



S2700 Series Ethernet Switches

Product Description

Issue 21

Date 2018-05-14

Copyright © Huawei Technologies Co., Ltd. 2018. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI 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://e.huawei.com>

About This Document

Intended Audience

This document is intended for network engineers responsible for network design and deployment. You should understand your network well, including the network topology and service requirements.

Privacy Statement

The switch provides the mirroring function for network monitoring and fault management, during which communication data may be collected. Huawei will not collect or save user communication information independently. Huawei recommends that this function be used in accordance with applicable laws and regulations. You should take adequate measures to ensure that users' communications are fully protected when the content is used and saved.

The switch provides the NetStream function for network traffic statistics collection and advertisement, during which data of users may be accessed. You should take adequate measures, in compliance with the laws of the countries concerned and the user privacy policies of your company, to ensure that user data is fully protected.






Disclaimer

This document is designed as a reference for you to configure your devices. Its contents, including web pages, command line input and output, are based on laboratory conditions. It provides instructions for general scenarios, but does not cover all use cases of all product models. The examples given may differ from your use case due to differences in software versions, models, and configuration files. When configuring your device, alter the configuration depending on your use case.

The specifications provided in this document are tested in lab environment (for example, the tested device has been installed with a certain type of boards or only one protocol is run on the device). Results may differ from the listed specifications when you attempt to obtain the maximum values with multiple functions enabled on the device.

Symbol Conventions

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

Symbol	Description
 DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
 CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
 NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
 NOTE	Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Contents

About This Document.....	ii
1 Product Overview.....	1
1.1 Introduction.....	1
1.2 Product Characteristics.....	1
2 Usage Scenarios.....	4
2.1 Enterprise Campus Network.....	4
2.2 Desktop Access.....	5
3 Performance Specifications.....	7
4 Product Performance.....	8
4.1 Product Features Supported by V200R012C00.....	8
4.2 Product Features Supported by V200R011C10.....	14
4.3 Product Features Supported by V200R011C00.....	20
4.4 Product Features Supported by V200R010C00.....	25
4.5 Product Features Supported by V200R009C00.....	31
4.6 Product Features Supported by V200R008C00.....	36
4.7 Product Features Supported by V200R007C00.....	42
4.8 Product Features Supported by V200R006C00.....	48
4.9 Product Features Supported by V200R005C00.....	53
4.10 Product Features Supported by V200R003C00.....	59
4.11 Product Features Supported by V100R006C05.....	65
5 Hardware Information.....	68
6 References.....	70

1 Product Overview

About This Chapter

[1.1 Introduction](#)

[1.2 Product Characteristics](#)

1.1 Introduction

The S2700 series Ethernet switches (S2700 for short) are next-generation energy-saving 100M Ethernet intelligent switches.

The S2700 utilizes cutting-edge switching technologies and Huawei Versatile Routing Platform (VRP) software to meet the demand for multi-service provisioning and access on Ethernet networks. It is easy to install and maintain and supports flexible VLAN deployment, comprehensive security and QoS policies, and energy-saving technologies. These features help enterprise customers build next-generation IT networks.

1.2 Product Characteristics

Easy Operations and Maintenance

The S2700 supports Easy-Operation, which simplifies installation, configuration, monitoring, and troubleshooting. This technology greatly reduces installation, configuration, and engineering costs, and improves the upgrade efficiency. The S2700 provides the command line interface (CLI) and web platform, supports alarm management and visualized configuration, and automatic command synchronization to a replacement switch.

The S2700 uses the ASIC chip and fanless design, which reduces mechanical faults and protects the equipment against damages caused by condensed water and dusts.

Flexible Service Control

The S2700 supports various ACLs. ACL rules can be applied to VLANs to flexibly control traffic on interfaces and schedule resources in VLANs.

The S2700 supports VLAN assignment based on interfaces, MAC addresses, protocols, and IP subnets. The flexibility in VLAN assignment facilitates network deployment and security guarantee, and is especially suitable for networks where users move frequently.

The S2700 supports GVRP, which dynamically distributes, registers, and propagates VLAN attributes to reduce the manual configuration workload of network administrators and ensure correct VLAN configuration. In addition, the S2700 supports SSHv2, HWTACACS, RMON, interface-based traffic statistics collection, and NQA to help in network planning and upgrade.

Comprehensive Security Measures

The S2700 supports DHCP snooping and generates user binding entries based on MAC addresses, IP addresses, IP address leases, VLAN IDs, and interface numbers of users. The DHCP snooping function protects networks against common attacks, such as bogus IP packet attacks, man-in-the-middle attacks, and bogus DHCP server attacks.

The S2700 can limit the number of MAC addresses learned on an interface to prevent packet flooding that occurs when an attacker frequently changes source MAC addresses. The switch supports strict ARP learning that prevents ARP spoofing from exhausting ARP entries to ensure normal Internet access. It also supports IP source check to prevent DoS attacks caused by IP address spoofing.

The S2700 supports centralized MAC address authentication and 802.1X authentication. It authenticates users based on static or dynamic bindings of user information such as the user name, IP address, MAC address, VLAN ID, and interface number. VLANs and ACLs can be applied to users dynamically.

Extensive Reliability Mechanisms

The S2700 supports intelligent stack (iStack), which virtualizes multiple switches into one logical switch. iStack improves the switching capacity and enhances reliability and scalability. The stacked switches are managed using a single IP address, which greatly reduces system operations and maintenance costs.

In addition to STP, RSTP, and MSTP, the S2700 also supports enhanced Ethernet reliability technologies such as Smart Link and RRPP, which implement millisecond-level protection switching to ensure network reliability.

The S2700 supports the Smart Ethernet Protection (SEP) protocol, a ring network protocol applied to the link layer of an Ethernet network. SEP provides fast switching within milliseconds without interrupting services, as well as simplicity, high reliability, convenient maintenance, and flexible topology, enabling users to manage and plan networks conveniently.

The S2700 supports G.8032, also called Ethernet Ring Protection Switch (ERPS). ERPS is based on traditional Ethernet MAC and bridging functions and uses the mature Ethernet OAM and Ring Automatic Protection Switching (Ring APS or R-APS) technologies to implement fast protection switching on Ethernet networks. ERPS supports multiple services and provides flexible networking, reducing the OPEX and CAPEX.

Comprehensive QoS Policies

The S2700 supports complex traffic classification based on VLAN IDs, MAC addresses, IP protocols, source addresses, destination addresses, priorities, or TCP/UDP port numbers of packets. By limiting the traffic rate on a per flow basis, the S2700 provides line-rate

forwarding on each interface to ensure high quality of the voice, video, and data services. Each interface supports eight queues and multiple queue scheduling algorithms, such as WRR, SP, and WRR+SP.

Powerful Surge Protection Capability

The S2700 adopts a patented surge protection technology to prevent lightning induced overvoltage. All interfaces of the S2700 have a surge protection capability of 6 kV. The patented surge protection technology greatly reduces the possibility of lightning damages on the equipment even in atrocious environments or in scenarios where grounding cannot be implemented.

Energy-Saving Design

The S2700 uses an energy-saving integrated circuit design to ensure efficient heat dissipation. Idle ports can enter the sleeping mode to reduce power consumption. The S2700 generates no noises because it does not have any fans. Radiation of the S2700 is within the range of radiation standards for electric appliances and has no harm to the human body.

Related Content

Support Community

- [Introduction to Huawei Fixed Switches](#)

2 Usage Scenarios

About This Chapter

[2.1 Enterprise Campus Network](#)

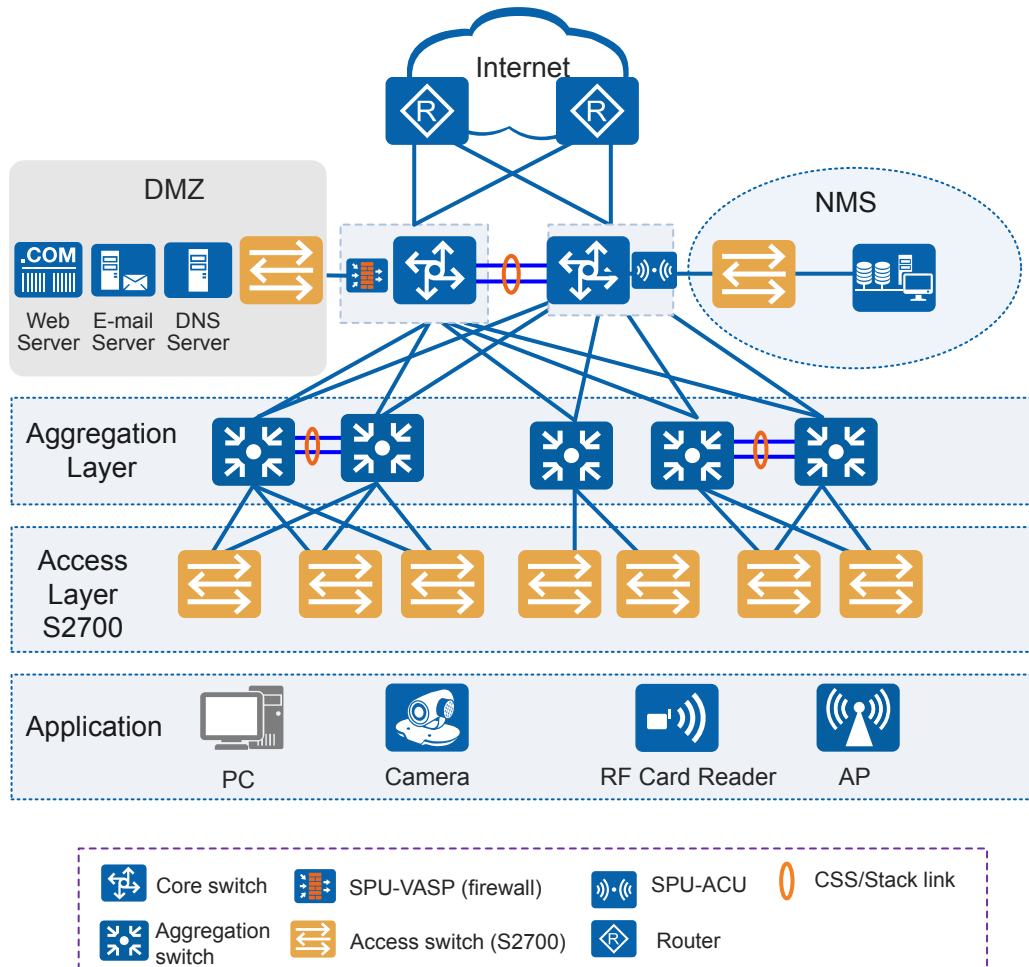
[2.2 Desktop Access](#)

2.1 Enterprise Campus Network

The S2700 switches can be deployed at the access layer of a campus network to build a high-performance, multi-service, and highly reliable enterprise network.

On the enterprise or campus network shown in the following figure, the S2700 switches connect to terminals using 100M electrical interfaces, and to aggregation switches using GE optical or electrical interfaces. The aggregation switches connect to the backbone network using bundled GE interfaces or 10G interfaces. The network provides a 10G backbone layer and 100M-to-the-desktop capability, meeting requirements for high bandwidth and multi-service operation.

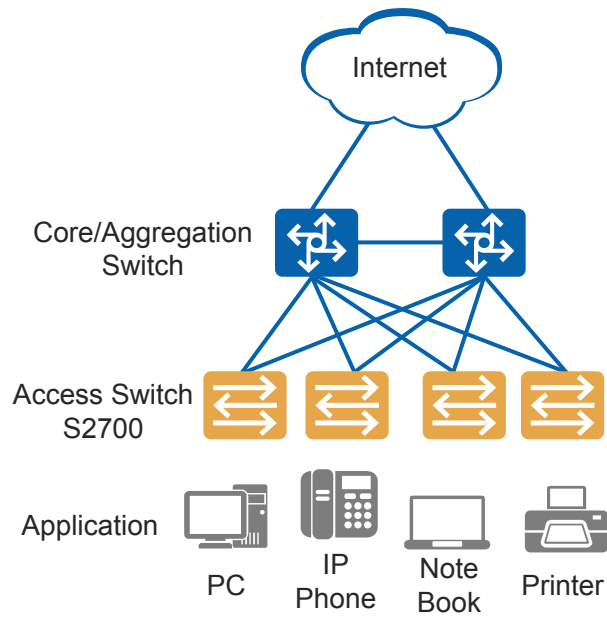
Figure 2-1 S2700 in an enterprise campus network



2.2 Desktop Access

As shown in the figure, the S2700 switches provide voice VLAN and NAC functions. With a small size, these switches can be used for desktop access.

Figure 2-2 Desktop access



3 Performance Specifications

The features mentioned in the "Introduction", "Product Characteristics", and "Usage Scenarios" sections are not supported on all S2700 models. For the feature support of specific product models, download their brochures or feature lists from [Huawei official website](#). (If your account is unauthorized, contact Huawei's support team).

4 Product Performance

About This Chapter

- [4.1 Product Features Supported by V200R012C00](#)
- [4.2 Product Features Supported by V200R011C10](#)
- [4.3 Product Features Supported by V200R011C00](#)
- [4.4 Product Features Supported by V200R010C00](#)
- [4.5 Product Features Supported by V200R009C00](#)
- [4.6 Product Features Supported by V200R008C00](#)
- [4.7 Product Features Supported by V200R007C00](#)
- [4.8 Product Features Supported by V200R006C00](#)
- [4.9 Product Features Supported by V200R005C00](#)
- [4.10 Product Features Supported by V200R003C00](#)
- [4.11 Product Features Supported by V100R006C05](#)

4.1 Product Features Supported by V200R012C00

Table 4-1 lists the features supported by the S2720 and S2750.

Table 4-1 Features supported by the S2720 and S2750

Feature		Description
Ethernet features	Ethernet	Full-duplex, half-duplex, and auto-negotiation modes on Ethernet interfaces
		Ethernet interface rates: 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, and auto-negotiation
		Flow control on interfaces

Feature		Description
		Jumbo frames
		Link aggregation
		Load balancing among links of a trunk
		Transparent transmission of Layer 2 protocol packets
		Device Link Detection Protocol (DLDP)
		Link Layer Discovery Protocol (LLDP)
		Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)
		Interface isolation and forwarding restriction
		Broadcast storm suppression
	VLAN	Access modes of LNP (link type negotiation protocol), access, trunk, hybrid, and QinQ
		Default VLAN
		VLAN assignment based on interfaces, MAC addresses, protocols, and IP subnets
		VLAN assignment based on the following policies: <ul style="list-style-type: none"> ● MAC address + IP address ● MAC address + IP address + interface number
		Adding double VLAN tags to packets based on interface
		VLAN mapping
		Selective QinQ
		MUX VLAN
		Voice VLAN
		Guest VLAN
GVRP	Generic Attribute Registration Protocol (GARP)	
	GARP VLAN Registration Protocol (GVRP)	
VCMP	VCMP (VLAN centralized management protocol)	
MAC	Automatic learning and aging of MAC addresses	
	Static, dynamic, and blackhole MAC address entries	
	Packet filtering based on source MAC addresses	
	Interface-based MAC learning limiting	
	Sticky MAC address entries	

Feature		Description
		MAC address flapping detection
		MAC address spoofing defense
		Port bridge
	ARP	Static and dynamic ARP entries
		ARP in a VLAN
		Aging of ARP entries
Ethernet loop protection	MSTP	STP
		RSTP
		MSTP
		VBST
		BPDU protection, root protection, and loop protection
		TC-BPDU attack defense
	Loopback-detect	Loop detection on an interface
	SEP	Smart Ethernet Protection (SEP)
	Smart Link	Smart Link
		Smart Link multi-instance
		Monitor Link
	RRPP	RRPP protective switchover
		Single RRPP ring, tangent RRPP ring, and intersecting RRPP ring
		Hybrid networking of RRPP rings and other ring networks
	ERPS	G.8032 v1/v2
Single closed ring		
Subring		
IPv4/IPv6 forwarding	IPv4 and unicast routes	Static IPv4 routes
		DHCP client
		DHCP server
		DHCP relay
	IPv6 features	IPv6 protocol stack
		ND and ND snooping

Feature		Description
		DHCPv6 snooping
Layer 2 multicast features	-	IGMPv1/v2/v3 snooping
		Fast leave
		IGMP snooping proxy
		MLD snooping
		Interface-based multicast traffic suppression
		Inter-VLAN multicast replication
		Controllable multicast
Stacking	-	Service interface supporting the stacking function
Ethernet OAM	EFM OAM (802.3ah)	Automatic discovery
		Link fault detection
		Link fault troubleshooting
		Remote loopback
	CFM OAM (802.1ag)	Software-level CCM
		MAC ping
		MAC trace
Y.1731	Delay and variation measurement	
QoS features	Traffic classifier	Traffic classification based on ACLs
		Traffic classification based on outer 802.1p priorities, outer VLAN IDs, source MAC addresses, and Ethernet types
	Traffic behavior	Access control after traffic classification
		Traffic policing based on traffic classification
		Re-marking based on traffic classification
		Associating traffic classifiers with traffic behaviors
	Traffic policing	Rate limiting on inbound and outbound interfaces
	Traffic shaping	Traffic shaping on interfaces and queues
	Congestion avoidance	Tail drop
	Congestion management	Priority Queuing (PQ)
Weighted Deficit Round Robin (WDRR)		

Feature		Description
		PQ+WDRR
		Weighted Round Robin (WRR)
		PQ+WRR
Configuration and maintenance	Login and configuration management	Command line configuration
		Error message and help information in English
		Login through console and Telnet terminals
		SSH1.5/SSH2
		Send function and data communication between terminal users
		Hierarchical user authority management and commands
		SNMP-based NMS management (eSight)
		Web page-based configuration and management
		EasyDeploy (client)
		Open Programmability System (OPS)
	NOTE Only the S2720EI supports this function.	
	File system	File system
		Directory and file management
		File upload and download through FTP, TFTP, SFTP, SCP, and FTPS
	Monitoring and maintenance	Hardware monitoring
		Reporting alarms on abnormal device temperature
		Second-time fault detection to prevent detection errors caused by instant interference
		Version matching check
		Information center and unified management over logs, alarms, and debugging information
		Electronic labels, and command line query and backup
		Virtual cable test (VCT)
		User operation logs
		Detailed debugging information for network fault diagnosis
		Network test tools such as traceroute and ping commands
	Port mirroring, flow mirroring, and remote mirroring	

Feature		Description
		Energy saving
	Version upgrade	Device software loading and online software loading
		BootROM online upgrade
		In-service patching
Security	AAA	Local authentication and authorization
		RADIUS authentication, authorization, and accounting
		HWTACACS authentication, authorization, and accounting
	NAC	802.1X authentication
		MAC address authentication
		Portal authentication
		Hybrid authentication
	ARP security	Dynamic ARP Inspection (DAI) and Static ARP Inspection (SAI)
		Egress ARP Inspection (EAI)
		ARP packet rate limiting based on source IP addresses, interfaces, and VLANs, and global ARP packet rate limiting
	IP security	ICMP attack defense
		IP source guard
	Local attack defense	CPU attack defense
	MFF	MAC-Forced Forwarding (MFF)
	DHCP snooping	DHCP snooping
		Option 82 function and dynamic rate limiting for DHCP packets
	Attack defense	Defense against flood attacks without IP payloads, attacks from IGMP null payload packets, LAND attacks, Smurf attacks, and attacks from packets with invalid TCP flag bits
		Defense against attacks from many fragments, attacks from many packets with offsets, attacks from repeated packet fragments, Tear Drop attacks, Syndrop attacks, NewTear attacks, Bonk attacks, Nesta attacks, Rose attacks, Fawx attacks, Ping of Death attacks, and Jolt attacks
Defense against TCP SYN flood attacks, UDP flood attacks (including Fraggle attacks and UDP diagnosis port attacks), and ICMP flood attacks		

Feature		Description
Network management	-	Ping and traceroute
		NQA
		Network Time Protocol (NTP)
		sFlow
		HTTP
		Hypertext Transfer Protocol Secure (HTTPS)
		SNMP v1/v2c/v3
		Standard MIB
		Remote network monitoring (RMON)

4.2 Product Features Supported by V200R011C10

Table 4-2 lists the features supported by the S2720 and S2750.

Table 4-2 Features supported by the S2720 and S2750

Feature		Description
Ethernet features	Ethernet	Full-duplex, half-duplex, and auto-negotiation modes on Ethernet interfaces
		Ethernet interface rates: 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, and auto-negotiation
		Flow control on interfaces
		Jumbo frames
		Link aggregation
		Load balancing among links of a trunk
		Transparent transmission of Layer 2 protocol packets
		Device Link Detection Protocol (DLDP)
		Link Layer Discovery Protocol (LLDP)
		Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)
		Interface isolation and forwarding restriction
		Broadcast storm suppression

Feature		Description
	VLAN	Access modes of LNP (link type negotiation protocol), access, trunk, hybrid, and QinQ
		Default VLAN
		VLAN assignment based on interfaces, MAC addresses, protocols, and IP subnets
		VLAN assignment based on the following policies: <ul style="list-style-type: none"> ● MAC address + IP address ● MAC address + IP address + interface number
		Adding double VLAN tags to packets based on interface
		VLAN mapping
		Selective QinQ
		MUX VLAN
		Voice VLAN
		Guest VLAN
	GVRP	Generic Attribute Registration Protocol (GARP)
		GARP VLAN Registration Protocol (GVRP)
	VCMP	VCMP (VLAN centralized management protocol)
	MAC	Automatic learning and aging of MAC addresses
		Static, dynamic, and blackhole MAC address entries
		Packet filtering based on source MAC addresses
		Interface-based MAC learning limiting
		Sticky MAC address entries
		MAC address flapping detection
MAC address spoofing defense		
Port bridge		
ARP	Static and dynamic ARP entries	
	ARP in a VLAN	
	Aging of ARP entries	
Ethernet loop protection	MSTP	STP
		RSTP
		MSTP

Feature		Description
		VBST
		BPDU protection, root protection, and loop protection
		TC-BPDU attack defense
		STP loop detection
	Loopback-detect	Loop detection on an interface
	SEP	Smart Ethernet Protection (SEP)
	Smart Link	Smart Link
		Smart Link multi-instance
		Monitor Link
	RRPP	RRPP protective switchover
		Single RRPP ring, tangent RRPP ring, and intersecting RRPP ring
		Hybrid networking of RRPP rings and other ring networks
	ERPS	G.8032 v1/v2
		Single closed ring
		Subring
IPv4/ IPv6 forwarding	IPv4 and unicast routes	Static IPv4 routes
		DHCP client
		DHCP server
		DHCP relay
	IPv6 features	IPv6 protocol stack
		ND and ND snooping
DHCPv6 snooping		
Layer 2 multicast features	-	IGMPv1/v2/v3 snooping
		Fast leave
		IGMP snooping proxy
		MLD snooping
		Interface-based multicast traffic suppression
		Inter-VLAN multicast replication
		Controllable multicast

Feature		Description
Stacking	-	Service interface supporting the stacking function
Ethernet OAM	EFM OAM (802.3ah)	Automatic discovery
		Link fault detection
		Link fault troubleshooting
		Remote loopback
	CFM OAM (802.1ag)	Software-level CCM
		MAC ping
		MAC trace
Y.1731	Delay and variation measurement	
QoS features	Traffic classifier	Traffic classification based on ACLs
		Traffic classification based on outer 802.1p priorities, outer VLAN IDs, source MAC addresses, and Ethernet types
	Traffic behavior	Access control after traffic classification
		Traffic policing based on traffic classification
		Re-marking based on traffic classification
		Associating traffic classifiers with traffic behaviors
	Traffic policing	Rate limiting on inbound and outbound interfaces
	Traffic shaping	Traffic shaping on interfaces and queues
	Congestion avoidance	Tail drop
	Congestion management	Priority Queuing (PQ)
		Weighted Deficit Round Robin (WDRR)
		PQ+WDRR
		Weighted Round Robin (WRR)
PQ+WRR		
Configuration and maintenance	Login and configuration management	Command line configuration
		Error message and help information in English
		Login through console and Telnet terminals
		SSH1.5/SSH2
		Send function and data communication between terminal users

Feature		Description
		Hierarchical user authority management and commands
		SNMP-based NMS management (eSight)
		Web page-based configuration and management
		EasyDeploy (client)
	File system	File system
		Directory and file management
		File upload and download through FTP, TFTP, SFTP, SCP, and FTPS
	Monitoring and maintenance	Hardware monitoring
		Reporting alarms on abnormal device temperature
		Second-time fault detection to prevent detection errors caused by instant interference
		Version matching check
		Information center and unified management over logs, alarms, and debugging information
		Electronic labels, and command line query and backup
		Virtual cable test (VCT)
		User operation logs
		Detailed debugging information for network fault diagnosis
		Network test tools such as traceroute and ping commands
		Port mirroring, flow mirroring, and remote mirroring
		Energy saving
	Version upgrade	Device software loading and online software loading
BootROM online upgrade		
In-service patching		
Security	AAA	Local authentication and authorization
		RADIUS authentication, authorization, and accounting
		HWTACACS authentication, authorization, and accounting
	NAC	802.1X authentication
		MAC address authentication
		Portal authentication

Feature		Description
		Hybrid authentication
	ARP security	Dynamic ARP Inspection (DAI) and Static ARP Inspection (SAI)
		Egress ARP Inspection (EAI)
		ARP packet rate limiting based on source IP addresses, interfaces, and VLANs, and global ARP packet rate limiting
	IP security	ICMP attack defense
		IP source guard
	Local attack defense	CPU attack defense
	MFF	MAC-Forced Forwarding (MFF)
	DHCP snooping	DHCP snooping
		Option 82 function and dynamic rate limiting for DHCP packets
	Attack defense	Defense against flood attacks without IP payloads, attacks from IGMP null payload packets, LAND attacks, Smurf attacks, and attacks from packets with invalid TCP flag bits
		Defense against attacks from many fragments, attacks from many packets with offsets, attacks from repeated packet fragments, Tear Drop attacks, Syndrop attacks, NewTear attacks, Bonk attacks, Nesta attacks, Rose attacks, Fawx attacks, Ping of Death attacks, and Jolt attacks
		Defense against TCP SYN flood attacks, UDP flood attacks (including Fraggle attacks and UDP diagnosis port attacks), and ICMP flood attacks
Network management	-	Ping and traceroute
		NQA
		Network Time Protocol (NTP)
		sFlow
		HTTP
		Hypertext Transfer Protocol Secure (HTTPS)
		SNMP v1/v2c/v3
		Standard MIB
		Remote network monitoring (RMON)

4.3 Product Features Supported by V200R011C00

Table 4-3 lists the features supported by the S2750.

Table 4-3 Features supported by the S2750

Feature		Description
Ethernet features	Ethernet	Full-duplex, half-duplex, and auto-negotiation modes on Ethernet interfaces
		Ethernet interface rates: 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, and auto-negotiation
		Flow control on interfaces
		Jumbo frames
		Link aggregation
		Load balancing among links of a trunk
		Transparent transmission of Layer 2 protocol packets
		Device Link Detection Protocol (DLDP)
		Link Layer Discovery Protocol (LLDP)
		Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)
		Interface isolation and forwarding restriction
		Broadcast storm suppression
	VLAN	Access modes of LNP (link type negotiation protocol), access, trunk, hybrid, and QinQ
		Default VLAN
		VLAN assignment based on interfaces, MAC addresses, protocols, and IP subnets
		VLAN assignment based on the following policies: <ul style="list-style-type: none"> ● MAC address + IP address ● MAC address + IP address + interface number
		Adding double VLAN tags to packets based on interface
		VLAN mapping
		Selective QinQ
MUX VLAN		
Voice VLAN		

Feature		Description
		Guest VLAN
	GVRP	Generic Attribute Registration Protocol (GARP)
		GARP VLAN Registration Protocol (GVRP)
	VCMP	VCMP (VLAN centralized management protocol)
	MAC	Automatic learning and aging of MAC addresses
		Static, dynamic, and blackhole MAC address entries
		Packet filtering based on source MAC addresses
		Interface-based MAC learning limiting
		Sticky MAC address entries
		MAC address flapping detection
		MAC address spoofing defense
		Port bridge
	ARP	Static and dynamic ARP entries
		ARP in a VLAN
		Aging of ARP entries
Ethernet loop protection	MSTP	STP
		RSTP
		MSTP
		VBST
		BPDU protection, root protection, and loop protection
		TC-BPDU attack defense
		STP loop detection
	Loopback-detect	Loop detection on an interface
	SEP	Smart Ethernet Protection (SEP)
	Smart Link	Smart Link
		Smart Link multi-instance
		Monitor Link
	RRPP	RRPP protective switchover
		Single RRPP ring, tangent RRPP ring, and intersecting RRPP ring

Feature		Description
	ERPS	Hybrid networking of RRPP rings and other ring networks
		G.8032 v1/v2
		Single closed ring
		Subring
IPv4/ IPv6 forwarding	IPv4 and unicast routes	Static IPv4 routes
		DHCP client
		DHCP server
		DHCP relay
	IPv6 features	IPv6 protocol stack
		ND and ND snooping
		DHCPv6 snooping
Layer 2 multicast features	-	IGMPv1/v2/v3 snooping
		Fast leave
		IGMP snooping proxy
		MLD snooping
		Interface-based multicast traffic suppression
		Inter-VLAN multicast replication
		Controllable multicast
Stacking	-	Service interface supporting the stacking function
Ethernet OAM	EFM OAM (802.3ah)	Automatic discovery
		Link fault detection
		Link fault troubleshooting
		Remote loopback
	CFM OAM (802.1ag)	Software-level CCM
		MAC ping
		MAC trace
Y.1731	Delay and variation measurement	
QoS features	Traffic classifier	Traffic classification based on ACLs
		Traffic classification based on outer 802.1p priorities, outer VLAN IDs, source MAC addresses, and Ethernet types

Feature		Description
	Traffic behavior	Access control after traffic classification
		Traffic policing based on traffic classification
		Re-marking based on traffic classification
		Associating traffic classifiers with traffic behaviors
	Traffic policing	Rate limiting on inbound and outbound interfaces
	Traffic shaping	Traffic shaping on interfaces and queues
	Congestion avoidance	Tail drop
	Congestion management	Priority Queuing (PQ)
		Weighted Deficit Round Robin (WDRR)
		PQ+WDRR
Weighted Round Robin (WRR)		
Configuration and maintenance	Login and configuration management	Command line configuration
		Error message and help information in English
		Login through console and Telnet terminals
		SSH1.5/SSH2
		Send function and data communication between terminal users
		Hierarchical user authority management and commands
		SNMP-based NMS management (eSight)
		Web page-based configuration and management
		EasyDeploy (client)
	File system	File system
		Directory and file management
		File upload and download through FTP, TFTP, SFTP, SCP, and FTPS
	Monitoring and maintenance	Hardware monitoring
		Reporting alarms on abnormal device temperature
		Second-time fault detection to prevent detection errors caused by instant interference

Feature		Description
		Version matching check
		Information center and unified management over logs, alarms, and debugging information
		Electronic labels, and command line query and backup
		Virtual cable test (VCT)
		User operation logs
		Detailed debugging information for network fault diagnosis
		Network test tools such as traceroute and ping commands
		Port mirroring, flow mirroring, and remote mirroring
		Energy saving
		Version upgrade
BootROM online upgrade		
In-service patching		
Security	AAA	Local authentication and authorization
		RADIUS authentication, authorization, and accounting
		HWTACACS authentication, authorization, and accounting
	NAC	802.1X authentication
		MAC address authentication
		Portal authentication
		Hybrid authentication
	ARP security	Dynamic ARP Inspection (DAI) and Static ARP Inspection (SAI)
		Egress ARP Inspection (EAI)
		ARP packet rate limiting based on source IP addresses, interfaces, and VLANs, and global ARP packet rate limiting
	IP security	ICMP attack defense
		IP source guard
	Local attack defense	CPU attack defense
MFF	MAC-Forced Forwarding (MFF)	
DHCP snooping	DHCP snooping	

Feature		Description
		Option 82 function and dynamic rate limiting for DHCP packets
	Attack defense	Defense against flood attacks without IP payloads, attacks from IGMP null payload packets, LAND attacks, Smurf attacks, and attacks from packets with invalid TCP flag bits
		Defense against attacks from many fragments, attacks from many packets with offsets, attacks from repeated packet fragments, Tear Drop attacks, Syndrop attacks, NewTear attacks, Bonk attacks, Nesta attacks, Rose attacks, Fawx attacks, Ping of Death attacks, and Jolt attacks
		Defense against TCP SYN flood attacks, UDP flood attacks (including Fraggle attacks and UDP diagnosis port attacks), and ICMP flood attacks
Network management	-	Ping and traceroute
		NQA
		Network Time Protocol (NTP)
		sFlow
		HTTP
		Hypertext Transfer Protocol Secure (HTTPS)
		SNMP v1/v2c/v3
		Standard MIB
		Remote network monitoring (RMON)

4.4 Product Features Supported by V200R010C00

Table 4-4 lists the features supported by the S2720 and S2750.

Table 4-4 Features supported by the S2720 and S2750

Feature		Description
Ethernet features	Ethernet	Full-duplex, half-duplex, and auto-negotiation modes on Ethernet interfaces
		Ethernet interface rates: 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, and auto-negotiation
		Flow control on interfaces
		Jumbo frames

Feature		Description
		Link aggregation
		Load balancing among links of a trunk
		Transparent transmission of Layer 2 protocol packets
		Device Link Detection Protocol (DLDP)
		Link Layer Discovery Protocol (LLDP)
		Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)
		Interface isolation and forwarding restriction
		Broadcast storm suppression
	VLAN	Access modes of LNP (link type negotiation protocol), access, trunk, hybrid, and QinQ
		Default VLAN
		VLAN assignment based on interfaces, MAC addresses, protocols, and IP subnets
		VLAN assignment based on the following policies: <ul style="list-style-type: none"> ● MAC address + IP address ● MAC address + IP address + interface number
		Adding double VLAN tags to packets based on interface
		VLAN mapping
		Selective QinQ
		MUX VLAN
		Voice VLAN
		Guest VLAN
		GVRP
	GARP VLAN Registration Protocol (GVRP)	
	VCMP	VCMP (VLAN centralized management protocol)
	MAC	Automatic learning and aging of MAC addresses
		Static, dynamic, and blackhole MAC address entries
		Packet filtering based on source MAC addresses
		Interface-based MAC learning limiting
		Sticky MAC address entries
		MAC address flapping detection

Feature		Description
		MAC address spoofing defense
		Port bridge
	ARP	Static and dynamic ARP entries
		ARP in a VLAN
		Aging of ARP entries
Ethernet loop protection	MSTP	STP
		RSTP
		MSTP
		VBST
		BPDU protection, root protection, and loop protection
		TC-BPDU attack defense
		STP loop detection
	Loopback-detect	Loop detection on an interface
	SEP	Smart Ethernet Protection (SEP)
	Smart Link	Smart Link
		Smart Link multi-instance
		Monitor Link
	RRPP	RRPP protective switchover
		Single RRPP ring, tangent RRPP ring, and intersecting RRPP ring
		Hybrid networking of RRPP rings and other ring networks
ERPS	G.8032 v1/v2	
	Single closed ring	
	Subring	
IPv4/IPv6 forwarding	IPv4 and unicast routes	Static IPv4 routes
		DHCP client
		DHCP server
		DHCP relay
	IPv6 features	IPv6 protocol stack
		ND and ND snooping

Feature		Description
		DHCPv6 snooping
Layer 2 multicast features	-	IGMPv1/v2/v3 snooping
		Fast leave
		IGMP snooping proxy
		MLD snooping
		Interface-based multicast traffic suppression
		Inter-VLAN multicast replication
		Controllable multicast
Stacking	-	Service interface supporting the stacking function
Ethernet OAM	EFM OAM (802.3ah)	Automatic discovery
		Link fault detection
		Link fault troubleshooting
		Remote loopback
	CFM OAM (802.1ag)	Software-level CCM
		MAC ping
		MAC trace
Y.1731	Delay and variation measurement	
QoS features	Traffic classifier	Traffic classification based on ACLs
		Traffic classification based on outer 802.1p priorities, outer VLAN IDs, source MAC addresses, and Ethernet types
	Traffic behavior	Access control after traffic classification
		Traffic policing based on traffic classification
		Re-marking based on traffic classification
		Associating traffic classifiers with traffic behaviors
	Traffic policing	Rate limiting on inbound and outbound interfaces
	Traffic shaping	Traffic shaping on interfaces and queues
	Congestion avoidance	Tail drop
	Congestion management	Priority Queuing (PQ)
Weighted Deficit Round Robin (WDRR)		

Feature		Description
		PQ+WDRR
		Weighted Round Robin (WRR)
		PQ+WRR
Configur ation and mainten ance	Login and configuration management	Command line configuration
		Error message and help information in English
		Login through console and Telnet terminals
		SSH1.5/SSH2
		Send function and data communication between terminal users
		Hierarchical user authority management and commands
		SNMP-based NMS management (eSight)
		Web page-based configuration and management
		EasyDeploy (client)
	File system	File system
		Directory and file management
		File upload and download through FTP, TFTP, SFTP, SCP, and FTPS
	Monitoring and maintenance	Hardware monitoring
		Reporting alarms on abnormal device temperature
		Second-time fault detection to prevent detection errors caused by instant interference
		Version matching check
		Information center and unified management over logs, alarms, and debugging information
		Electronic labels, and command line query and backup
		Virtual cable test (VCT)
		User operation logs
		Detailed debugging information for network fault diagnosis
		Network test tools such as traceroute and ping commands
		Port mirroring, flow mirroring, and remote mirroring
	Energy saving	
	Version upgrade	Device software loading and online software loading

Feature		Description
		BootROM online upgrade
		In-service patching
Security	AAA	Local authentication and authorization
		RADIUS authentication, authorization, and accounting
		HWTACACS authentication, authorization, and accounting
	NAC	802.1X authentication
		MAC address authentication
		Portal authentication
		Hybrid authentication
	ARP security	Dynamic ARP Inspection (DAI) and Static ARP Inspection (SAI)
		Egress ARP Inspection (EAI)
		ARP packet rate limiting based on source IP addresses, interfaces, and VLANs, and global ARP packet rate limiting
	IP security	ICMP attack defense
		IP source guard
	Local attack defense	CPU attack defense
	MFF	MAC-Forced Forwarding (MFF)
	DHCP snooping	DHCP snooping
Option 82 function and dynamic rate limiting for DHCP packets		
Attack defense	Defense against flood attacks without IP payloads, attacks from IGMP null payload packets, LAND attacks, Smurf attacks, and attacks from packets with invalid TCP flag bits	
	Defense against attacks from many fragments, attacks from many packets with offsets, attacks from repeated packet fragments, Tear Drop attacks, Syndrop attacks, NewTear attacks, Bonk attacks, Nesta attacks, Rose attacks, Fawx attacks, Ping of Death attacks, and Jolt attacks	
	Defense against TCP SYN flood attacks, UDP flood attacks (including Fraggle attacks and UDP diagnosis port attacks), and ICMP flood attacks	
Network management	-	Ping and traceroute
	-	NQA

Feature		Description
		Network Time Protocol (NTP)
		sFlow
		HTTP
		Hypertext Transfer Protocol Secure (HTTPS)
		SNMP v1/v2c/v3
		Standard MIB
		Remote network monitoring (RMON)

4.5 Product Features Supported by V200R009C00

Table 4-5 lists the features supported by the S2720 and S2750.

Table 4-5 Features supported by the S2720 and S2750

Feature		Description
Ethernet features	Ethernet	Full-duplex, half-duplex, and auto-negotiation modes on Ethernet interfaces
		Ethernet interface rates: 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, and auto-negotiation
		Flow control on interfaces
		Jumbo frames
		Link aggregation
		Load balancing among links of a trunk
		Transparent transmission of Layer 2 protocol packets
		Device Link Detection Protocol (DLDP)
		Link Layer Discovery Protocol (LLDP)
		Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)
		Interface isolation and forwarding restriction
		Broadcast storm suppression
	VLAN	Access modes of LNP (link type negotiation protocol), access, trunk, hybrid, and QinQ
Default VLAN		

Feature		Description
		VLAN assignment based on interfaces, MAC addresses, protocols, and IP subnets
		VLAN assignment based on the following policies: <ul style="list-style-type: none"> ● MAC address + IP address ● MAC address + IP address + interface number
		Adding double VLAN tags to packets based on interface
		VLAN mapping
		Selective QinQ
		MUX VLAN
		Voice VLAN
		Guest VLAN
	GVRP	Generic Attribute Registration Protocol (GARP)
		GARP VLAN Registration Protocol (GVRP)
	VCMP	VCMP (VLAN centralized management protocol)
	MAC	Automatic learning and aging of MAC addresses
		Static, dynamic, and blackhole MAC address entries
		Packet filtering based on source MAC addresses
		Interface-based MAC learning limiting
		Sticky MAC address entries
		MAC address flapping detection
		MAC address spoofing defense
	Port bridge	
	ARP	Static and dynamic ARP entries
		ARP in a VLAN
		Aging of ARP entries
	Ethernet loop protection	MSTP
RSTP		
MSTP		
VBST		
BPDU protection, root protection, and loop protection		
TC-BPDU attack defense		

Feature		Description	
		STP loop detection	
	Loopback-detect	Loop detection on an interface	
	SEP	Smart Ethernet Protection (SEP)	
	Smart Link		Smart Link
			Smart Link multi-instance
			Monitor Link
	RRPP		RRPP protective switchover
			Single RRPP ring, tangent RRPP ring, and intersecting RRPP ring
			Hybrid networking of RRPP rings and other ring networks
	ERPS		G.8032 v1/v2
			Single closed ring
		Subring	
IPv4/ IPv6 forwarding	IPv4 and unicast routes	Static IPv4 routes	
		DHCP client	
		DHCP server	
		DHCP relay	
	IPv6 features	IPv6 protocol stack	
		ND and ND snooping	
		DHCPv6 snooping	
Layer 2 multicast features	-	IGMPv1/v2/v3 snooping	
		Fast leave	
		IGMP snooping proxy	
		MLD snooping	
		Interface-based multicast traffic suppression	
		Inter-VLAN multicast replication	
		Controllable multicast	
Stacking	-	Service interface supporting the stacking function	
Ethernet OAM	EFM OAM (802.3ah)	Automatic discovery	
		Link fault detection	

Feature		Description
		Link fault troubleshooting
		Remote loopback
	CFM OAM (802.1ag)	Software-level CCM
		MAC ping
		MAC trace
	Y.1731	Delay and variation measurement
QoS features	Traffic classifier	Traffic classification based on ACLs
		Traffic classification based on outer 802.1p priorities, outer VLAN IDs, source MAC addresses, and Ethernet types
	Traffic behavior	Access control after traffic classification
		Traffic policing based on traffic classification
		Re-marking based on traffic classification
		Associating traffic classifiers with traffic behaviors
	Traffic policing	Rate limiting on inbound and outbound interfaces
	Traffic shaping	Traffic shaping on interfaces and queues
	Congestion avoidance	Tail drop
	Congestion management	Priority Queuing (PQ)
		Weighted Deficit Round Robin (WDRR)
		PQ+WDRR
		Weighted Round Robin (WRR)
		PQ+WRR
Configuration and maintenance	Login and configuration management	Command line configuration
		Error message and help information in English
		Login through console and Telnet terminals
		SSH1.5/SSH2
		Send function and data communication between terminal users
		Hierarchical user authority management and commands
		SNMP-based NMS management (eSight)
		Web page-based configuration and management

Feature		Description
		EasyDeploy (client)
	File system	File system
		Directory and file management
		File upload and download through FTP, TFTP, SFTP, SCP, and FTPS
	Monitoring and maintenance	Hardware monitoring
		Reporting alarms on abnormal device temperature
		Second-time fault detection to prevent detection errors caused by instant interference
		Version matching check
		Information center and unified management over logs, alarms, and debugging information
		Electronic labels, and command line query and backup
		Virtual cable test (VCT)
		User operation logs
		Detailed debugging information for network fault diagnosis
		Network test tools such as traceroute and ping commands
		Port mirroring, flow mirroring, and remote mirroring
		Energy saving
	Version upgrade	Device software loading and online software loading
		BootROM online upgrade
		In-service patching
	Security	AAA
RADIUS authentication, authorization, and accounting		
HWTACACS authentication, authorization, and accounting		
NAC		802.1X authentication
		MAC address authentication
		Portal authentication
		Hybrid authentication
ARP security		Dynamic ARP Inspection (DAI) and Static ARP Inspection (SAI)
		Egress ARP Inspection (EAI)

Feature		Description
		ARP packet rate limiting based on source IP addresses, interfaces, and VLANs, and global ARP packet rate limiting
	IP security	ICMP attack defense
		IP source guard
	Local attack defense	CPU attack defense
	MFF	MAC-Forced Forwarding (MFF)
	DHCP snooping	DHCP snooping
		Option 82 function and dynamic rate limiting for DHCP packets
	Attack defense	Defense against flood attacks without IP payloads, attacks from IGMP null payload packets, LAND attacks, Smurf attacks, and attacks from packets with invalid TCP flag bits
		Defense against attacks from many fragments, attacks from many packets with offsets, attacks from repeated packet fragments, Tear Drop attacks, Syndrop attacks, NewTear attacks, Bonk attacks, Nesta attacks, Rose attacks, Fawx attacks, Ping of Death attacks, and Jolt attacks
		Defense against TCP SYN flood attacks, UDP flood attacks (including Fraggle attacks and UDP diagnosis port attacks), and ICMP flood attacks
Network management	-	Ping and traceroute
		NQA
		Network Time Protocol (NTP)
		sFlow
		HTTP
		Hypertext Transfer Protocol Secure (HTTPS)
		SNMP v1/v2c/v3
		Standard MIB
		Remote network monitoring (RMON)

4.6 Product Features Supported by V200R008C00

Table 4-6 lists the features supported by the S2750.

Table 4-6 Features supported by the S2750

Feature		Description
Ethernet features	Ethernet	Full-duplex, half-duplex, and auto-negotiation modes on Ethernet interfaces
		Ethernet interface rates: 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, and auto-negotiation
		Flow control on interfaces
		Jumbo frames
		Link aggregation
		Load balancing among links of a trunk
		Transparent transmission of Layer 2 protocol packets
		Device Link Detection Protocol (DLDP)
		Link Layer Discovery Protocol (LLDP)
		Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)
		Interface isolation and forwarding restriction
		Broadcast storm suppression
		VLAN
	Default VLAN	
	VLAN assignment based on interfaces, MAC addresses, protocols, and IP subnets	
	VLAN assignment based on the following policies: <ul style="list-style-type: none"> ● MAC address + IP address ● MAC address + IP address + interface number 	
	Adding double VLAN tags to packets based on interface	
	VLAN mapping	
	Selective QinQ	
	MUX VLAN	
Voice VLAN		
Guest VLAN		
GVRP	Generic Attribute Registration Protocol (GARP)	
	GARP VLAN Registration Protocol (GVRP)	
VCMP	VCMP (VLAN centralized management protocol)	

Feature		Description
	MAC	Automatic learning and aging of MAC addresses
		Static, dynamic, and blackhole MAC address entries
		Packet filtering based on source MAC addresses
		Interface-based MAC learning limiting
		Sticky MAC address entries
		MAC address flapping detection
		MAC address spoofing defense
		Port bridge
	ARP	Static and dynamic ARP entries
		ARP in a VLAN
Aging of ARP entries		
Ethernet loop protection	MSTP	STP
		RSTP
		MSTP
		VBST
		BPDU protection, root protection, and loop protection
		TC-BPDU attack defense
		STP loop detection
	Loopback-detect	Loop detection on an interface
	SEP	Smart Ethernet Protection (SEP)
	Smart Link	Smart Link
		Smart Link multi-instance
		Monitor Link
	RRPP	RRPP protective switchover
		Single RRPP ring, tangent RRPP ring, and intersecting RRPP ring
		Hybrid networking of RRPP rings and other ring networks
	ERPS	G.8032 v1/v2
		Single closed ring
		Subring

Feature		Description	
IPv4/ IPv6 forwarding	IPv4 and unicast routes	Static IPv4 routes	
		DHCP client	
		DHCP server	
		DHCP relay	
	IPv6 features	IPv6 protocol stack	
		ND and ND snooping	
DHCPv6 snooping			
Layer 2 multicast features	-	IGMPv1/v2/v3 snooping	
		Fast leave	
		IGMP snooping proxy	
		MLD snooping	
		Interface-based multicast traffic suppression	
		Inter-VLAN multicast replication	
Stacking	-	Service interface supporting the stacking function	
		Ethernet OAM	EFM OAM (802.3ah)
			Automatic discovery
			Link fault detection
			Link fault troubleshooting
		Remote loopback	
CFM OAM (802.1ag)	Software-level CCM		
	MAC ping		
	MAC trace		
Y.1731	Delay and variation measurement		
QoS features	Traffic classifier	Traffic classification based on ACLs	
		Traffic classification based on outer 802.1p priorities, outer VLAN IDs, source MAC addresses, and Ethernet types	
	Traffic behavior	Access control after traffic classification	
		Traffic policing based on traffic classification	
		Re-marking based on traffic classification	
		Associating traffic classifiers with traffic behaviors	

Feature		Description	
	Traffic policing	Rate limiting on inbound and outbound interfaces	
	Traffic shaping	Traffic shaping on interfaces and queues	
	Congestion avoidance	Tail drop	
	Congestion management	Priority Queuing (PQ)	
		Weighted Deficit Round Robin (WDRR)	
		PQ+WDRR	
		Weighted Round Robin (WRR)	
		PQ+WRR	
	Configuration and maintenance	Login and configuration management	Command line configuration
			Error message and help information in English
Login through console and Telnet terminals			
SSH1.5/SSH2			
Send function and data communication between terminal users			
Hierarchical user authority management and commands			
SNMP-based NMS management (eSight)			
Web page-based configuration and management			
EasyDeploy (client)			
File system		File system	
		Directory and file management	
		File upload and download through FTP, TFTP, SFTP, SCP, and FTPS	
Monitoring and maintenance		Hardware monitoring	
		Reporting alarms on abnormal device temperature	
		Second-time fault detection to prevent detection errors caused by instant interference	
		Version matching check	
		Information center and unified management over logs, alarms, and debugging information	
		Electronic labels, and command line query and backup	

Feature		Description
		Virtual cable test (VCT)
		User operation logs
		Detailed debugging information for network fault diagnosis
		Network test tools such as traceroute and ping commands
		Port mirroring, flow mirroring, and remote mirroring
		Energy saving
	Version upgrade	Device software loading and online software loading
		BootROM online upgrade
		In-service patching
Security	AAA	Local authentication and authorization
		RADIUS authentication, authorization, and accounting
		HWTACACS authentication, authorization, and accounting
	NAC	802.1X authentication
		MAC address authentication
		Portal authentication
		Hybrid authentication
	ARP security	Dynamic ARP Inspection (DAI) and Static ARP Inspection (SAI)
		Egress ARP Inspection (EAI)
		ARP packet rate limiting based on source IP addresses, interfaces, and VLANs, and global ARP packet rate limiting
	IP security	ICMP attack defense
		IP source guard
	Local attack defense	CPU attack defense
	MFF	MAC-Forced Forwarding (MFF)
	DHCP snooping	DHCP snooping
Option 82 function and dynamic rate limiting for DHCP packets		
Attack defense	Defense against flood attacks without IP payloads, attacks from IGMP null payload packets, LAND attacks, Smurf attacks, and attacks from packets with invalid TCP flag bits	

Feature		Description
		Defense against attacks from many fragments, attacks from many packets with offsets, attacks from repeated packet fragments, Tear Drop attacks, Syndrop attacks, NewTear attacks, Bonk attacks, Nesta attacks, Rose attacks, Fawx attacks, Ping of Death attacks, and Jolt attacks
		Defense against TCP SYN flood attacks, UDP flood attacks (including Fraggle attacks and UDP diagnosis port attacks), and ICMP flood attacks
Network management	-	Ping and traceroute
		NQA
		Network Time Protocol (NTP)
		sFlow
		HTTP
		Hypertext Transfer Protocol Secure (HTTPS)
		SNMP v1/v2c/v3
		Standard MIB
		Remote network monitoring (RMON)

 **NOTE**

Features marked with * are added in V200R008.

4.7 Product Features Supported by V200R007C00

[Table 4-7](#) lists the features supported by the S2750.

Table 4-7 Features supported by the S2750

Feature		Description
Ethernet features	Ethernet	Full-duplex, half-duplex, and auto-negotiation modes on Ethernet interfaces
		Ethernet interface rates: 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, and auto-negotiation
		Flow control on interfaces
		Jumbo frames
		Link aggregation
		Load balancing among links of a trunk

Feature		Description
		Transparent transmission of Layer 2 protocol packets
		Device Link Detection Protocol (DLDP)
		Link Layer Discovery Protocol (LLDP)
		Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)
		Interface isolation and forwarding restriction
		Broadcast storm suppression
	VLAN	Access modes of LNP (link type negotiation protocol), access, trunk, hybrid, and QinQ
		Default VLAN
		VLAN assignment based on interfaces, MAC addresses, protocols, and IP subnets
		VLAN assignment based on the following policies: <ul style="list-style-type: none"> ● MAC address + IP address ● MAC address + IP address + interface number
		Adding double VLAN tags to packets based on interface
		VLAN mapping
		Selective QinQ
		MUX VLAN
		Voice VLAN
		Guest VLAN
	GVRP	Generic Attribute Registration Protocol (GARP)
		GARP VLAN Registration Protocol (GVRP)
	VCMP	VCMP (VLAN centralized management protocol)
	MAC	Automatic learning and aging of MAC addresses
		Static, dynamic, and blackhole MAC address entries
Packet filtering based on source MAC addresses		
Interface-based MAC learning limiting		
Sticky MAC address entries		
MAC address flapping detection		
MAC address spoofing defense		
Port bridge		

Feature		Description
	ARP	Static and dynamic ARP entries
		ARP in a VLAN
		Aging of ARP entries
Ethernet loop protection	MSTP	STP
		RSTP
		MSTP
		VBST
		BPDU protection, root protection, and loop protection
		TC-BPDU attack defense
		STP loop detection
	Loopback-detect	Loop detection on an interface
	SEP	Smart Ethernet Protection (SEP)
	Smart Link	Smart Link
		Smart Link multi-instance
		Monitor Link
	RRPP	RRPP protective switchover
		Single RRPP ring, tangent RRPP ring, and intersecting RRPP ring
		Hybrid networking of RRPP rings and other ring networks
ERPS	G.8032 v1/v2	
	Single closed ring	
	Subring	
IPv4/IPv6 forwarding	IPv4 and unicast routes	Static IPv4 routes
		DHCP client
		DHCP server
		DHCP relay
	IPv6 features	IPv6 protocol stack
		ND and ND snooping
		DHCPv6 snooping

Feature		Description
Layer 2 multicast features	-	IGMPv1/v2/v3 snooping
		Fast leave
		IGMP snooping proxy
		MLD snooping
		Interface-based multicast traffic suppression
		Inter-VLAN multicast replication
		Controllable multicast
Stacking	-	Service interface supporting the stacking function
Ethernet OAM	EFM OAM (802.3ah)	Automatic discovery
		Link fault detection
		Link fault troubleshooting
		Remote loopback
	CFM OAM (802.1ag)	Software-level CCM
		MAC ping
		MAC trace
Y.1731	Delay and variation measurement	
QoS features	Traffic classifier	Traffic classification based on ACLs
		Traffic classification based on outer 802.1p priorities, outer VLAN IDs, source MAC addresses, and Ethernet types
	Traffic behavior	Access control after traffic classification
		Traffic policing based on traffic classification
		Re-marking based on traffic classification
		Associating traffic classifiers with traffic behaviors
	Traffic policing	Rate limiting on inbound and outbound interfaces
	Traffic shaping	Traffic shaping on interfaces and queues
	Congestion avoidance	Tail drop
	Congestion management	Priority Queuing (PQ)
		Weighted Deficit Round Robin (WDRR)
PQ+WDRR		

Feature		Description
		Weighted Round Robin (WRR)
		PQ+WRR
Configuration and maintenance	Login and configuration management	Command line configuration
		Error message and help information in English
		Login through console and Telnet terminals
		SSH1.5/SSH2
		Send function and data communication between terminal users
		Hierarchical user authority management and commands
		SNMP-based NMS management (eSight)
		Web page-based configuration and management
		EasyDeploy (client)
	File system	File system
		Directory and file management
		File upload and download through FTP, TFTP, SFTP, SCP, and FTPS
	Monitoring and maintenance	Hardware monitoring
		Reporting alarms on abnormal device temperature
		Second-time fault detection to prevent detection errors caused by instant interference
		Version matching check
		Information center and unified management over logs, alarms, and debugging information
		Electronic labels, and command line query and backup
		Virtual cable test (VCT)
		User operation logs
		Detailed debugging information for network fault diagnosis
		Network test tools such as traceroute and ping commands
		Port mirroring, flow mirroring, and remote mirroring
Energy saving		
Version upgrade	Device software loading and online software loading	
	BootROM online upgrade	

Feature		Description
		In-service patching
Security	AAA	Local authentication and authorization
		RADIUS authentication, authorization, and accounting
		HWTACACS authentication, authorization, and accounting
	NAC	802.1X authentication
		MAC address authentication
		Portal authentication
		Hybrid authentication
	ARP security	Dynamic ARP Inspection (DAI) and Static ARP Inspection (SAI)
		Egress ARP Inspection (EAI)
		ARP packet rate limiting based on source IP addresses, interfaces, and VLANs, and global ARP packet rate limiting
	IP security	ICMP attack defense
		IP source guard
	Local attack defense	CPU attack defense
	MFF	MAC-Forced Forwarding (MFF)
	DHCP snooping	DHCP snooping
Option 82 function and dynamic rate limiting for DHCP packets		
Attack defense	Defense against flood attacks without IP payloads, attacks from IGMP null payload packets, LAND attacks, Smurf attacks, and attacks from packets with invalid TCP flag bits	
	Defense against attacks from many fragments, attacks from many packets with offsets, attacks from repeated packet fragments, Tear Drop attacks, Syndrop attacks, NewTear attacks, Bonk attacks, Nesta attacks, Rose attacks, Fawx attacks, Ping of Death attacks, and Jolt attacks	
	Defense against TCP SYN flood attacks, UDP flood attacks (including Fraggle attacks and UDP diagnosis port attacks), and ICMP flood attacks	
Network management	-	Ping and traceroute
		NQA
		Network Time Protocol (NTP)

Feature		Description
		sFlow
		HTTP
		Hypertext Transfer Protocol Secure (HTTPS)
		SNMP v1/v2c/v3
		Standard MIB
		Remote network monitoring (RMON)

4.8 Product Features Supported by V200R006C00

[Table 4-8](#) lists the features supported by the S2750.

Table 4-8 Features supported by the S2750

Feature		Description
Ethernet features	Ethernet	Full-duplex, half-duplex, and auto-negotiation modes on Ethernet interfaces
		Ethernet interface rates: 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, and auto-negotiation
		Flow control on interfaces
		Jumbo frames
		Link aggregation
		Load balancing among links of a trunk
		Transparent transmission of Layer 2 protocol packets
		Device Link Detection Protocol (DLDP)
		Link Layer Discovery Protocol (LLDP)
		Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)
		Interface isolation and forwarding restriction
		Broadcast storm suppression
	VLAN	Access modes of LNP (link type negotiation protocol), access, trunk, hybrid, and QinQ
Default VLAN		
VLAN assignment based on interfaces, MAC addresses, protocols, and IP subnets		

Feature		Description
		VLAN assignment based on the following policies: <ul style="list-style-type: none"> ● MAC address + IP address ● MAC address + IP address + interface number
		Adding double VLAN tags to packets based on interface
		VLAN mapping
		Selective QinQ
		MUX VLAN
		Voice VLAN
		Guest VLAN
	GVRP	Generic Attribute Registration Protocol (GARP)
		GARP VLAN Registration Protocol (GVRP)
	VCMP	VCMP (VLAN centralized management protocol)
	MAC	Automatic learning and aging of MAC addresses
		Static, dynamic, and blackhole MAC address entries
		Packet filtering based on source MAC addresses
		Interface-based MAC learning limiting
		Sticky MAC address entries
		MAC address flapping detection
		MAC address spoofing defense
	Port bridge	
	ARP	Static and dynamic ARP entries
		ARP in a VLAN
		Aging of ARP entries
Ethernet loop protection	MSTP	STP
		RSTP
		MSTP
		VBST
		BPDU protection, root protection, and loop protection
		TC-BPDU attack defense
		STP loop detection

Feature		Description	
	Loopback-detect	Loop detection on an interface	
	SEP	Smart Ethernet Protection (SEP)	
	Smart Link	Smart Link	
		Smart Link multi-instance	
		Monitor Link	
	RRPP	RRPP protective switchover	
		Single RRPP ring, tangent RRPP ring, and intersecting RRPP ring	
		Hybrid networking of RRPP rings and other ring networks	
	ERPS	G.8032 v1/v2	
		Single closed ring	
		Subring	
	IPv4/ IPv6 forwarding	IPv4 and unicast routes	Static IPv4 routes
DHCP client			
DHCP server			
DHCP relay			
IPv6 features		IPv6 protocol stack	
		ND and ND snooping	
	DHCPv6 snooping		
Layer 2 multicast features	-	IGMPv1/v2/v3 snooping	
		Fast leave	
		IGMP snooping proxy	
		MLD snooping	
		Interface-based multicast traffic suppression	
		Inter-VLAN multicast replication	
		Controllable multicast	
Stacking	-	Service interface supporting the stacking function	
Ethernet OAM	EFM OAM (802.3ah)	Automatic discovery	
		Link fault detection	
		Link fault troubleshooting	

Feature		Description
		Remote loopback
	CFM OAM (802.1ag)	Software-level CCM
		MAC ping
		MAC trace
Y.1731	Delay and variation measurement	
QoS features	Traffic classifier	Traffic classification based on ACLs
		Traffic classification based on outer 802.1p priorities, outer VLAN IDs, source MAC addresses, and Ethernet types
	Traffic behavior	Access control after traffic classification
		Traffic policing based on traffic classification
		Re-marking based on traffic classification
		Associating traffic classifiers with traffic behaviors
	Traffic policing	Rate limiting on inbound and outbound interfaces
	Traffic shaping	Traffic shaping on interfaces and queues
	Congestion avoidance	Tail drop
	Congestion management	Priority Queuing (PQ)
		Weighted Deficit Round Robin (WDRR)
		PQ+WDRR
		Weighted Round Robin (WRR)
PQ+WRR		
Configuration and maintenance	Login and configuration management	Command line configuration
		Error message and help information in English
		Login through console and Telnet terminals
		SSH1.5/SSH2
		Send function and data communication between terminal users
		Hierarchical user authority management and commands
		SNMP-based NMS management (eSight)
		Web page-based configuration and management
		EasyDeploy (client)

Feature		Description
	File system	File system
		Directory and file management
		File upload and download through FTP, TFTP, SFTP, SCP, and FTPS
	Monitoring and maintenance	Hardware monitoring
		Reporting alarms on abnormal device temperature
		Second-time fault detection to prevent detection errors caused by instant interference
		Version matching check
		Information center and unified management over logs, alarms, and debugging information
		Electronic labels, and command line query and backup
		Virtual cable test (VCT)
		User operation logs
		Detailed debugging information for network fault diagnosis
		Network test tools such as traceroute and ping commands
		Port mirroring, flow mirroring, and remote mirroring
		Energy saving
Version upgrade	Device software loading and online software loading	
	BootROM online upgrade	
	In-service patching	
Security	AAA	Local authentication and authorization
		RADIUS authentication, authorization, and accounting
		HWTACACS authentication, authorization, and accounting
	NAC	802.1X authentication
		MAC address authentication
		Portal authentication
		Hybrid authentication
	ARP security	Dynamic ARP Inspection (DAI) and Static ARP Inspection (SAI)
		Egress ARP Inspection (EAI)

Feature		Description
		ARP packet rate limiting based on source IP addresses, interfaces, and VLANs, and global ARP packet rate limiting
	IP security	ICMP attack defense
		IP source guard
	Local attack defense	CPU attack defense
	MFF	MAC-Forced Forwarding (MFF)
	DHCP snooping	DHCP snooping
		Option 82 function and dynamic rate limiting for DHCP packets
	Attack defense	Defense against flood attacks without IP payloads, attacks from IGMP null payload packets, LAND attacks, Smurf attacks, and attacks from packets with invalid TCP flag bits
		Defense against attacks from many fragments, attacks from many packets with offsets, attacks from repeated packet fragments, Tear Drop attacks, Syndrop attacks, NewTear attacks, Bonk attacks, Nesta attacks, Rose attacks, Fawx attacks, Ping of Death attacks, and Jolt attacks
		Defense against TCP SYN flood attacks, UDP flood attacks (including Fraggle attacks and UDP diagnosis port attacks), and ICMP flood attacks
Network management	-	Ping and traceroute
		NQA
		Network Time Protocol (NTP)
		sFlow
		HTTP
		Hypertext Transfer Protocol Secure (HTTPS)
		SNMP v1/v2c/v3
		Standard MIB
		Remote network monitoring (RMON)

4.9 Product Features Supported by V200R005C00

[Table 4-9](#) lists the features supported by the S2750.

Table 4-9 Features supported by the S2750

Feature		Description
Ethernet features	Ethernet	Full-duplex, half-duplex, and auto-negotiation modes on Ethernet interfaces
		Ethernet interface rates: 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, and auto-negotiation
		Flow control on interfaces
		Jumbo frames
		Link aggregation
		Load balancing among links of a trunk
		Transparent transmission of Layer 2 protocol packets
		Device Link Detection Protocol (DLDP)
		Link Layer Discovery Protocol (LLDP)
		Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)
		Interface isolation and forwarding restriction
		Broadcast storm suppression
		VLAN
	Default VLAN	
	VLAN assignment based on interfaces, MAC addresses, protocols, and IP subnets	
	VLAN assignment based on the following policies: <ul style="list-style-type: none"> ● MAC address + IP address ● MAC address + IP address + interface number 	
	Adding double VLAN tags to packets based on interface	
	VLAN mapping	
	Selective QinQ	
	MUX VLAN	
Voice VLAN		
Guest VLAN		
GVRP	Generic Attribute Registration Protocol (GARP)	
	GARP VLAN Registration Protocol (GVRP)	
VCMP	VCMP (VLAN centralized management protocol)	

Feature		Description
	MAC	Automatic learning and aging of MAC addresses
		Static, dynamic, and blackhole MAC address entries
		Packet filtering based on source MAC addresses
		Interface-based MAC learning limiting
		Sticky MAC address entries
		MAC address flapping detection
		MAC address spoofing defense
		Port bridge
	ARP	Static and dynamic ARP entries
		ARP in a VLAN
Aging of ARP entries		
Ethernet loop protection	MSTP	STP
		RSTP
		MSTP
		VBST
		BPDU protection, root protection, and loop protection
		TC-BPDU attack defense
		STP loop detection
	Loopback-detect	Loop detection on an interface
	SEP	Smart Ethernet Protection (SEP)
	Smart Link	Smart Link
		Smart Link multi-instance
		Monitor Link
	RRPP	RRPP protective switchover
		Single RRPP ring, tangent RRPP ring, and intersecting RRPP ring
		Hybrid networking of RRPP rings and other ring networks
	ERPS	G.8032 v1/v2
		Single closed ring
Subring		

Feature		Description
IPv4/ IPv6 forwarding	IPv4 and unicast routes	Static IPv4 routes
		DHCP client
		DHCP server
		DHCP relay
	IPv6 features	IPv6 protocol stack
		ND and ND snooping
		DHCPv6 snooping
Layer 2 multicast features	-	IGMPv1/v2/v3 snooping
		Fast leave
		IGMP snooping proxy
		MLD snooping
		Interface-based multicast traffic suppression
		Inter-VLAN multicast replication
		Controllable multicast
Stacking	-	Service interface supporting the stacking function
Ethernet OAM	EFM OAM (802.3ah)	Automatic discovery
		Link fault detection
		Link fault troubleshooting
		Remote loopback
	CFM OAM (802.1ag)	Software-level CCM
		MAC ping
		MAC trace
Y.1731	Delay and variation measurement	
QoS features	Traffic classifier	Traffic classification based on ACLs
		Traffic classification based on outer 802.1p priorities, outer VLAN IDs, source MAC addresses, and Ethernet types
	Traffic behavior	Access control after traffic classification
		Traffic policing based on traffic classification
		Re-marking based on traffic classification
		Associating traffic classifiers with traffic behaviors

Feature		Description	
	Traffic policing	Rate limiting on inbound and outbound interfaces	
	Traffic shaping	Traffic shaping on interfaces and queues	
	Congestion avoidance	Tail drop	
	Congestion management	Priority Queuing (PQ)	
		Weighted Deficit Round Robin (WDRR)	
		PQ+WDRR	
		Weighted Round Robin (WRR)	
		PQ+WRR	
	Configuration and maintenance	Login and configuration management	Command line configuration
			Error message and help information in English
Login through console and Telnet terminals			
SSH1.5/SSH2			
Send function and data communication between terminal users			
Hierarchical user authority management and commands			
SNMP-based NMS management (eSight)			
Web page-based configuration and management			
EasyDeploy (client)			
File system		File system	
		Directory and file management	
		File upload and download through FTP, TFTP, SFTP, SCP, and FTPS	
Monitoring and maintenance		Hardware monitoring	
		Reporting alarms on abnormal device temperature	
		Second-time fault detection to prevent detection errors caused by instant interference	
		Version matching check	
		Information center and unified management over logs, alarms, and debugging information	
		Electronic labels, and command line query and backup	

Feature		Description
		Virtual cable test (VCT)
		User operation logs
		Detailed debugging information for network fault diagnosis
		Network test tools such as traceroute and ping commands
		Port mirroring, flow mirroring, and remote mirroring
		Energy saving
	Version upgrade	Device software loading and online software loading
		BootROM online upgrade
		In-service patching
Security	AAA	Local authentication and authorization
		RADIUS authentication, authorization, and accounting
		HWTACACS authentication, authorization, and accounting
	NAC	802.1X authentication
		MAC address authentication
		Portal authentication
		Hybrid authentication
	ARP security	Dynamic ARP Inspection (DAI) and Static ARP Inspection (SAI)
		Egress ARP Inspection (EAI)
		ARP packet rate limiting based on source IP addresses, interfaces, and VLANs, and global ARP packet rate limiting
	IP security	ICMP attack defense
		IP source guard
	Local attack defense	CPU attack defense
	MFF	MAC-Forced Forwarding (MFF)
	DHCP snooping	DHCP snooping
Option 82 function and dynamic rate limiting for DHCP packets		
Attack defense	Defense against flood attacks without IP payloads, attacks from IGMP null payload packets, LAND attacks, Smurf attacks, and attacks from packets with invalid TCP flag bits	

Feature		Description
		Defense against attacks from many fragments, attacks from many packets with offsets, attacks from repeated packet fragments, Tear Drop attacks, Syndrop attacks, NewTear attacks, Bonk attacks, Nesta attacks, Rose attacks, Fawx attacks, Ping of Death attacks, and Jolt attacks
		Defense against TCP SYN flood attacks, UDP flood attacks (including Fraggle attacks and UDP diagnosis port attacks), and ICMP flood attacks
Network management	-	Ping and traceroute
		NQA
		Network Time Protocol (NTP)
		sFlow
		HTTP
		Hypertext Transfer Protocol Secure (HTTPS)
		SNMP v1/v2c/v3
		Standard MIB
		Remote network monitoring (RMON)

4.10 Product Features Supported by V200R003C00

Table 4-10 lists the features supported by the S2750.

Table 4-10 Features supported by the S2750

Feature		Description
Ethernet features	Ethernet	Full-duplex, half-duplex, and auto-negotiation modes on Ethernet interfaces
		Ethernet interface rates: 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, and auto-negotiation
		Flow control on interfaces
		Jumbo frames
		Link aggregation
		Load balancing among links of a trunk
		Transparent transmission of Layer 2 protocol packets
		Device Link Detection Protocol (DLDP)

Feature		Description
		Link Layer Discovery Protocol (LLDP)
		Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)
		Interface isolation and forwarding restriction
		Broadcast storm suppression
	VLAN	Access modes of access, trunk, hybrid, and QinQ
		Default VLAN
		VLAN assignment based on interfaces, MAC addresses, protocols, and IP subnets
		VLAN assignment based on the following policies: <ul style="list-style-type: none"> ● MAC address + IP address ● MAC address + IP address + interface number
		Adding double VLAN tags to packets based on interface
		VLAN mapping
		Selective QinQ
		MUX VLAN
		Voice VLAN
		Guest VLAN
	GVRP	Generic Attribute Registration Protocol (GARP)
		GARP VLAN Registration Protocol (GVRP)
	MAC	Automatic learning and aging of MAC addresses
		Static, dynamic, and blackhole MAC address entries
		Packet filtering based on source MAC addresses
		Interface-based MAC learning limiting
		Sticky MAC address entries
		MAC address flapping detection
		MAC address spoofing defense
Port bridge		
ARP	Static and dynamic ARP entries	
	ARP in a VLAN	
	Aging of ARP entries	

Feature		Description
Ethernet loop protection	MSTP	STP
		RSTP
		MSTP
		BPDU protection, root protection, and loop protection
		TC-BPDU attack defense
		STP loop detection
	Loopback-detect	Loop detection on an interface
	SEP	Smart Ethernet Protection (SEP)
	Smart Link	Smart Link
		Smart Link multi-instance
		Monitor Link
	RRPP	RRPP protective switchover
		Single RRPP ring, tangent RRPP ring, and intersecting RRPP ring
		Hybrid networking of RRPP rings and other ring networks
	ERPS	G.8032 v1/v2
		Single closed ring
		Subring
IPv4/IPv6 forwarding	IPv4 and unicast routes	Static IPv4 routes
		DHCP client
	IPv6 features	IPv6 protocol stack
		ND and ND snooping
Layer 2 multicast features	-	IGMPv1/v2/v3 snooping
		Fast leave
		IGMP snooping proxy
		MLD snooping
		Interface-based multicast traffic suppression
		Inter-VLAN multicast replication
		Controllable multicast

Feature		Description
Stacking	-	Service interface supporting the stacking function
Ethernet OAM	EFM OAM (802.3ah)	Automatic discovery
		Link fault detection
		Link fault troubleshooting
		Remote loopback
	CFM OAM (802.1ag)	Software-level CCM
		MAC ping
		MAC trace
Y.1731	Delay and variation measurement	
QoS features	Traffic classifier	Traffic classification based on ACLs
		Traffic classification based on outer 802.1p priorities, outer VLAN IDs, source MAC addresses, and Ethernet types
	Traffic behavior	Access control after traffic classification
		Traffic policing based on traffic classification
		Re-marking based on traffic classification
		Associating traffic classifiers with traffic behaviors
	Traffic policing	Rate limiting on inbound and outbound interfaces
	Traffic shaping	Traffic shaping on interfaces and queues
	Congestion avoidance	Tail drop
	Congestion management	Priority Queuing (PQ)
		Weighted Deficit Round Robin (WDRR)
		PQ+WDRR
		Weighted Round Robin (WRR)
PQ+WRR		
Configuration and maintenance	Login and configuration management	Command line configuration
		Error message and help information in English
		Login through console and Telnet terminals
		SSH1.5/SSH2
		Send function and data communication between terminal users

Feature		Description
		Hierarchical user authority management and commands
		SNMP-based NMS management (eSight)
		Web page-based configuration and management
		EasyDeploy (client)
	File system	File system
		Directory and file management
		File upload and download through FTP, TFTP, SFTP, SCP, and FTPS
	Monitoring and maintenance	Hardware monitoring
		Reporting alarms on abnormal device temperature
		Second-time fault detection to prevent detection errors caused by instant interference
		Version matching check
		Information center and unified management over logs, alarms, and debugging information
		Electronic labels, and command line query and backup
		Virtual cable test (VCT)
		User operation logs
		Detailed debugging information for network fault diagnosis
		Network test tools such as traceroute and ping commands
		Port mirroring, flow mirroring, and remote mirroring
		Energy saving
	Version upgrade	Device software loading and online software loading
BootROM online upgrade		
In-service patching		
Security	AAA	Local authentication and authorization
		RADIUS authentication, authorization, and accounting
		HWTACACS authentication, authorization, and accounting
	NAC	802.1X authentication
		MAC address authentication
		Portal authentication

Feature		Description
		Hybrid authentication
	ARP security	Dynamic ARP Inspection (DAI) and Static ARP Inspection (SAI)
		Egress ARP Inspection (EAI)
		ARP packet rate limiting based on source IP addresses, interfaces, and VLANs, and global ARP packet rate limiting
	IP security	ICMP attack defense
		IP source guard
	Local attack defense	CPU attack defense
	MFF	MAC-Forced Forwarding (MFF)
	DHCP snooping	DHCP snooping
		Option 82 function and dynamic rate limiting for DHCP packets
	Attack defense	Defense against flood attacks without IP payloads, attacks from IGMP null payload packets, LAND attacks, Smurf attacks, and attacks from packets with invalid TCP flag bits
		Defense against attacks from many fragments, attacks from many packets with offsets, attacks from repeated packet fragments, Tear Drop attacks, Syndrop attacks, NewTear attacks, Bonk attacks, Nesta attacks, Rose attacks, Fawx attacks, Ping of Death attacks, and Jolt attacks
		Defense against TCP SYN flood attacks, UDP flood attacks (including Fraggle attacks and UDP diagnosis port attacks), and ICMP flood attacks
Network management	-	Ping and traceroute
		NQA
		Network Time Protocol (NTP)
		sFlow
		HTTP
		Hypertext Transfer Protocol Secure (HTTPS)
		SNMP v1/v2c/v3
		Standard MIB
		Remote network monitoring (RMON)

4.11 Product Features Supported by V100R006C05

Table 4-11 lists the features supported by the S2700.

Table 4-11 List of software features

Attribute		Description
Ethernet features	Ethernet	<ul style="list-style-type: none"> ● Operating modes, including full duplex, half duplex, and auto-negotiation ● Operating rates of an Ethernet interface, including 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, and auto-negotiation ● Flow control on interfaces ● Jumbo frames ● Link aggregation ● Load balancing among the links of a trunk ● Port isolation and forwarding restriction on ports ● Traffic suppression
	VLAN	<ul style="list-style-type: none"> ● Access modes of access, trunk, hybrid, and QinQ ● Default VLAN ● VLAN mapping ● Voice VLAN
	MAC	<ul style="list-style-type: none"> ● Automatic learning and aging of MAC addresses ● Static, dynamic, and blackhole MAC address entries ● Packet filtering based on source MAC addresses ● Limitation on MAC address learning on interfaces
	ARP	<ul style="list-style-type: none"> ● Static and dynamic ARP entries ● ARP in a VLAN ● Aging of ARP entries
	LLDP	LLDP
Ethernet loop protection	MSTP	<ul style="list-style-type: none"> ● STP ● RSTP ● MSTP ● BPDU protection, root protection, loop protection ● Partitioned STP and BPDU tunnels
Layer 2 multicast	Layer 2 multicast	<ul style="list-style-type: none"> ● IGMP snooping ● Prompt leave ● Multicast traffic control ● Controllable multicast

Attribute		Description
QoS	Traffic classification	<ul style="list-style-type: none"> ● Traffic classification based on the combination of the L2 protocol header, IP quintuple, outgoing interface, and 802.1p field ● Traffic classification based on the C-VID and C-PRI of QinQ packets
	Traffic behaviors	<ul style="list-style-type: none"> ● Access control after traffic classification ● Traffic policing based on traffic classification ● Re-marking based on traffic classification ● Class-based packet queuing ● Combination of traffic classification and traffic behaviors
	Queue scheduling	<ul style="list-style-type: none"> ● PQ ● WRR ● PQ+WRR
	Rate limit on interfaces	Rate limit on interfaces
Configuration and maintenance	Terminal service	<ul style="list-style-type: none"> ● Configurations through command lines ● Help information in English and Chinese ● Login through console and Telnet terminals ● Information exchange between terminals through the send function
	File system	<ul style="list-style-type: none"> ● File system ● Directory and file management ● File upload and download through FTP, TFTP or SFTP
	Debugging and maintenance	<ul style="list-style-type: none"> ● Centralized management of logs, alarms, and debugging information ● Electronic label ● User operation logs ● Detailed debugging information for diagnosing network faults ● Network test tools such as traceroute and ping commands ● Interface mirroring and flow mirroring
	Version upgrade	<ul style="list-style-type: none"> ● Software loading on the entire equipment and online software loading ● Online upgrade of the BootROM ● In-service patching

Attribute		Description
Security	-	<ul style="list-style-type: none"> ● Hierarchical command line protection to prevent unauthorized users from accessing the device ● SSH v2.0 ● RADIUS authentication and HWTACACS authentication ● ACL filtering ● DHCP packet filtering (with Option 82) ● Defense against control packet attacks ● Defense against attacks of source address spoofing, LAND, SYN flood (TCP SYN), smurf, ping flood (ICMP echo), Teardrop, and Ping of Death
Network management	-	<ul style="list-style-type: none"> ● Ping and traceroute ● SNMPv1/v2c/v3 ● Standard MIB ● RMON

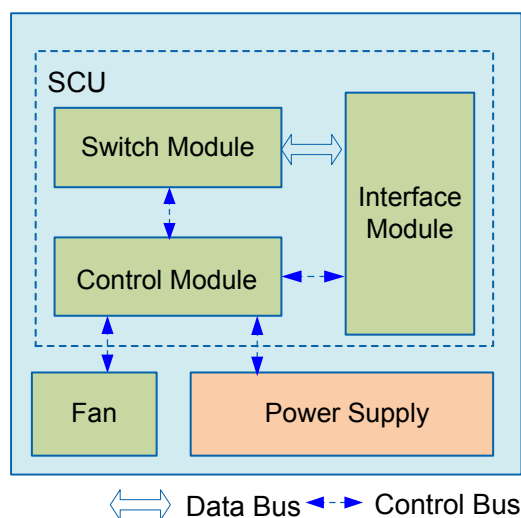
5 Hardware Information

For the version mappings, appearance and structure, port description, indicator description, power supply configuration, heat dissipation, and specifications of the S2700, see the Chassis section in the *S2700 Hardware Description*.

Figure 5-1 shows the logical structure of hardware modules in the switch.

Hardware modules of the switch refer to the Switch Control Unit (SCU), power supply, and fan.

Figure 5-1 Logical structure of hardware modules



SCU

The SCU is built in the S2700. Each switch has one SCU.

The SCU provides packet switching and device management. It integrates the main control module, switching module, and interface module.

Main Control Module

The main control module provides the following functions:

- Processes protocol packets.
- Manages the system and monitors the system performance according to instructions of the user, and reports the device running status to the user.
- Monitors and maintains the interface module and switching module.

Switching Module

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

The switching module uses high-performance chips to provide rate-speed forwarding and fast switching of data with different priorities.

Interface Module

The interface module provides Ethernet interfaces for Ethernet service transmission.

Power Supply

For details about S2700 power supply configuration, see the Power Modules section in the *S2700 Hardware Description*.

Fan Modules

For details about fan modules in different models, see "Heat Dissipation" under Chassis in the *S2700 Hardware Description*.

Pluggable Modules for Interfaces

For specifications of various pluggable modules for interfaces, see the Pluggable Modules for Interfaces section in the *S2700 Hardware Description*.

6 References

You can download the *Switch Standard and Protocol Compliance List* from the [Huawei official website](#).