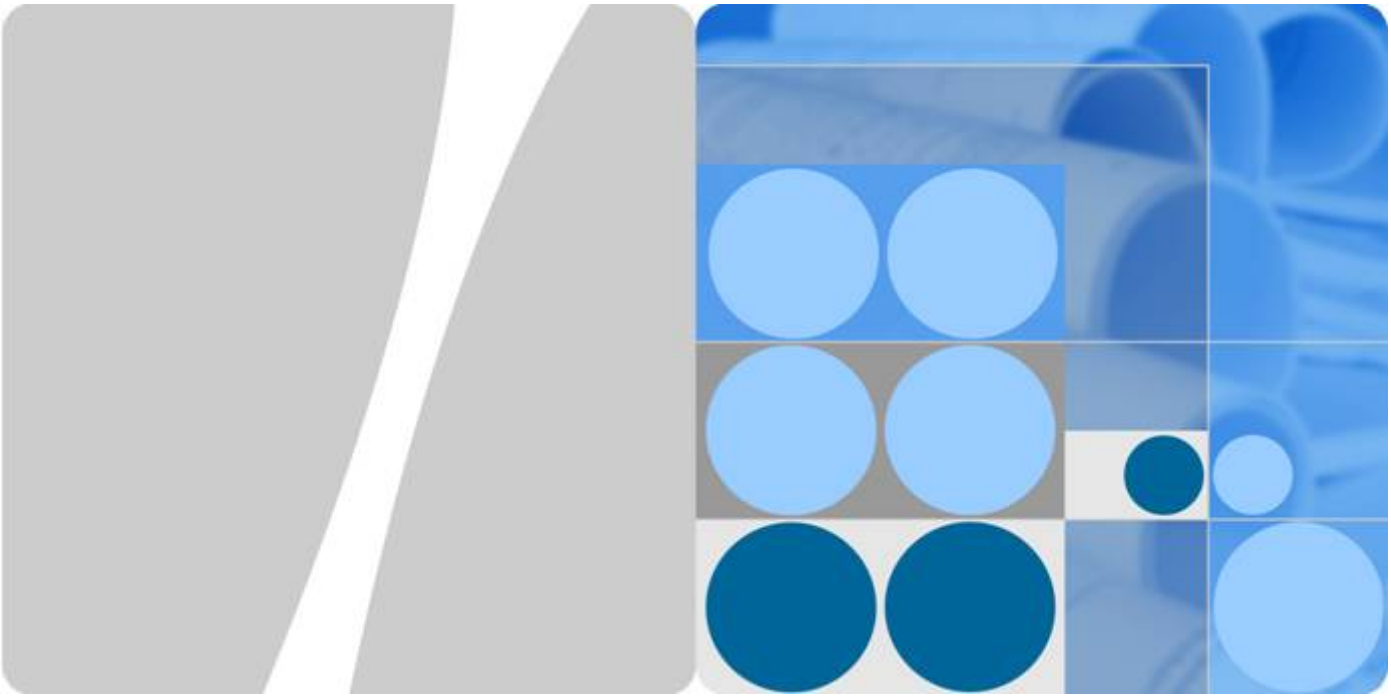


S7700 Smart Routing Switch

V200R001C00

Product Description

Issue 05

Date 2012-12-12

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

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 product positioning and features, product architecture, link features, service features, application scenarios, operation and maintenance, and technical specifications of the S7700 Smart Routing Switch .

This document provides an overall description of the S7700 Smart Routing Switch , which helps intended readers get a general understanding of all the product features.

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 injury.
WARNING	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injury.
CAUTION	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
TIP	Indicates a tip that may help you solve a problem or save 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 issue contains all updates made in previous issues.

Changes in Issue 05 (2012-12-12)

Based on issue 04 (2012-10-20), the document is updated as follows:

The following information is modified:

- Some contents are optimized.

Changes in Issue 04 (2012-10-20)

Based on issue 03 (2012-09-03), the document is updated as follows:

The following information is modified:

- **6.1 Physical Specifications**.

Changes in Issue 03 (2012-09-03)

Based on issue 02 (2012-05-23), the document is updated as follows:

The following information is modified:

- Some contents are optimized.

Changes in Issue 02 (2012-05-23)

Based on issue 01 (2012-03-15), the document is updated as follows:

The following information is modified:

- The documentation is modified according to updates in product features.

Changes in Issue 01 (2012-03-15)

This is the first release.

Contents

1 Introduction

About This Chapter

This section describes the features and position of the S7700 series switches.

1.1 System Overview

As the demand for IP-based triple play services keeps increasing, Metropolitan Area Networks (MANs) must meet increasingly higher requirements for transmission quality and quantity. In view of such demand, Huawei has developed the S7700 Smart Routing Switch (S7700 for short), a high-end network device.

The S7700 is mainly used to access, aggregate, and transmit services across a MAN. As an access and aggregation switch, the S7700 provides line-speed Fast Ethernet (FE), Gigabit Ethernet (GE), and 10GE interfaces. The S7700 can be deployed in enterprise networks and data centers, providing high-density interfaces and rich value-added service (VAS) capabilities.

The S7700 comes in three different models: S7703, S7706, and S7712. The S7703 supports a maximum of three line processing units (LPUs); the S7706 supports a maximum of six LPUs; the S7712 supports a maximum of 12 LPUs.

The S7700 operates on Huawei's Versatile Routing Platform (VRP) operating system and uses hardware-based forwarding and non-blocking data switching technology. The S7700 features carrier-class reliability, line-speed forwarding capability, Quality of Service (QoS), service processing capabilities, and is highly extensible. The S7700 provides rich enterprise network features, including firewall, Network Address Translation (NAT), network traffic analysis, IPSec VPN, and load balancing, meeting the requirements of various services on enterprise networks.

NOTE

The release in Russia does not provide IPSec VPN.

In addition, the S7700 has versatile network access capabilities in Layer 2 switching and MultiProtocol Label Switching (EoMPLS) Ethernet transmission services. The S7700 also supports rich IP services and provides broadband access, triple play, IP leased line, and Virtual Private Network (VPN) services.

1.2 System Features

The S7700 series switches provide high-density Ethernet interfaces. This section describes their capabilities, features and reliability.

Extensibility

System extensibility includes:

- Service extensibility: The SRU supports FSUA, which allows for future service development.
- Power supply: For the S7700, the maximum power of AC power supply modules is 800 W, and the maximum power of DC power supply modules is 1600 W. The S7700 series support 1+1 backup of DC power supply modules or 1+1/2+2 backup of AC power supply modules.

  Two types of PoE power supply modules are available: 800 W and 2200 W.

  PoE power supply modules can work independently, or in 3+1 or 2+2 redundancy mode.

Powerful Forwarding Capabilities

On the S7700, the hardware carries out two-level packet replication when forwarding multicast packets. That is, the SFU replicates multicast packets to the LPU, and the LPU's forwarding engine replicates the multicast packets to its interfaces.

Table 1-1 System specifications

System specifications	S7712	S7706	S7703
Switching capacity (bit/s)	2T **NOTE** The switching capacity can be expanded to 5.12 Tbit/s in the future.	2T **NOTE** The switching capacity can be expanded to 5.12 Tbit/s in the future.	768G **NOTE** The switching capacity can be expanded to 1.92 Tbit/s in the future.
Backplane capacity (bit/s)	12T	6T	3T
Forwarding capacity (pps)	1344M **NOTE** The forwarding capability can be expanded to 3360 Mpps in the future.	1152M **NOTE** The forwarding capability can be expanded to 2880 Mpps in the future.	576M **NOTE** The forwarding capability can be expanded to 1440 Mpps in the future.

Functions and Features

- The S7700 provides the following Layer 2 service features:
  - VLAN
  - Generic Attribute Registration Protocol (GARP)/Generic VLAN Registration Protocol (GVRP)
  - Selective QinQ
  - RRPP
  - Smart Ethernet Protection (SEP)
  - Smart Link
  - STP, RSTP, and MSTP
  - Link aggregation
  - DHCP snooping
  - IGMP snooping
  - IPV6 ND snooping
  - MLD snooping
  - Ethernet OAM
- The S7700 provides the following IP services:

  - IPv4 unicast routing protocols, including Routing Information Protocol (RIP), Open Shortest Path First (OSPFv2), Intermediate System-to-Intermediate System (IS-IS), Border Gateway Protocol (BGP), and Multiprotocol Border Gateway Protocol (MBGP)
  - IPv6 unicast routing protocols, including RIPng, OSPFv3, ISISv6, and BGP+
  - Multicast routing protocols, including IGMP, MLD, Multicast Source Discovery Protocol (MSDP), multicast VLAN, PIM-DM, PIM-SM, and PIM-SSM
  - VRRP
  - DHCP relay, DHCP server, and Option82
  - Distributed and integrated NetStream
- The S7700 provides the following MPLS services:
  - MPLS forwarding
  - LDP
  - MPLS-TE
  - MPLS-OAM
- The S7700 provides the following VPN services:
  - VPLS
  - VLL
  - BGP/MPLS IP VPN
- The S7700 provides the following intranet features:
  - The S7700, which functions as the network access device (NAD), supports Portal authentication, 802.1x authentication, and MAC address authentication.
  - PoE
  - Service distribution
- Firewall/NAT
- Load balancing
- IPSec VPN

  NOTE

  The release in Russia does not provide IPSec VPN.
- Wireless Local Area Network Access Controller (WLAN AC)

Security Design

The S7700 uses a distributed structure, guaranteeing the separation between the data plane and the control plane. This provides users with industry-grade security performance.

The S7700 provides the following security features:

- Three user authentication modes: local authentication, Remote Authentication Dial in User Service (RADIUS) authentication, and Huawei Terminal Access Controller Access Control System (HWTACACS) authentication.
- Hardware-based packet filtering and sampling, which guarantees high performance and high scalability
- Multiple authentication methods including plain text authentication and Message Digest 5 (MD5) for upper-layer routing protocols such as OSPF, IS-IS, RIP, and BGP-4
- ACL on forwarding plane and control plane

- Anti-attack features: The S7700's blacklist and CAR functions limit which packets can be sent to the CPU.
- Port security
- URPF
- DHCP snooping and DHCP snooping over VPLS
- MAC limit and MAC Forced Forwarding (MFF)
- IP source trail, ARP attack defense, ICMP attack defense, and broadcast traffic suppression
- Blacklist and attack trace: The S7700 filters out blacklisted user traffic and displays attackers' physical interfaces and VLAN IDs.
- Whitelist: The S7700 uses a user whitelist to provide a high-priority channel for protocol packets transmitted to the CPU.

Carrier-Class Reliability

Using a single monitoring unit, the S7700 manages and maintains the entire system. The monitoring unit manages, monitors, and maintains the boards, fans, and power modules.

The S7700 complies with Electro Magnetic Compatibility (EMC) standards, and the S7700's modular design implements electromagnetic shield between boards.

The S7700 meets carrier-class and high-end device reliability requirements. The S7700 provides the following reliability features outlined in **Table 1-2**.

Table 1-2 Carrier-class reliability features

Item	Description	
System protection	The boards, power modules, and fans are hot swappable.	
	The monitoring unit is totally independently from the service system.	
	The system can operate normally for 96 hours after a single fan fails.	
	The MPUs work in 1+1 backup mode.	
	The S7700 supports AC/DC power supplies working in 1+1 backup mode and AC power supplies working in 2+2 backup mode.	
	Key components such as the clocks and management buses work in backup mode.	
	Protection against system abnormalities	The system can restart automatically and recover data when abnormalities occur.
		The system resets boards when abnormalities occur and resumes the boards' work.
		The system automatically restores interface configurations.
	The system provides protection against over-current and over-voltage for power modules and interfaces.	
	The system provides protection against mis-insertion of boards.	

Item	Description	
	Power alarm monitoring	The system provides alarm prompt, alarm indication, running status query, and alarm status query.
	Voltage and environment temperature monitoring	
Reliability design	The system uses distributed hardware-based forwarding.	
	The control channel is independent from the service channel, ensuring a non-blocking control channel.	
	The system features system and board fault detection, alarm indicators, and an NMS.	
Upgradability	The system supports in-service patching.	
	The system supports version rollback.	
	The system supports online BootROM upgrade.	
	The system supports error checking and correcting (ECC) random access memory (RAM).	
Fault tolerance	Data backup	The system supports hot backup of data between active and standby units. When the active unit fails, the standby unit automatically takes over data transmission duties to prevent data loss.
	Synchronization configuration	The system supports synchronization between MPUs and LPUs.
	The system can automatically select and boot applications.	
	The system supports automatic BootROM upgrade and restoration.	
	The system can back up configuration files to a remote FTP server.	
	The system can automatically select and run configuration files.	
	The system provides abnormality monitoring for the system software, automatic restoration, and log recording.	
Operational security	The system provides password protection for system operations.	
	The system provides hierarchical command protection using configuration of user login and command levels.	
	The system can lock the terminal using the command line to prevent illegal use.	
	The system provides operation and confirmation prompts for some commands that may have a negative impact on system performance.	

Item	Description
Operations and maintenance center	The system uses Huawei's generic integrated Network Management System platform.

Easy Maintenance

The S7700 provides the following maintenance features:

- The S7700 supports Ethernet OAM, providing point-to-point Ethernet fault management within the first mile of the directly connected user side Ethernet link. The S7700 supports automatic neighbor discovery, link fault monitoring, remote fault notification, and remote loopback configuration as defined in IEEE 802.3ah, and continuity check (CC) fault detection, MAC Ping, and MAC Trace as defined in IEEE 802.1ag. The S7700 also supports Y.1731 delay and jitter measurements.
- The S7700 supports MPLS OAM, providing fault detection techniques such as Ping and TraceRoute on MPLS networks.
- The S7700 supports 802.1ag, 802.3ah, BFD session status association, and end-to-end OAM.
- The S7700 supports traffic statistics based on physical interfaces, VLAN IDs, MPLS LSPs, and ACLs.
- The S7700 supports eSight, which provides resource management, topology management, and configuration file management, batch configuration. In addition, eSight can show important performance indicators in diagrams and tables to facilitate device management.
- The S7700 supports different configuration methods such as end-to-end configuration, batch configuration, and configuration wizard. At the same time, it provides corresponding default configuration templates.
- The S7700 supports Telnet-based remote maintenance.
- The S7700 supports in-service upgrade. When the system is operating normally, it can be upgraded through FTP or TFTP. In addition, the active/standby switchover function ensures services are not interrupted during the upgrade.
- The S7700 supports hot patch, upgrading only the features that need to be optimized, so services are not interrupted when a patch is being installed.
- The S7700 supports version rollback. If a system software upgrade or patch fails, the S7700 can return to earlier version.

2 Architecture

About This Chapter

This section describes the appearance, hardware structure and software architecture of the S7700

2.1 S7700 Series System Structure
This section describes the appearance and component layout.

2.2 Hardware Layout
This section describes the hardware structure, including the backplane, MCU, SRU, LPU, CMU, FSU and clock board of the S7700.

2.3 Software Architecture
This section describes the relationship between the S7700's operating system and its software features.

2.1 S7700 Series System Structure

This section describes the appearance and component layout.

The S7700 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 S7700 can be installed in either the International Electrotechnical Commission (IEC) 297 cabinet or a European Telecommunications Standards Institute (ETSI) cabinet.

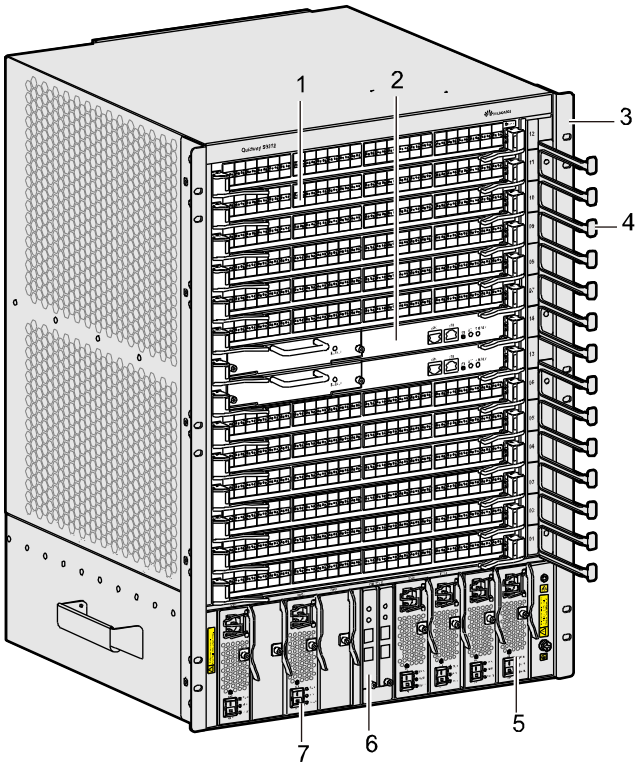
NOTE

- The SRU and CMU are applicable only to the S7712 and S7706.
- The MCU is applicable only to the S7703.

2.1.1 S7712

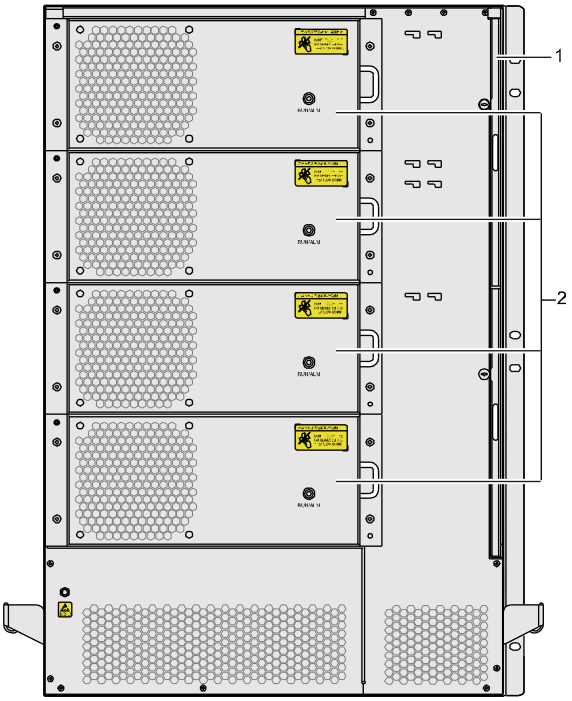
The S7712 is 15 U (1 U = 44.45 mm) high. When the chassis has no cable divider installed, the dimensions are 442 mm x 476 mm x 663.95 mm (W x D x H). When the chassis has cable dividers installed, the dimensions are 442 mm x 585 mm x 663.95 mm (W x D x H). **Figure 2-1** and **Figure 2-2** show the appearance and components of the S7712. **Figure 2-3** shows the layout of slots on the S7712.

Figure 2-1 Appearance and components of the S7712 (1)



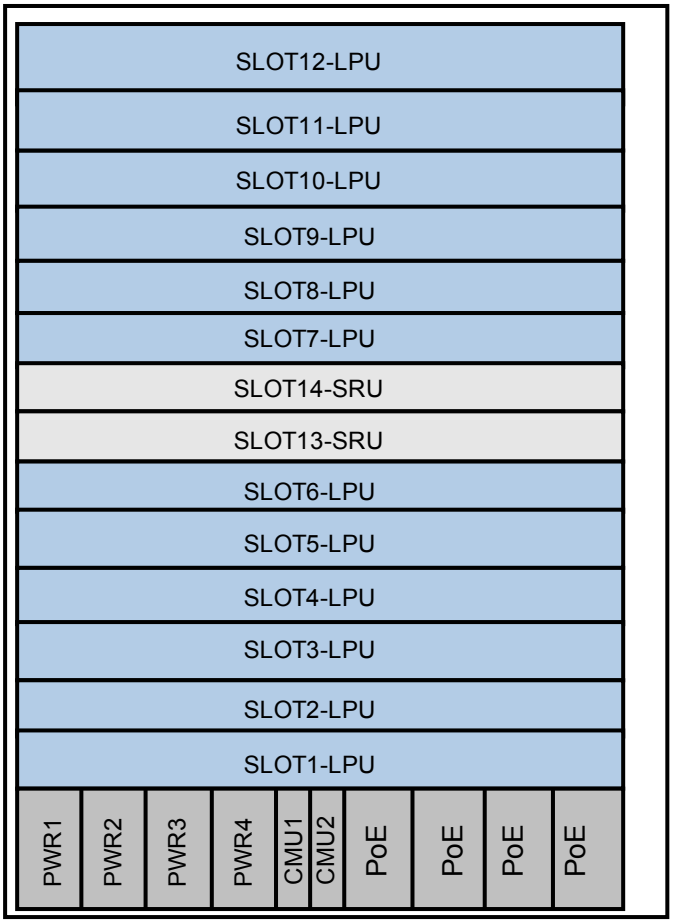
1. LPU
2. SRU
3. Rack-mounting ear
4. Cable divider
5. PoE power module
6. CMU
7. Power supply

Figure 2-2 Appearance and components of the S7712 (2)



1. Air filter 2. Fan

Figure 2-3 Layout of slots on the S7712



The S7712 uses an integrated chassis of which the main components are described in **Table 2-1**.

Table 2-1 Components of the S7712

Component	Description	Reference
SRU	The SRUs are installed in slot 13 and slot 14 and work in 1+1 hot backup mode with the data switching units working in load balancing mode. The interval between slot 13 and slot 14 is 1.4 inches.	See SRU-Main Control Unit.
LPU	The LPUs are installed in slots 1-12. The interval between each two slots is 1.4 inches.	See Boards.
CMU	The CMUs are installed in slots CMU1 and CMU2, working in 1+1 hot backup mode.	See CMU - Centralized Monitoring Unit.

Component	Description	Reference
Fan module	The fan modules are installed at the rear of the equipment. The equipment must be equipped with four fan modules.	See Fan Module.
Power supply	The power supplies are installed in slots PWR1 to PWR4. The S7712 can use DC or AC power supplies.	See Power Supply.
Cable divider	The cable distribution posts are located on the right side of the board cage of the S7712.	-
Cable	The cables of the S7712 include internal cables (such as power cables and signal cables), optical fibers, and external cables.	See Cables.

NOTE

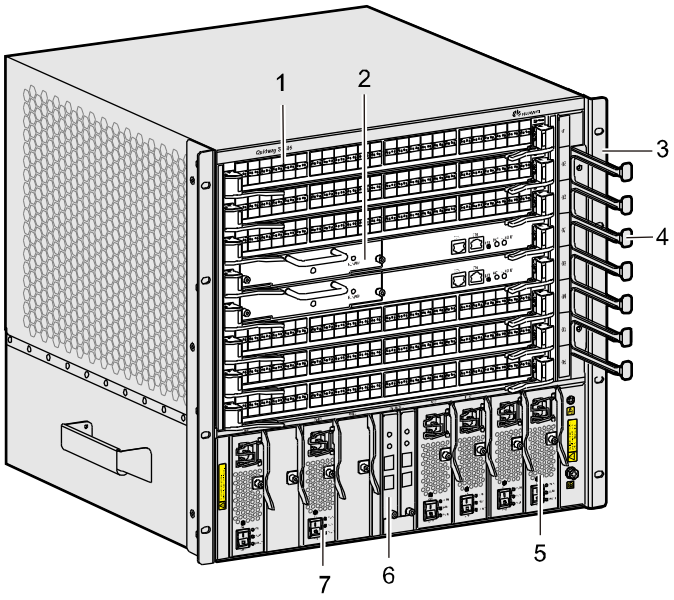
Only AC power supplies can be installed in PoE power slots. On an S7700, the 2200 W AC power supply can only be installed in the PoE slot.

- When an AC power supply is inserted into the PoE power slot, it is used as a PoE power supply, and provides power for powered devices (PDs) by using the Ethernet PoE electrical interface board.
- When an AC power supply is inserted into slots PWR1 to PWR4, it provides power for the entire device.
- The S7712 has PoE chassis and non-PoE chassis, which are identified by the nameplates and silkscreens on power slots.

2.1.2 S7706

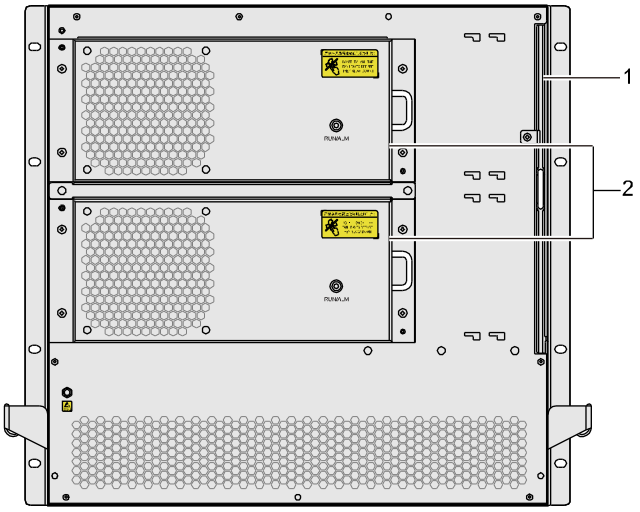
The S7706 is 10 U (1 U = 44.45 mm) high. When the chassis has no cable divider installed, the dimensions are 442 mm x 476 mm x 441.7 mm (W x D x H). When the chassis has cable dividers installed, the dimensions are 442 mm x 585 mm x 441.7 mm (W x D x H). **Figure 2-4** and **Figure 2-5** show the appearance and components of the S7706. **Figure 2-6** shows the layout of slots on the S7706.

Figure 2-4 Appearance and components of the S7706 (1)



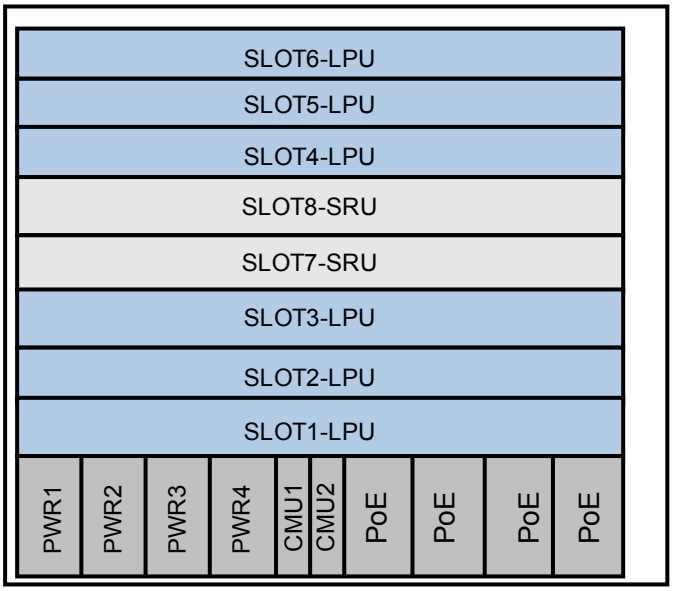
1. LPU
2. SRU
3. Rack-mounting ear
4. Cable divider
5. PoE power module
6. CMU
7. Power supply

Figure 2-5 Appearance and components of the S7706 (2)



1. Air filter
2. Fan

Figure 2-6 Layout of slots on the S7706



The S7706 uses an integrated chassis of which the main components are described in **Table 2-2**.

Table 2-2 Components of the S7706

Component	Description	Reference
SRU	The SRUs are installed in slot 7 and slot 8 and work in 1+1 hot backup mode with the data switching units working in load balancing mode. The interval between slot 7 and slot 8 is 1.4 inches.	See SRU-Main Control Unit.
LPU	The LPUs are installed in slots 1-6. The interval between each two slots is 1.4 inches.	See Boards.
CMU	The CMUs are installed in slots CMU1 and CMU2, working in 1+1 hot backup mode.	See CMU - Centralized Monitoring Unit.
Fan module	The fan modules are installed at the rear of the equipment. The equipment must be equipped with two fan modules.	See Fan Module.
Power supply	The power supplies are installed in slots PWR1 to PWR4. The S7706 can use DC or AC power supplies.	See Power Supply.
Cable divider	The cable distribution posts are located on the right side of the board cage of the S7706.	-
Cable	The cables of the S7706 include internal cables (such as power cables and signal cables), optical fibers, and external cables.	See Cables.

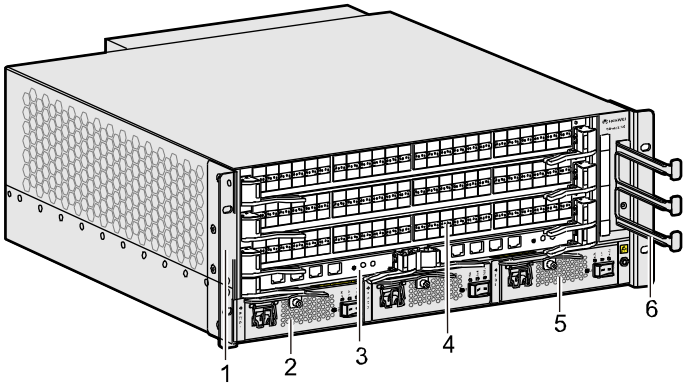
NOTE

- Only AC power supplies can be installed in PoE power slots. On an S7700, the 2200 W AC power supply can only be installed in the PoE slot.
- When an AC power supply is inserted into the PoE power slot, it is used as a PoE power supply, and provides power for powered devices (PDs) by using the Ethernet PoE electrical interface board.
- When an AC power supply is inserted into slots PWR1 to PWR4, it provides power for the entire device.
- The S7706 has PoE chassis and non-PoE chassis, which are identified by the nameplates and silkscreens on power slots.

2.1.3 S7703

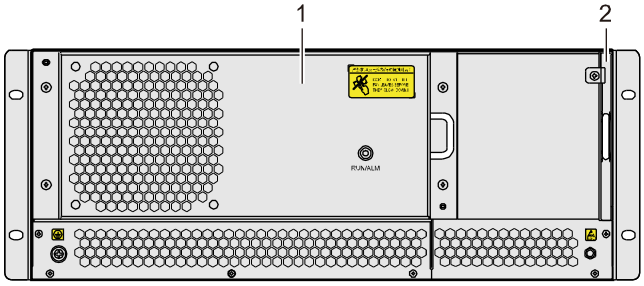
The S7703 is 4 U (1 U = 44.45 mm) high. When the chassis has no cable divider installed, the dimensions are 442 mm x 476 mm x 175 mm (W x D x H). When the chassis has cable dividers installed, the dimensions are 442 mm x 585 mm x 175 mm (W x D x H). **Figure 2-7** and **Figure 2-8** show the appearance and components of the S7703. **Figure 2-9** shows the layout of slots on the S7703.

Figure 2-7 Appearance and components of the S7703 (1)



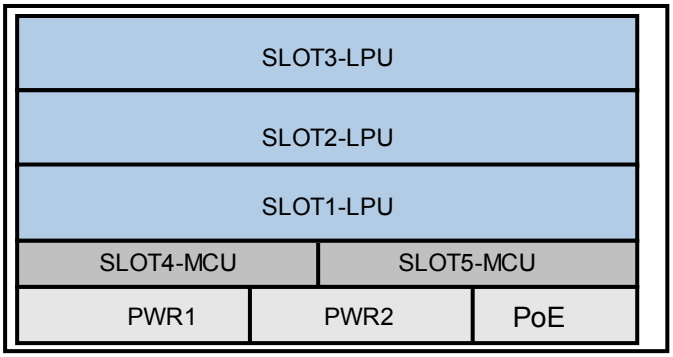
1. Rack-mounting ear
2. Power supply
3. MCU
4. LPU
5. PoE power module
6. Cable divider

Figure 2-8 Appearance and components of the S7703 (2)



1. Fan
2. Air filter

Figure 2-9 Layout of slots on the S7703



The S7703 uses an integrated chassis of which the main components are described in **Table 2-3**.

Table 2-3 Components of the S7703

Component	Description	Reference
MCU	The MCUs are installed in slot 4 and slot 5 and work in 1+1 hot backup mode. The interval between slot 4 and slot 5 is 0.8 inches.	See MCUA-Main Control Unit.
LPU	The LPUs are installed in slots 1-3. The interval between each two slots is 1.4 inches.	See Boards.
Fan module	The fan modules are installed at the rear of the equipment. The equipment must be equipped with one fan module.	See Fan Module.
Power supply	The power supplies are installed in slots PWR1 and PWR2. The S7703 can use DC or AC power supplies.	See Power Supply.
Cable divider	The cable distribution posts are located on the right side of the board cage of the S7703.	-
Cable	The cables of the S7703 include internal cables (such as power cables and signal cables), optical fibers, and external cables.	See Cables.

NOTE

- Only AC power supplies can be installed in PoE power slots. On an S7700, the 2200 W AC power supply can only be installed in the PoE slot.
- When an AC power supply is inserted into the PoE power slot, it is used as a PoE power supply, and provides power for powered devices (PDs) by using the Ethernet PoE electrical interface board.
- When an AC power supply is inserted into slots PWR1 to PWR2, it provides power for the entire device.

2.2 Hardware Layout

This section describes the hardware structure, including the backplane, MCU, SRU, LPU, CMU, FSU and clock board of the S7700.

Figure 2-10 shows the hardware structure of the S7703.

Figure 2-10 Hardware layout of the S7703

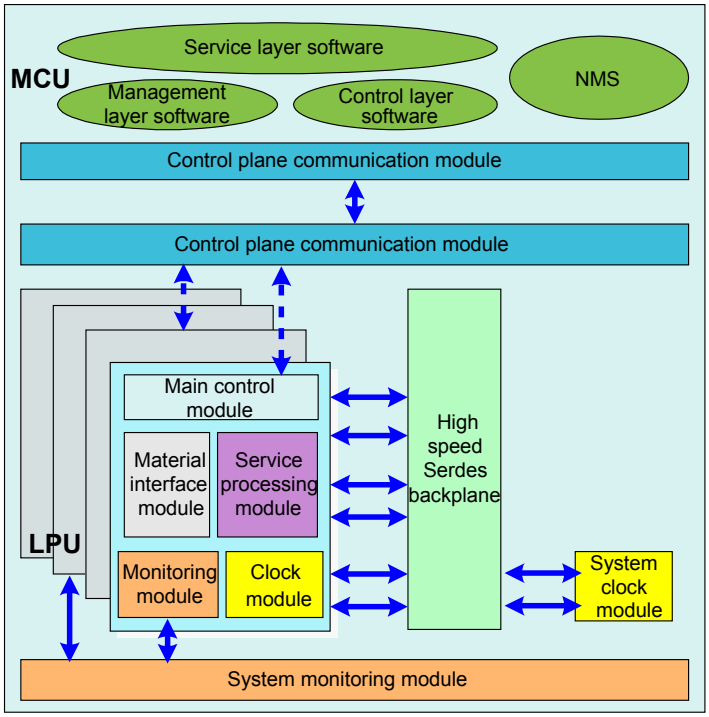
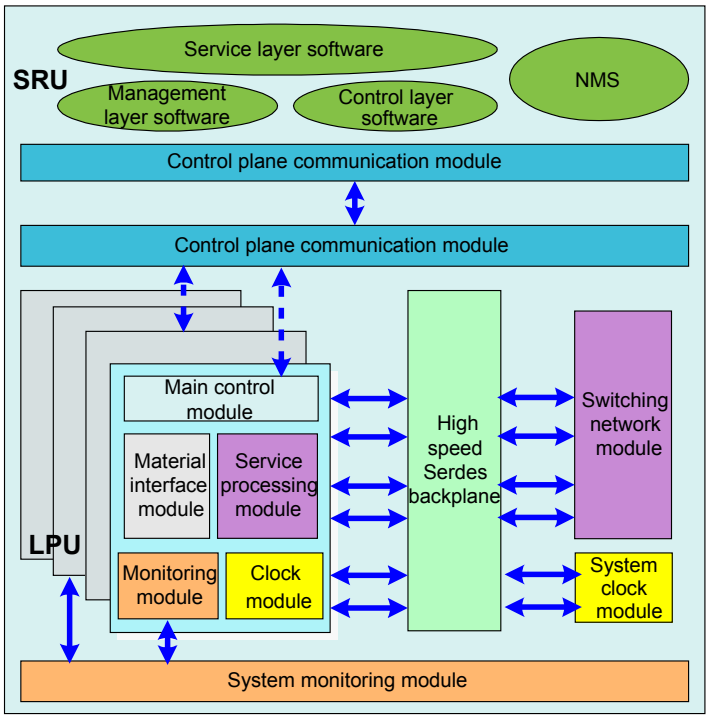


Figure 2-11 shows the hardware structure of the S7706 and S7712.

Figure 2-11 Hardware structure of the S7706 and S7712



2.2.1 Backplane

The S7700 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 S7700 backplane provides two control unit slots. The S7703's backplane provides 3 LPU slots, the S7706's backplane provides 6 LPU slots, and the S7712's backplane provides 12 LPU slots.

2.2.2 SRU

The SRU is the control board of S7706 and S7712. The SRU integrates multiple functional modules such as a data switching module, main control module, FSUA,Compact Flash (CF) module, and system monitoring 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 S7700'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 2-4 SRU switching capabilities

SRU	Service Switching Capability
SRUA	512 Gbit/s
SRUB	1 Tbit/s

2.2.3 MCU

The MCU is the control board of S7703. The MCU integrates the main control module, CF module, system monitoring module.

The S7700'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 S7706 and S7712. The CMU monitors and manages the power modules, fan modules, and PoE power modules.

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

2.2.5 LPU

LPUs are used to process packets and provide service interfaces. The following tables list the LPUs supported by the S7700.

NOTE

LPUs are classified into S series boards, E series boards, F series boards:

- S series boards are SA boards, for example, 24-port 100M/1000M Ethernet optical LPU (**SA**, SFP)-32K MAC address entries.
- E series boards include EA, EC, and ED boards, for example, 48-port 100M Ethernet optical LPU (**EA**, SFP)-32K MAC address entries.
- F series boards include FA and FC boards, for example, 48-port 1000M Ethernet electrical LPU (**FA**, RJ45)-32K MAC address entries.

Table 2-5 Ethernet LPUs

Name	Description
F48TA	48-port 10/100BASE-T interface line card (EA, RJ45)-32K MAC address entries

Name	Description
F48TC	48-port 10/100BASE-T interface line card (EC, RJ45)-128K MAC address entries
F48TFA	48-port 10/100BASE-T interface line card (FA, RJ45)-32K MAC address entries
G48SA	48-port 100/1000BASE-X interface line card (EA, SFP)-32K MAC address entries
G48SC	48-port 100/1000BASE-X interface line card (EC, SFP)-128K MAC address entries
G48SD	48-port 100/1000BASE-X interface line card (ED, SFP)-512K MAC address entries
G48SFA	48-port 100/1000BASE-X interface line card (FA, SFP)-32K MAC address entries
G48TA	48-port 10/100/1000BASE-T interface line card (EA, RJ45)-32K MAC address entries
G48TC	48-port 10/100/1000BASE-T interface line card (EC, RJ45)-128K MAC address entries
G48TFA	48-port 10/100/1000BASE-T interface line card (FA, RJ45)-32K MAC address entries
G48CEAT	36-port 10/100/1000BASE-T and 12-port 100/1000BASE-X interface line card (EA, RJ45/SFP)–32K MAC address entries
G48VA	48-port 10/100/1000BASE-T PoE interface line card (EA, RJ45, PoE)-32K MAC address entries
X4UXA	4-port 10GBASE-X interface line card (EA, XFP)-32K MAC address entries
X4UXC	4-port 10GBASE-X interface line card (EC, XFP)-128K MAC address entries
X2UXA	2-port 10GBASE-X interface line card (EA, XFP)-32K MAC address entries
X2UXC	2-port 10GBASE-X interface line card (EC, XFP)-128K MAC address entries
X4UXD	4-port 10GBASE-X interface line card (EC, XFP)-512K MAC address entries
G24SA	24-port 100/1000BASE-X interface line card (SA, SFP)-32K MAC address entries
G24SC	24-port 100/1000BASE-X interface line card (EC, SFP)-128K MAC address entries
G24CA	24-port 100/1000BASE-X and 8-port 10/100/1000BASE-T interface line card (SA, SFP/RJ45)
X12SA	12-port 10GBASE-X interface line card (SA, SFP+)
T24XA	24-port 10/100/1000BASE-T and 2-port 10GBASE-X interface line card (EA, RJ45/XFP)-32K MAC address entries

Name	Description
S24XA	24-port 100/1000BASE-X and 2-port 10GBASE-X interface line card (EA, SFP/XFP)-32K MAC address entries
G24TFA	24-port 10/100/1000BASE-T interface line card (FA, RJ45)-32K MAC address entries
X40SFC	40-port 10GE Ethernet optical interface line card (FC, SFP+)
X16SFC	16-port 10GE Ethernet optical interface line card (FC, SFP+)

NOTE

- The Small Form-factor pluggable (SFP) is a hot pluggable optical module.
- The 10 Gigabit Small Form-Factor Pluggable (XFP) is a 10G hot pluggable optical module.
- The 10 Gigabit Small Form-Factor Pluggable (SFP+) is a 10G hot pluggable optical module. Its caliber is smaller than the caliber of the XFP optical module.
- By default, the transmission rate of an optical interface is 1000 Mbit/s and the 100M/1000M auto-negotiation is not supported. To use 100 Mbit/s optical interfaces, you must configure it manually.

2.2.6 FSU

The Flexible Service Unit A (FSUA) is applied to the S7706 and S7712. It supports the following functions:

- Hardware-based Ethernet OAM
- Hardware-based MPLS OAM
- Hardware-based Bidirectional Forwarding Detection (BFD)
- DoS attack protection for the SRU's Central Processing Unit (CPU)

NOTE

Software-based Ethernet OAM, MPLS OAM, BFD and NQA functions are available in other LPUs.

FSUA is an optional subcard on the SRU of the S7706 and S7712. Users have the option to install the FSUA according to the service requirement.

Table 2-6 FSUA

Name	Description
20 Gbit/s FSUA	Provides 20 Gbit/s service switching capability.

2.2.7 VSU

The Virtual Switch Unit (VSU) connects multiple devices to form a stack.

On the S7712 and S7706, the VSTSA acts the VSU, and is installed on the SRU. You can configure the VSTSA according to service requirements. For the VSTSA, "VS" represents the virtual switch, "T" represents the electrical interface, "S" represents the standard series, and "A" represents the version.

Table 2-7 Stacking cards

Name	Description
VSTSA	Handles device stacking.

2.2.8 SPU

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

The SPU used on the S7700 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 2-8 SPU

Name	Description
VAMPA	Processes value-added services.

2.3 Software Architecture

This section describes the relationship between the S7700's operating system and its software features.

The S7700 runs the latest VRP version (VRPv5), which consists of the following components:

- System service plane, which provides the following functions:
  - Task management
  - Memory management
  - Timer
  - Software loading and patching

  This enhances the modular technologies, thus facilitating easier system upgrades and customization.
- General control plane

  The core of the VRP data communication platform. It handles basic security and QoS, and provides the following functions:

  - Link management
  - IP protocol stacking
  - Routing protocol processing

  It controls the data forwarding plane and carries out various device functions.

- Data forwarding plane

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

- Service control plane

  Controls and manages system data based on users or interfaces. It implements authentication, authorization, and accounting (AAA) for users through the DHCP Option 82 field. It also implements authentication for access interfaces through IEEE 802.1x.

- System management plane

  Provides user interfaces and manages input/output ports, acting as the basis of network management and maintenance.

3 Service Features

About This Chapter

This section describes the major service functions of the S7700, including IP features,MPLS, MPLS L2VPN, MPLS L3VPN, QoS, Ethernet, Ethernet OAM, NAC, multicast, reliability, LLDP, security, stacking, Web network management, firewall/NAT, load balancing, IPSec VPN, NetStream, and WLAN AC.

NOTE

The release in Russia does not provide IPSec VPN.

The S7700 provides NAC, firewall, NAT, load balancing and WLAN AC for enterprise networks.

3.10 MPLS

This section describes the basics of MPLS, MPLS TE, and MPLS OAM.

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 S7700 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 S7700 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 S7700 also supports double-tagged VLAN mappings.

- 2:2 VLAN mapping

  The S7700 can map user side double-tagged packets to network side double-tagged packets. Additionally, the S7700 can replace both the outer and inner tags of a packet.
- 2 to 1 VLAN mapping

  The S7700 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 S7700 supports the CoS-based VLAN mapping. It can map multiple C-VLAN tags to the same S-VLAN tag according to the CoS.

For details about VLAN Mapping, refer to the section "VLAN" in the *S7700 Smart Routing Switch Feature Description - Ethernet*.

3.1.3 Selective QinQ

Selective QinQ expands the VLAN tag space, enabling the S7700 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 S7700 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 S7700's powerful hardware implements selective QinQ using traffic classification based on ACLs, permitting the S7700 to flexibly add S-VLAN tags or modify C-VLAN tags.

For details about selective QinQ, refer to the section "QinQ" in *S7700 Smart Routing Switch Feature Description - Ethernet*.

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 S7700 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 S7700.

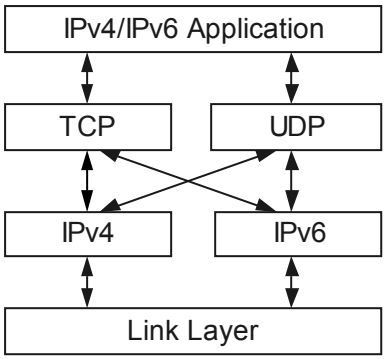
NOTE

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 S7700 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.

For details about IPv4refer to the section "IPv4" in *S7700 Smart Routing Switch Feature Description - IP Service*.

3.2.3 IPv6 Features

The S7700 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

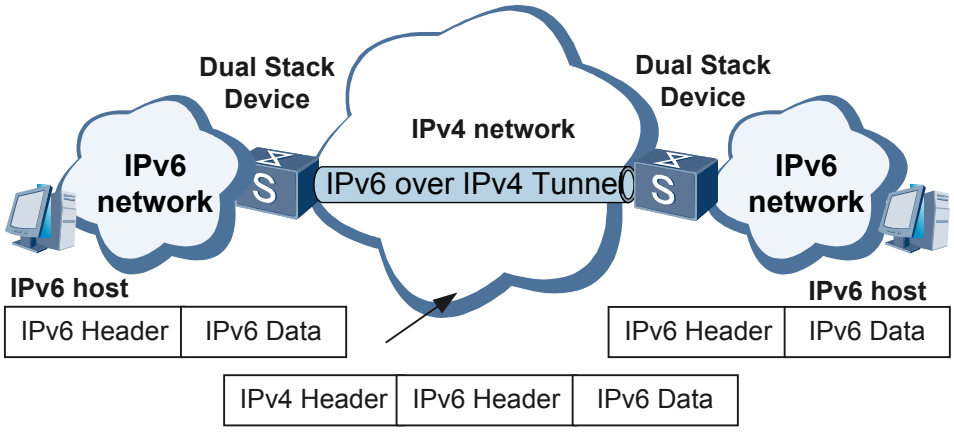
For details about IPv6, refer to the section "IPv6"in *S7700 Smart Routing Switch Feature Description - IP Service*.

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 S7700 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.

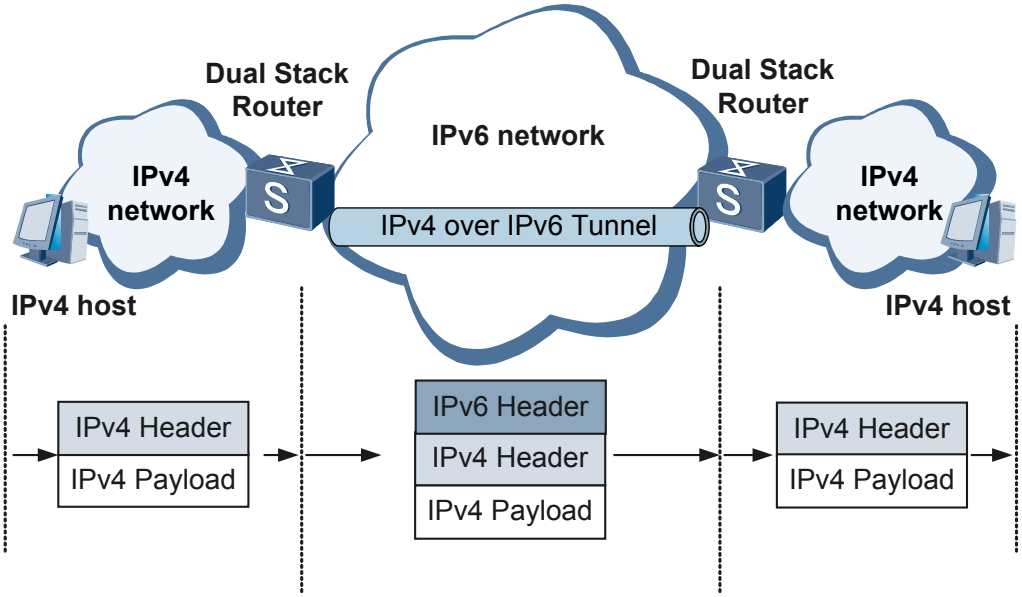
  Compared with a manual tunnel, a 6to4 tunnel can be a P2MP connection, whereas a manual tunnel is a P2P connection. Routers using a 6to4 tunnel are not configured in pairs. Similar to routers on an automatic tunnel, a router on a 6to4 tunnel can search for the other end of the tunnel. However, since 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.

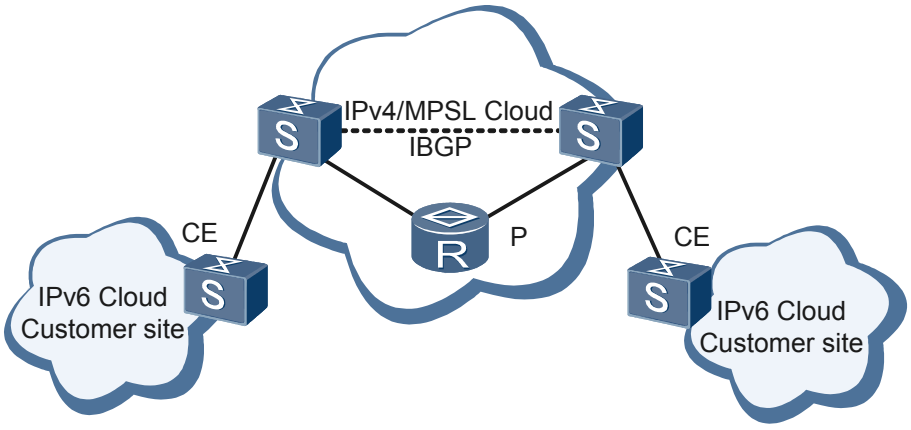
Figure 3-3 Network diagram of an IPv4 over IPv6 tunnel



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.

The IGP protocol used on the ISP network can be OSPF or IS-IS, and the protocol used between CE routers and 6PE routers can be a static routing protocol, an IGP, or EBGP.

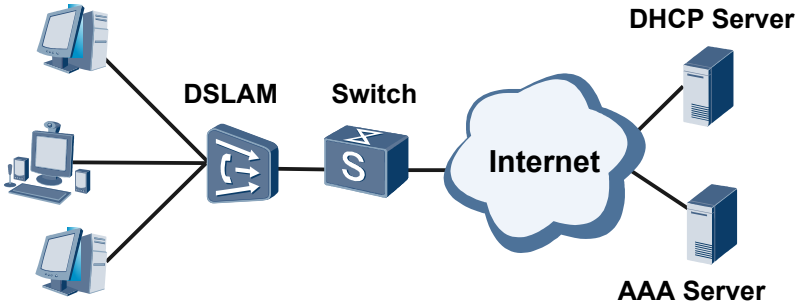
If the IPSs want to use the IPv4/MPLS networks to exchange IPv6 traffic, they can just update the PE router. Therefore, using the 6PE feature as an IPv6 transition mechanism is a cost-effective solution for ISPs.

3.2.5 IP Session

This section describes the IP session feature supported by the S7700.

As shown in **Figure 3-5**, Switch represents the S7700.

Figure 3-5 Networking diagram of an IP session



The S7700 can assign IP addresses to terminate and authenticate IP sessions.

An STB or VoIP terminal sends a DHCP Request message to which the S7700 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 S7700 sends the VLAN (QinQ) information or DHCP Relay Agent information to the AAA server to authenticate the terminal. If the authentication is successful, the S7700 assigns an IP address to that terminal.

The S7700 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 S7700 supports multicast features including IGMP snooping, IGMP proxy, static multicast, multicast across VLANs.

3.3.1 Multicast Routing Protocol

The S7700 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 S7700 can filter the routes based on routing policies. When forwarding IP multicast packets, the S7700 can filter and forward packets based on these policies.

For details about Link Aggregation, refer to the *S7700 Smart Routing Switch Feature Description - Multicast*.

3.3.2 IGMP Snooping and MLD Snooping

Located between the host and the multicast router, the S7700 can statically configure multicast forwarding entries. In addition, the S7700 maintains the multicast group, the VLAN ID mapping and outbound ports by listening to passing IGMP/MLD messages. The S7700 dynamically sets up a Layer 2 forwarding table for multicast packets.

When the S7700 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 S7700's ports are attached to only one host, the S7700 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 S7700 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 S7700 can act as querier for the following multicast functions:

- Run queries.

- Establish multicast forwarding tables on Layer 2 networks.

Multicast Packet Suppression

If the S7700 receives a Report packet or Leave packet from users within a short period of time, the S7700 checks whether the same Report packet or Leave packet has been received during the suppression period. The S7700 then decides whether to send the packets to the router, reducing the number of IGMP/MLD packets handled by the router.

Controllable Multicast

The S7700 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 S7700 can be deployed between multiple DSLAMs and an upstream multicast router. If IGMP/MLD is not enabled for some VLANs on the S7700, the S7700 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 S7700 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 S7700 can copy up to 127 copies of multicast packets of different VLANs to each port.

The S7700 forwards multicast packets through the multicast VLAN, and copies the packets based on the multicast entries. The S7700 then sends these packets to different users' VLANs. Using the multicast VLAN technique, the S7700 can converge the multicast packets from all user VLANs into one or several VLANs.

Multicast VLAN enables the S7700 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 S7700.

NOTE

For details about Link Aggregation, refer to the *S7700 Smart Routing Switch Feature Description - QoS*.

3.4.1 Hierarchical Traffic Policing

The S7700 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 S7700 to monitor incoming traffic. If the rate is too high, the S7700 chooses to discard packets or reset packet priorities.

The S7700 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 S7700 applies service parameters to packets that match certain ACL rules. Re-marking is implemented as follows:

- The S7700 applies self-defined service parameters to packets.
- The S7700 applies service parameters as defined by the mapping table according to packets' Differentiated Services Code Point (DSCP).
- The S7700 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 S7700 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 S7700 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 S7700 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 S7700 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 S7700 can manually bind multiple ports to an Eth-Trunk interface. The S7700 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 S7700 can aggregate links on different LPUs, improving service reliability.

For details about Link Aggregation, refer to the section "Trunk" in *S7700 Smart Routing Switch Feature Description - Ethernet*.

3.5.2 DLDP

The S7700 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.

For details about DLDP, refer to the section "DLDP" in *S7700 Smart Routing Switch Feature Description - Reliability*.

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.

For details about RRPP, refer to the section "RRPP" in *S7700 Smart Routing Switch Feature Description - Reliability*.

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.

For details about Smart Link, refer to the section "Smart Link" in *S7700 Smart Routing Switch Feature Description - Reliability*.

3.5.5 Ethernet OAM

The S7700 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 S7700 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 S7700 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 S7700 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 S7700s. 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 S7700 supports the Ethernet performance management. The S7700 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 S7700 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 S7700 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 S7700 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 S7700 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 S7700 supports the association among BFD, 802.3ad, and 802.1ag to provide an end-to-end OAM solution.

For details about BFD, refer to the section "BFD" in *S7700 Smart Routing Switch Feature Description - Reliability*.

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 S7700 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.

For details about LSP protection switchover, refer to the section "MPLS OAM" in *S7700 Smart Routing Switch Feature Description - MPLS*.

3.5.9 Equipment Level Reliability

Hot Backup

The S7700 supports hot backup for its key components including the SRU/MCU, power modules, and fan modules.

- SRU/MCU

The S7700 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 PoE function is only supported by AC power modules. The S7703 does not support the backup of PoE power modules. The S7706 and the S7712 support PoE power modules working in 3+1 mode, 2+2 mode, or.no backup mode.
- Fan modules

  Each fan frame of the S7700 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 S7700 are all hot swappable.

WARNING

FSUA is not hot swappable.

- SRUs/MCUs

  When the S7700 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 S7700, hot swapping one or two of them will not interrupt services.
- Fan frames

  Hot swapping fan frames will not affect S7700 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.

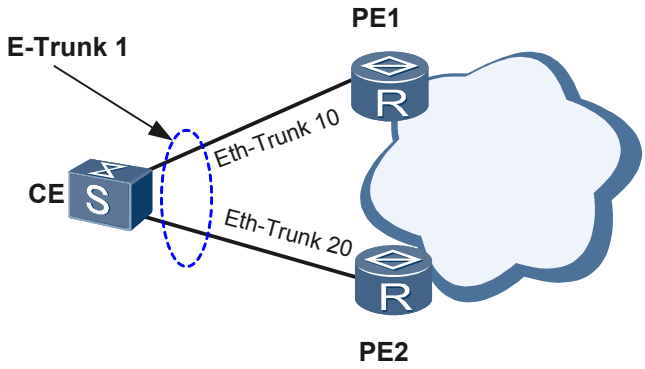
E-Trunk Composed of Ethernet Interfaces on Different Devices

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



Stacking

A single switch cannot meet the demands of increasing data center access volume and ensure network reliability. The S7700 uses specialized switch stacking technology to meet these growing demands.

In a CSS, multiple S7700s are connected through dedicated stacking cables to form a logical switch.

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 S7700 separates the control channel from the service channel, creating a non-blocking control channel. The S7700 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 S7700 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 S7700 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 S7700 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.

S7700 commands are divided into 4 levels, and login users are also divided according to these 4 levels. After logging in to the S7700, users can only run commands that correspond to their user level.

The S7700 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 S7700 can also lock the terminal through the command line to prevent unauthorized use.

Remote Login Through SSH

The S7700 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 S7700 supports SNMPv3 encryption and authentication to authenticate the management packets from the NMS.

Authentication, Authorization, and Accounting

The S7700 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 S7700 defend against unauthorized user login.

Hierarchical CPU Protection

The S7700 supports two levels of CPU protection:

- LPU level

  Based on protocol type, the S7700 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 S7700 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 S7700 can effectively control the passing packets.

The S7700 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 S7700 listens to the sent DHCP packets. The S7700 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 S7700 can also insert or strip a packet's Option 82 field.

- After receiving a request packet from the DHCP client, the S7700 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 S7700 analyzes the Option 82 field to select the appropriate forwarding port. The S7700 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 S7700 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 S7700 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 S7700 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 S7700 forwards or discards incoming packets with new MAC addresses as configured.

Blackhole MAC Entries

The S7700 supports blackhole MAC entries. When the S7700 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 S7700 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 S7700 to specific interfaces and preventing MAC spoofing attacks.

Broadcast Suppression

The S7700 can limit the transmission rate of broadcast packets, multicast packets, and unknown unicast packets according to their interfaces.

The S7700 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 S7700 provides LLDP and NetStream network management functions.

3.7.1 LLDP

The S7700 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.

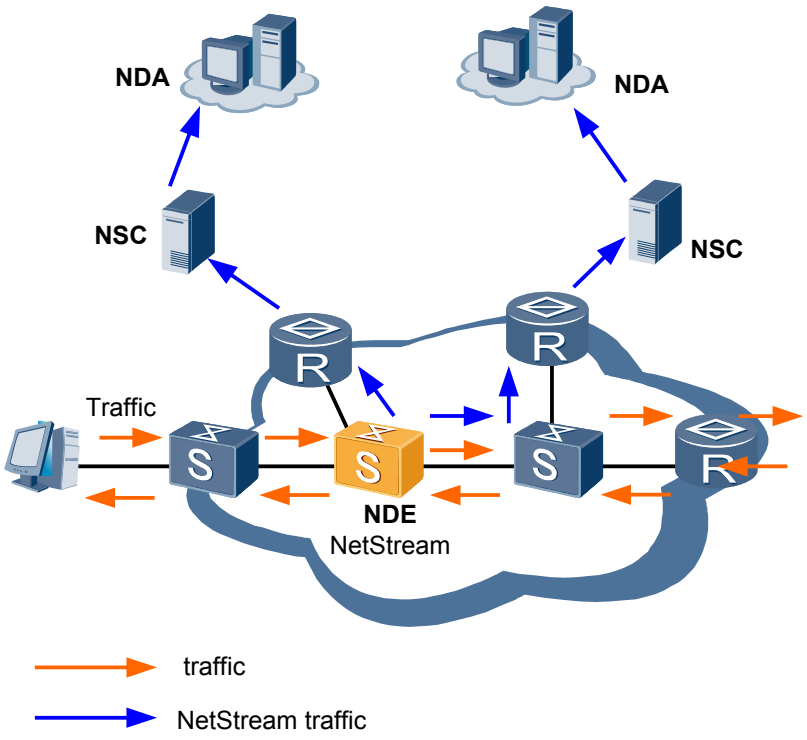
Using the LLDP, a local network management station can acquire link layer information for all devices in the local network. It can also collect detailed information about network topology and topology changes, expanding the scope of network management.

Ports with LLDP enabled on the S7700 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 S7700 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 S7700 supports both distributed NetStream and integrated NetStream.

For details about netstream, refer to the section "NetStream" in *S7700 Smart Routing Switch Feature Description - Network Management*.

3.8 PoE

On intranets, PoE can be used to provide centralized power for terminals such as IP phones, Access Points (APs), portable device chargers, POS machines, cameras, and data collection devices through the 10Base-T, 100Base-TX, or 1000Base-T Ethernet.

Terminals are powered when they access the network, so additional indoor power cabling is not required.

According to IEEE802.3af and IEEE 802.3at, PoE involves PSEs and PDs.

The PSEs provide power for other devices and are classified as Midspan (the PoE module is installed outside the switch) and Endpoint (the PoE module is integrated with the switch) PSEs. IEEE 802.3af and IEEE 802.3at allow Endpoint PSEs to use copper line pairs connected to pins 1 and 2 and pins 3 and 6 or pins 4 and 5 and pins 7 and 8 for power supply. Endpoint PSEs are compatible with 10Base-T, 100Base-TX, and 1000Base-T interfaces, and are more widely used than the Midspan PSE.

The S7700 is an Endpoint PSE, complying with IEEE 802.3af or IEEE 802.3at. Each interface provides 30 W of power.

On the S7700, each interface supporting PoE provides three power supply priorities for PDs, that is, critical, high, and low. When the power consumption of PDs is greater than the total PSE power, the PSE first provides power to the PD on the interface with the highest priority. If different interfaces have the same priority, the PSE provides power for PDs in descending order of port numbers; therefore, the PD on the interface with the smallest interface number obtains power supply first.

For details about PoE, refer to the section "PoE" in *S7700 Smart Routing Switch Feature Description - Device Management*.

3.9 Enterprise Network Features

The S7700 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 S7700 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

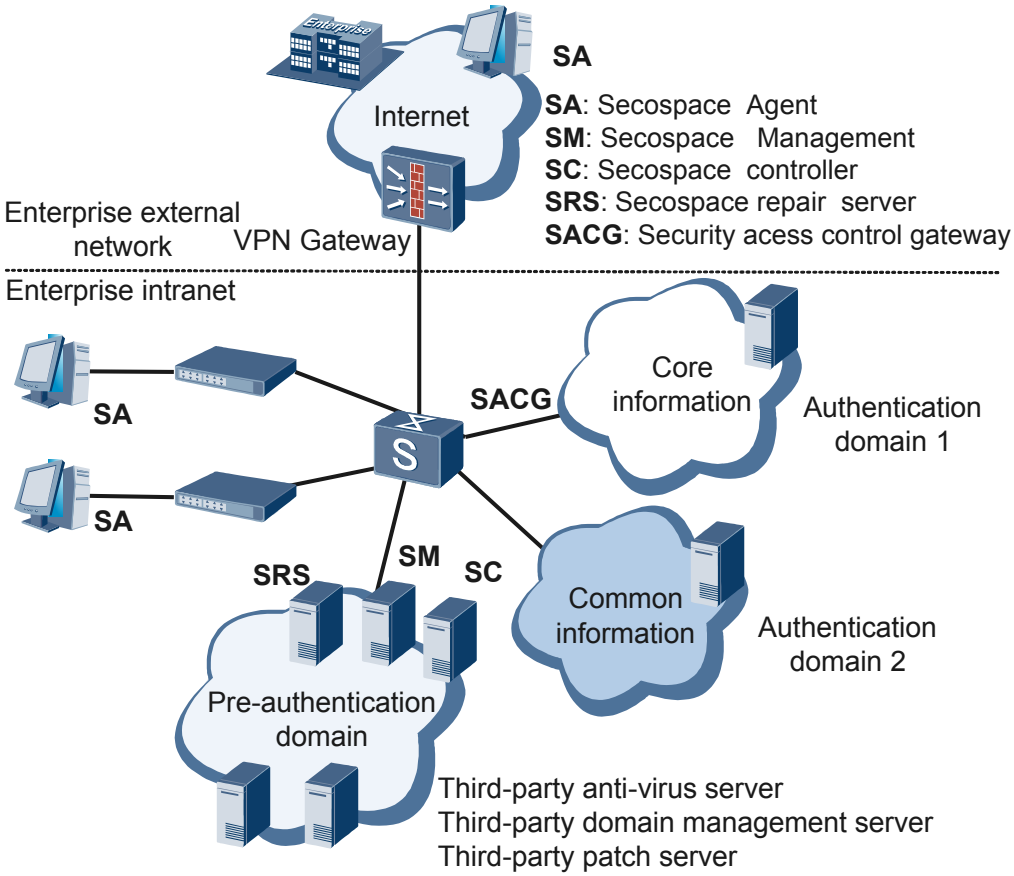
When functioning as a network access device, the S7700 provides the following functions:

- 802.1X access, including port mode and MAC mode
- Portal access
- Relay authentication in which the S7700 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 S7700 provides a distributed firewall with a 10 Gbit/s processing capacity to provide high-performance security for large enterprises, carriers, and data center networks. The S7700

supports the external attack defense, internal network security, traffic monitoring, email filtering, Web page filtering, and application layer filtering, effectively ensuring network security.

The S7700 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 S7700 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.

For details about firewall, refer to *S7700 Smart Routing Switch Feature Description - SPU*.

3.9.3 NAT

The S7700 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 S7700 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

For details about NAT, refer to *S7700 Smart Routing Switch Feature Description - SPU*.

3.9.4 Load Balancing

The S7700 provides server load balancing for Layers 4 through Layer 7 services and supports deployment of multiple applications and server clusters.

The S7700 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 S7700 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 S7700 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 S7700 switches can initiate IPSec VPN tunnel negotiation to peer ends. When deployed in headquarters, they can accept tunnel negotiation requests from branches.

For details about IPSec VPN, see the *S7700 Smart Routing Switch Feature Description - SPU*.

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 S7700 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

This section describes the basics of MPLS, MPLS TE, and MPLS OAM.

NOTE

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

The S7700 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 S7700 can act as the PE device or Provider (P) device on an MPLS network.

The S7700 supports multiple MPLS features, including Label Distribution Protocol (LDP) or Resource Reservation Protocol for Traffic Engineering (RSVP-TE), MPLS TE, and MPLS OAM.

3.10.1 Basic MPLS Functions

The S7700 supports the following basic MPLS functions:

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

For details about MPLS Functions, refer to the section "MPLS LDP" in *S7700 Smart Routing Switch Feature Description - MPLS*.

3.10.2 MPLS TE

The S7700 supports the MPLS Traffic Engineering (TE). MPLS TE is a technique that integrates TE with MPLS. Using MPLS TE, the S7700 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 S7700 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

For details about MPLS TE, refer to the section "MPLS TE" in *S7700 Smart Routing Switch Feature Description - MPLS*.

3.10.3 MPLS OAM

The S7700 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 S7700 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 S7700 triggers a protection switchover using a Forward Defection Indicator (FDI) message and a Backward Defect Indicator (BDI) message.

The S7700 supports 1:1 and N:1 protection switchover of LSPs using an active LSP and a standby LSP. When the active LSP fails, the S7700 promptly switches services to the standby LSP. This greatly improves the reliability of MPLS networks.

For details about MPLS OAM, refer to the section "MPLS OAM" in *S7700 Smart Routing Switch Feature Description - MPLS*.

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 S7700 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.

For details about VLL, refer to the section "VLL" in *S7700 Smart Routing Switch Feature Description - VPN*.

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 S7700 functions as the PE device on a VPLS network, transmitting VPLS services by establishing through-connection between PEs.

The S7700 supports VPLS in the following modes:

- Martini
- Kompella

For details about VPLS, refer to the section "VPLS" in *S7700 Smart Routing Switch Feature Description - VPN*.

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 S7700 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 S7700 supports HVPLS in Martini mode.

On the VPLS or HVPLS network, the S7700 maps services of different types to different Virtual Switch Instances (VSIs). The S7700 then transparently transmits these services to NPE or PE-AGG through the VPLS or HVPLS network.

For details about HVPLS, refer to the section "VPLS" in *S7700 Smart Routing Switch Feature Description - VPN*.

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 S7700 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.

For details about MPLS L3VPN, refer to the section "BGP/MPLS IP VPN" in *S7700 Smart Routing Switch Feature Description - VPN*.

4 Application Scenarios

About This Chapter

This section describes the typical networking and applications of the S7700.

4.1 Overview
This section describes the S7700's position within the access layer and convergence layer in a MAN.

4.2 MPLS L2VPN
This section describes how MPLS VPN can be applied to a network.

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.

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

4.5 Smart Link in Dual-Homing Networking
This section describes how Smart Link functions in dual-homing networks.

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

4.7 QoS
This section describes how QoS is applied in a MAN.

4.8 Selective QinQ
This section describes how selective QinQ functions on a network.

4.9 IPTV Service
This section describes the S7700's networking and application policy for the IPTV service.

4.10 NAC
This section describes how the S7700 implements NAC on a network.

4.11 Firewall
This section describes the firewall networking and policy of the S7700.

4.12 Application of the WLAN AC

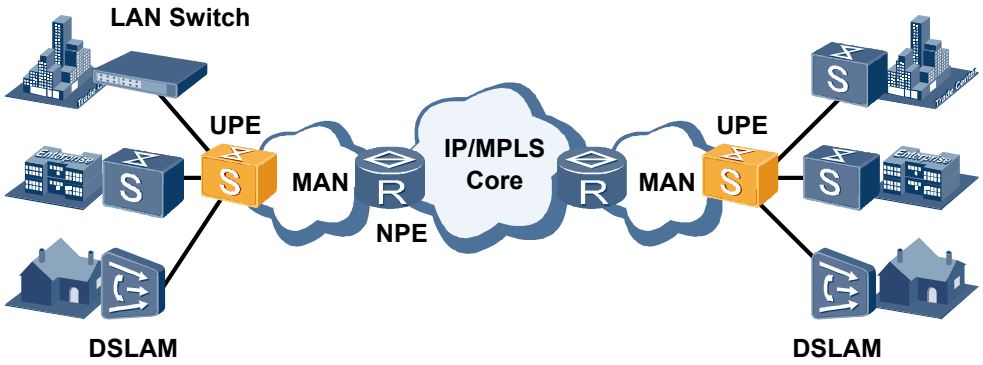
This section describes how the S7700 functions as an AC on a WLAN.

4.1 Overview

This section describes the S7700's position within the access layer and convergence layer in a MAN.

The S7700 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 S7700 deployed in a MAN



Acting as the UPE device in a MAN, the S7700 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 S7700 also connects to the upstream NPE devices, such as the Huawei ME60 and NE40E. Additionally, the S7700 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 S7700 system supports 4K VLL instances and up to 1K VPLS instances.

As shown in **Figure 4-2** and **Figure 4-3**, the S7700 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)

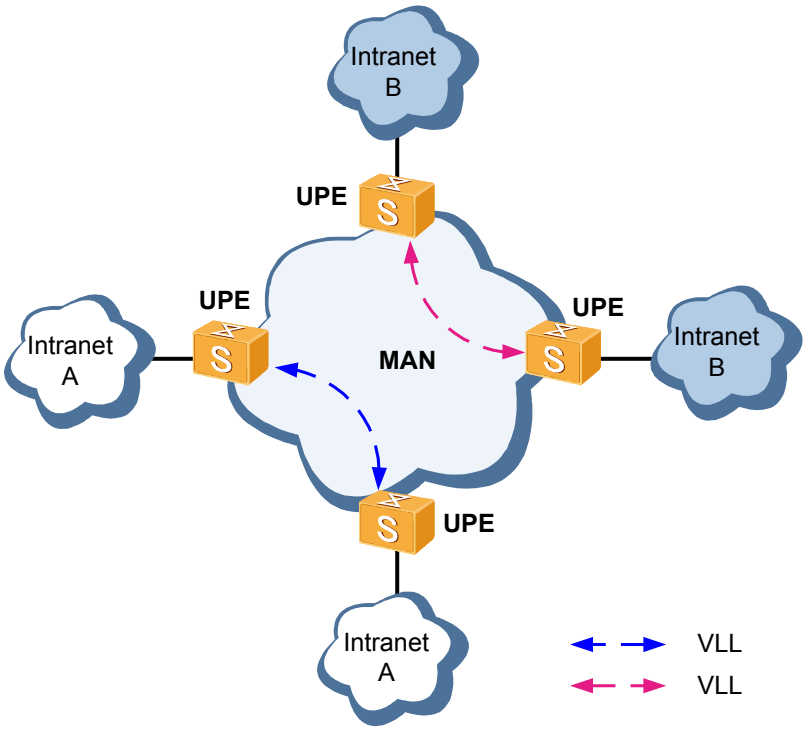
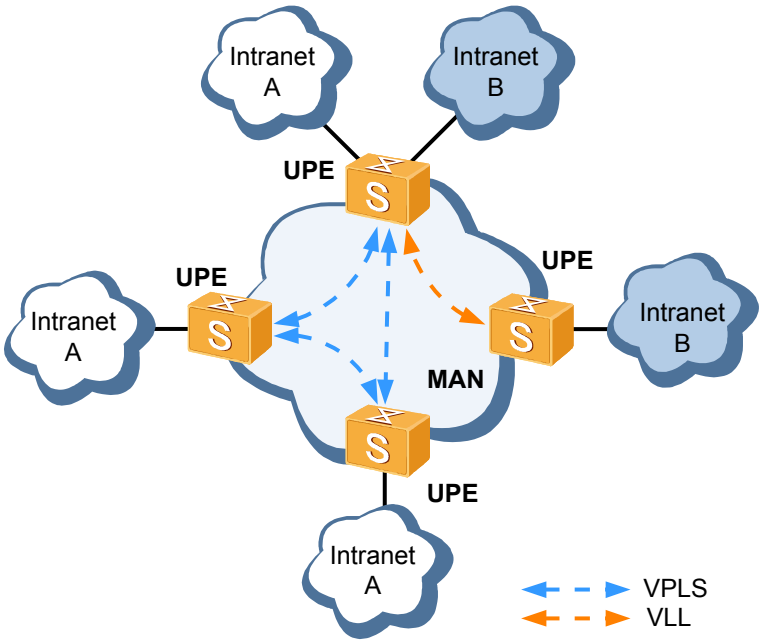


Figure 4-3 Network diagram of multipoint-to-multipoint VPN (VPLS)

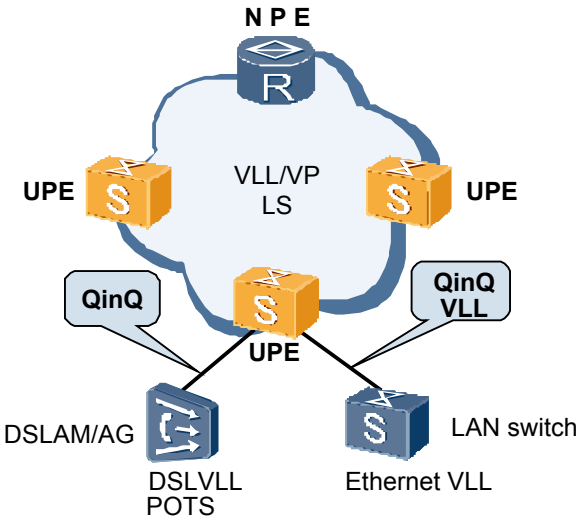


As shown in **Figure 4-4**, by cooperating with the DSLAM, Access Gateway (AG), and Layer 2 switches, the S7700 maps access services to VLL or VPLS services.

- Along with the DSLAM/AG, the S7700 maps QinQ tunnels to VLL or VPLS service instances, facilitating Digital Subscriber Line (DSL)-based VLL services.
- Along with Layer 2 switches, the S7700 maps QinQ tunnels and VLL tunnels to VLL or VPLS service instances.

The S7700 handles multiple services at both the access and convergence layers. The S7700 can map specific personal services such as broadband access and VoIP to VLL or VPLS service instances.

Figure 4-4 Network diagram of an S7700 running VPN services on a CE-supported network



The S7700 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.

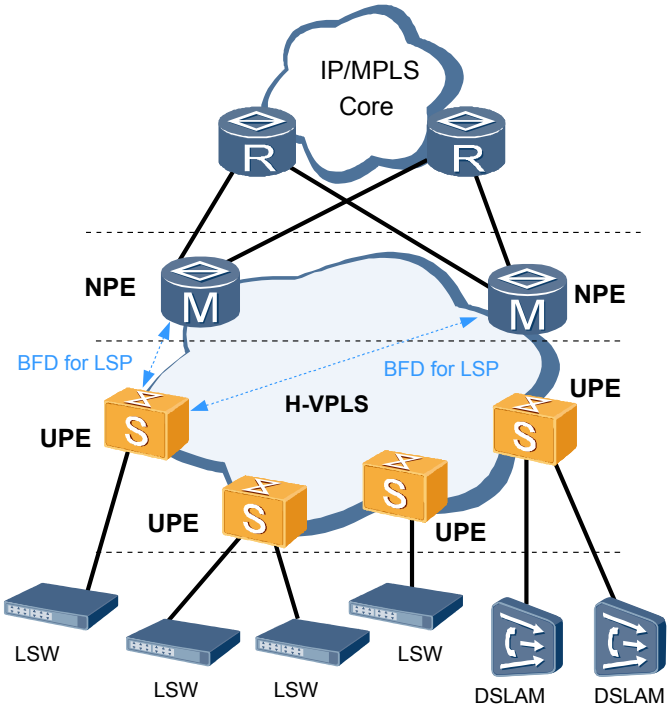
The S7700 supports HVPLS for link protection between two NPEs in dual-homing mode. On an HVPLS network, the S7700 acts as a UPE device to converge services from the CE.

The S7700 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 S7700 running HVPLS on a UPE+NPE network



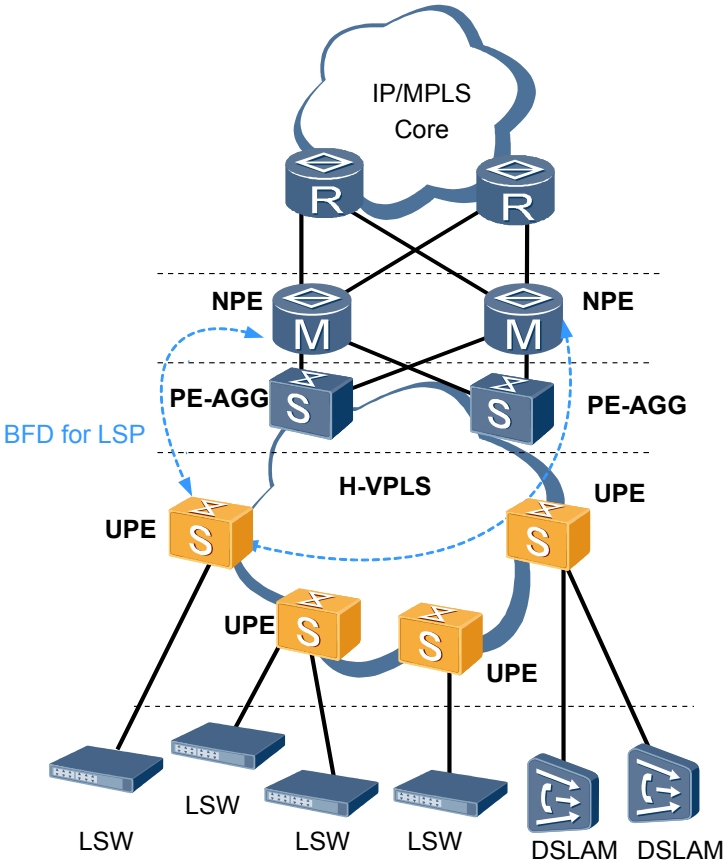
As shown in **Figure 4-5**, on the HVPLS network, the S7700 acts as the UPE device. The Huawei ME60 and NE40E routers can be used as the NPE devices.

- As the UPE device, the S7700 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 S7700 can serve as the PE-AGG or UPE device as shown in **Figure 4-6**.

Figure 4-6 Network diagram of an S7700 running HVPLS on a UPE+PE-AGG+NPE network



In this networking mode:

- The S7700 functions the same in this network architecture as in "**UPE+NPE Network Architecture**."
- The S7700 terminates VPLS tunnels and transparently transmits services to NPE devices.
- The NPE devices decapsulate VLAN and QinQ packets.
- Link protection between the S7700 and the NPE device is implemented using BFD for LSP.

4.4 RRPP

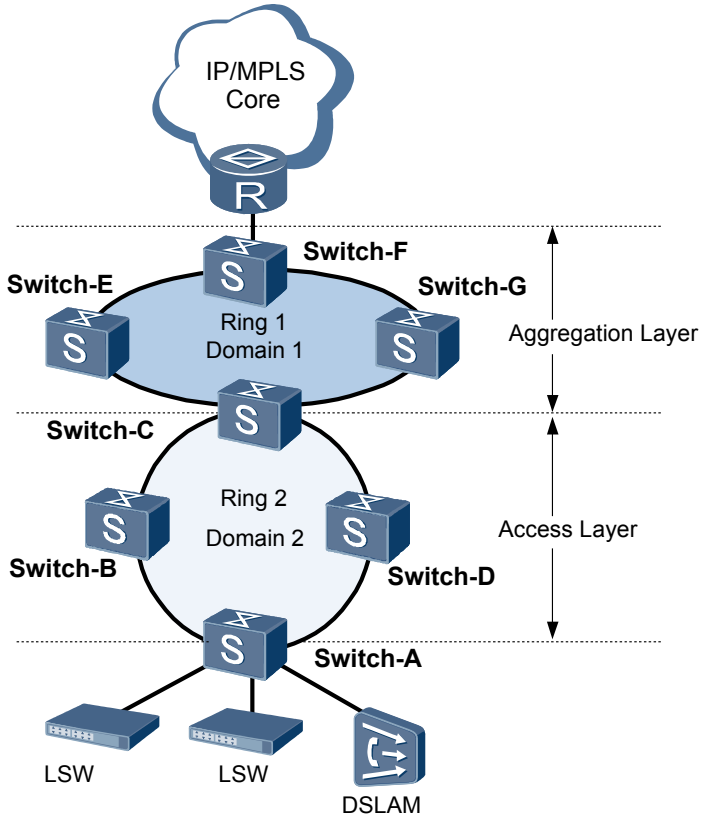
This section describes how RRPP implements fast protection switchover on ring networks.

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.

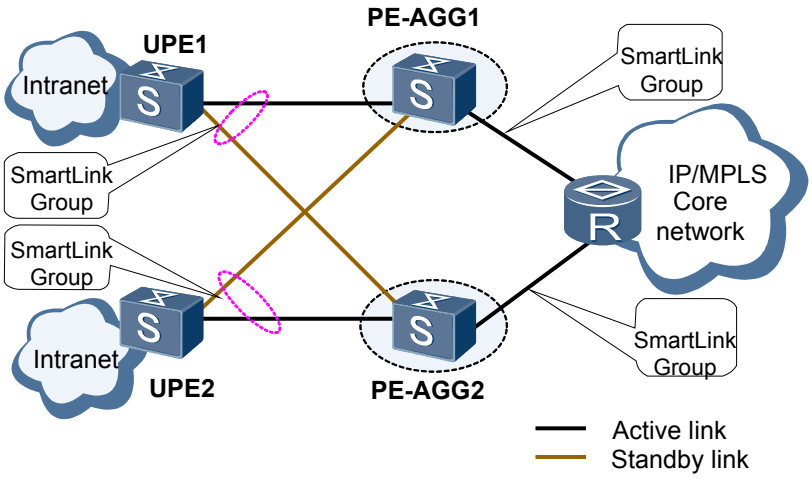
At this time, the network topology changes, so the original ARPs and FIBs of the nodes cannot direct Layer 3 forwarding. After unblocking the secondary port, the master node immediately requires other nodes on the ring to re-learn MAC address entries. The Layer 2 traffic on the RRPP ring is then switched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

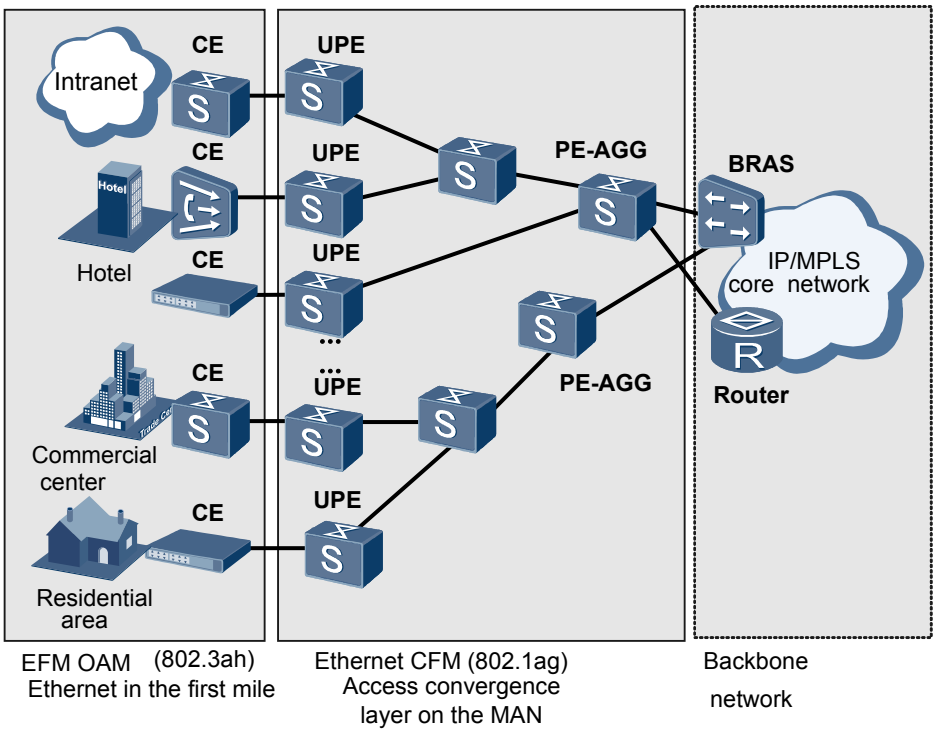
The Monitor Link group can be configured on PE-AGG 1 and PE-AGG 2 to associate uplink interface with downlink interface.

4.6 Ethernet OAM

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

With Ethernet OAM, the S7700 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.

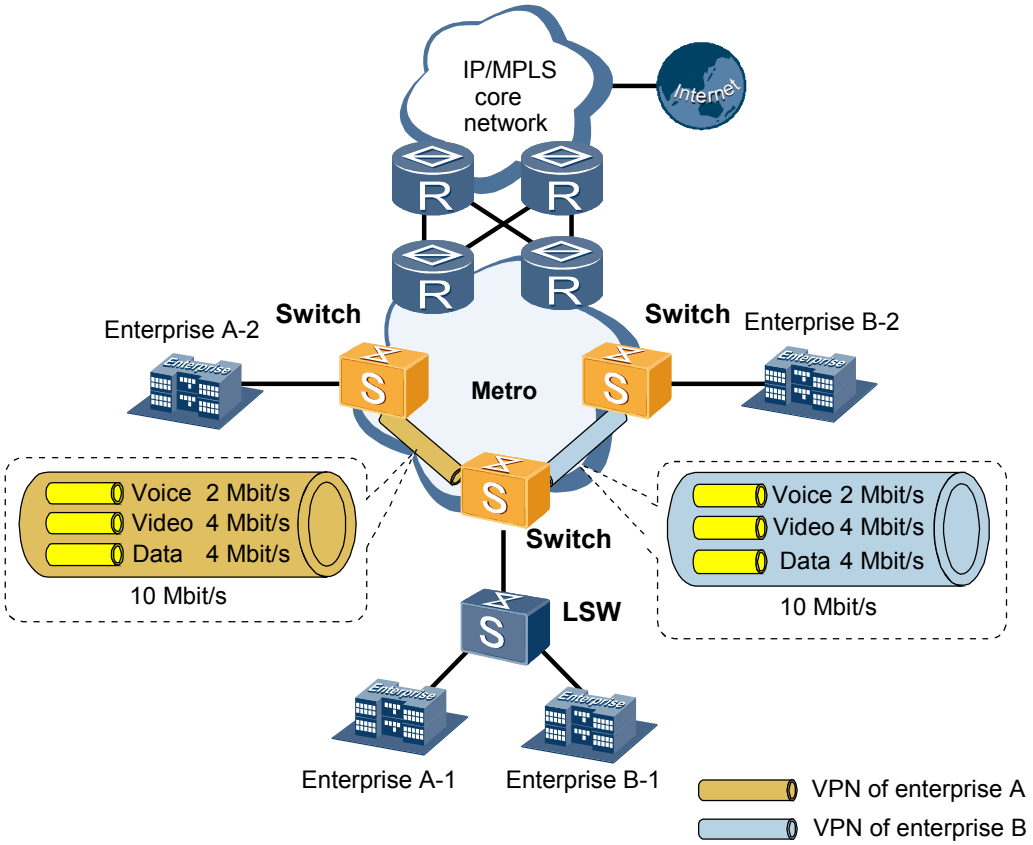
EFM OAM is enabled on CEs and UPEs. EFM OAM can test link connectivity of user services by periodically exchanging OAMPDUs between CEs and NPEs. EFM OAM monitors link performance by detecting error frames, error codes, and error frame seconds on the link. This provides transmission services conforming 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 S7700.

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.

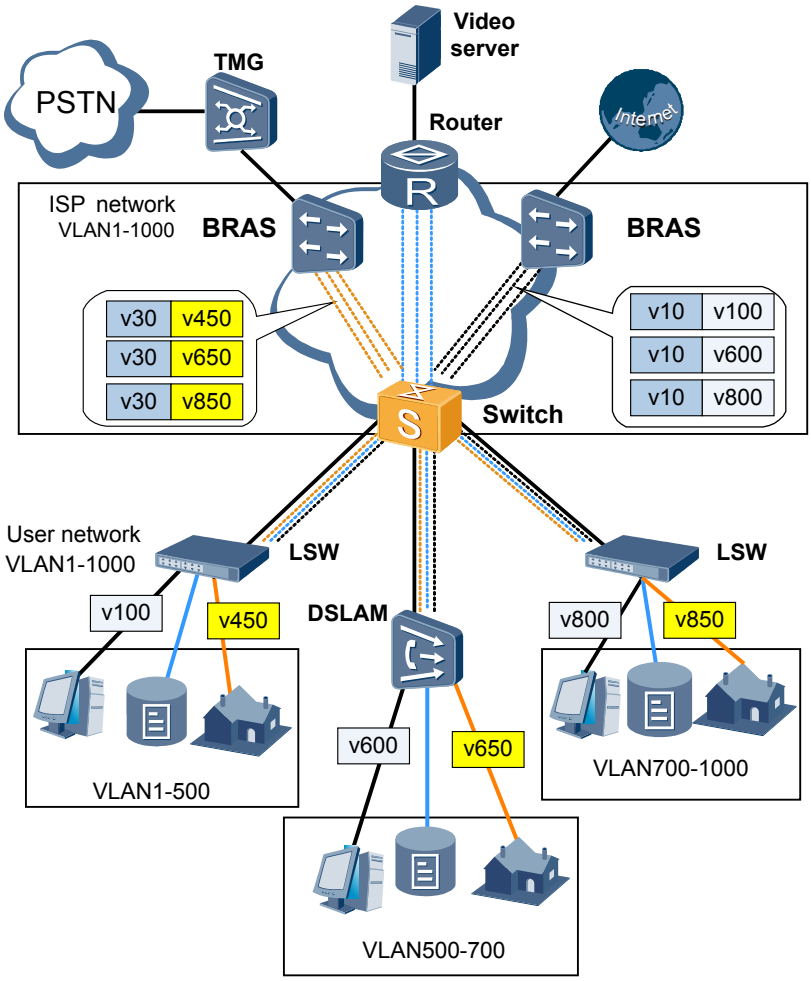
By applying level-2 traffic management on the Switch, you can meet the above service and user network resource requirements.

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 S7700.

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 S7700 can converge services and choose different paths for various services to more effectively facilitate network deployment.

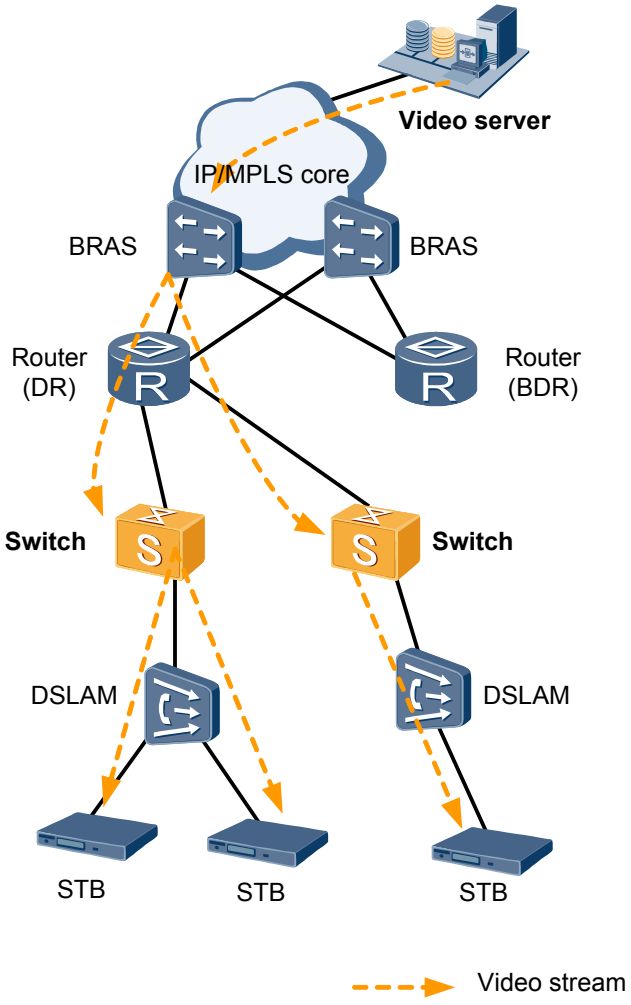
4.9 IPTV Service

This section describes the S7700's networking and application policy for the IPTV service.

4.9.1 IPTV Networking

The S7700 supports IPTV network as outlined in **Figure 4-12**.

Figure 4-12 Network diagram of IPTV implementation



The S7700'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**:

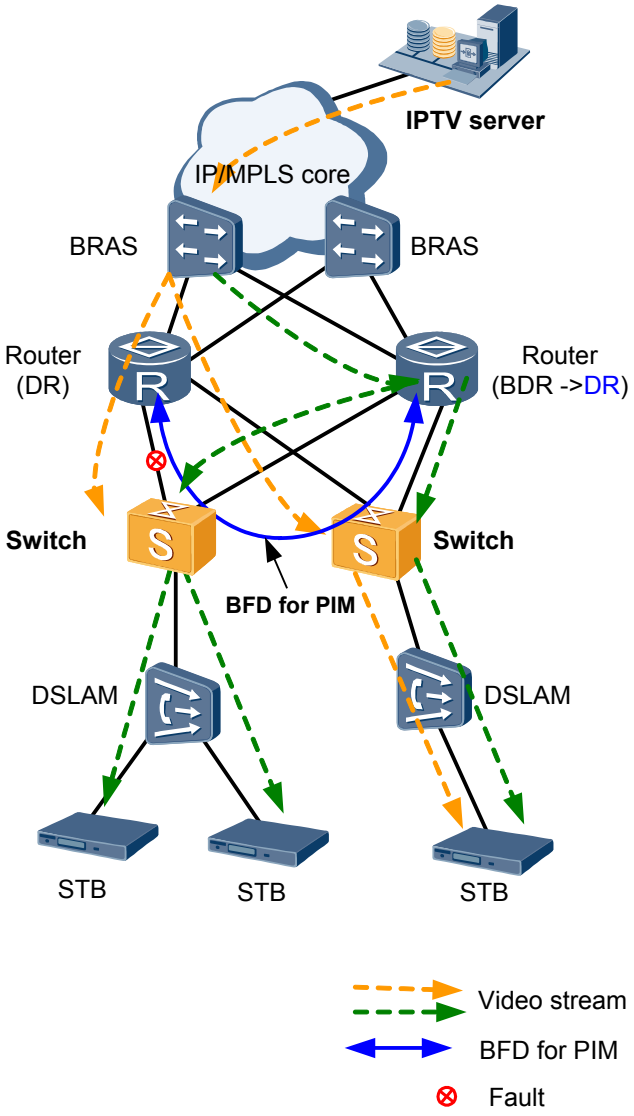
- The routers run the PIM protocol and act as either Designated Routers (DRs) or Backup Designated Routers (BDRs). A DR processes IGMP packets and copies video stream from the IPTV server.
- By enabling IGMP snooping on the Switch to listen to IGMP packets, the Switch only sends an IGMP request packet 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 S7700 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 S7700 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:

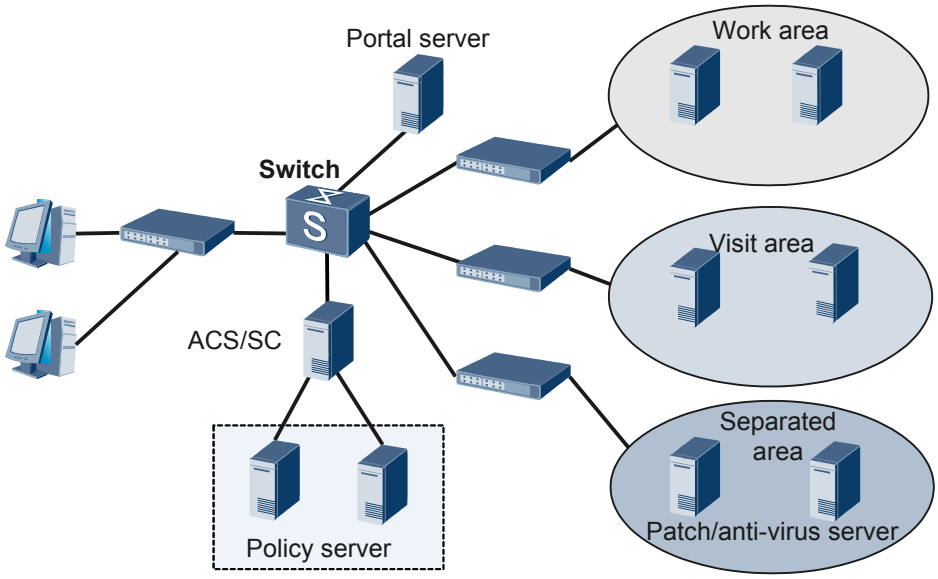
1. BFD for PIM is enabled between the two routers to monitor link status.
2. When faults occur on the link, the Switch, or one of the routers, BFD for PIM detects faults within 50 ms.
3. The router on the right acts as the BDR swiftly switching to DR when a fault occurs. Thus both routers become DRs 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 S7700 implements NAC on a network.

In **Figure 4-14**, Switch represents the S7700.

Figure 4-14 Network diagram of the S7700 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 S7700 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.

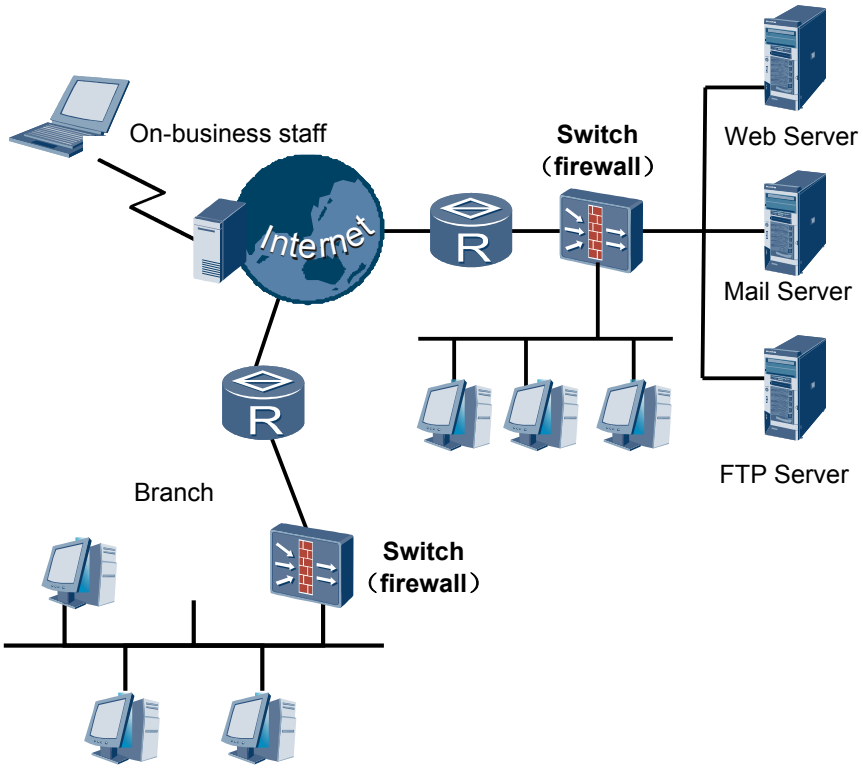
4.11 Firewall

This section describes the firewall networking and policy of the S7700.

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.

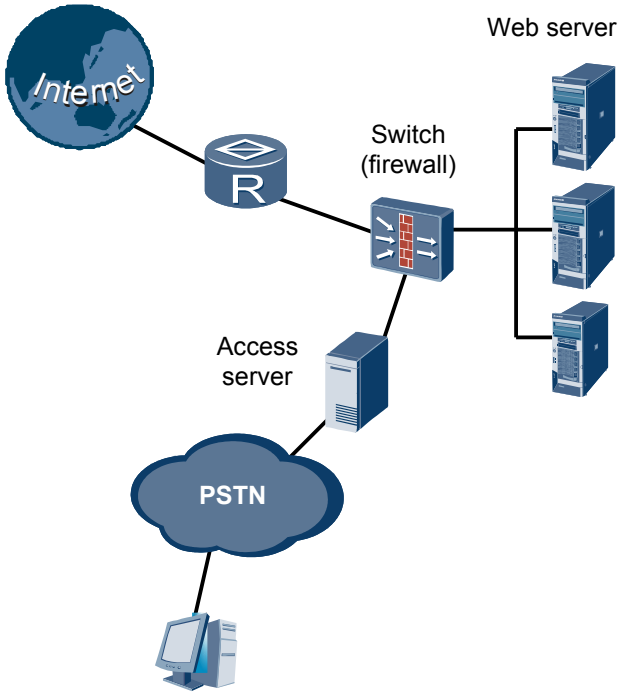
Figure 4-15 Enterprise intranet firewall network diagram



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.

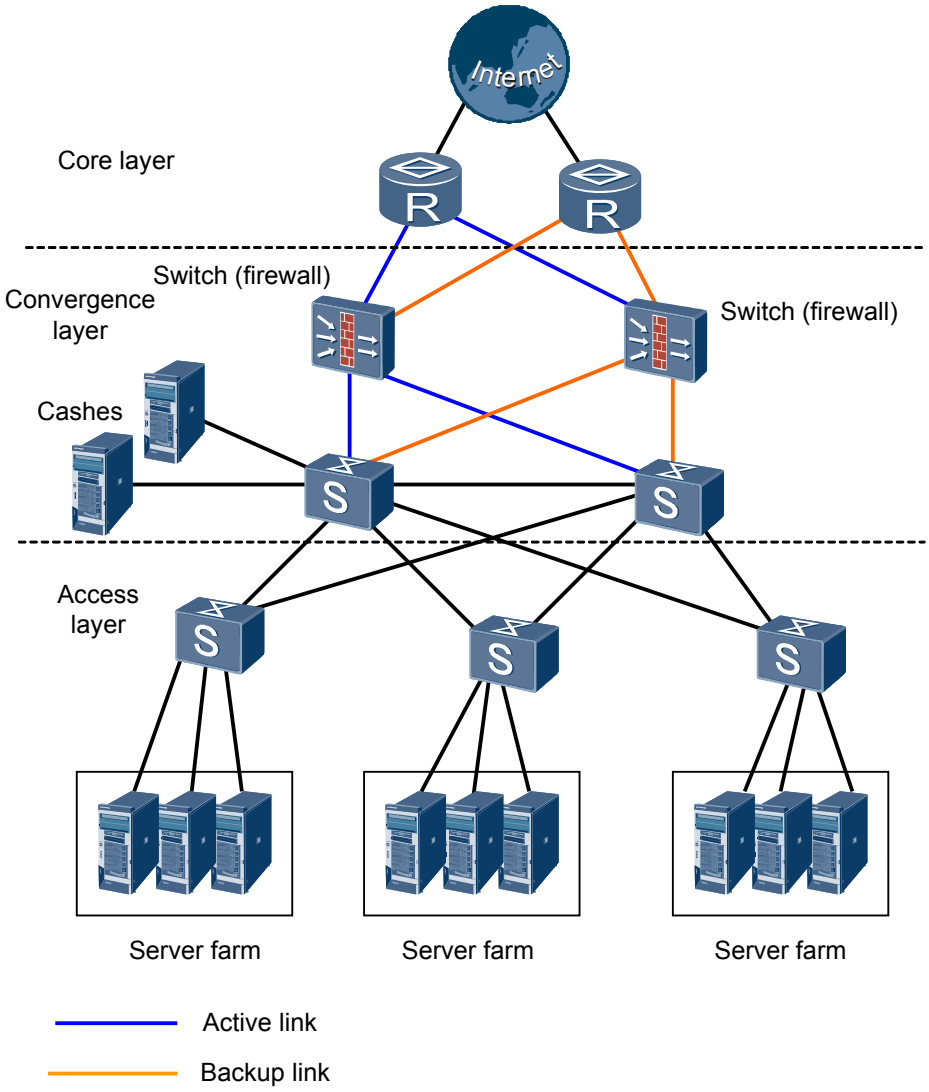
Figure 4-16 Network diagram of an ISP network firewall



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



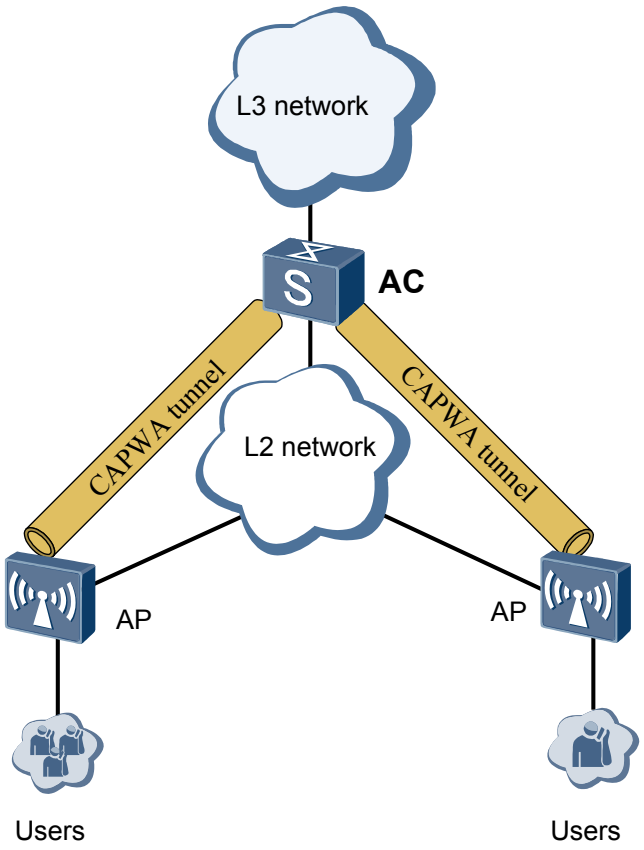
4.12 Application of the WLAN AC

This section describes how the S7700 functions as an AC on a WLAN.

S7700 (AC) Functions as Gateway

S7700 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 S7700 (AC) functioning as the gateway between Layer 2 and Layer 3 networks

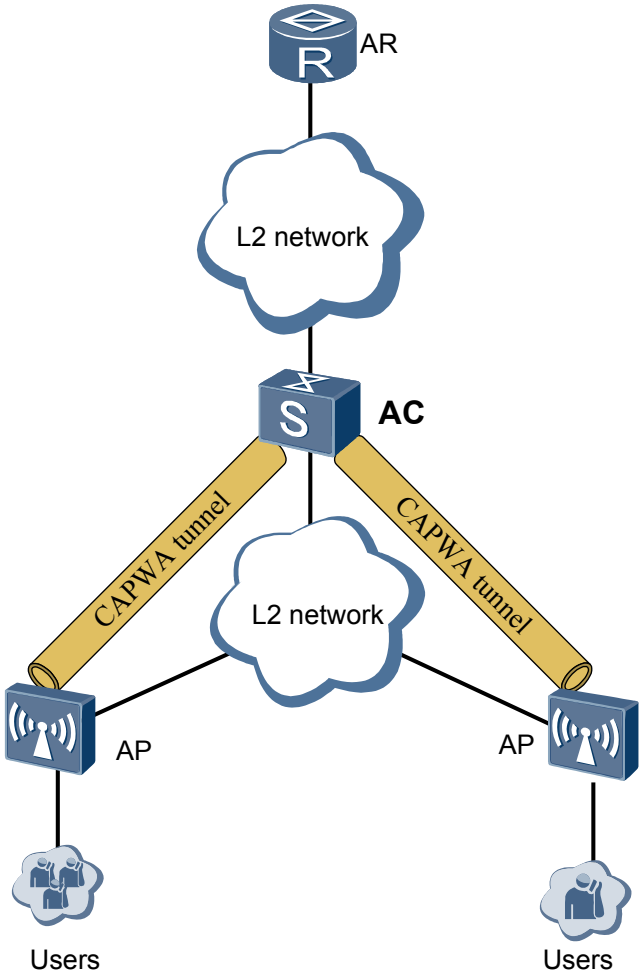


- The AC and APs are connected through a Layer 2 network. The data packets of APs and AC are forwarded over the CAPWA tunnel or forwarded directly.
- The AC functions as a gateway to terminate Layer 2 packets and forward the packets through Layer 3.
- The AC controls the access and configurations of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

S7700 (AC) Functions as a Layer 2 Device

S7700 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 S7700 (AC) functioning as the Layer 2 device

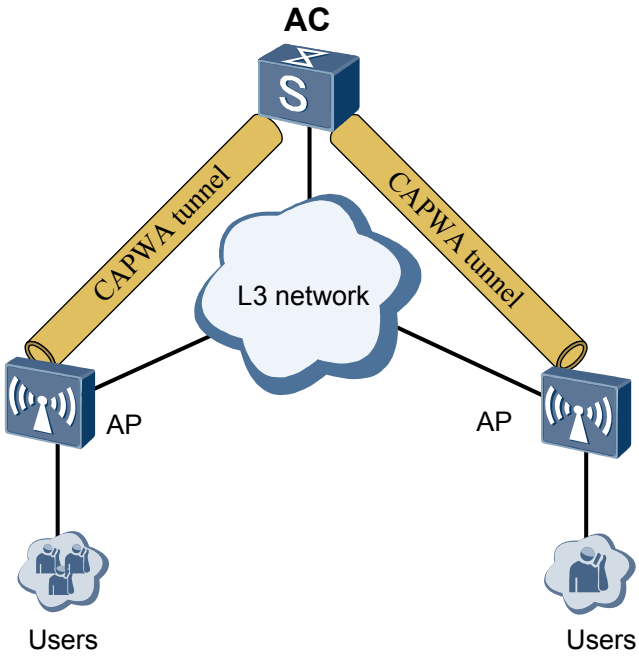


- The AC and APs are connected through a Layer 2 network. The data packets of APs and AC are forwarded over the CAPWA tunnel or forwarded directly.
- The AR functions as a gateway. The AC functions as a Layer 2 device used to terminate tunnel packets and forward user packets through Layer 2.
- The AC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

S7700 (AC) Functions as a Layer 3 Device

The S7700 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 S7700 (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 S7700 system and outlines the features of the S7700 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.

5.2 NMS
The NMS handles resource management, topology management, configuration management, fault management, performance management, and security management for the S7700.

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 S7700 supports the following methods of configuration and management:

- Command line interface (CLI)

  Users can configure and manage the S7700 by connecting to the console port or ETH port.
- NMS

  Users can use SNMP to configure and manage the S7700 through the network management station.
- Web network management

  The Web server is embedded in the S7700. Users can configure the S7700 by logging in through a web browser.

Flexible Login Modes

The S7700 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 S7700 through other service ports.

To satisfy different security demands, the S7700 offers various measures to authenticate user login, including:

- Non-authentication
- Local authentication
- AAA authentication

5.1.2 Management and Monitoring

Hardware Monitoring

The S7700 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 S7700 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 S7700 provides the following tools for testing connectivity and recording packet transmission paths on IP networks:

- Ping
- Trace

The S7700 provides the following tools for testing connectivity and recording packet transmission paths on MPLS networks:

- MPLS ping
- MPLS trace

The S7700 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 S7700 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 S7700 supports system trace to carry out advanced software testing and diagnostics. The S7700 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 S7700 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 S7700 port configured to monitor another port and examining the received packet, ISPs can observe all packets the S7700 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 S7700'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 In-Service Software Upgrade and Patching

In-Service Upgrade

The S7700 supports local and remote system software upgrade.

- Local upgrade

  When the S7700 is booted, the software can be upgraded through the BootROM menu.

- Remote upgrade

  The S7700 supports active and standby main process units. To ensure uninterrupted services when upgrading software on the S7700, it is recommended to first upgrade the standby main process unit before carrying out active/standby switchover. After upgrading the standby main process unit, upgrade the active main process unit.

In-Service Patching

The S7700 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 S7700 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 S7700.

Web Network Management

To facilitate maintenance and use of the S7700, the Web network management is introduced.

Web network management is a Web server embedded in the S7700. Users can log in using PCs to manage and maintain the S7700. By using Web network management, maintenance personnel only need to configure IP addresses and Web-based NMS accounts on the S7700, 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:

- Security Management

  This section describes how to ensure eSight security by managing users, roles, rights, and operation sets.

- Log Management

  Logs record important user operations. With log management, you can view and filter logs, and view detailed system logs. eSight manages operation, security, and system logs. There are three log levels: warning, minor, and risk.

- Resource Management

With resource management, you can add and delete NEs, and manage them by subnet depending on their physical locations.

- Topology Management

  With topology management, managed NEs and their connection status are displayed in the topology view. The managed objects are organized in subviews. You can use the topology view to check the status of the entire network in real time.

- Alarm Management

  Alarm management allows you to monitor the network operating status in real time. You can browse alarms, handle alarms, set alarm rules, and send remote alarm notifications.

- Performance Management

  eSight can monitor the key performance indicators (KPIs) of a network in real time and collect performance statistics. eSight provides graphical user interfaces (GUIs) so that you can manage network performance easily.

- Physical Resource Management

  eSight allows you to query devices, frames, boards, subcards, and ports.

- Report Management

  eSight generates instant and periodic reports, and allows you to export reports to a file in any of the following formats: PDF, Excel, Word, and PowerPoint. eSight provides a variety of report templates, and it also provides a report design tool that allows you to flexibly customize report templates.

- Custom Device Management

  eSight provides user-defined device management to help enterprise users manage devices from different manufacturers. You can customize device types, performance counters, alarm parameters, configuration file parameters, and device panels.

- Configuration File Management

  eSight allows you to back up, restore, and compare device configuration files, and manage baseline file versions. When faults occur on the network, you can compare the configuration file in use with the configuration file that was saved when the network was running normally. By checking the added, modified, and deleted information, you can quickly locate the fault and resolve it.

- Smart Configuration Tool

  The smart configuration tool uses templates and planning tables to configure services for Huawei devices in batches. The template applies when multiple devices have the same configurations and the planning table applies when multiple devices have similar configurations.

- SLA Management

  SLA management measures and diagnoses the network performance, by sending diagnostic messages between devices or links.

- MPLS VPN Management

  eSight BGP/MPLS VPN provides end-to-end (E2E) monitoring for MPLS VPN services. It displays various information for monitoring purposes, including service performance information, service reports, service topology, SLA data, and service alarms. It also offers a rapid diagnosis function for troubleshooting.

- Lower-Layer NMSs

eSight allows you to divide a network into several layers to manage NEs on the network by layer. eSight provides links for lower-layer NMSs. By clicking a link, you can view alarms, performance counters, reports, and the network topology on a lower-layer NMS.

- eSight Home Page

  The eSight home page displays important monitoring information and allows you to specify the type of monitoring information displayed.

- Data Backup and Restoration

  eSight provides an independent Web service to back up or restore the database.

6 Technical Specifications

About This Chapter

This section lists the S7700'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 S7700.

Table 6-1 Physical specifications of the S7700

Item		S7712	S7706	S7703
Dimensions (W x D x H, excluding the rack-mounting ears)		442 mm x 476 mm x 663.95 mm (15 U high)	442 mm x 476 mm x 441.7 mm (10 U high)	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.		3000 W	1600 W	800 W
Noise at normal temperature (acoustic power)		64.6 dB	61.6 dB	58.6 dB
Weight (empty/fully loaded)		25 kg/70 kg	15 kg/42 kg	10 kg/22 kg
DC input	Rated voltage	-48 V DC/-60 V DC		
	Maximum voltage range	-48 V: -38.4 V DC to -57.6 V DC -60 V: -48 V DC to -72 V DC		
AC input	Rated voltage	220 V AC, 50/60 Hz	110/220 V AC, 50/60 Hz	110/220 V AC, 50/60 Hz

Item		S7712	S7706	S7703
	Rated voltage range	200 V AC to 240 V AC, 47 Hz to 63 Hz	100 V AC to 120 V AC and 200 V AC to 240 V AC, 47 Hz to 63 Hz	100 V AC to 120 V AC and 200 V AC to 240 V AC, 47 Hz to 63 Hz
	Maximum voltage range	90 V AC to 290 V AC (The output power is half of the maximum power when the input voltage is in the range of 90 V AC to 175 V AC.)		
PoE	Power input mode	Built-in. Only the AC power supply is supported.	Built-in. Only the AC power supply is supported.	Built-in. Only the AC power supply is supported.
	Redundancy mode of power supplies	The S7712 supports power supplies in 3+1, 2+2, or 4+0 mode.	The S7706 supports power supplies in 3+1, 2+2, or 4+0 mode.	The S7703 does not support backup of AC power modules.
	Output power consumption	8800 W	8800 W	2200 W
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 S7700.

Table 6-2 System configuration of the S7700

Item	S7712	S7706	S7703	Notes
Processor	700MHz (Dominant frequency)	700MHz (Dominant frequency)	500 MHz (Dominant frequency)	-
DDR2 SDRAM	1GB	1GB	512 MB	-
NVRAM	512 KB	512 KB	512 KB	Battery supply
Flash	64MB	64MB	64 MB	-
CF card	512 MB	512 MB	512 MB	The CF card serves as a mass storage device to save data files and logs.
Switching capacity (bit/s)	2T **NOTE** The switching capacity can be expanded to 5.12 Tbit/s in the future.	2T **NOTE** The switching capacity can be expanded to 5.12 Tbit/s in the future.	768G **NOTE** The switching capacity can be expanded to 1.92 Tbit/s in the future.	Bidirectional, sum of switching capacities of the two MPUs
Backplane capacity (bit/s)	12T	6T	3T	-
Forwarding capability (pps)	1344M **NOTE** The forwarding capability can be expanded to 3360 Mpps in the future.	1152M **NOTE** The forwarding capability can be expanded to 2880 Mpps in the future.	576M **NOTE** The forwarding capability can be expanded to 1440 Mpps in the future.	-
Number of LPU slots	12	6	3	LPU (Optional)

Item	S7712	S7706	S7703	Notes
Number of SRU/MCU slots	2	2	2	S7706/S7712: SRU S7703: full mesh
Max transmission rate of an LPU port	48×GE, 40×10GE	48×GE, 40×10GE	48×GE, 40×10GE	-

Calculating Switching Capacity and Interface Capacity

- Calculating the switching capacity
  - Switching capacities of S7706 and S7712

    Switching capacity = Switching capacity of an SRU x Number of SRUs
  - Switching capacity of S7703

    The bidirectional forwarding rate in each slot is 120 Gbit/s.

    Use S7703 as an example. Switching capacity = 128 x 3 x 2 = 768 (Gbit/s). The value 3 indicates the number of slots on S7703 and the value 2 indicates bidirectional forwarding.
- Calculating the interface capacity

  The interface capacity of the S7700 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 S7700.

  For example:

  Each LPU of the supports a maximum of 48 GE interfaces. Take S7712 for example. A switch has 12 slots, which can accommodate twelve 48-port GE interface LPUs. The entire device can provide a maximum of 576 GE interfaces. That is, the interface density is 576. The transmission rate of each GE interface is 1 Gbit/s; therefore, the interface capacity of the S7712 is 576 Gbit/s.

6.3 Performance and Capacity

This section describes the performance specifications of the software and hardware of the S7700.

Table 6-3 Performance specifications of the S7700

Attribute	Service Feature	Specifications
Availability	Availability	> 0.9999959
	Mean Time Between Failure (MTBF)	> 24.1 years

Attribute	Service Feature	Specifications
	Mean Time To Repair (MTTR)	0.5 hours
	Downtime	1.22 minutes/year
Ethernet	Number of MAC addresses supported by each LPU	● ED board: 512 K ● EC/FC board: 128 K ● EA/SA/FA board: 32 K
	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
	MAC address learning rate	More than 3000 per second
	Number of ARP entries	16 K
	Number of ARP entries supported by each LPU	● EA/EC/ED board: 16 K ● SA/FA/FC board: 8 K
QoS	Number of QoS queues on a port	8
	CAR	● ED/EC/EA/FA/FC board: 8 kbit/s ● SA board: 64 kbit/s
ACL	ACLv4	Number of IPv4 ACLs supported by each LPU: ● ED board: 70K for inbound traffic; 1000 for outbound traffic ● EC board: 38K for inbound traffic; 1000 for outbound traffic ● EA board: 6000 for inbound traffic; 1000 for outbound traffic ● SA (24GE) board: 3000 for inbound traffic; 500 for outbound traffic ● SA (X12SA) board: 1200 for inbound traffic; 500 for outbound traffic ● FA (G48SFA/G48TFA/ F48TFA) board: 1200 for inbound traffic; 500 for outbound traffic ● FC (X40SFC) board: 1500 for inbound traffic; 1000 for outbound traffic

Attribute	Service Feature	Specifications
	ACLv6	Number of IPv6 ACLs supported by each LPU: ● ED board: 67K for inbound traffic; 250 for outbound traffic ● EC board: 35K for inbound traffic; 250 for outbound traffic ● EA board: 3000 for inbound traffic; 250 for outbound traffic ● SA (24GE): 1500 for inbound traffic; 250 for outbound traffic ● SA (X12SA): 250 for inbound traffic; 120 for outbound traffic ● FA (G48SFA/G48TFA/ F48TFA): 250 for inbound traffic; 120 for outbound traffic ● FC (X40SFC): 750 for inbound traffic; 500 for outbound traffic
MPLS	Number of LSPs	8 K
	Number of local LDP neighbors	● FA board: 64 ● Others: 512
	Number of remote LDP neighbors	1024
L2VPN	Number of VLL entries	4 K
	Number of VSI entries	1 K
L3VPN	Number of VRFs	2 K
	Number of VPN routes	● S7706/S7712: 512 K ● S7703: 180 K
IP session	-	8 K on each LPU and 16 K on the entire system
IP unicast	IPv4 forwarding	IPv4 forwarding at line speed
	Number of routing entries	● S7706/S7712: 1000K ● S7703: 300K
	IPv4 FIB	● ED board: S7706/S7712: 512K S7703: 220K ● EC board: 128 K ● EA board: 16 K ● SA/FA board: 12K ● FC board: 16K

Attribute	Service Feature	Specifications
	IPv6 FIB	● ED board: S7706/S7712: 256K S7703: 110K ● EC board: 64 K ● EA board: 8 K ● SA/FA board: 6K ● FC board: 8K
Multicast	Number of static multicast routes	256
	Number of L2 multicast forwarding entries	1 K
	Number of L3 multicast forwarding entries	● ED/EC/EA board: 4 K ● SA/FA board: 2 K
Reliability	BFD	● BFD sessions: 2 K ● 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: – S7706/S7712: 4 K – S7703: 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: If no FSU is configured, the delay measurement is within 1 ms; if an FSU is configured, the delay measurement is within 1 us.

Attribute	Service Feature	Specifications
	RRPP	● Maximum number of RRPP instances: 48 ● Rings supported by the entire system: 64 ● Rings supported by each LPU: 5 ● 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: 48 ● Maximum number of Smart Link groups on the entire system: 16 ● The switchover time is less than 50 ms.
	MSTP	● Maximum number of instances on the entire system: 48 ● The switchover time is less than 100 ms.
	SEP	● Maximum number of segments on the entire system: 256 ● The convergence time is less than 50 ms

6.4 List of Software Features

This section describes the software features of the S7700.

Table 6-4 Software features list of the S7700

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.
PoE	-	● Supports IEEE 802.3af/802.3at. ● Each interface provides 30 W of power.
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+2 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.