, the S9700 supports the end-to-end Ethernet fault management.

- Hierarchical MD

  IEEE 802.1ag detects end-to-end Ethernet connectivity and locates faults. It provides different levels of Maintenance Domains (MDs). 802.1ag packets from a low-level MD will not be forwarded to a high-level MD. This ensures network security and maintainability.

  An MD is defined in IEEE 802.1ag as a network deployed with Ethernet OAM. An MD is a Multiple Spanning Tree (MST) domain composed of multiple interconnected S9700s. Multiple service instances (SIs) can be configured in an MD. Each SI associates with a VLAN. An SI consists of multiple devices. The interface connected to the customer equipment (CE) is called the Maintenance association End Point (MEP), and other interfaces, called the Maintenance association Internal Points (MIPs), connect different MEPs. MEPs and MIPs are called the Maintenance Points (MPs). All MEPs in an SI make up a Maintenance Association (MA). The fault detection is performed on all MEPs in an MA.

  Part of the network in an MD may be maintained by another administrator, that is, MDs may be nested. Different levels of OAMs can run in an MA. The MD level differentiates OAMs at different levels. The MD level is carried in OAM packets. OAM packets from a low-level MP are discarded by a high-level MP.

- End-to-End Fault Detection and Location

  ISPs and Internet Context Providers (ICPs) use fault detection to guarantee QoS and reduce maintenance expense. Fault detection is implemented by sending and detecting CC packets periodically.

  MAC ping and MAC Traceroute is implemented to locate network faults by sending Loop Back (LB) and Link Trace (LT) packets defined in IEEE 802.1ag.

  - MAC Ping

    MAC ping implemented by sending LB packets can detect whether a device on the network is reachable and acquire the network status and the delay parameter.

    An MAC ping test can be carried out between any two devices on the network as long as the following conditions are met:

    The MAC ping test is initiated by an MEP.

    The two devices are MPs in the same MA.

    Two devices can exchange Ethernet service packets.

  - MAC Traceroute

    MAC Traceroute implemented by sending LT packets can detect the actual service path and the faulty point between two devices on a network.

Conditions to implement MAC Traceroute are the same as those to implement MAC ping.

Ethernet Performance Management

Performance management is used to measure the packet loss ratio, delay, and jitter during packet transmission. It also collects statistics on various types of packets, including the number of sent and received bytes and number of error packets.

Conforming to the ITU-T Y.1731 standard, the S9700 supports the Ethernet performance management. The S9700 measures the delay, jitter and packet loss ratio during the transmission by inserting the timestamp in the LB packets defined in IEEE 802.1ag. In this way, the S9700 can detect performance and obtain end-to-end performance parameters of a certain service flow in a specified period or on a specified network segment. You can configure the device to measure performance parameters periodically and export these parameters in the NMS report.

By using performance management tools, an ISP can monitor the network running status and locate faults through the NMS. The ISP can then check whether the forwarding capability of the network complies with the Service Level Agreement (SLA) signed with users. These operations are not performed on the user-side network, which greatly reduces network maintenance expenses.

3.5.6 BFD

The S9700 supports BFD to implement fast detection and monitor the link connectivity.

BFD performs fast link failure detection using the "Hello" protocol. Detection packets are transmitted periodically from both ends of a bidirectional link. If the S9700 fails to receive a detection packet from the peer end within a certain period of time, it indicates that a segment of the bidirectional link has failed. BFD then triggers the switchover mechanism to ensure network reliability.

BFD supports failure detection in milliseconds. BFD also supports asynchronous detection.

The S9700 supports the following BFD detection methods:

- Link detection
- IP routing connectivity detection
- LSP, CR-LSP, and MPLE TE protection group connectivity detection
- BFD detection on VPLS networks

  It also processes diagnostic packets that manage VPLS switchover and performs the switchover.

The S9700 supports the association among BFD, 802.3ad, and 802.1ag to provide an end-to-end OAM solution.

3.5.7 ERPS

On a Layer 2 switching network, packets will be generated and transmitted infinitely once a loop occurs, causing a broadcast storm. All available bandwidth is consumed by the broadcast storm, and therefore valid packets cannot be transmitted on the network.

Ethernet Ring Protection Switching (ERPS) is defined in ITU-T G.8032 Recommendation. It prevents logical loops on a ring network by blocking redundant links.

ERPSv1 supports only the single-ring topology. When there is no faulty link on a ring network, ERPS can eliminate loops on the network. When a link fails on the ring network, ERPS can immediately restore the communication between the nodes on the network. Compared with other ring network protocols, ERPS has the following advantages:

- The network converges fast.
- ERPS is a standard protocol published by the ITU-T; therefore devices from different vendors can communicate with each other when they run ERPS.

3.5.8 LSP Protection Switchover

The S9700 supports MPLS OAM and fast detection of LSP faults. A standby LSP can be set for the active LSP to implement 1+1 LSP backup. When the active LSP fails, services are fast switched to the standby LSP, greatly improving network reliability.

3.5.9 Equipment Level Reliability

Hot Backup

The S9700 supports hot backup for its key components including the SRU/MCU, power modules, and fan modules.

- SRU/MCU

  The S9700 can be equipped with two SRUs/MCUs running in 1+1 backup mode.
- The two SRUs/MCUs in 1+1 backup mode support two types of protection switchover:
  - Automatic protection switchover

    Triggered by the system upon a serious fault or an active SRU/MCU reset.
  - Forcible protection switchover

    Triggered by commands through the console port. You can also prevent the SRU/MCU active/standby switchover through the console port.

After an active/standby switchover occurs, the standby SRU/MCU immediately takes over all services, ensuring service continuity and system availability.

- Power modules

  If one of the power modules fails, the other power modules immediately take over services without interruption.

  The S9700 does not support PoE boards.
- Fan modules

  Each fan frame of the S9700 provides two fan frame layers for backup. If one fan frame fails, the other fan frame ensures that the ambient temperature does not exceed 45°C. A single fan frame working alone to control ambient temperature can normally work at least for a maximum 96 hours.

  When a fan fails, the system generates an alarm message.

Hot Swap

The SRU, MCU, LPU, CMU, power modules, and fan frames of the S9700 are all hot swappable.

- SRUs/MCUs

  When the S9700 has two SRUs/MCUs working in 1+1 backup mode, hot swapping the standby SRU/MCU does not interrupt services. Hot swapping the active SRU/MCU, however, causes a fast switchover of services to the standby SRU/MCU. The data switching units on the two SRUs support load balancing. When an SRU is removed, data service traffic may be lost.

- LPUs
- Power modules

  When four power modules are all running on the S9700, hot swapping one or two of them will not interrupt services.
- Fan frames

  Hot swapping fan frames will not affect S9700 services.
- Air filters

  The air filter is not powered and is easily swapped for convenient routine cleaning.

Inter-SIC Eth-Trunk

Multiple Ethernet ports, either on the same SIC or different SICs, can be bound to a logical Eth-Trunk interface, creating a backup between ports and implementing traffic load balancing.

When one member port in an Eth-Trunk interface fails, that port's services are automatically carried by other ports in the Eth-Trunk interface. In this case, the Eth-Trunk interface can still handle services normally, ensuring service transmission is not affected.

Since bound ports belong to different SICs, inter-SIC Eth-Trunk reduces the impact of one SIC fault and eliminates single-site faults.

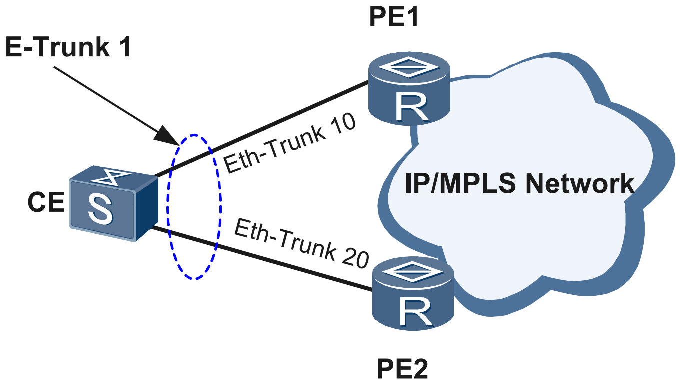
E-Trunk Composed of Ethernet Interfaces on Different Devices

As an extension to the Link Aggregation Protocol (LACP) that implements link aggregation on a single device, the Enhanced Trunk (E-Trunk) protocol implements link aggregation across different devices, improving link reliability.

The E-Trunk is mainly applied to CEs that are dual homed to VPLS, VLL, or PWE3 networks. In these situations, E-Trunk protects the links between the CEs and PEs, preventing faults on PEs. Before the E-Trunk is implemented in a system, a CE can only be connected to a PE through an Eth-Trunk.

If the Eth-Trunk or the PE fails, the CE cannot communicate with the PE. However, once the E-Trunk implemented, the CE can be dual homed to two PEs, ensuring effective backup between devices.

Figure 3-6 Networking diagram of an E-Trunk



CSS

A single switch cannot meet the demands of increasing data center access volume and ensure network reliability. The S9700 uses specialized Cluster Switch System (CSS) technology to meet these growing demands.

The S9706 and S9712 support CSS. Two switches can be connected through service interfaces to function as one logical switch. The S9706 and S9712 support short-distance and long-distance CSS.

The stacking technology provides users with the following benefits:

- Protecting investments during network capacity expansion
- Simplifying configuration and management during capacity expansion: multiple physical switches form a logical switch
- Improving system reliability through switch redundancy and backup

Preventing Hardware Abnormalities

The S9700 separates the control channel from the service channel, creating a non-blocking control channel. The S9700 supports the following measures for protecting against abnormalities:

- Error correction for memory chip faults.
- Protection against power input interface mis-insertion.
- Fan frames with independent power supply channels, ensuring redundancy.
- Over-current and over-voltage protection for power and interface modules.
- Protection against board mis-insertion to avoid inserting H-SICs into L-SIC slots.
- Monitoring and alarm systems for the power modules, voltage, and ambient temperature.

Operation Protection

The S9700 supports the following protection measures:

- In-service BootROM upgrade, in-service patching, and version rollback.
- Data hot backup between the active and standby units. The active unit automatically switches to the standby state when failures occur on the active unit to prevent data loss.
- Regular synchronization of configurations between the LPUs and SRUs/MCUs.
- VRP system software exception monitoring, including automatic restoration and log records.
- Dying gasp that records key fault information.

The S9700 provides prompt for improper operations. If the commands negatively impacting system performance are entered, the system requests users to confirm the operations.

3.6 Security

This section describes the security measures for devices and services.

3.6.1 Device Security

Hierarchical Command Lines

To ensure security, the S9700 authenticates users when using Ethernet ports to Telnet into a device. Users can log in to configure and maintain the device only after they are authenticated.

S9700 commands are divided into 4 levels, and login users are also divided according to these 4 levels. After logging in to the S9700, users can only run commands that correspond to their user level.

The S9700 supports the extension of command levels and user levels, which can be mapped from four levels to 16 levels. Command level mapping is an effective means of managing and extending the variety of available user levels.

The S9700 can also lock the terminal through the command line to prevent unauthorized use.

Remote Login Through SSH

The S9700 supports Secure Shell (SSH) v1.5 and v2. On unsecured networks, SSH provides powerful security and authentication services for login users and can help defend against attacks.

Encryption Authentication in SNMP

The S9700 supports SNMPv3 encryption and authentication to authenticate the management packets from the NMS.

Authentication, Authorization, and Accounting

The S9700 supports Authentication, Authorization and Accounting (AAA). AAA supports three types of user authentication:

- Local authentication
- Remote Authentication Dial-In User Service (RADIUS)
- Huawei Terminal Access Controller Access Control System (HWTACACS) authentication

AAA can authenticate and authorize login users in combination with hierarchical command line protection and authenticate NMS administrators, helping the S9700 defend against unauthorized user login.

Hierarchical CPU Protection

The S9700 supports two levels of CPU protection:

- LPU level

  Based on protocol type, the S9700 performs flow control for protocol packets and management packets sent from the LPU to the SRU's CPU. This protects the channel between the LPU and the CPU from being congested with packets caused by Denial of Service (DoS) attacks.
- SRU level

  When the CPU receives protocol packets and management packets sent from the LPU, the S9700 performs traffic classification, re-marking, flow control, and the whitelist functions on the packets and implements QoS and rate limit on the CPU. This protects the CPU against Distributed DoS (DDoS), IP spoofing, and SYN Flood attacks.

3.6.2 Service Security

ACL-based Packet Filtering

Packet filtering is used to filter unauthorized or unwanted packets. By filtering packets, the S9700 can effectively control the passing packets.

The S9700 filters packets based on user-defined rules. For example, it can filter packets according to the source or destination address of the packet. Packet filtering does not check the state of sessions and does not analyze the data.

DHCP Snooping/Option 82

When deployed between the server and client of the Dynamic Host Configuration Protocol (DHCP), the S9700 listens to the sent DHCP packets. The S9700 then sets up a table binding the IP address with a MAC address according to the monitoring results. This suppresses unauthorized packets from being transmitted. The S9700 can also insert or strip a packet's Option 82 field.

- After receiving a request packet from the DHCP client, the S9700 inserts the Option 82 field into the packet. The DHCP server then assigns IP addresses by identifying the Option 82 field.
- The DHCP server inserts the Option 82 field into the response packet. The S9700 analyzes the Option 82 field to select the appropriate forwarding port. The S9700 then strips the Option 82 field and forwards the packet to the user.

The Option 82 field records the user circuit's ID number, which can be used to effectively defend against DHCP packet tampering.

Similarly, with the IP session feature, the S9700 checks the IP addresses, MAC addresses, interface numbers, and VLAN IDs of packets according to VLAN or Option 82 information to prevent unauthorized users from forging IP addresses.

MAC Address Learning Limit

The S9700 can restrict the maximum number of MAC entries learned by a port. This can defend against attacks using forged MAC entries and prevent the MAC table resources from being used up.

The S9700 scan limit the number of MAC addresses based on the following factors:

- Ports
- VLAN IDs
- VSIs

When the number of MAC addresses learned by a port exceeds the pre-defined threshold, the S9700 forwards or discards incoming packets with new MAC addresses as configured.

Blackhole MAC Entries

The S9700 supports blackhole MAC entries. When the S9700 receives a packet, it compares the packet's destination MAC address with the MAC entries in the blackhole MAC table. If the packet's MAC address matches an entry in the table, the packet is dropped.

After detecting that certain packets with specific MAC addresses are attack packets, the administrator can set a blackhole MAC entry to filter these packets based on that MAC address, preventing attacks using that MAC addresses.

MAC+VLAN-based Port Binding

To improve interface security, the S9700 allows network administrators to add static entries to the MAC address table. Static entries identify mappings between specific MAC addresses, VLAN IDs, and interfaces, binding the S9700 to specific interfaces and preventing MAC spoofing attacks.

Broadcast Suppression

The S9700 can limit the transmission rate of broadcast packets, multicast packets, and unknown unicast packets according to their interfaces.

The S9700 can also limit the maximum traffic percentage of broadcast packets, multicast packets, and unknown unicast packets to control broadcast packet traffic volume.

3.7 Network Management Features

The S9700 provides LLDP and NetStream network management functions.

3.7.1 LLDP

The S9700 supports the Link Layer Discovery Protocol (LLDP).

LLDP conforms to IEEE 802.1ab. LLDP discovers adjacency relationships between devices on the link layer and provides interconnected devices with each other's connection information.

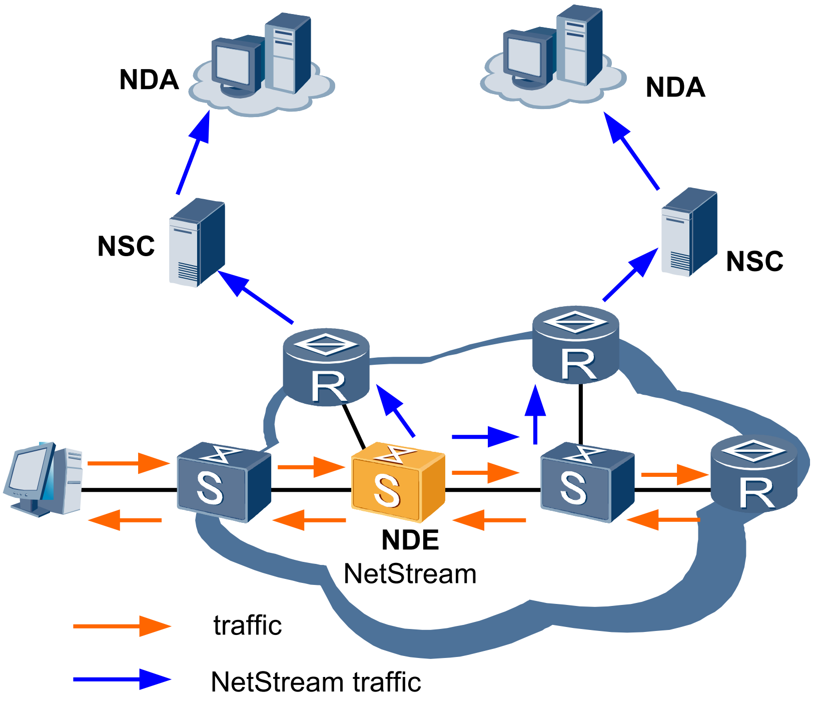
Using the LLDP, a local network management station can acquire link layer information for all devices in the local network. It can also collect detailed information about network topology and topology changes, expanding the scope of network management.

Ports with LLDP enabled on the S9700 periodically notify neighbors of their status. If the port's status changes, it sends updates of the current state to those neighbors directly connected to it. The neighbors store the port's status in the standard SNMP MIB. The NMS then searches the MIB for the link layer information of the network in order to calculate the network's topology.

3.7.2 NetStream

With an overall increase in network services and applications, users require detailed statistical analysis of network traffic. NetStream provides network administrators with detailed records of data network activity.

Figure 3-7 Network diagram of NetStream



NDE: Netstream Data Exporter NSC: Netstream Collector NDA: Netstream Data Analyzer

NetStream provides the following functions:

- Network management and planning
- Enterprise accounting and department billing
- ISP billing report
- Data storage
- Data collection for business

Due to the connectionless-oriented features of IP networks, communication between different types of services are implemented by transmitting IP datagrams from one terminal to another. Such IP datagrams actually constitute a service's data flow across a network. Most data traffic on the network is temporary and bidirectional.

Based on packets' destination IP address, source IP address, destination port number, source port number, protocol number, Type of Service (ToS), and incoming or outgoing interface, NetStream identifies different streams and collects statistics for these steams independently.

The NDE regularly sends traffic statistics to the NSC for additional processing and then forwards the statistics to the NDA. The report generated based on these analysis results acts as the basis for accounting and networking planning.

The S9700 supports:

- NDE
- IPv4/IPV6/MPLS packet sampling
- Fix-packet sampling and fix-time sampling
- Original traffic, flexible traffic, and aggregation traffic

- V5/V8/V9 packet export format

The S9700 supports both distributed NetStream and integrated NetStream.

3.7.3 sFlow

Sampled Flow (sFlow) is a traffic monitoring technology that collects and analyzes traffic statistics.

sFlow provides interface-based traffic analysis and displays traffic statistics in graphs or reports, facilitating preventive maintenance especially on enterprise networks without specialized network administrators.

NetStream is a technology that collects and analyzes statistics on network flows. Network devices need to preliminarily collect and analyze network flows, and store statistics in the cache. When the cache overflows or flow statistics expire, the statistics are exported. Compared with NetStream, sFlow does not require a cache, network devices only sample packets, and a remote collector collects and analyzes traffic statistics. Therefore, sFlow has the following advantages over NetStream:

- Saves resources and lowers costs. No cache is required, and a small number of network devices are used, which lower costs.
- Flexible collector deployment. A collector collects and analyzes traffic statistics based on various traffic characteristics as required. The collector is deployed flexibly.

3.8 Clock

This section describes the clock synchronization and calibration mechanisms supported by the S9700.

The S9700 supports clock synchronization at the physical layer and calibration mechanisms. These mechanisms ensure precision time-keeping for mobile communication services.

The S9700 uses clock data from signals transmitted over the physical transport link to synchronize the physical-layer clock frequency. The S9700 can obtain clock data from the synchronized Ethernet links.

3.9 Enterprise Network Features

The S9700 provides NAC, firewall, NAT, load balancing and WLAN AC for enterprise networks.

3.9.1 NAC

This section describes the basics of network admission control (NAC).

NAC was developed to protect enterprise intranets against attacks from emerging hacker technologies such as new viruses and worms. By using NAC, the S9700 only allows authorized or trusted devices to access the network.

The main components of NAC are as follows:

- NAC agent program installed on each terminal

- Network access device
- Policy server or AAA server
- Anti-virus server
- Management system

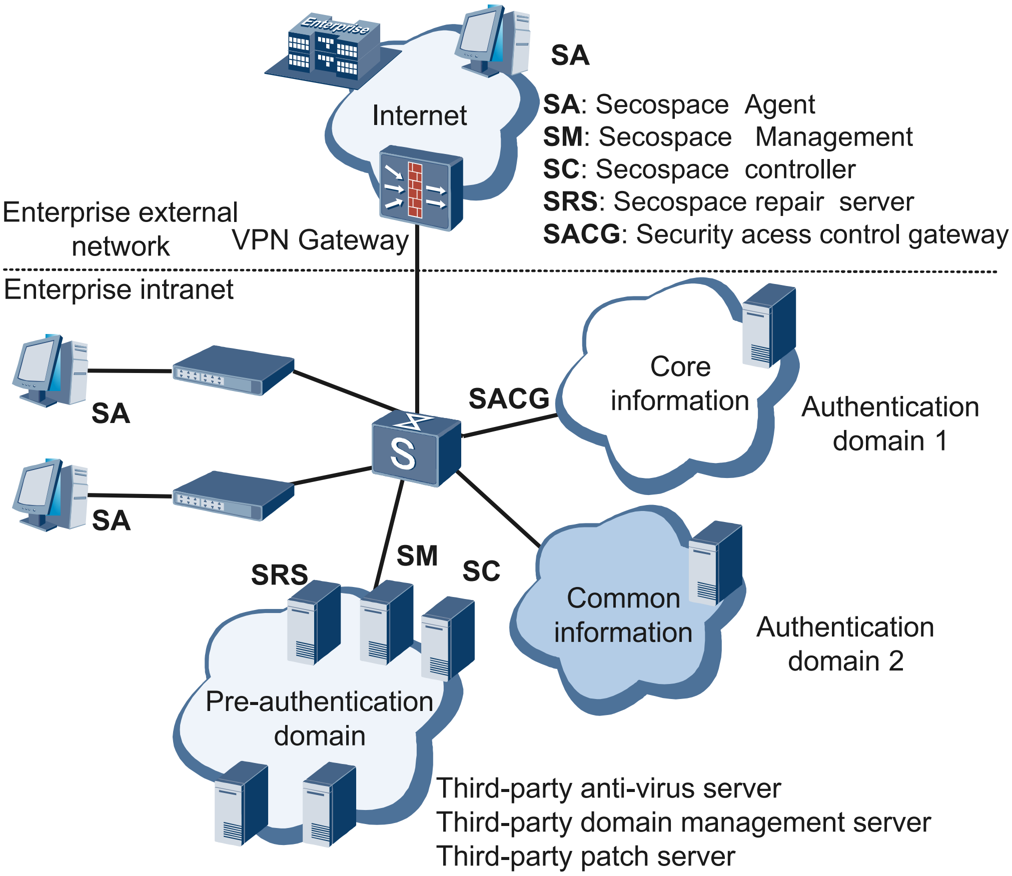
When functioning as a network access device, the S9700 provides the following functions:

- 802.1X access, including port mode and MAC mode
- Portal access
- Relay authentication in which the S9700 obtains user entries through DHCP snooping

In addition, the NAC function is applicable to the following special scenarios:

- Best-effort: Users can access the network when the RADIUS server is Down.
- Privileged users and devices without an agent, such as printer and IP phone

Figure 3-8 Network diagram containing major NAC components



3.9.2 Firewall

The S9700 provides a distributed firewall with a 10 Gbit/s processing capacity to provide high-performance security for large enterprisesand data center networks. The S9700 supports the external attack defense, internal network security, traffic monitoring, email filtering, Web page filtering, and application layer filtering, effectively ensuring network security.

The S9700 provides the following firewall functions:

- Packet filtering firewall
- Stateful firewall
- ASPF
- Blacklist
- Whitelist
- Port mapping
- Traffic statistics and traffic monitoring
- Firewall log
- Virtual firewall

The S9700 supports hot backup of firewalls in a two-node cluster. The session table and status information are backed up in real time between the master and backup firewalls. If the master firewall fails, the backup firewall seamlessly takes over the master firewall's responsibilities.

3.9.3 NAT

The S9700 provides NAT for many-to-one mapping, many-to-many mapping, static network segment mapping, bidirectional conversion, and DNS mapping for enterprises. It supports the NAT Application Level Gateway (ALG) for NAT transversal between multiple application layer protocols.

The S9700 provides the following NAT functions:

- NAT address pool
- NAPT
- Static NAT/NAPT
- Easy IP
- NAT server
- Twice NAT
- Source address associated with the VPN before NAT is performed
- NAT server associated with the VPN
- NAT ALG

3.9.4 Load Balancing

The S9700 provides server load balancing for Layers 4 through Layer 7 services and supports deployment of multiple applications and server clusters.

The S9700 supports the following load balancing algorithms:

- WRR
- Least connection
- Least bandwidth
- Load-based
- Response time-based
- Source IP address-based
- Destination IP address-based

- Source and destination IP addresses-based
- Layer 4 content-based
- HTTP packet URL-based
- HTTP packet header-based
- Cookie and content-based

3.9.5 IPSec VPN

The S9700 switches provide the IPSec VPN feature to protect data confidentiality and integrity, and prevent replay during transmission. The IPSec VPN feature provides secure IP communication between sites and between enterprise branches and headquarters.

The IPSec VPN feature of the S9700 supports the following functions:

- Manual IPSec tunnel
- IKEv1 and IKEv2
- Diffie-Hellman key exchange algorithm
- Dead peer detection (DPD)
- Authentication Header (AH) and Encapsulation Security Protocol (ESP)
- Tunnel mode and transport mode
- Message digest algorithm 5 (MD5) and secure hash algorithm 1 (SHA-1) for authentication
- Data Encryption Standard (DES), triple-DES (3DES), and Advanced Encryption Standard (AES) for encryption
- NAT traversal

The S9700 switches can initiate IPSec VPN tunnel negotiation to peer ends. When deployed in headquarters, they can accept tunnel negotiation requests from branches.

3.9.6 WLAN AC

A Wireless Local Area Network (WLAN) wirelessly links two or more computers or devices, and enabling fast Ethernet access between them. The primary advantage of WLANs is that terminals can access a network through a wireless medium rather than a physical cable which facilitates easier network construction and allows users to move around without interrupting communication. Thus WLAN is much more flexible than traditional wired access.

WLAN uses radio as the transmission medium, with a physical range of tens of meters. WLAN uses cables on the backbone layer, and subscribers access the WLAN by using one or multiple wireless access points (WAPs). WLANs are popular on campuses and in business centers, airports, and other public areas.

IEEE 802.11 is widely used by WLANs.

The S9700 functions as an access controller (AC) and provides the following WLAN functions.

AP Management

- Access points (APs) and ACs can be connected through a Layer 2 or Layer 3 network.
- APs and ACs can communicate through an IPv4 network.
- APs automatically discover reachable ACs.
  - APs discover ACs using DHCP Option 43.

  - APs discover ACs using DNS.
  - APs discover ACs using CAPWAP.
- AC access is controlled.
- AP software can be upgraded.
- APs can download configuration data.
- Huawei APs use the Option 60 field for identification.
- APs can be debugged and maintained.
  - ACs can query status information and performance statistics regarding specific APs.
  - ACs can query brief information regarding all APs.
  - ACs can restore the factory settings of APs.
  - ACs can debug AP channels through Telnet.

Control And Provisioning of Wireless Access Points (CAPWAP)

- CAPWAP control tunnels and data tunnels are both supported.
- CAPWAP control tunnels can be encrypted by using DTLS, but CAPWAP data tunnels cannot.
- Layer 2 network data can be forwarded directly and forwarded through channels.
- The Layer 3 network data is forwarded through channels.
- CAPWAP packets can be fragmented and reassembled.
- CAPWAP channel supports heartbeat detection and can be re-established after disconnection.

WLAN User Management

- Dot1X authentication is supported.
- Portal authentication is supported.
- MAC address authentication is supported.
- pre-share-key (PSK) authentication is supported.
- EAPOL-Key negotiation mechanism is supported.
- User access can be controlled based on APs and SSIDs.
- Users can be associated and re-associated.
- Users can roam under an AC.
- Load balancing is performed based on sessions or flows.
- WLAN supports AAA.

WLAN Radio Management

- Country code is supported.
- Radio type, transmission rate, and transmit power can be set.
- Radio working channels can be configured.
- Radio interference can be monitored and eliminated.
- Wireless MAC layer parameters can be set.
- Radio attributes can be configured and queried.

- Performance statistics of radio frequency interfaces can be collected and queried.
- Coverage holes can be detected and covered.

WLAN Security

- WEP Open-System link authentication and encryption are supported.
- WEP Share-Key link authentication and encryption are supported.
- WPA PSK authentication and encryption are supported.
- WPA Dot1X authentication and encryption are supported.
- WPA2 PSK authentication and encryption are supported.
- WPA2 Dot1X authentication and encryption are supported.
- WAPI authentication and encryption are supported.
- TKIP/CCMP encryption is supported.
- HMAC-MD5 algorithm is supported.
- Key update can be triggered by multiple conditions.
  - Distributed group keys can be updated.
  - Update of multicast keys can be triggered by a user's offline message.
  - Update of multicast keys can be carried out by a user manually.
- User blacklist and whitelist are supported.
- Unauthorized clients can be detected.
- Unauthorized APs can be detected (Rogue AP detection).
- Flood attacks can be detected.
- Weak IV and spoofing attacks can be detected.

WLAN QoS

- WMM (802.11e) is supported.
- Wireless-side priority can be mapped to wired-side.
- Wireless-side priority can be mapped to the CAPWAP channel.
- Bandwidth can be limited based on users.
- Bandwidth can be limited based on SSIDs.

AC Reliability

- The ACs support 1+1 cold backup.
- The ACs support load balance.

3.10 MPLS & VPN

NOTE

To implement MPLS functions, apply for and purchase the license from the local Huawei vendor.

The S9700 can be used to construct MPLS networks. Services that are external to MPLS networks are forwarded based on VLAN IDs and MAC addresses. Services within an MPLS network are transmitted based on MPLS labels. This solves problems concerning VLAN tag capacity and limits the number of MAC table entries.

The S9700 can act as the PE device or Provider (P) device on an MPLS network.

The S9700 supports multiple MPLS & VPN features, including Label Distribution Protocol (LDP) or Resource Reservation Protocol for Traffic Engineering (RSVP-TE), MPLS TE, MPLS OAM, VLL, VPLS, and MPLS L3VPN.

3.10.1 Basic MPLS Functions

The S9700 supports the following basic MPLS functions:

- LDP
- Static LSP
- Two-layer MPLS labels
- 802.1p priority mapping to the MPLS EXP field

3.10.2 MPLS TE

The S9700 supports the MPLS Traffic Engineering (TE). MPLS TE is a technique that integrates TE with MPLS. Using MPLS TE, the S9700 can create an LSP tunnel to a specified path and implement re-optimization. MPLS TE also provides protection against link or node failures by using path backup and fast reroute.

The S9700 supports the following MPLS TE features:

- TE extension based on IGP protocols including IS-IS and OSPF to collect network information
- Preemption, route pinning, and re-optimization of CR-LSP
- Establishment of CR-LSP based on RSVP TE; hot standby backup and basic backup functions of the MPLS TE tunnels
- Constraint Shortest Path First (CSPF) algorithm used to calculate the shortest path of CR-LSP
- MPLS TE tunnel and the following tunnel features:
  - MPLS TE tunnel loop detection
  - Routing and labeling record
  - MPLS TE tunnel re-establishment
  - Tunnel priority

3.10.3 MPLS OAM

The S9700 supports MPLS OAM to perform end-to-end tunnel fault detection and prompt protection switchover within 50 ms when an LSP link fails. MPLS OAM conforms to ITU-T Y. 1710, Y.1711, and Y.1720 recommendations to provide fast detection of LSP connectivity. The LSP connectivity detection interval can be adjusted as required.

Using MPLS OAM, the S9700 can rapidly detect, locate, and report faults in MPLS networks by using Connectivity Verification (CV) messages and Fast Failure Detection (FFD) messages. When a fault occurs, the S9700 triggers a protection switchover using a Forward Defection Indicator (FDI) message and a Backward Defect Indicator (BDI) message.

The S9700 supports 1:1 and N:1 protection switchover of LSPs using an active LSP and a standby LSP. When the active LSP fails, the S9700 promptly switches services to the standby LSP. This greatly improves the reliability of MPLS networks.

3.10.4 VLL

VLL is an emulation of a traditional leased line. By emulating a leased line through an IP network, it provides asymmetric, low cost point-to-point virtual leased line services. VLL is mainly applied in the access and convergence layers of a MAN.

The S9700 supports the following four modes of VLL:

- Martini

  The Martini mode uses double labels. The inner label uses the extended LDP as the signaling protocol to transmit information. The Martini mode conforms to draft-martini-l2circuit-trans-mpls. Martini extends LDP by adding the FEC type in the VC FEC to exchange the VC label.

- Kompella

  The Kompella mode uses MP-BGP as the signaling protocol. PEs set up BGP sessions to each other to discover L2VPN nodes. Kompella uses BGP as the signaling protocol to transmit Layer 2 information and VC labels to establish L2VPN in end-to-end (CE to CE) mode on an MPLS network.

- SVC

  The SVC outer label (public network tunnel) functions the same as the Martini mode. The inner label is manually specified during VC configuration without the need of VC label transmission signaling. The network topology and SVC packet interaction are also the same as in the Martini mode. Thus, the SVC is a simplified version of the Martini.

- CCC

  In Circuit Cross Connect (CCC), VCs are statically configured, similar to SVC. Different from the common MPLS L2VPN, CCC uses a single label to transmit user data. This label is used for label exchange on each Label Switching Router (LSR). Thus, the CCC uses the LSP exclusively. Static LSPs must be configured in both directions.

3.10.5 VPLS

Virtual Private LAN Service (VPLS) is used to connect more than one Ethernet LAN segment through a Packet Switched Network (PSN) and have them operate in an environment similar to a LAN. Using VPLS, an ISP can establish multipoint-to-multipoint VPN connections between widely dispersed users. This can even include enterprises located in different cities.

The S9700 functions as the PE device on a VPLS network, transmitting VPLS services by establishing through-connection between PEs.

The S9700 supports VPLS in the following modes:

- Martini
- Kompella

3.10.6 HVPLS

VPLS through-connections are required between PEs. For multiple nodes or across a large geographic area, a large-scale VPLS network is required. This requires twice as many PEs as there are established connections. In this case, HVPLS is used to establish a large-scale VPLS network.

The S9700 mainly functions as the User Provider Edge (UPE) device on an HVPLS network, converging services from CEs to Network Provider Edges (NPEs) or PE-AGGs (PE-Aggregation).

The S9700 supports HVPLS in Martini mode.

On the VPLS or HVPLS network, the S9700 maps services of different types to different Virtual Switch Instances (VSIs). The S9700 then transparently transmits these services to NPE or PE-AGG through the VPLS or HVPLS network.

3.10.7 MPLS L3VPN

This section describes the basics of MPLS L3VPN.

BGP/MPLS VPN provides Layer 3 VPN services over an MPLS network. MPLS facilitates the implementation of IP-based VPN services and meets the expansibility and manageability requirements of VPNs. The S9700 supports MPLS VPNs. A single access point can be configured with multiple VPNs, each of which identifies a type of services. This allows different types of services to be transmitted in a flexible manner over networks.

4 Application Scenarios

About This Chapter

This section describes the typical networking and applications of the S9700.

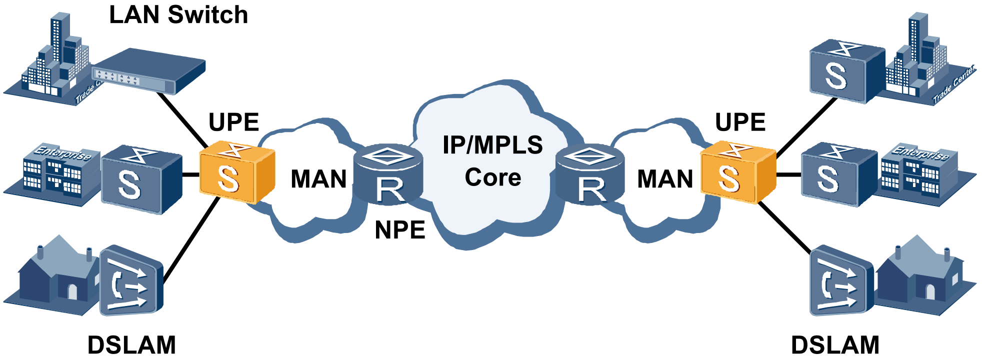
This section describes how the S9700 functions as an AC on a WLAN.

4.1 Overview

This section describes the S9700's position within the access layer and convergence layer in a MAN.

The S9700 is deployed at the access layer and convergence layer of a MAN. **Figure 4-1** shows a representative networking diagram.

Figure 4-1 Networking diagram of an S9700 deployed in a MAN



Acting as the UPE device in a MAN, the S9700 converges Internet, VPN, IPTV, and VoIP services from downstream devices such as Digital Subscriber Line Access Multiplexer (DSLAM) and LAN switches such as S2700 and S3700.

The S9700 also connects to the upstream NPE devices, such as the Huawei ME60 and NE40E. Additionally, the S9700 can act as a PE-AGG in complex networks to implement multiple levels of aggregation.

4.2 MPLS L2VPN

This section describes how MPLS VPN can be applied to a network.

The whole S9700 system supports 4K VLL instances and up to 1K VPLS instances.

As shown in **Figure 4-2** and **Figure 4-3**, the S9700 functions as the UPE on a L2VPN network, supporting VLL and VPLS and providing point-to-point and multipoint-to-multipoint VPN services.

Figure 4-2 Network diagram of point-to-point VPN (VLL)

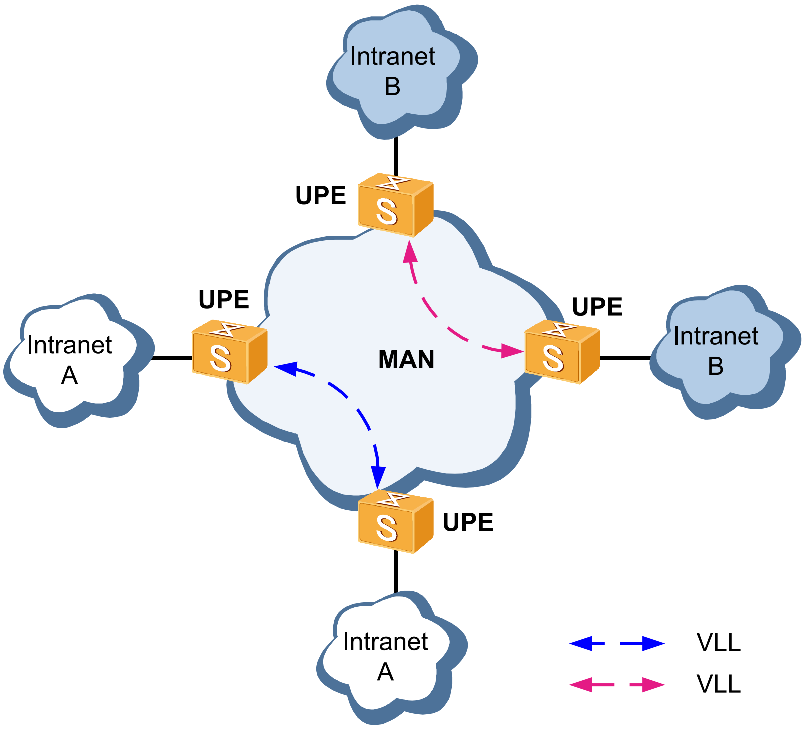
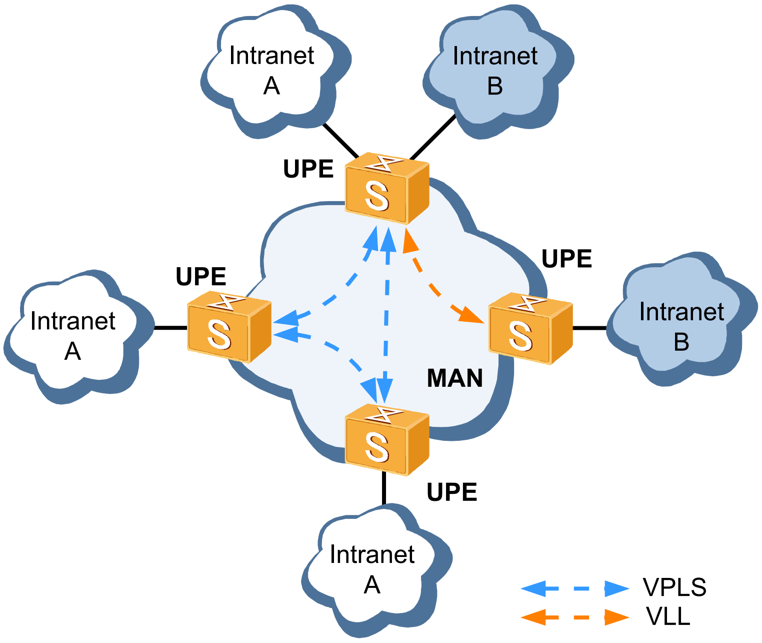


Figure 4-3 Network diagram of multipoint-to-multipoint VPN (VPLS)

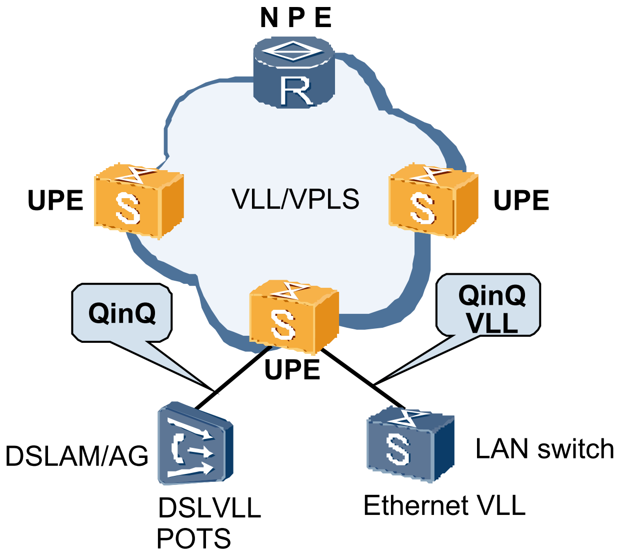


As shown in **Figure 4-4**, by cooperating with the DSLAM, Access Gateway (AG), and Layer 2 switches, the S9700 maps access services to VLL or VPLS services.

- Along with the DSLAM/AG, the S9700 maps QinQ tunnels to VLL or VPLS service instances, facilitating Digital Subscriber Line (DSL)-based VLL services.
- Along with Layer 2 switches, the S9700 maps QinQ tunnels and VLL tunnels to VLL or VPLS service instances.

The S9700 handles multiple services at both the access and convergence layers. The S9700 can map specific personal services such as broadband access and VoIP to VLL or VPLS service instances.

Figure 4-4 Network diagram of an S9700 running VPN services on a CE-supported network



The S9700 provides low-cost VLL or VPLS solutions, allowing MPLS and MPLS VPN to be applied at the edge convergence layer.

- Solves the issue of pure Ethernet with respect to scalability, carrier-class reliability, and manageability.
- Lessens the burden on higher-level NPEs and eliminates single-site faults.
- Customizes services through distributed service processing using services implemented by devices at the edge convergence layer.

4.3 Dual-homing Protection Using HVPLS

This section describes how HVPLS can be applied at the access layer and convergence layer of a MAN.

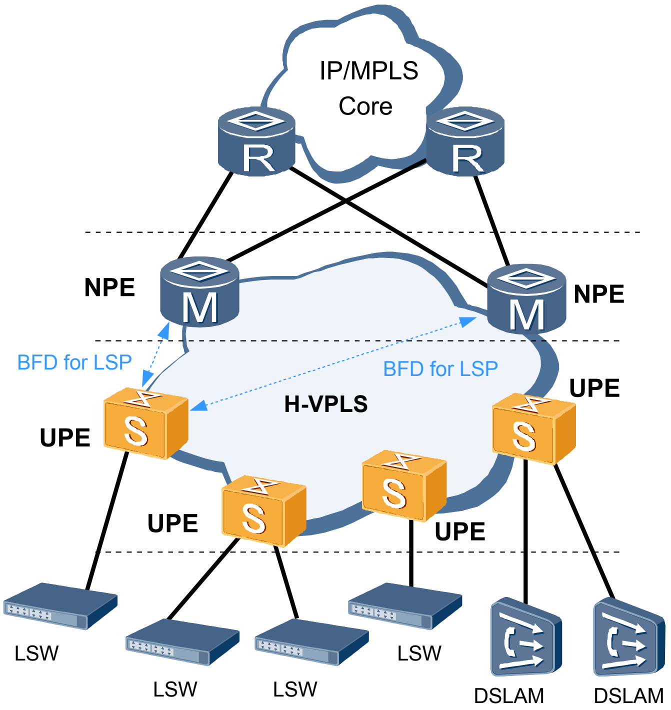
The S9700 supports HVPLS for link protection between two NPEs in dual-homing mode. On an HVPLS network, the S9700 acts as a UPE device to converge services from the CE.

The S9700 supports the following HVPLS network architectures:

- UPE+NPE Network Architecture
- UPE+PE-AGG+NPE Network Architecture

4.3.1 UPE+NPE Network Architecture

Figure 4-5 Network diagram of an S9700 running HVPLS on a UPE+NPE network



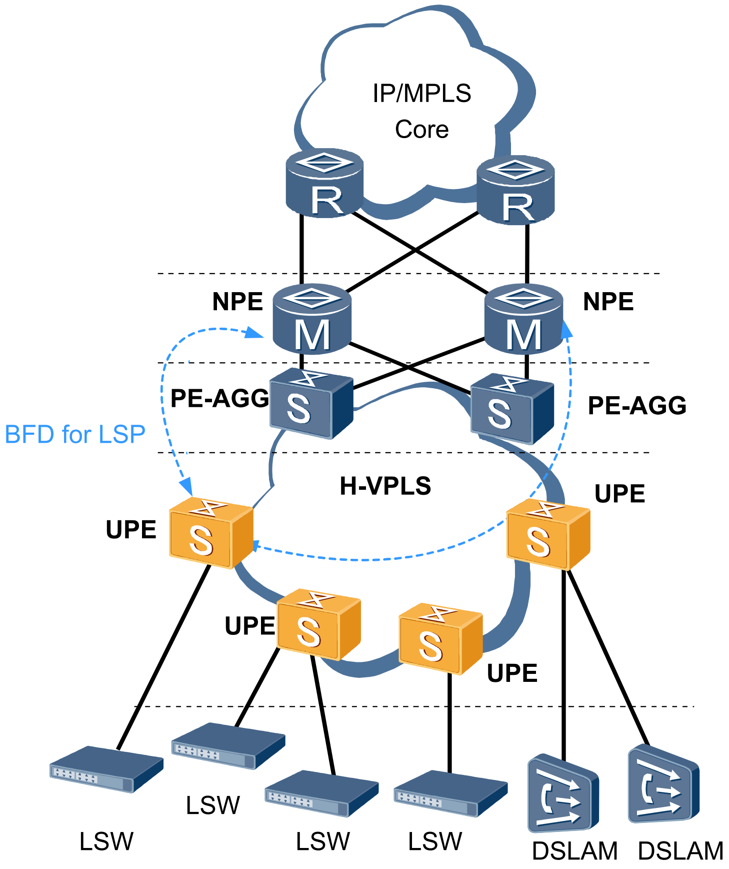
As shown in **Figure 4-5**, on the HVPLS network, the S9700 acts as the UPE device. The Huawei ME60 and NE40E routers can be used as the NPE devices.

- As the UPE device, the S9700 accesses services and classifies traffic using selective QinQ. Different services can be mapped to different VSIs and then transparently transmitted to NPE devices through HVPLS.
- The NPE terminates services on the Pseudo Wire (PW) tunnel and then process services based on VLAN ID and QinQ information.
- Link protection on an HVPLS network is carried out using an MPLS TE protection group combined with BFD for LSP.

4.3.2 UPE+PE-AGG+NPE Network Architecture

PE-AGG devices can be added between UPE and NPE devices. PE-AGG devices aggregate services, terminate VPLS, and transparently transmit services to NPE devices. The S9700 can serve as the PE-AGG or UPE device as shown in **Figure 4-6**.

Figure 4-6 Network diagram of an S9700 running HVPLS on a UPE+PE-AGG+NPE network



In this networking mode:

- The S9700 functions the same in this network architecture as in "**UPE+NPE Network Architecture**."
- The S9700 terminates VPLS tunnels and transparently transmits services to NPE devices.
- The NPE devices decapsulate VLAN and QinQ packets.
- Link protection between the S9700 and the NPE device is implemented using BFD for LSP.

4.4 RRPP

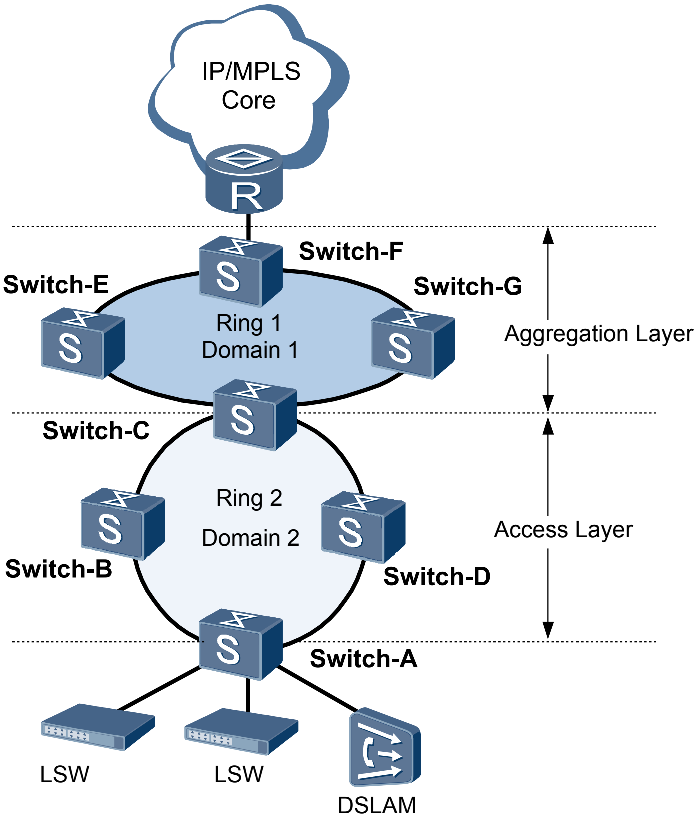
This section describes how RRPP implements fast protection switchover on ring networks.

When common Ethernet ring networks are used, RRPP is used instead of MSTP to achieve fast convergence of network topologies.

Generally, metro Ethernets use two-layer rings:

- The convergence layer lies between PE-AGGs, for example, RRPP Domain 1 shown in **Figure 4-7**.
- The access layer lies between PE-AGGs and UPEs, for example, RRPP Domain 2 shown in **Figure 4-7**.

Figure 4-7 Network diagram of RRPP applied to intersecting RRPP rings



As shown in **Figure 4-7**, Ring 1 belongs to Domain 1; Ring 2 belongs to Domain 2. Ring 1 and Ring 2 are tangent at Switch-C.

- On Ring 1, Switch-C is the master node; Switch-C, Switch-E, Switch-F, and Switch-G are PE-AGGs.
- On Ring 2, Switch-C is the master node; Switch-A, Switch-B, and Switch-D are UPEs.

For multiple tangent RRPP rings, a ring failure will not affect other domains. The RRPP ring convergence process in a domain is the same as that of a single ring.

On RRPP rings, Layer 2 and Layer 3 services can be fast switched in the event of link faults.

- Fast switch of Layer 2 services

  In normal situations, the data flow travels along Switch-A → Switch-B → Switch-C on Ring 2. If the link between Switch-A and Switch-B fails, the data flow switches to another path on the RRPP ring.

  After the link between Switch-A and Switch-B fails, the master node is notified of the link fault and immediately unblocks the secondary port.

  At this time, the network topology changes, the original MAC address tables of the nodes cannot correctly direct Layer 2 forwarding. Thus, Layer 2 traffic is interrupted. After unblocking the secondary port, the master node immediately requires other nodes on the ring to re-learn MAC address entries. The Layer 2 traffic on the RRPP ring is then switched to travel along Switch-A → Switch-D → Switch-C.

- Fast switch of Layer 3 services

In normal situations, the data flow travels along Switch-C → Switch-E → Switch-F on Ring 1. If the link between Switch-C and Switch-E fails, the data flow switches to another path on the RRPP ring.

After the link between Switch-C and Switch-E fails, the master node is notified of the link fault and immediately unblocks the secondary port.

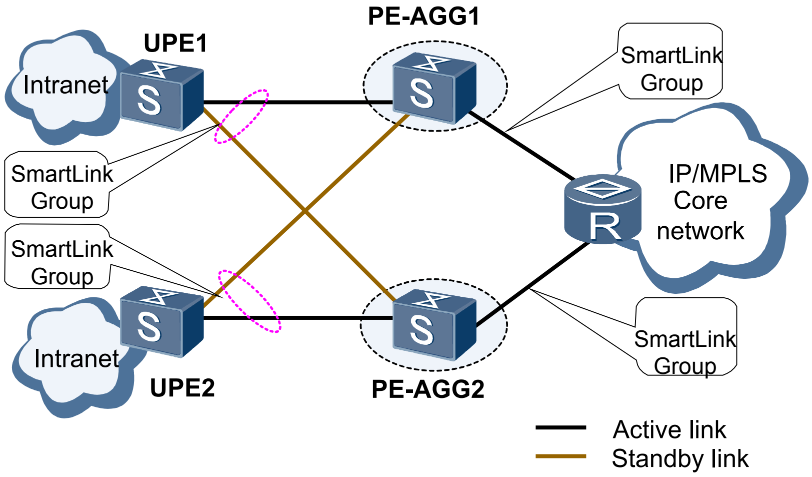
At this time, the network topology changes, so the original ARPs and FIBs of the nodes cannot direct Layer 3 forwarding. After unblocking the secondary port, the master node immediately requires other nodes on the ring to re-learn MAC address entries. The Layer 2 traffic on the RRPP ring is then switched to travel along Switch-C → Switch-G → Switch-F.

4.5 Smart Link in Dual-Homing Networking

This section describes how Smart Link functions in dual-homing networks.

Generally, Smart Link is used on dual-homing Ethernet networks for fast switching of links.

Figure 4-8 Network diagram of Smart Link deployed in a dual-homing network



Smart Link can be deployed anywhere on a MAN to provide dual-homing connections. Using Smart Link, UPE 1 or UPE 2 is dual-homed to PE-AGG 1 and PE-AGG 2.

As shown in the figure, Smart Link group is configured on UPE 1 and UPE 2, and upstream devices only need to receive and send Flush packets. In the two uplinks, one link forwards packets while the other is blocked. When the active link fails, Smart Link quickly senses the fault and switches traffic to the standby link.

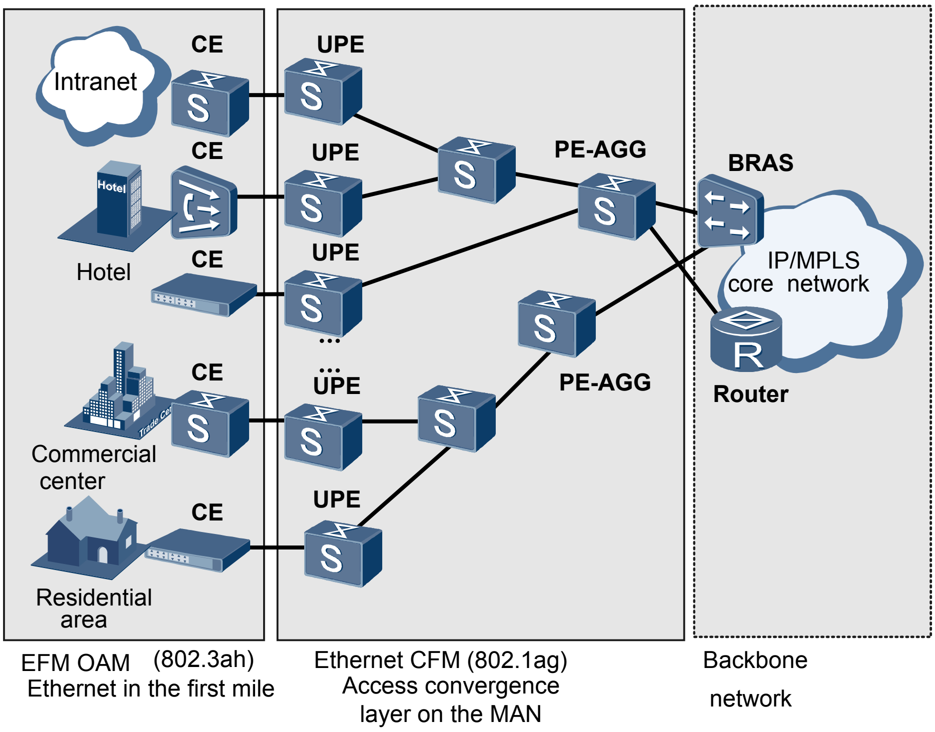
The Monitor Link group can be configured on PE-AGG 1 and PE-AGG 2 to associate uplink interface with downlink interface.

4.6 Ethernet OAM

This section describes how Ethernet OAM is applied in a MAN.

With Ethernet OAM, the S9700 can carry out fault detection and protection switchover within 50 ms.

Figure 4-9 Network diagram of Ethernet OAM deployed on a MAN



Ethernet Connectivity Fault Management (CFM) can be applied at the access convergence layer on a MAN. MDs are classified according to the ISP managing the devices. All devices that are managed by the same ISP can be added to the same MD. MAs are assigned based on service types and are associated with VLANs. MEPs within an MA periodically exchange CCMs to test network connectivity. After Ethernet CFM detects a connectivity fault, alarms are generated and MAC ping and MAC trace commands are executed to verify and locate the fault.

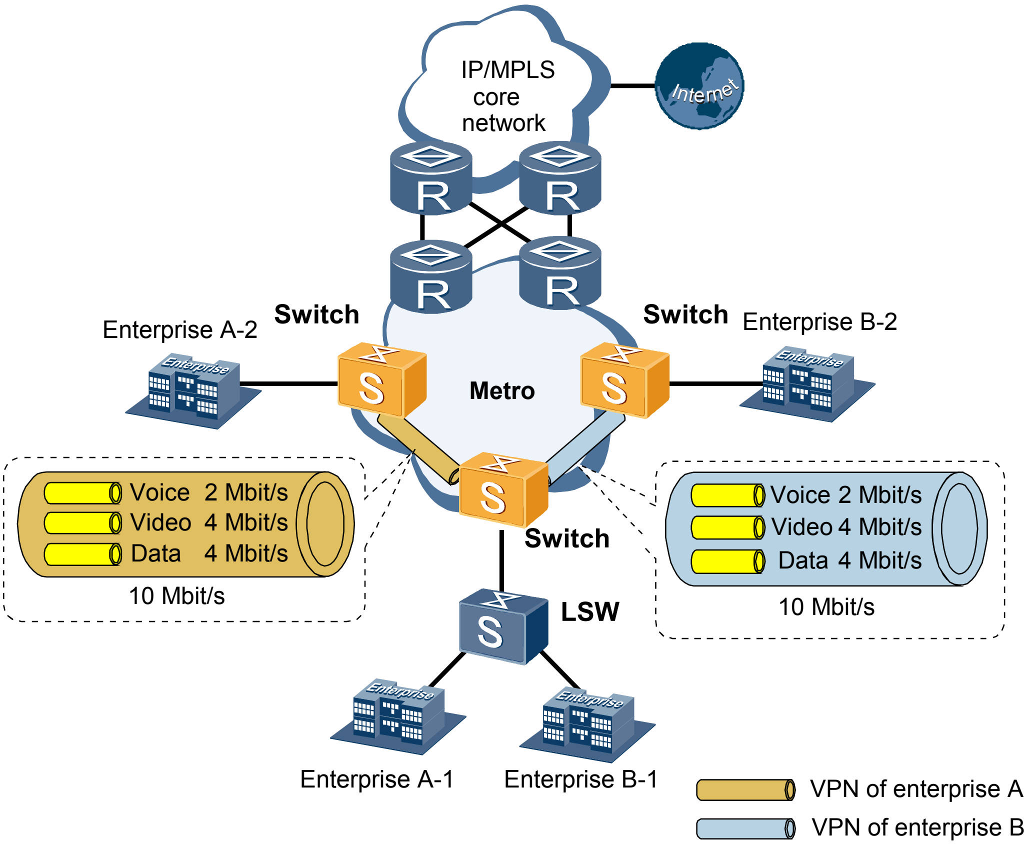
EFM OAM is enabled on CEs and UPEs. EFM OAM can test link connectivity of user services by periodically exchanging OAMPDUs between CEs and NPEs. EFM OAM monitors link performance by detecting error frames, error codes, and error frame seconds on the link. This provides transmission services conforming to a Service Level Agreement (SLA). Additionally, EFM OAM provides alarms when faults occur.

4.7 QoS

This section describes how QoS is applied in a MAN.

In **Figure 4-10**, enterprise A has two subdivisions: enterprise A-1 and enterprise A-2; enterprise B has two subdivisions: enterprise B-1 and enterprise B-2. Ethernet VLL transmits voice, video, and data services between the subdivisions of each enterprise. Meanwhile, each subdivision requires access to the Internet. In **Figure 4-10**, Switch represents the S9700.

Figure 4-10 Network diagram of QoS deployed on a MAN



Enterprise A has the following requirements:

- Ethernet VLL services between enterprise A-1 and enterprise A-2 require a minimum of 10 Mbit/s to ensure service quality.
  - Voice services

    2 Mbit/s minimum bandwidth
  - Video services

    4 Mbit/s minimum bandwidth
  - Data services

    4 Mbit/s minimum bandwidth. The remaining idle bandwidth must also be occupied by data services. Thus, the peak bandwidth requirement is 10 Mbit/s.

Enterprise B has the same requirements as enterprise A.

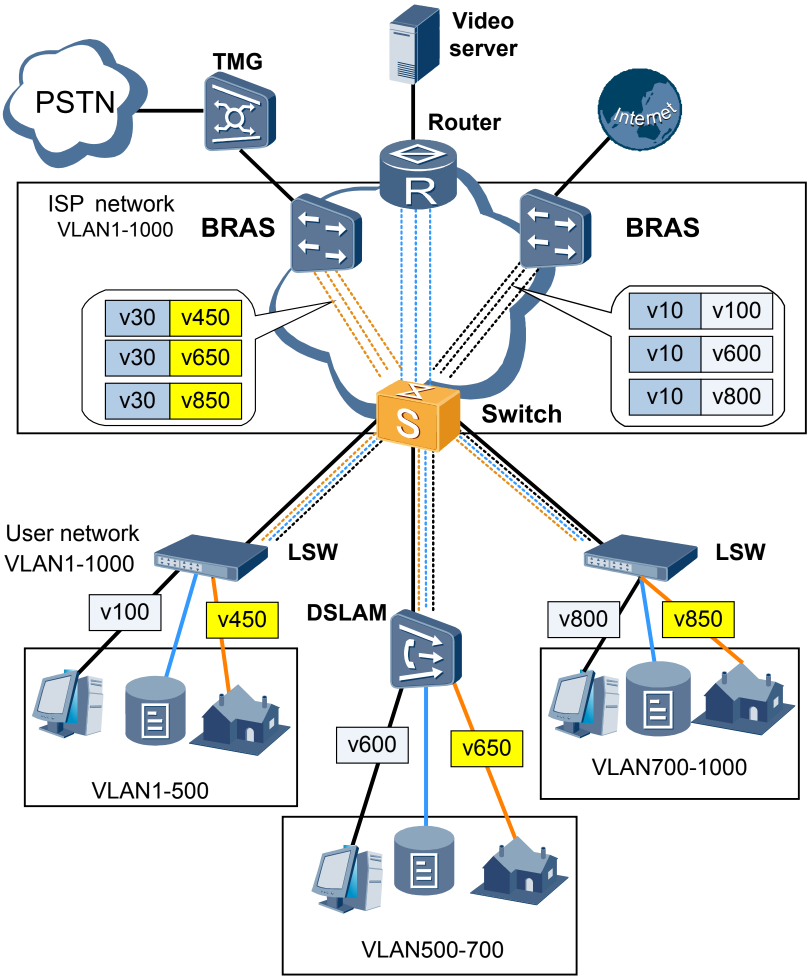
By applying level-2 traffic management on the Switch, you can meet the above service and user network resource requirements.

4.8 Selective QinQ

This section describes how selective QinQ functions on a network.

Selective QinQ networking is demonstrated in **Figure 4-11**, where Switch represents the S9700.

Figure 4-11 Network diagram of selective QinQ



The three enterprise networks shown in **Figure 4-11**, all need to transmit data, voice, and video services. The Switch can append an outer ISP VLAN tag to packets belonging to each kind of access service. For example:

- Add an outer ISP VLAN tag VLAN 10 for data services belonging to VLAN 100, VLAN 600, and VLAN800 from the customer networks.
- Add an outer ISP VLAN tag VLAN 30 for video services belonging to VLAN 450, VLAN 650, and VLAN850 from the customer networks.

Using selective QinQ, the S9700 can converge services and choose different paths for various services to more effectively facilitate network deployment.

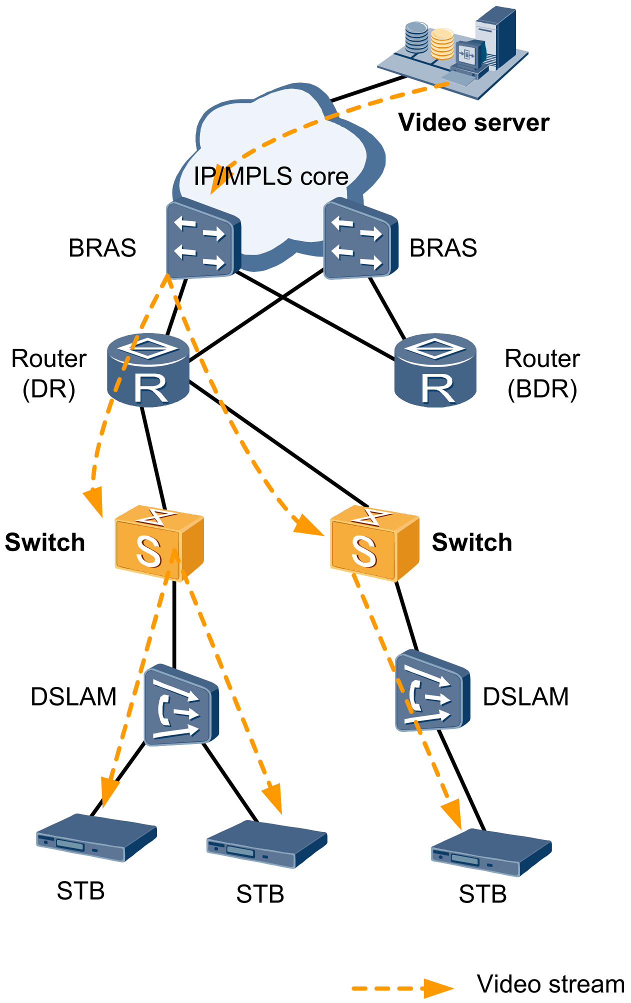
4.9 IPTV Service

This section describes the S9700's networking and application policy for the IPTV service.

4.9.1 IPTV Networking

The S9700 supports IPTV network as outlined in **Figure 4-12**.

Figure 4-12 Network diagram of IPTV implementation



The S9700's IGMP snooping and multicast VLAN functions allow it to serve as the multicast duplication and control point at the access layer of a MAN to provide large-capacity multicast services. The multicast traffic can be copied within or across VLANs.

The DSLAM device acts as an IGMP proxy.

In the network diagram shown in **Figure 4-12**:

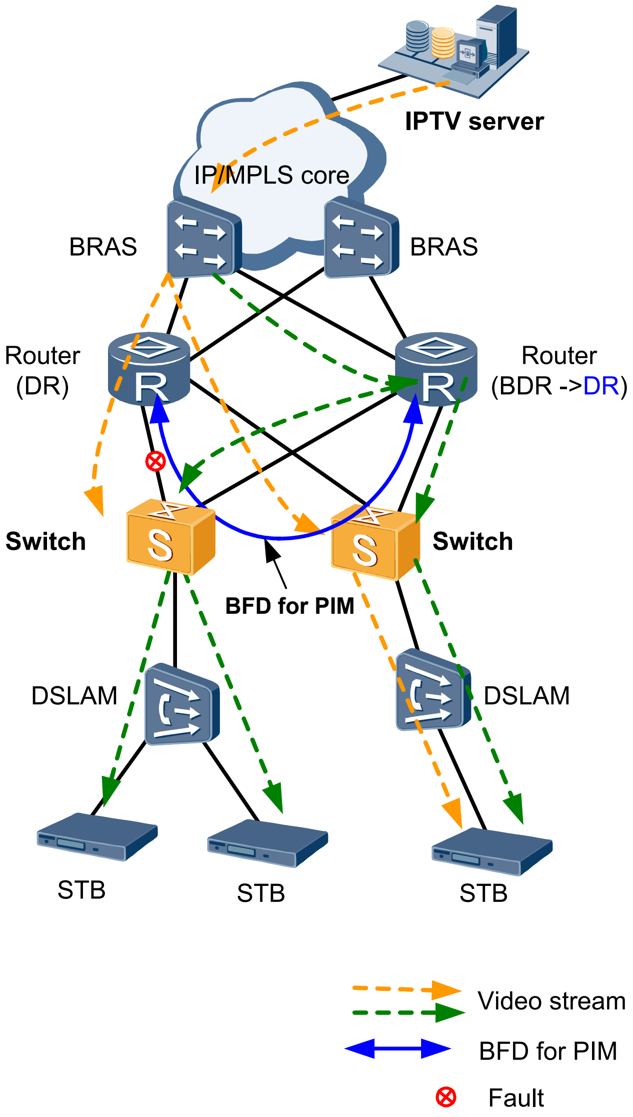
- The routers run the PIM protocol and act as either Designated Routers (DRs) or Backup Designated Routers (BDRs). A DR processes IGMP packets and copies video stream from the IPTV server.
- By enabling IGMP snooping on the Switch to listen to IGMP packets, the Switch only sends an IGMP request packet to join the multicast group. This establishes the multicast forwarding group. Static multicast groups can be created for popular multicast channels.
- The Switch copies multicast data to the DSLAM based on the multicast forwarding table.

In addition, the S9700 supports port prompt-join or prompt-leave, facilitating fast switching in IPTV services.

4.9.2 IPTV Service Protection

As shown in Figure 4-13, along with NPEs in the network, the S9700 acts as a protection mechanism for IPTV services.

Figure 4-13 Network diagram of IPTV service protection



The following mechanism provides protection for IPTV services:

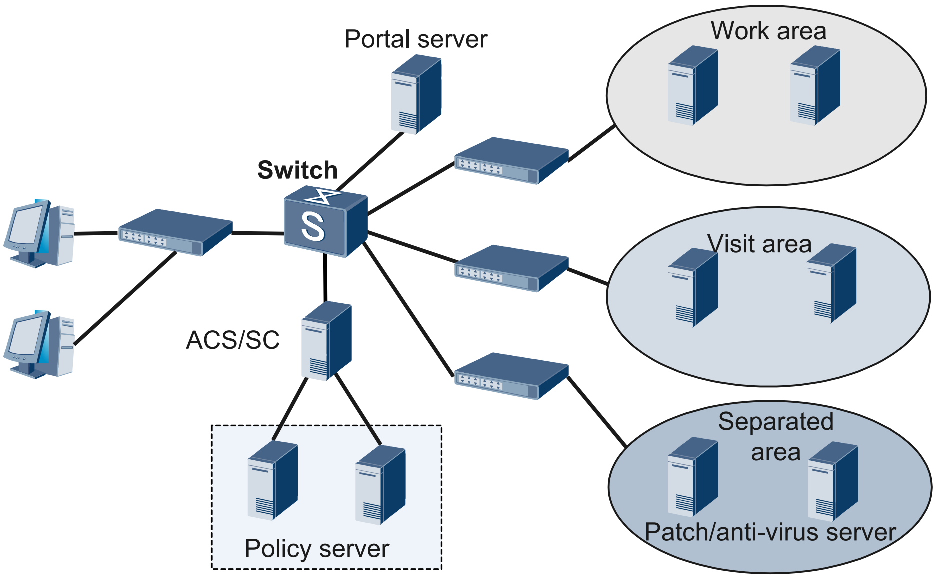
1. BFD for PIM is enabled between the two routers to monitor link status.
2. When faults occur on the link, the Switch, or one of the routers, BFD for PIM detects faults within 50 ms.
3. The router on the right acts as the BDR swiftly switching to DR when a fault occurs. Thus both routers become DRs forwarding multicast packets simultaneously.
4. When faults recover, the routers run as DR and BDR again to resume services.

4.10 NAC

This section describes how the S9700 implements NAC on a network.

In **Figure 4-14**, Switch represents the S9700.

Figure 4-14 Network diagram of the S9700 implementing NAC



On an enterprise intranet, a personal computer (PC) does not require terminal software. The captive portal server redirects login users to the login page, where users are required to enter user names and passwords. Then the NAD, namely, the Switch, submits the user name and password to the RADIUS server for authentication. Users can only access resources in the separated area until they are authenticated.

The ACS or SC, which is similar to a RADIUS server, returns a message notifying that the users have been authenticated.

The PC and ACS set up an HTTP link and the ACS verifies the security of the PC. After the security of the PC is verified, the user can access the common data area or core data area depending on the user's authority level.

The S9700 provides a Session-Time-Out timer, which allows users to go online temporarily if the authentication server, for example, a RADIUS server, does not respond. When a user goes online in this case, the Session-Time-Out timer starts. However, the user will be requested to authenticate again when the Session-Time-Out timer expires.

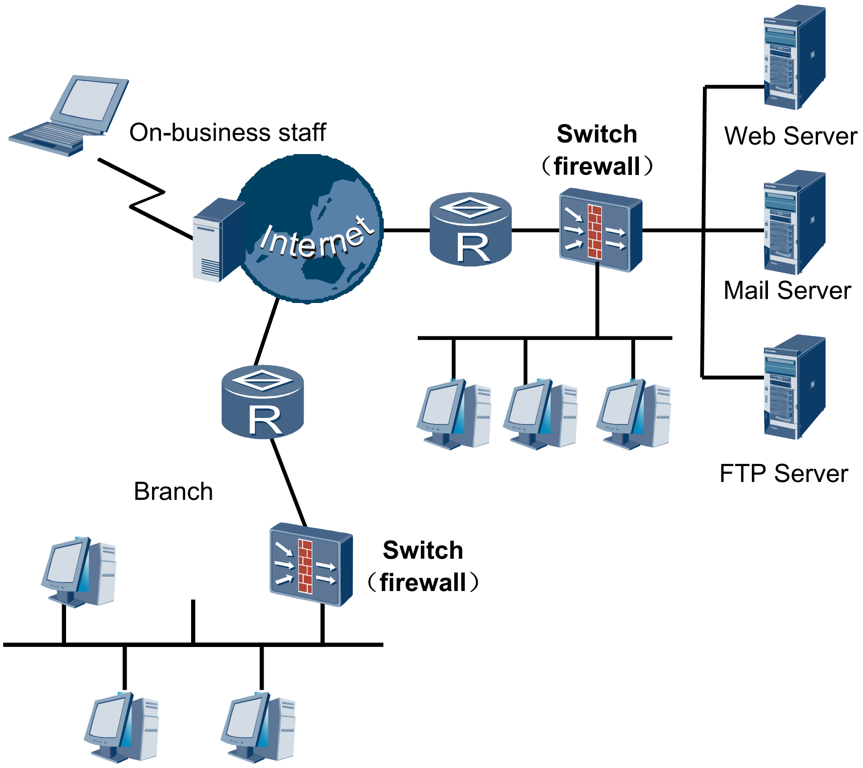
4.11 Firewall

This section describes the firewall networking and policy of the S9700.

Enterprise Intranet

The switch that provides the firewall is deployed at the egress of a company's headquarters. When providing external services such as Web, FTP, and email services, the switch prevents internal resources of the headquarters from being attacked on the Internet. The switch provides NAT for the company's staff who need to access the Internet, and functions as a remote VPN access point for other branches. The branch egress is where the firewall is deployed: The switch prevents the headquarters' internal resources from being attacked on the Internet and provides VPN services for the branch staff who need to access the headquarters network. **Figure 4-15** shows the networking of the firewall on the enterprise intranet.

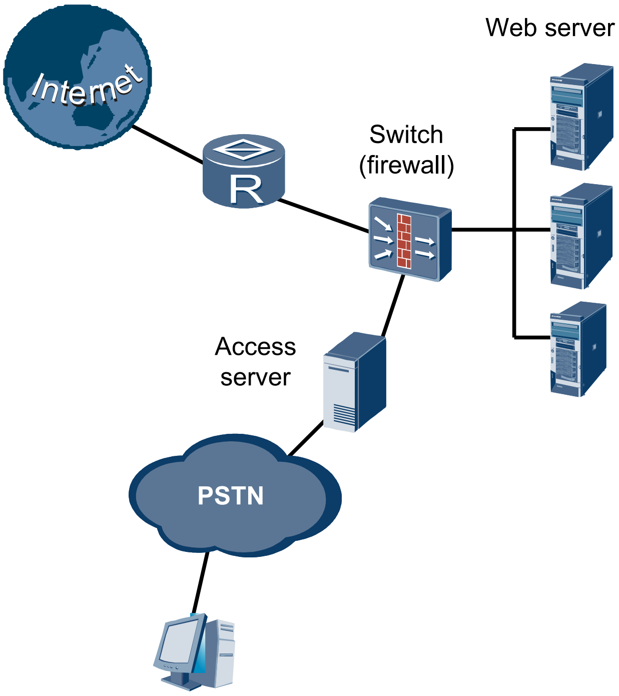
Figure 4-15 Enterprise intranet firewall network diagram



ISP Network

The switch that provides the firewall function is deployed at the egress of the ISP. It protects ISP servers and ISP users, prevents attacks from the Internet, and functions as a NAT gateway allowing users to access the Internet. **Figure 4-16** shows the typical ISP network.

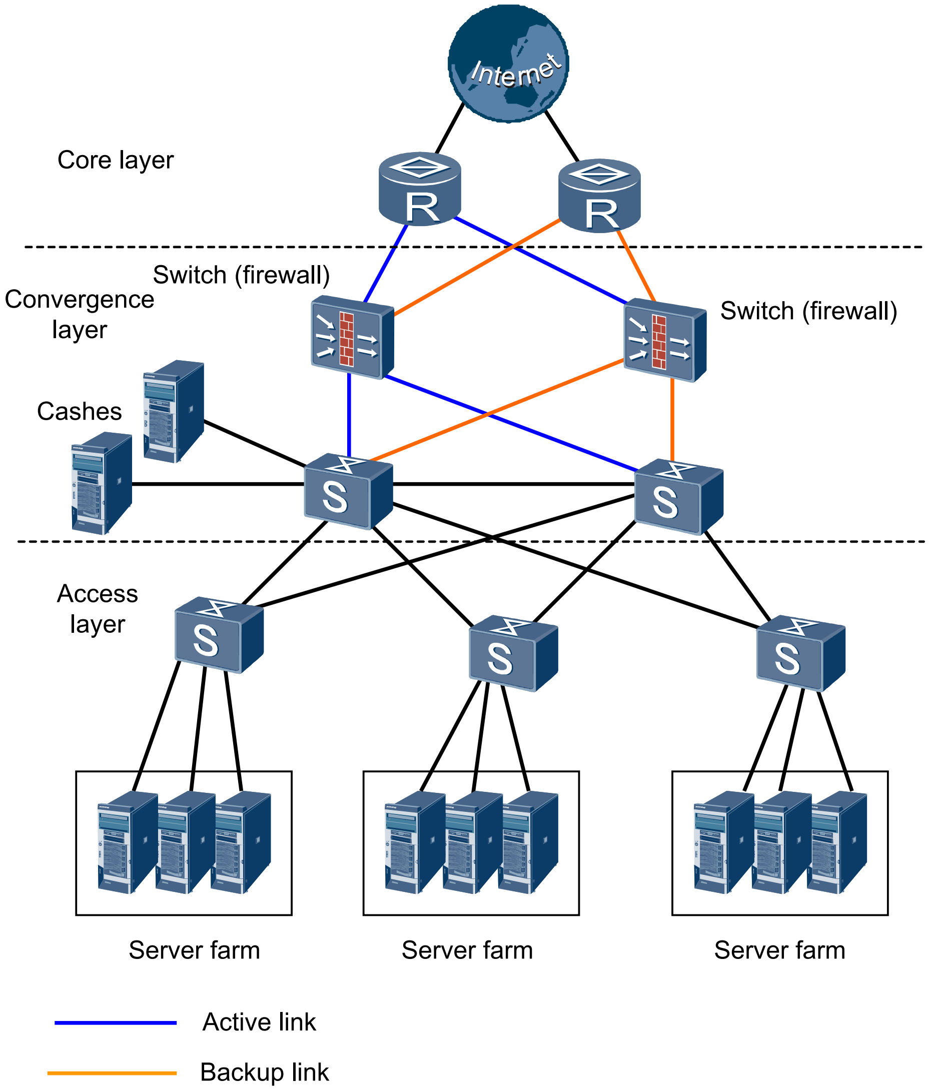
Figure 4-16 Network diagram of an ISP network firewall



Data Center

The switch that provides the firewall function is deployed at the egress of the data center. It protects the servers in the data center against attacks from the Internet and protects essential data stored in the data center. The firewall is deployed at the egress of the data center; therefore, you need to deploy the firewalls in redundancy mode to ensure high availability of the data center. **Figure 4-17** shows the typical data center's firewall.

Figure 4-17 Network diagram of a data center's firewall



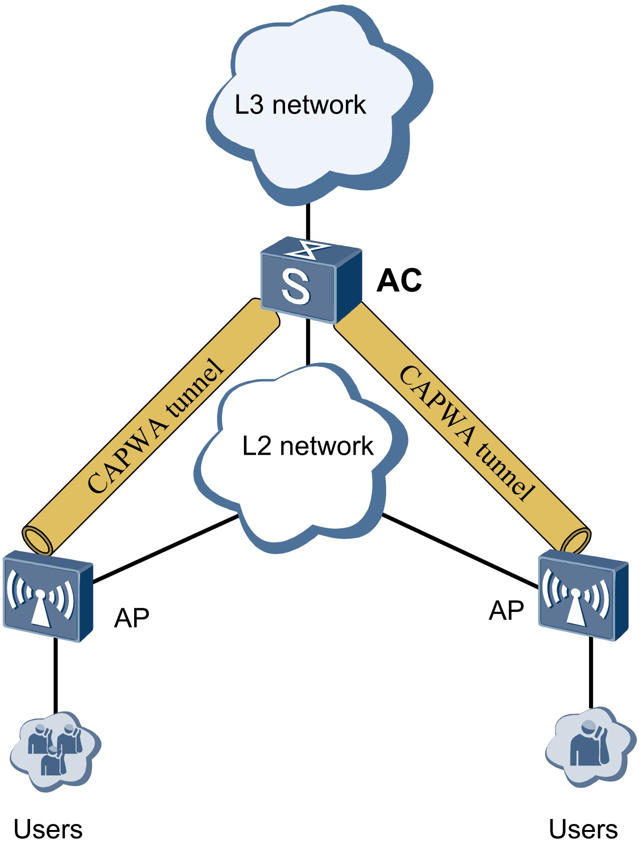
4.12 Application of the WLAN AC

This section describes how the S9700 functions as an AC on a WLAN.

S9700 (AC) Functions as Gateway

S9700 functions as an AC on a WLAN and as a gateway between the Layer 2 and Layer 3 networks. As shown in **Figure 4-18**:

Figure 4-18 Network diagram of an S9700 (AC) functioning as the gateway between Layer 2 and Layer 3 networks

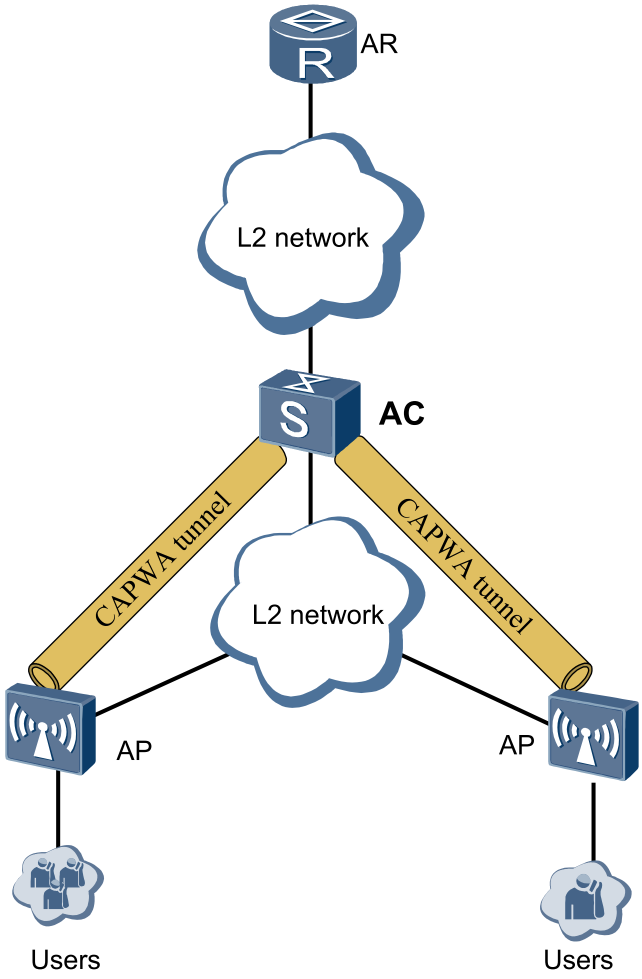


- The AC and APs are connected through a Layer 2 network. The data packets of APs and AC are forwarded over the CAPWA tunnel or forwarded directly.
- The AC functions as a gateway to terminate Layer 2 packets and forward the packets through Layer 3.
- The AC controls the access and configurations of APs, and controls the access and authentication process of WLAN users.

S9700 (AC) Functions as a Layer 2 Device

S9700 functions as an AC on a WLAN and is located in Layer 2 network. As shown in **Figure 4-19**:

Figure 4-19 Network diagram of an S9700 (AC) functioning as the Layer 2 device

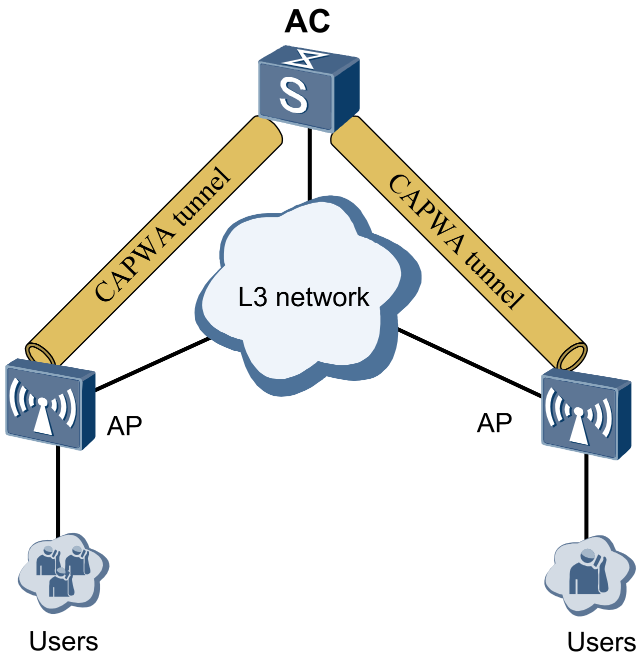


- The AC and APs are connected through a Layer 2 network. The data packets of APs and AC are forwarded over the CAPWA tunnel or forwarded directly.
- The AR functions as a gateway. The AC functions as a Layer 2 device used to terminate tunnel packets and forward user packets through Layer 2.
- The AC controls the access and configurations of APs, and controls the access and authentication process of WLAN users.

S9700 (AC) Functions as a Layer 3 Device

The S9700 functioning as an AC is the wireless data forwarding center located in the central equipment room. The APs can be located indoors or outdoors. The AC and APs are in different network segments, as shown in **Figure 4-20**.

Figure 4-20 Network diagram of an S9700 (AC) functioning as a Layer 3 device



- A Layer 3 network exists between the AC and APs, and data packets are transmitted over tunnels.
- The AC controls the access and configurations of APs, and controls the access and authentication process of WLAN users.

5 Operation and Maintenance

About This Chapter

This section describes the tools available for maintenance and management of the S9700 system and outlines the features of the S9700 network management system.

5.1 Maintenance and Management

This section describes configuration and login methods, measures for monitoring devices and debugging faults, and the software upgrade process and in-service patching.

5.1.1 Configuration Modes

Multiple Maintenance Modes

The S9700 supports the following methods of configuration and management:

- Command line interface (CLI)

  Users can configure and manage the S9700 by connecting to the console port or ETH port.

- NMS

  Users can use SNMP to configure and manage the S9700 through the network management station.

Flexible Login Modes

The S9700 provides the following ports to support local and remote login:

- Console port

  Users connect to the console port through the terminals' RS-232 serial ports.

- ETH port

  Users connect to the ETH port through Telnet or SSH.

In addition, users can telnet into the S9700 through other service ports.

To satisfy different security demands, the S9700 offers various measures to authenticate user login, including:

- Non-authentication
- Local authentication
- AAA authentication

5.1.2 Management and Monitoring

Hardware Monitoring

The S9700 provides the following hardware monitoring functions:

- MCU, SRU, LPU, CMU, power module, and fan frame panel are equipped with indicators to monitor their running status.
- In-service board detection, hot swap detection, Watch Dog, board resetting, fan module monitoring, power module monitoring, active/standby switchover and log recording for users' reference.
- Automatic board temperature monitoring to control system temperature.
- Statistics on abnormal and error packets.

- Statistics on protocol packets to be delivered to the CPU and packet details.
- CPU and memory utilization information.

Management and Maintenance

The S9700 provides the following management and maintenance functions:

- Multi-user operations and user interface (UI) in two languages: Chinese and English.
- Flexible online help for command lines. Command line descriptor searches keywords using a partial match, speeding up command input.
- Hierarchical command lines and user authority management, preventing unauthorized users from logging in.
- Alarm classification and filtering.
- DosKey-like history command function.
- Local and remote software loading and upgrading and version rollback, backup, saving, and clearing of version information.
- Information collection at different layers such as the port, Layer 2, or Layer 3.
- Information center that provides uniform management of logs, traps and debugging information and redirection of information.
- Display of system status, version, and environment parameters.

5.1.3 Diagnosis and Debugging

Ping and Trace

The S9700 provides the following tools for testing connectivity and recording packet transmission paths on IP networks:

- Ping
- Trace

The S9700 provides the following tools for testing connectivity and recording packet transmission paths on MPLS networks:

- MPLS ping
- MPLS trace

The S9700 provides the following tools to check link-layer connectivity of devices on the network and obtain network status and delay information:

- MAC Ping
- MAC TraceRoute

Debugging

The S9700 provides debugging commands for each feature. The debugging information is extensive and detailed to easily diagnose faults. Each debugging command supports multiple parameters. Debugging can be enabled or disabled on specified interfaces for specified services through the console port.

The debugging commands can display the following information for each feature:

- Critical events
- Process status
- Packet transmission and processing
- Packet resolution
- State switchover
- Error check

Trace

The S9700 supports system trace to carry out advanced software testing and diagnostics. The S9700 also uses trace to record important events online including task switching, interrupting, queue reading and writing, and system exceptions.

In the event of system failure, the system can refer to the trace information to isolate faults after rebooting. Users can enable and disable the trace function.

Mirroring

The S9700 supports port mirroring and flow mirroring.

- Port mirroring

  Incoming traffic, outgoing traffic, or both incoming and outgoing traffic is copied from one port to the port configured to monitor it.
- Traffic mirroring

  All traffic from one port is copied from one port to the port configured to monitor it.

By connecting a host with an S9700 port configured to monitor another port and examining the received packet, ISPs can observe all packets the S9700 inputs and outputs. The mirroring function provides basic traffic detection, fault allocation, and data analysis.

Virtual Cable Detection

Virtual cable detection allows users to monitor the status of cables connected to the S9700's Ethernet interfaces in the following aspects:

- Whether short circuits or open circuits are present on receive or transmit cables
- Length of faulty cable

5.1.4 Software Upgrade and In-Service Patching

Software Upgrade

The S9700 supports local and remote system software upgrade.

- Local upgrade

  When the S9700 is booted, the software can be upgraded through the BootROM menu.
- Remote upgrade

  You can use FTP, SFTP, or TFTP to load new system software to the S9700 to complete an upgrade when the switch is running.

In-Service Patching

The S9700 supports in-service patching. The features of in-service patching are as follows:

- Service is uninterrupted while patches are loaded.
- Installed patches can either be confirmed or removed without interrupting services.
- Clear step-by-step prompts and status updates are provided for easy installation.

Version Rollback

The S9700 supports version rollback. The features of version rollback are as follows:

- If at some point the upgraded version ceases to function properly, users can restart the software using an earlier version to boot the system.
- If faults occur during the upgrading or patching process, the system can be easily recovered to its pre-upgrade/patch status.

5.2 NMS

The NMS handles resource management, topology management, configuration management, fault management, performance management, and security management for the S9700.

Web Network Management

To facilitate maintenance and use of the S9700, the Web network management is introduced.

Web network management is a Web server embedded in the S9700. Users can log in using PCs to manage and maintain the S9700. By using Web network management, maintenance personnel only need to configure IP addresses and Web-based NMS accounts on the S9700, and then enter IP addresses in the address bar of the Microsoft Internet Explorer. The operations are easy to learn and perform, and network management efficiency is greatly improved.

eSight

The eSight network management system manages enterprise networks using the following features:

- Manages other vendors' devices.
- Manages specific services by analyzing network flows and focusing on core services.
- Manages application software, IT devices (such as servers and printers), and network devices.
- User-oriented operation and maintenance system: Ensures desktop access security by performing authentication, authorization, and accounting (AAA) on network access users.
- Secondary development platform: Provides a secondary development platform for customizing network management functions.
- Northbound integration: Integrates with upper-layer OSS system.

6 Technical Specifications

About This Chapter

This section lists the S9700's physical specifications, power supply parameters, and performance.

6.1 Physical Specifications

This section describes the dimensions, power consumption, weight, voltage, and working environment parameters of the S9700.

Table 6-1 Physical specifications of the S9700

Item	S9712	S9706	S9703
Dimensions (W x D x H, excluding the rack-mounting ears)	● Having cable dividers installed: 442 mm x 585 mm x 663.95 mm (15 U high) ● Having no cable divider installed: 442 mm x 476 mm x 663.95 mm (15 U high)	● Having cable dividers installed: 442 mm x 585 mm x 441.7 mm (10 U high) ● Having no cable divider installed: 442 mm x 476 mm x 441.7 mm (10 U high)	● Having cable dividers installed: 442 mm x 585 mm x 175 mm (4 U high) ● Having no cable divider installed: 442 mm x 476 mm x 175 mm (4 U high)
Cabinet	N66E or N68E	N66E or N68E	N66E or N68E
Maximum power (full configuration) **NOTE** The heat dissipation value of a device equals the current power consumption of the device.	4400 W	2200 W	1100 W
Weight (empty/fully loaded)	37 kg/70 kg	29 kg/45 kg	11 kg/25 kg
Noise at normal temperature	69.7 dB	67 dB	64.5 dB

Item		S9712	S9706	S9703
Power specifications		● DC input voltage – Rated voltage: -48 V DC/-60 V DC – Voltage range: -38.4 V DC to -72 V DC ● AC input voltage – Rated voltage: 110 V AC/220 V AC, 50/60 Hz – Voltage range: 90 V AC to 290 V AC; 47 Hz to 63 Hz (When the input voltage is in the range of 90 V AC to 175 V AC, the power module provides up to half of the maximum output power.)		
Ambient temperature	Long-term	0°C to 45°C		
	Short-term	-5°C to 55°C		
	Storage	-40°C to 70°C		
Humidity	Long-term	5% RH to 85% RH, non-condensing		
	Short-term	0% RH to 95% RH, non-condensing		
	Storage	0% RH to 95% RH, non-condensing		
Altitude	Long-term	< 3000 m		
	Storage	< 5000 m		

NOTE

- The temperature and humidity are measured 1.5 m above the floor and 0.4 m at the front of the cabinet. There should be no protection board at the front or back of the cabinet.
- Short-term means that the continuous operation time does not exceed 48 hours and the accumulated time per year does not exceed 15 days.

6.2 System Configuration

This section describes the switching capacity, backplane capacity, and forwarding rate of the S9700.

Table 6-2 System configuration of the S9700

Item	S9712	S9706	S9703	Notes
Processor	1.2GHz (Dominant frequency)	1.2GHz (Dominant frequency)	500 MHz (Dominant frequency)	-
DDR3 SDRAM	2GB	2GB	512 MB	-
Flash Memory	128MB	128MB	Standard 64 MB, scalable to 128 MB	-
CF card	512 MB	512 MB	512 MB	The CF card serves as a mass storage device to save data files and logs.
Backplane capacity	19.2 Tbit/s	14.4 Tbit/s	7.2 Tbit/s	-
Switching capacity	3.84 Tbit/s **NOTE** The switching capacity can be expanded to 5.12 Tbit/s or 7.68 Tbit/s in the future.	3.84 Tbit/s **NOTE** The switching capacity can be expanded to 5.76 Tbit/s in the future.	2.88 Tbit/s	Bidirectional, sum of switching capacities of the two MPUs
Forwarding capability	2880 Mpps **NOTE** The forwarding capability can be expanded to 3840 Mpps or 5760 Mpps in the future.	2880 Mpps **NOTE** The forwarding capability can be expanded to 4320 Mpps in the future.	1440 Mpps	-
Number of LPU slots	12	6	3	LPU (Optional)
Number of SRU/MCU slots	2	2	2	S9706/S9712: SRU S9703: full mesh
Maximum port density	576xFE, 576xGE, 480x10GE, 96x40GE	288xFE, 288xGE, 240x10GE, 48x40GE	144xFE, 144xGE, 120x10GE, 24x40GE	-

Calculating Switching Capacity

- Switching capacity of S9703

  The per slot unidirectional forwarding speed of the S9703 is 480 Gbit/s. Therefore, the switching capacity of the S9703 is 2880 Gbit/s (480 x 3 x 2 = 2880). In the equation, 3 is the number of LPU slots in the S9703 chassis, and 2 means that traffic is forwarded bidirectionally.

- Switching capacities of S9706 and

  Switching capacity = Switching capacity of an SRU x Number of SRUs

  Each SRU of the S9706 provides a switching capacity of 1920 Mbit/s. Each S9706 chassis can be equipped with two SRUs; therefore, the switching capacity of the S9706 is 3.84 Tbit/s (1.92 x 2 = 3.84).

  Each SRU of the S9712 provides a switching capacity of 1920 Mbit/s. Each S9712 chassis can be equipped with two SRUs; therefore, the switching capacity of the S9712 is 3.84 Tbit/s (1.92 x 2 = 3.84).

Calculating Interface Capacity

The interface capacity of the S9700 is calculated using the following formula:

Interface capacity = Maximum interface rate x Interface density

The maximum interface rate is the maximum transmission rate on each interface.

The interface density indicates the number of a specified type of interfaces on the S9700.

- Each LPU of the S9703 provides a maximum of 40 10GE interfaces, and each S9703 chassis provides 3 LPU slots. A chassis can provide a maximum of 120 10GE interfaces. That is, the interface density is 120. The transmission rate of each 10GE interface is 10 Gbit/s; therefore, the interface capacity of the S9703 is 1200 Gbit/s.
- Each LPU of the S9706 provides a maximum of 40 10GE interfaces, and each S9706 chassis provides 6 LPU slots. A chassis can provide a maximum of 240 10GE interfaces. That is, the interface density is 240. The transmission rate of each 10GE interface is 10 Gbit/s; therefore, the interface capacity of the S9706 is 2400 Gbit/s.
- Each LPU of the S9712 provides a maximum of 40 10GE interfaces, and each S9712 chassis provides 12 LPU slots. A chassis can provide a maximum of 480 10GE interfaces. That is, the interface density is 480. The transmission rate of each 10GE interface is 10 Gbit/s; therefore, the interface capacity of the S9712 is 4800 Gbit/s.

6.3 Performance and Capacity

This section describes the performance specifications of the software of the S9700.

Table 6-3 Performance specifications of the S9700

Attribute	Service Feature	Specifications
Ethernet	Number of MAC addresses supported by each LPU	● ED board: 512 K ● EC/BC/FC board: 128 K ● EA/SA/FA board: 32 K

Attribute	Service Feature	Specifications
	Number of VLANs	4 K
	Number of trunk groups and number of interfaces supported by each trunk group	128 trunk groups, each of which supports a maximum of 8 interfaces
	Number of ARP entries	16 K
	Number of ARP entries supported by each LPU	● EA/EC/BC/ED board: 16 K ● SA/FA/FC board: 8 K (16 K on EH1D2L02QFC0 and EH1D2L08QFC0)
QoS	Number of QoS queues on a port	8
	CAR	● ED/EC/BC/EA/FA/FC board: 8 kbit/s ● SA (EH1D2G24SSA0/ EH1D2S24CSA0) board: 64 kbit/s ● SA (EH1D2X12SSA0) board: 8 kbit/s
ACL	ACLv4	Number of IPv4 ACLs supported by each LPU: ● ED board: 70K for inbound traffic; 1K for outbound traffic ● EC/BC board: 38K for inbound traffic; 1K for outbound traffic ● EA board: 6K for inbound traffic; 1K for outbound traffic ● FC board: 1K for inbound traffic; 512 for outbound traffic ● FA board: 1.5K for inbound traffic; 256 for outbound traffic ● SA (EH1D2G24SSA0/ EH1D2S24CSA0) board: 3K for inbound traffic; 512 for outbound traffic ● SA (EH1D2X12SSA0) board: 1.5K for inbound traffic; 512 for outbound traffic ● OSP: 6K for inbound traffic; 1K for outbound traffic

Attribute	Service Feature	Specifications
	ACLv6	Number of IPv6 ACLs supported by each LPU: ● ED board: 67K for inbound traffic; 256 for outbound traffic ● EC/BC board: 35K for inbound traffic; 256 for outbound traffic ● EA board: 3K for inbound traffic; 256 for outbound traffic ● FA board: 512 for inbound traffic; 128 for outbound traffic ● FC board: 512 for inbound traffic; 128 for outbound traffic ● SA (EH1D2G24SSA0/ EH1D2S24CSA0) board: 1K for inbound traffic; 128 for outbound traffic ● SA (EH1D2X12SSA0) board: 512 for inbound traffic; 128 for outbound traffic ● OSP: 3K for inbound traffic; 256 for outbound traffic
MPLS	Number of LSPs	● ED/EC/BC/EA board: 8 K ● FC/FA board: 4 K ● Others: not supported
	Number of LDP neighbors	● ED/EC/BC/EA/FC board: 512 local neighbors, 1024 remote neighbors ● FA board: 64 local neighbors, 1024 remote neighbors ● Others: not supported
L2VPN	Number of VLL entries	4 K
	Number of VSI entries	1 K
L3VPN	Number of VRFs	2 K
	Number of VPN routes	● S9706/S9712: 500,000 ● S9703: 140,000
	Number of routing entries	● S9706/S9712: 1000 K ● S9703: 300 K

Attribute	Service Feature	Specifications
	IPv4 FIB	● ED board: 512 K ● EC/BC board: 128 K ● EA board: 16 K ● SA/FA board: 12 K ● FC board: 8 K
	IPv6 FIB	● ED board: 256 K ● EC/BC board: 64 K ● EA board: 8 K ● SA/FA board: 6 K ● FC board: 4 K
Multicast	Number of static multicast routes	256
	Number of L2 multicast forwarding entries	1 K
	Number of L3 multicast forwarding entries	● ED/EC/BC/EA/FA board: 4 K ● SA board: 2 K
Reliability	BFD	● BFD sessions: 2000 ● Minimum fault discovery duration: If no FSU is configured, the duration is 3s; if an FSU is configured, the duration is 50 ms.
	Ethernet OAM	● 802.1ag Up to 64 MDs can be created on the entire system. The number of MAs on the entire system is as follows: – S9706/S9712: 4 K – S9703: 2 K Detection time: 3.3 ms/10 ms/ 100 ms/1s/10s/1 min/10 min ● 802.3ah Detection time: 100 ms/1s ● Y.1731: delay measurement within 1 ms

Attribute	Service Feature	Specifications
	RRPP	● Maximum number of RRPP instances: 64 ● Rings supported by the entire system: 64 ● Rings supported by each LPU: 12 major rings, 18 subrings ● Maximum number of RRPP domains: 64
	VRRP	● VRRP backup groups on the entire system: 255 ● VRRP backup groups on the entire system: 16 ● Virtual IP addresses in each VRRP backup group: 16 ● Switchover time: If no FSU is configured, the time is 3s; if an FSU is configured, the time is 50 ms.
	SmartLink	● Maximum number of instances on the entire system: 64 ● Maximum number of Smart Link groups on the entire system: 16 ● Switchover time: less than 50 ms
	MSTP	● Maximum number of instances on the entire system: 64 ● Switchover time: second level
	SEP	● Maximum number of segments on the entire system: 256 ● Convergence time: less than 50 ms

6.4 List of Software Features

This section describes the software features of the S9700.

Table 6-4 Software features list of the S9700

Feature		Description
Ethernet	Ethernet	● Supports full-duplex, half-duplex, and auto-negotiation. ● Supports 10/100/1000 Mbit/s, 10 Gbit/s rate Ethernet ports. ● Supports Ethernet port rate auto-negotiation. ● Supports flow control on ports. ● Supports Jumbo packets. ● Supports ports bundled into an Eth-trunk. ● Supports load balancing among links in the trunk. ● Supports port isolation and forwarding restriction. ● Supports broadcast storm suppression.
	VLAN	● Supports Access, Trunk, Hybrid, and QinQ access modes. ● Supports default VLAN. ● Supports 1:1 VLAN mapping. ● Supports N:1 VLAN mapping. ● Supports 802.1p-based VLAN mapping. ● Supports QinQ. ● Supports selective QinQ. ● Supports VLAN switching.
	MAC	● Supports automatic MAC address learning and aging. ● Supports static, dynamic, and blackhole MAC entries. ● Supports MAC address learning limits based on ports and VLANs.
	ARP	● Supports static and dynamic ARP. ● Supports ARP in VLAN. ● Supports ARP entry aging.
	Smart Link	● Supports Smart Link. ● Supports Smart Link multi-instance. ● Supports Monitor Link.
	DLDP	Supports unidirectional link detection.
	LLDP	Supports LLDP.
	Virtual cable test	Supports virtual cable detection.

Feature		Description
Protection against Ethernet loops	MSTP	● Supports STP. ● Supports RSTP. ● Supports MSTP. ● Supports BPDU guard, root guard, and loop guard. ● Supports BPDU tunnel.
	RRPP	● Supports RRPP. ● Supports RRPP multi-instance.
	Loop detection	● Support loop detection.
IP routing	IPv4 unicast	● Network management interface supports IPv4 unicast data packets. ● Network management interface supports static IPv4 unicast routes. ● Supports RIP, OSPF, IS-IS, and BGP. ● Supports the DHCP server and the DHCP relay. ● Supports DHCP snooping.
	IPv6 unicast	● Supports RIP, OSPFv3, ISISv6, and BGP+. ● Supports TCP6, ping IPv6, tracert IPv6, and socket IPv6. ● Supports DHCPv6 snooping. ● Supports ND Snooping
	IPv4/IPv6 transition	● Supports the IPv6 over IPv4 tunnel. ● Supports IPv4 over IPv6. ● Supports 6FE.
Multicast	-	● Supports IGMP, MLD, MSDP, PIM-DM, PIM-SM, and PIM-SSM. ● Supports IGMPv1, IGMPv2, IGMPv3 snooping. ● Supports MLDv1 snooping. ● Supports prompt leave. ● Controls multicast traffic. ● Supports multicast VLAN. ● Supports multicast querier. ● Suppresses multicast protocol packets. ● Supports multicast ACL. ● Supports multicast copy. ● Supports multicast VPN

Feature		Description
MPLS	Basic MPLS functions	● Supports static LSP. ● Supports static mapping between VLAN and MPLS SVC to provide virtual dedicated Ethernet lines. ● Supports L2VPN and L3VPN. ● Supports two-layer MPLS labels. ● Supports MPLS over Ethernet. ● Maps the 802.1p priority to the EXP field in the MPLS packet.
	MPLS OAM	● Supports LSP **ping** and LSP **traceroute**. ● Supports automatic fault detection. ● Supports 1+1 protection of LSP.
	MPLS-TE	● Supports MPLS-TE tunnels. ● Supports MPLS-TE protection group.
	VLL/HVPLS	● Supports VLL in SVC, Martini, Kompella or CCC mode. ● Supports VPLS in Martini or Kompella mode. ● Supports HVPLS in LSP and QinQ mode. ● Supports VLL and VPLS after VLAN switching.
Ethernet OAM	Ethernet OAM	● Supports P2P Ethernet fault management defined in IEEE 802.3ah. ● Supports Ethernet OAM defined in IEEE 802.1ag. ● Supports MAC ping and MAC trace.
BFD	-	● Supports BFD physical link detection. ● Supports connectivity detection for IP. ● Supports connectivity detection for LSP, CR-LSP, and MPLS TE protection group. ● Supports BFD detection on the VPLS network. ● Supports VPLS-based BFD and manages and processes VPLS switchover diagnostics information.
QoS	Traffic classification	● Supports classification based on Layer 2 protocol header, Layer 3 protocol, Layer 4 protocol, 802.1p priority, or combinations. ● Supports C-VID-based QinQ packet classification.

Feature		Description
	Traffic behavior	● Controls access of classified packets. ● Supports CAR-based traffic policing. ● Supports classifier-based packet re-marking. ● Supports classified packet queuing. ● Supports mixed use of traffic classification and traffic behavior.
	Queue scheduling	● Supports PQ, WRR, DRR, PQ+WRR, and PQ +DRR scheduling.
	Congestion avoidance	● Supports WRED. ● Supports tail drop.
	Traffic shaping	● Supports outbound traffic shaping.
	Traffic policing	Supports two-level traffic policing.
Clock	-	● Ethernet clock synchronization
Enterprise network	NAC	● Supports 802.1x authentication. ● Supports MAC address authentication. ● Supports Portal authentication. ● Supports MAC address bypass authentication. ● Supports direct authentication.
	Firewall	● Packet filtering ● ASPF ● Supports attack defense. ● Supports transparent firewall. ● Supports firewall multi-instance.
	NAT	● Supports the NAT address pool. ● Supports NAPT. ● Supports the NAT server. ● Supports static NAT/NAPT. ● Supports Easy IP. ● Supports ALG. ● Supports NAT multi-instance.
	Load balancing	● Supports server detection. ● Supports session holding. ● Supports multiple load balancing algorithms. ● Supports server load balancing at Layers 4 through 7.

Feature		Description
	IPSec VPN **NOTE** The release in Russia does not provide IPSec VPN.	● Supports IKEv1/v2 negotiation. ● Supports AH and ESP modes. ● Supports detection through Keepalive messages. ● Supports NAT traversal. ● Supports manual static SA configuration. ● Supports multiple encryption algorithms.
	WLAN AC	● Supports AP Management. ● Supports Control And Provisioning of Wireless Access Points (CAPWAP). ● Supports WLAN User Management. ● Supports WLAN Radio Management. ● Supports WLAN Security. ● Supports WLAN QoS.
Configuration and maintenance	Terminal services	● Supports CLI configuration. ● Supports prompt and help information in English and Chinese. ● Supports terminal services through the Console port or Telnet. ● Supports the Send function, allowing terminals to communicate with each other.
	File system	● Supports file system. ● Supports directory and file management. ● Supports file uploading and downloading through FTP and TFTP.
	Debug and maintenance	● Supports unified management of logs, traps, and debugging information. ● Supports electronic labels. ● Supports user logs. ● Supports detailed debugging information to assist troubleshooting. ● Supports black box. ● Supports network testing tools such as **traceroute** and **ping** commands. ● Supports port mirroring and traffic mirroring.

Feature		Description
	Availability	- Supports 1+1 or 2+1 backup mode for power modules and N+1 backup mode for fan modules. - Supports hot swappable SRUs/MCUs, LPUs, fan modules, and power modules. - Supports 1+1 backup mode for SRUs/MCUs. - Supports automatic switchover and forcible switchover for the SRUs/MCUs. - Supports Ethernet port bundling on different boards.
	Software upgrade	- Supports in-service VRP system software upgrade. - Supports in-service BootROM upgrade. - Supports in-service patch. - Supports version rollback.
Security and management	System security	- Supports hierarchical commands to protect against unauthorized users. - Supports SSH v1.5 and v2.0. - Supports RADIUS and HWTACACS authentication. - Supports ACL filtering. - Defends against DoS, SYN flood of TCP, UDP flood, broadcast storms, and large traffic. - Supports MAC address learning limits. - Supports blackhole MAC. - Supports port isolation. - Supports packet filtering. - Supports CPU channel guard. - Supports IP address-based ARP packet suppression. - Supports blacklist and whitelist. - Supports attack trace. - Supports Automatic Laser Shutdown (ALS)
	Network management	- Supports ping and traceroute functions. - Supports SNMPv1/v2c/v3. - Supports standard MIB. - Supports RMON.