

S7700 Smart Routing Switch

Product Description

Issue **23**
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 Mapping Between the S7700 Series Switches and Software Versions.....	1
2 Product Overview.....	2
2.1 Introduction.....	2
2.2 Product Characteristics.....	2
3 Usage Scenarios.....	6
3.1 Large-scale Enterprise Campus Network.....	6
3.2 Small- or Medium-scale Enterprise Campus Network.....	7
4 Performance Specifications.....	9
5 Product Performance.....	10
5.1 Product Features Supported by V200R012C00.....	10
5.2 Product Features Supported by V200R011C10.....	18
5.3 Product Features Supported by V200R010C00.....	27
5.4 Product Features Supported by V200R009C00.....	35
5.5 Product Features Supported by V200R008C00.....	43
5.6 Product Features Supported by V200R007C00.....	51
5.7 Product Features Supported by V200R006C00.....	60
5.8 Product Features Supported by V200R005C00.....	68
5.9 Product Features Supported by V200R003C00.....	76
6 Hardware Information.....	85
7 References.....	86

1

Mapping Between the S7700 Series
Switches and Software Versions

Table 1-1 lists the mapping between S7700 series switches and software versions.

Table 1-1 Mapping between the S7700 series switches and software versions

Device Series	Device Model	Software Version
S7700	S7703	V100R003C01 and later versions
	S7706	V100R003C01 and later versions
	S7712	V100R003C01 and later versions

2 Product Overview

About This Chapter

[2.1 Introduction](#)

[2.2 Product Characteristics](#)

2.1 Introduction

The S7700 series smart routing switches (S7700 for short) are high-end switches designed for next-generation enterprise networks. The S7700 series uses Huawei's intelligent multi-layer switching technology to provide intelligent service optimization methods, such as MPLS VPN, traffic analysis, comprehensive QoS policies, controllable multicast, load balancing, and security, in addition to high-performance L2/L3 switching services. The S7700 switches can function as aggregation or core switches in a campus network or data center to provide wireless access, voice, video, and data services, helping enterprises build an integrated end-to-end network.

The S7700 comes in the following models: S7703, S7706, and S7712. These models support a maximum of 3, 6, and 12 line processing units (LPUs), respectively.

2.2 Product Characteristics

Agile Switches for Agile Networks

- With the native AC capability, the S7700 series allows enterprises to build a wireless network without additional hardware AC devices. The T-bit AC capability avoids performance bottlenecks on independent AC devices and can help organizations better cope with challenges in the high-speed wireless era.
- The S7700's unified user management function authenticates both wired and wireless users, ensuring a consistent experience of wired and wireless users. The S7700 supports various authentication methods, including 802.1X, MAC address, and Portal authentication, and can manage users based on user groups, domains, and time ranges.

These facilitate user and service management and enable a transformation from device-centered to user-centered management.

- Super Virtual Fabric (SVF) technology can virtualize fixed switches into line cards of an S7700 switch and virtualize APs into switch ports. With this technology, a physical network with core/aggregation switches, access switches, and APs can be virtualized into one logical switch, offering the simplest network management solution.
- Packet Conservation Algorithm for Internet (iPCA) technology can monitor network quality for any service flow at any network node, anytime, without extra costs. It can detect temporary service interruptions within 1 second and accurately identify faulty ports. This cutting-edge fault detection technology allows for fine granular management.
- The service chaining function can orchestrate value-added service capabilities, such as firewall, antivirus expert system (AVE), and application security gateway (ASG). Then these capabilities can be used by campus network entities (such as switches, routers, AC, AP, and terminals), regardless of physical locations. The service chaining function supports more flexible value-added service deployment and reduces equipment and maintenance costs.

Powerful Service Processing Capabilities

The S7700's highly scalable backplane enables an upgrade of port bandwidth to 40 Gbit/s and is compatible with the currently used cards, protecting investment.

- The high 10GE port density helps to build an all-10G core networks in campus networks and data centers.
- With a multi-service routing and switching platform, the S7700 provides wireless access, voice, video, and data services, helping to build a multi-service network with high availability and low-latency.
- The S7700 supports distributed L2/L3 MPLS VPN functions, including Multiprotocol Label Switching (MPLS), virtual private LAN service (VPLS), hierarchical VPLS (HVPLS), and virtual leased line (VLL), providing secure access for enterprise VPN users.
- The S7700 supports L2/L3 multicast protocols, such as Protocol Independent Multicast Sparse Mode (PIM SM), PIM Dense Mode (DM), Multicast Listener Discovery (MLD), and Internet Group Management Protocol (IGMP) snooping. These multicast protocols ensure high-quality HD video surveillance and video conferencing services.

Carrier-Grade Reliability and Visualized Fault Diagnosis

The S7700 provides redundant backup for key components, including MPUs, power modules, and fans, all of which are hot swappable. The reliability design achieves a high availability of 0.99999.

The S7700 implements the Cluster Switch System (CSS) function through switch fabrics, addressing the problem of low switching efficiency caused by multiple switching processes during inter-chassis forwarding. A CSS system provides 256 Gbit/s cluster bandwidth, highest in the industry. The links between chassis in a cluster can be bundled to improve link utilization and eliminate single-point failures. S7700 switches can also use service ports as CSS ports and be connected using optical fibers to set up a cluster. This expands the distance allowed between cluster member chassis.

The S7700 has a dedicated fault detection subcard that provides hardware-based OAM functions including IEEE 802.3ah, 802.1ag, and ITU-Y.1731. Hardware-based OAM implements between 50 ms and 200 ms fault detection in particular scenarios and can check

session connectivity of all terminals in real time when a network fault occurs. The S7700 can also be managed by an NMS. The NMS provides a graphical fault diagnosis interface and traverses all network elements and links automatically to detect and locate faults quickly. The S7700 implements seamless switchover between the master and slave MPUs and supports graceful restart to ensure nonstop forwarding. The S7700 is ready to support the in-service software upgrade (ISSU) function, which can ensure uninterrupted transmission of key services during software upgrades.

Well-Designed QoS Mechanisms to Improve Voice and Video User Experience

The S7700's QoS control mechanisms classify traffic based on information from the link layer to the application layer. With advanced queue scheduling and congestion control algorithms, the S7700 performs accurate multi-level scheduling for data flows, satisfying enterprises' QoS requirements for a variety of services and user terminals.

The S7700 supports hardware-based low-latency queues for multicast packets so that video services can be processed with high priority and low latency. This guarantees high quality of video conference and video conferencing services in an enterprise. The S7700 uses innovative priority scheduling algorithms to optimize the QoS queuing mechanism for voice and video services. The improved queuing mechanism shortens the latency of the VoIP service and eliminates the pixelation effect in the video service, improving user experience.

High Performance in IPv6 Service Processing to Allow Seamless Migration from IPv4 to IPv6

The S7700 software and hardware platforms support IPv6. The S7700 has been granted an IPv6 Network Access License and the IPv6 Ready Logo Phase 2 Certification by the Ministry of Industry and Information Technology. It supports the IPv4/IPv6 dual stack, various tunneling technologies, IPv6 static routing, RIPng, OSPFv3, BGP+, IS-ISv6, and IPv6 multicast, allowing for pure IPv6 networking and combined IPv4 and IPv6 networking.

Superb Traffic Analysis Capability for Real-Time Network Performance Monitoring

The S7700 supports NetStream for real-time collection and analysis of network traffic statistics. It supports the V5, V8, and V9 NetStream formats and provides aggregation traffic templates to reduce loads on the network collector. NetStream supports real-time traffic sampling, dynamic report generation, traffic attribute analysis, and traffic exception traps. This function help you monitor real-time traffic information and analyze device throughput, so as to make decisions on network structure optimization and capacity expansion.

Comprehensive Security Mechanisms Against Internal and External Security Threats

The S7700 can use an integrated firewall module to provide virtual firewall and multi-instance NAT functions, allowing multiple VPN customers to share the same firewall. The firewall card uses application-specific packet filter (ASPF) to check and filter application-layer packets based on complex rules. The firewall module provides the following security functions:

- Comprehensive network admission control (NAC) solutions for enterprise networks: The S7700 supports MAC address authentication, Portal authentication, 802.1X authentication, and DHCP snooping-triggered authentication. These authentication

methods ensure security of various access modes such as dumb terminal access, mobile access, and centralized IP address allocation.

- Two-level CPU protection mechanism: The S7700 supports CPU hardware queues and separates the data plane from the control plane. This helps defend against DoS attacks and unauthorized access, and prevents control plane overloading.

Integrated AC Module to Provide Wireless Access

The S7700's wireless AC module supports radio frequency (RF) management and allows APs to automatically select their radio channels and power. APs can adjust their power and channels when their signals conflict. The received signal strength indicator (RSSI) and signal-to-noise ratio (SNR) are updated in real time so that the AC can know the radio environment of each wireless user. The RF management function helps improve network availability.

The AC module supports 802.1X authentication, MAC address authentication, Portal authentication, and WLAN authentication and privacy infrastructure (WAPI), providing access authentication for terminals of different types and security levels.

The AC module supports Layer 2 and Layer 3 roaming and allows STAs to rapidly roam between APs. It supports 1+1 and N+1 cold backup between ACs and load balancing among ACs, which improve network reliability.

Innovative Energy-Saving Chip, Allowing Intelligent Power Consumption Control

The S7700 uses innovative energy-saving chips, which can dynamically adjust power on all ports based on traffic volume. An idle port enters the sleeping mode to reduce power consumption. The S7700 supports Power over Ethernet (PoE) and uses different energy management modes depending on the powered device (PD) type, providing flexibility in energy management. The S7700 supports Energy Efficient Ethernet (IEEE 802.3az). Transceivers on line cards can quickly transition to the lower power idle state to reduce power consumption when no traffic is being transmitted.

Related Content

Support Community

[Introduction to Modular Switches](#)

3 Usage Scenarios

About This Chapter

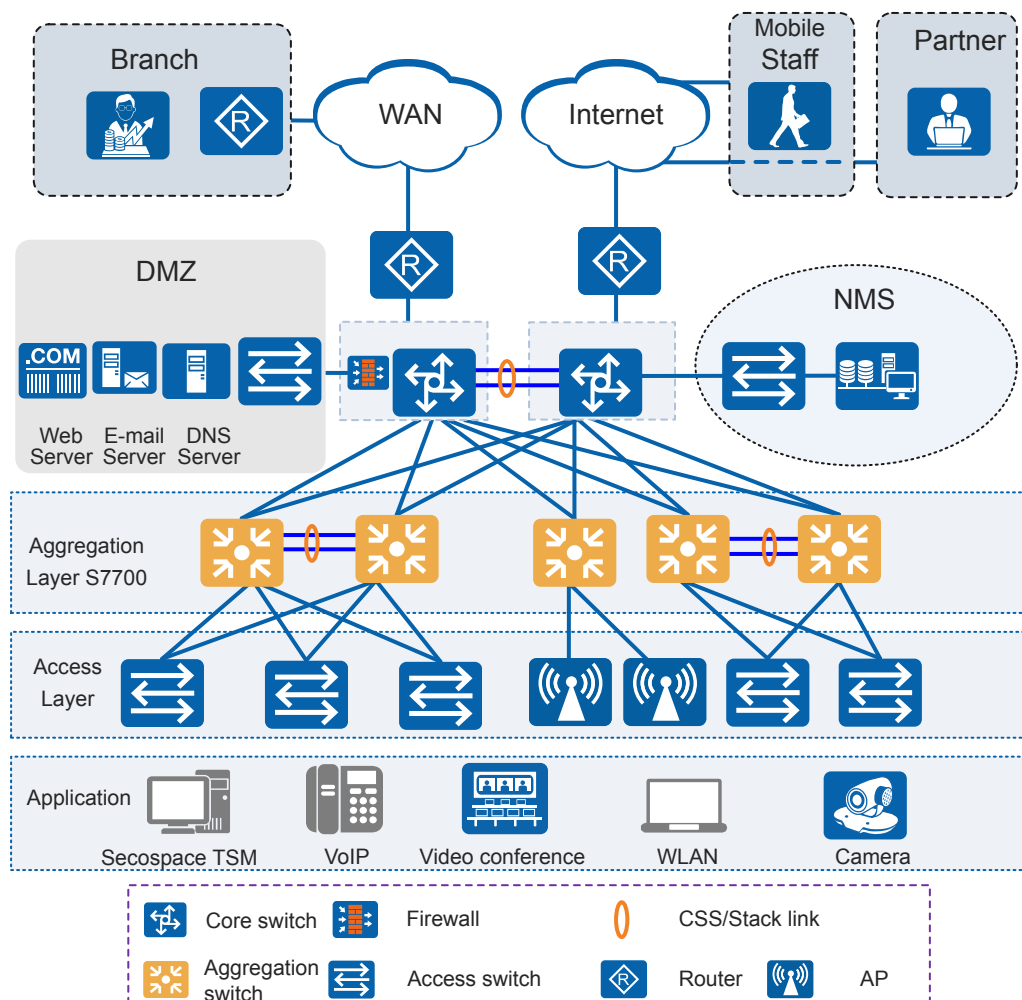
[3.1 Large-scale Enterprise Campus Network](#)

[3.2 Small- or Medium-scale Enterprise Campus Network](#)

3.1 Large-scale Enterprise Campus Network

As shown in [Figure 3-1](#), S7700 switches are deployed at the aggregation layer of a large-scale campus network, creating a highly reliable, scalable, and easy-to-manage enterprise campus network.

Figure 3-1 S7700 in a large-scale enterprise campus network



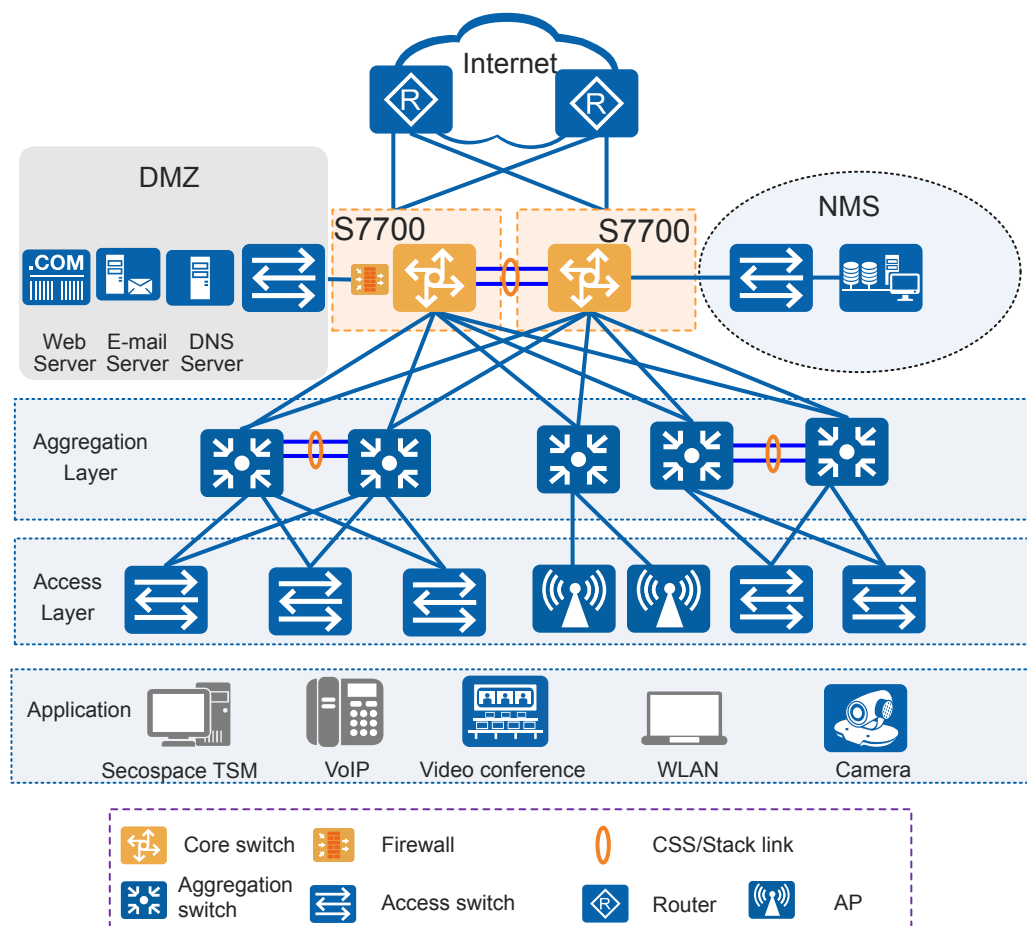
The S7700 switches use innovative cluster switching system (CSS) technology to reduce the data forwarding latency, improve the IT network efficiency, and enhance competitiveness of the enterprise.

The S7700 switches support hardware-based Ethernet OAM/BFD and hardware CPU queues, which enhance network reliability and security.

3.2 Small- or Medium-scale Enterprise Campus Network

As shown in [Figure 3-2](#), the S7700 switches function as core devices in a small- or medium-scale campus network, providing a cost-effective, reliable, and easy-to-deploy network solution.

Figure 3-2 S7700 in a small- or medium-scale enterprise campus network



The S7700 switches use innovative cluster switching system (CSS) technology to reduce the data forwarding latency, improve the IT network efficiency, and enhance competitiveness of the enterprise.

The S7700 switches support reliability technologies such as hardware-based Ethernet OAM and BFD to ensure service continuity.

The S7700's compact chassis and left-to-back airflow design leave more space for cabling, save space in the equipment room, reduce power consumption.

4 Performance Specifications

The features mentioned in the "Introduction", "Product Characteristics", and "Usage Scenarios" sections are not supported on all S7700 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).

5 Product Performance

About This Chapter

[5.1 Product Features Supported by V200R012C00](#)

[5.2 Product Features Supported by V200R011C10](#)

[5.3 Product Features Supported by V200R010C00](#)

[5.4 Product Features Supported by V200R009C00](#)

[5.5 Product Features Supported by V200R008C00](#)

[5.6 Product Features Supported by V200R007C00](#)

[5.7 Product Features Supported by V200R006C00](#)

[5.8 Product Features Supported by V200R005C00](#)

[5.9 Product Features Supported by V200R003C00](#)

5.1 Product Features Supported by V200R012C00

The following table lists features supported by the S7700.

Table 5-1 Features supported by the S7700

Feature		Description
Ethernet features	Ethernet	Full-duplex, half-duplex, and auto-negotiation modes on Ethernet interfaces
		Rates of an Ethernet interface: 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, 10 Gbit/s, 40 Gbit/s, 100 Gbit/s, and auto-negotiation
		Flow control on interfaces
		Jumbo frames
		Link aggregation

Feature		Description
		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
		Broadcast storm suppression
	VLAN	Access modes of access, trunk, hybrid, QinQ, and LNP
		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
		Double VLAN tags insertion based on interfaces
		Super VLAN
		VLAN mapping
		Selective QinQ
		MUX VLAN
		Voice VLAN
		Guest VLAN
	GVRP	Generic Attribute Registration Protocol (GARP)
		GARP VLAN Registration Protocol (GVRP)
	VCMP	VLAN Central Management Protocol (VCMP)
	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
		Configuring MAC address learning priorities for interfaces
		Port bridge
	ARP	Static and dynamic ARP entries
		ARP in a VLAN
		Aging of ARP entries
		Proxy ARP
		ARP entry with multiple outbound interfaces
Ethernet loop protection	MSTP	STP
		RSTP
		MSTP
		BPDU protection, root protection, and loop protection
		TC-BPDU attack defense
		STP loop detection
		VBST
	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
		VRF
		DHCP client
		DHCP server

Feature		Description
		DHCP relay
		URPF check
		Routing policies
		RIPv1/RIPv2
		OSPF
		BGP
		MBGP
		IS-IS
		PBR (redirection in a traffic policy)
	Multicast routing features	IGMPv1/v2/v3
		PIM-DM
		PIM-SM
		MSDP
		Multicast routing policies
		RPF
	IPv6 features	IPv6 protocol stack
		ND and ND snooping
		DHCPv6 snooping
		RIPng
		DHCPv6 server
		DHCPv6 relay
		OSPFv3
		BGP4+, ISIS for IPv6
		VRRP6
		MLDv1 and MLDv2
		PIM-DM for IPv6
		PIM-SM for IPv6
	IP transition technology	4 over 6 tunnel
		6 over 4 tunnel
		6PE

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
MPLS&VPN	Basic MPLS functions	LDP
		Double MPLS labels
		Mapping from DSCP to EXP priorities in MPLS packets
		Mapping from 802.1p priorities to EXP priorities in MPLS packets
	MPLS TE	MPLS TE tunnel
		MPLS TE protection group
	MPLS OAM	LSP ping and LSP traceroute
		Automatic detection of LSP faults
		1+1 protection switchover of LSPs
	VPN	Multi-VPN-Instance CE (MCE)
		VLL in SVC, Martini, CCC, and Kompella modes
		VLL FRR
		VPLS
		MPLS L3VPN
		HVPLS in LSP and QinQ modes
Device reliability	BFD	Basic BFD functions
		BFD for static route/IS-IS/OSPF/BGP
		BFD for PIM
		BFD for VRRP
		BFD for VLL FRR
	CSS	<ul style="list-style-type: none">● Cluster card supporting CSS● Service interface supporting CSS
	Others	VRRP

Feature		Description
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
	OAM association	Association between 802.1ag and 802.3ah
		Association between 802.3ah and 802.1ag
	Y.1731	Delay and variation measurement
QoS features	Traffic classifier	Traffic classification based on ACLs
		Traffic classification based on outer 802.1p priorities, inner VLAN IDs, outer VLAN IDs, source MAC addresses, and Ethernet types
		Traffic classification based on inner 802.1p priorities
	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	Weighted Random Early Detection (WRED)
	Congestion management	Priority Queuing (PQ)
		Weighted Deficit Round Robin (WDRR)
		PQ+WDRR
		Weighted Round Robin (WRR)
		PQ+WRR
	HQoS	Hierarchical Quality of Service

Feature		Description
Configuration and maintenance	Login and configuration management	Command line configuration
		Messages and help information in English and Chinese
		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)
		EasyDeploy (commander)
		Easy deployment and maintenance
		SVF
		Open Programmability System (OPS)
		Open Intelligent Diagnosis System (OIDS)
	File system	File system
		Directory and file management
		File upload and download through FTP, TFTP, SFTP, SCP, and FTPS
	Monitoring and maintenance	Hardware monitoring
		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

Feature		Description
Security	Version upgrade	Device software loading and online software loading
		BootROM online upgrade
		In-service patching
	ARP security	ARP packet rate limiting based on source MAC addresses
		ARP packet rate limiting based on source IP addresses, interfaces, and VLANs, and global ARP packet rate limiting
		ARP anti-spoofing
		Association between ARP and STP
		ARP gateway anti-collision
		Dynamic ARP Inspection (DAI) and Static ARP Inspection (SAI)
		Egress ARP Inspection (EAI)
	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 dynamically limiting the rate of 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 Fraggie attacks and UDP diagnosis port attacks), and ICMP flood attacks
User access and authentication	AAA	Local authentication and authorization
		RADIUS authentication, authorization, and accounting
		HWTACACS authentication, authorization, and accounting
		Destination Address Accounting (DAA)

Feature		Description
	NAC	802.1X authentication
		MAC address authentication
		Portal authentication
		MAC address bypass authentication
		PPP over Ethernet (PPPoE)
	Policy association	Policy association
Network management	-	Ping and traceroute
		NQA
		iPCA
		Network Time Protocol (NTP)
		sFlow
		NetStream
		SNMP v1/v2c/v3
		Standard MIB
		HTTP
		Hypertext Transfer Protocol Secure (HTTPS)
		Remote network monitoring (RMON)
		RMON2
WLAN	-	AP Management Specifications
		Radio Management Specifications
		WLAN Service Management Specifications
		WLAN QoS
		WLAN Security Specifications
		WLAN user management specifications
VXLAN	-	Virtual eXtensible Local Area Network (VXLAN)

5.2 Product Features Supported by V200R011C10

The following table lists features supported by the S7700.

Table 5-2 Features supported by the S7700

Feature		Description
Ethernet features	Ethernet	Full-duplex, half-duplex, and auto-negotiation modes on Ethernet interfaces
		Rates of an Ethernet interface: 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, 10 Gbit/s, 40 Gbit/s, 100 Gbit/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
		Broadcast storm suppression
	VLAN	Access modes of access, trunk, hybrid, QinQ, and LNP
		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
		Double VLAN tags insertion based on interfaces
		Super VLAN
		VLAN mapping
		Selective QinQ
		MUX VLAN
		Voice VLAN
		Guest VLAN
	GVRP	Generic Attribute Registration Protocol (GARP)
		GARP VLAN Registration Protocol (GVRP)

Feature		Description
	VCMP	VLAN Central Management Protocol (VCMP)
	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
		Configuring MAC address learning priorities for interfaces
		Port bridge
	ARP	Static and dynamic ARP entries
		ARP in a VLAN
		Aging of ARP entries
		Proxy ARP
		ARP entry with multiple outbound interfaces
Ethernet loop protection	MSTP	STP
		RSTP
		MSTP
		BPDU protection, root protection, and loop protection
		TC-BPDU attack defense
		STP loop detection
		VBST
	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

Feature		Description
IPv4/IPv6 forwarding	ERPS	G.8032 v1/v2
		Single closed ring
		Subring
	IPv4 and unicast routes	Static IPv4 routes
		VRF
		DHCP client
		DHCP server
		DHCP relay
		URPF check
		Routing policies
		RIPv1/RIPv2
		OSPF
		BGP
		MBGP
		IS-IS
		PBR (redirection in a traffic policy)
	Multicast routing features	IGMPv1/v2/v3
		PIM-DM
		PIM-SM
		MSDP
		Multicast routing policies
		RPF
	IPv6 features	IPv6 protocol stack
		ND and ND snooping
		DHCPv6 snooping
		RIPng
		DHCPv6 server
		DHCPv6 relay
		OSPFv3
		BGP4+, ISIS for IPv6

Feature		Description
		VRRP6
		MLDv1 and MLDv2
		PIM-DM for IPv6
		PIM-SM for IPv6
	IP transition technology	4 over 6 tunnel
		6 over 4 tunnel
		6PE
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
MPLS&VPN	Basic MPLS functions	LDP
		Double MPLS labels
		Mapping from DSCP to EXP priorities in MPLS packets
		Mapping from 802.1p priorities to EXP priorities in MPLS packets
	MPLS TE	MPLS TE tunnel
		MPLS TE protection group
	MPLS OAM	LSP ping and LSP traceroute
		Automatic detection of LSP faults
		1+1 protection switchover of LSPs
	VPN	Multi-VPN-Instance CE (MCE)
		VLL in SVC, Martini, CCC, and Kompella modes
		VLL FRR
		VPLS
		MPLS L3VPN
		HVPLS in LSP and QinQ modes

Feature		Description
Device reliability	BFD	Basic BFD functions
		BFD for static route/IS-IS/OSPF/BGP
		BFD for PIM
		BFD for VRRP
		BFD for VLL FRR
	CSS	<ul style="list-style-type: none"> Cluster card supporting CSS Service interface supporting CSS
	Others	VRRP
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
	OAM association	Association between 802.1ag and 802.3ah
		Association between 802.3ah and 802.1ag
	Y.1731	Delay and variation measurement
QoS features	Traffic classifier	Traffic classification based on ACLs
		Traffic classification based on outer 802.1p priorities, inner VLAN IDs, outer VLAN IDs, source MAC addresses, and Ethernet types
		Traffic classification based on inner 802.1p priorities
	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

Feature		Description
	Congestion avoidance	Weighted Random Early Detection (WRED)
	Congestion management	Priority Queuing (PQ)
		Weighted Deficit Round Robin (WDRR)
		PQ+WDRR
		Weighted Round Robin (WRR)
		PQ+WRR
	HQoS	Hierarchical Quality of Service
Configuration and maintenance	Login and configuration management	Command line configuration
		Messages and help information in English and Chinese
		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)
		EasyDeploy (commander)
		Easy deployment and maintenance
		SVF
	File system	File system
		Directory and file management
		File upload and download through FTP, TFTP, SFTP, SCP, and FTPS
	Monitoring and maintenance	Hardware monitoring
		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	ARP security	ARP packet rate limiting based on source MAC addresses
		ARP packet rate limiting based on source IP addresses, interfaces, and VLANs, and global ARP packet rate limiting
		ARP anti-spoofing
		Association between ARP and STP
		ARP gateway anti-collision
		Dynamic ARP Inspection (DAI) and Static ARP Inspection (SAI)
		Egress ARP Inspection (EAI)
	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 dynamically limiting the rate of 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

Feature		Description
		Defense against TCP SYN flood attacks, UDP flood attacks (including Fraggle attacks and UDP diagnosis port attacks), and ICMP flood attacks
User access and authentication	AAA	Local authentication and authorization
		RADIUS authentication, authorization, and accounting
		HWTACACS authentication, authorization, and accounting
		Destination Address Accounting (DAA)
	NAC	802.1X authentication
		MAC address authentication
		Portal authentication
		MAC address bypass authentication
		PPP over Ethernet (PPPoE)
	Policy association	Policy association
Network management	-	Ping and traceroute
		NQA
		iPCA
		Network Time Protocol (NTP)
		sFlow
		NetStream
		SNMP v1/v2c/v3
		Standard MIB
		HTTP
		Hypertext Transfer Protocol Secure (HTTPS)
		Remote network monitoring (RMON)
		RMON2
WLAN	-	AP Management Specifications
		Radio Management Specifications
		WLAN Service Management Specifications
		WLAN QoS
		WLAN Security Specifications

Feature		Description
		WLAN user management specifications
VXLAN	-	Virtual eXtensible Local Area Network (VXLAN)

5.3 Product Features Supported by V200R010C00

The following table lists the features supported by the S7700.

Table 5-3 Features supported by the S7700

Feature		Description
Ethernet features	Ethernet	Operating modes of full-duplex, half-duplex, and auto-negotiation
		Rates of an Ethernet interface: 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, 10 Gbit/s, 40 Gbit/s, 100 Gbit/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
		Broadcast storm suppression
	VLAN	Access modes of access, trunk, hybrid, QinQ, and LNP
		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
		Double VLAN tags insertion based on interfaces
		Super VLAN

Feature		Description
		VLAN mapping
		Selective QinQ
		MUX VLAN
		Voice VLAN
		Guest VLAN
	GVRP	Generic Attribute Registration Protocol (GARP)
		GARP VLAN Registration Protocol (GVRP)
	VCMP	VLAN Central Management Protocol (VCMP)
	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
		Configuring MAC address learning priorities for interfaces
		Port bridge
	ARP	Static and dynamic ARP entries
		ARP in a VLAN
		Aging of ARP entries
		Proxy ARP
		ARP entry with multiple outbound interfaces
Ethernet loop protection	MSTP	STP
		RSTP
		MSTP
		BPDU protection, root protection, and loop protection
		TC-BPDU attack defense
		STP loop detection
		VBST
	Loopback-detect	Loop detection on an interface

Feature		Description
	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
		VRF
		DHCP client
		DHCP server
		DHCP relay
		URPF check
		Routing policies
		RIPv1/RIPv2
		OSPF
		BGP
		MBGP
		IS-IS
		PBR (redirection in a traffic policy)
	Multicast routing features	IGMPv1/v2/v3
		PIM-DM
		PIM-SM
		MSDP
		Multicast routing policies
		RPF

Feature		Description
	IPv6 features	IPv6 protocol stack
		ND and ND snooping
		DHCPv6 snooping
		RIPng
		DHCPv6 server
		DHCPv6 relay
		OSPFv3
		BGP4+, ISIS for IPv6
		VRRP6
		MLDv1 and MLDv2
		PIM-DM for IPv6
		PIM-SM for IPv6
	IP transition technology	4 over 6 tunnel
		6 over 4 tunnel
		6PE
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
MPLS&V PN	Basic MPLS functions	LDP
		Double MPLS labels
		Mapping from DSCP to EXP priorities in MPLS packets
		Mapping from 802.1p priorities to EXP priorities in MPLS packets
	MPLS TE	MPLS TE tunnel
		MPLS TE protection group
	MPLS OAM	LSP ping and LSP traceroute

Feature		Description
		Automatic detection of LSP faults
		1+1 protection switchover of LSPs
	VPN	Multi-VPN-Instance CE (MCE)
		VLL in SVC, Martini, CCC, and Kompella modes
		VLL FRR
		VPLS
		MPLS L3VPN
		HVPLS in LSP and QinQ modes
Device reliability	BFD	Basic BFD functions
		BFD for static route/IS-IS/OSPF/BGP
		BFD for PIM
		BFD for VRRP
		BFD for VLL FRR
	CSS	<ul style="list-style-type: none">● Cluster card supporting CSS● Service interface supporting CSS
Ethernet OAM	Others	VRRP
	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
	OAM association	Association between 802.1ag and 802.3ah
		Association between 802.3ah and 802.1ag
QoS features	Traffic classifier	Delay and variation measurement
		Traffic classification based on ACLs
		Traffic classification based on outer 802.1p priorities, inner VLAN IDs, outer VLAN IDs, source MAC addresses, and Ethernet types
		Traffic classification based on inner 802.1p priorities

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	Weighted Random Early Detection (WRED)
	Congestion management	Priority Queuing (PQ)
		Weighted Deficit Round Robin (WDRR)
		PQ+WDRR
		Weighted Round Robin (WRR)
		PQ+WRR
	HQoS	Hierarchical Quality of Service
Configuration and maintenance	Login and configuration management	Command line configuration
		Messages and help information in English and Chinese
		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)
		EasyDeploy (commander)
		Easy deployment and maintenance
		SVF
	File system	File system
		Directory and file management

Feature		Description
		File upload and download through FTP, TFTP, SFTP, SCP, and FTPS
	Monitoring and maintenance	Hardware monitoring
		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	ARP security	ARP packet rate limiting based on source MAC addresses
		ARP packet rate limiting based on source IP addresses, interfaces, and VLANs, and global ARP packet rate limiting
		ARP anti-spoofing
		Association between ARP and STP
		ARP gateway anti-collision
		Dynamic ARP Inspection (DAI) and Static ARP Inspection (SAI)
		Egress ARP Inspection (EAI)
	IP security	ICMP attack defense
		IP source guard
	Local attack defense	CPU attack defense
	MFF	MAC-Forced Forwarding (MFF)

Feature		Description
	DHCP Snooping	DHCP snooping
		Option 82 function and dynamically limiting the rate of 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
User access and authentication	AAA	Local authentication and authorization
		RADIUS authentication, authorization, and accounting
		HWTACACS authentication, authorization, and accounting
		Destination Address Accounting (DAA)
	NAC	802.1X authentication
		MAC address authentication
		Portal authentication
		MAC address bypass authentication
		PPP over Ethernet (PPPoE)
	Policy association	Policy association
Network management	-	Ping and traceroute
		NQA
		iPCA
		Network Time Protocol (NTP)
		sFlow
		NetStream
		SNMP v1/v2c/v3
		Standard MIB
		HTTP

Feature		Description
		Hypertext Transfer Protocol Secure (HTTPS)
		Remote network monitoring (RMON)
		RMON2
WLAN	-	AP Management Specifications
		Radio Management Specifications
		WLAN Service Management Specifications
		WLAN QoS
		WLAN Security Specifications
		WLAN user management specifications

5.4 Product Features Supported by V200R009C00

The following table lists the features supported by the S7700.

Table 5-4 Features supported by the S7700

Feature		Description
Ethernet features	Ethernet	Operating modes of full-duplex, half-duplex, and auto-negotiation
		Rates of an Ethernet interface: 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, 10 Gbit/s, 40 Gbit/s, 100 Gbit/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
		Broadcast storm suppression
	VLAN	Access modes of access, trunk, hybrid, QinQ, and LNP

Feature		Description
		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
		Double VLAN tags insertion based on interfaces
		Super VLAN
		VLAN mapping
		Selective QinQ
		MUX VLAN
		Voice VLAN
		Guest VLAN
	GVRP	Generic Attribute Registration Protocol (GARP)
		GARP VLAN Registration Protocol (GVRP)
	VCMP	VLAN Central Management Protocol (VCMP)
	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
		Configuring MAC address learning priorities for interfaces
		Port bridge
	ARP	Static and dynamic ARP entries
		ARP in a VLAN
		Aging of ARP entries
		Proxy ARP
		ARP entry with multiple outbound interfaces
Ethernet loop protection	MSTP	STP
		RSTP

Feature		Description
		MSTP
		BPDU protection, root protection, and loop protection
		TC-BPDU attack defense
		STP loop detection
		VBST
	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	Static IPv4 routes
		VRF
		DHCP client
		DHCP server
		DHCP relay
		URPF check
		Routing policies
		RIPv1/RIPv2
		OSPF
		BGP
		MBGP
		IS-IS
		PBR (redirection in a traffic policy)

Feature		Description
	Multicast routing features	IGMPv1/v2/v3
		PIM-DM
		PIM-SM
		MSDP
		Multicast routing policies
		RPF
	IPv6 features	IPv6 protocol stack
		ND and ND snooping
		DHCPv6 snooping
		RIPng
		DHCPv6 server
		DHCPv6 relay
		OSPFv3
		BGP4+, ISIS for IPv6
		VRRP6
		MLDv1 and MLDv2
		PIM-DM for IPv6
		PIM-SM for IPv6
	IP transition technology	4 over 6 tunnel
		6 over 4 tunnel
		6PE
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
MPLS&V PN	Basic MPLS functions	LDP
		Double MPLS labels

Feature		Description
		Mapping from DSCP to EXP priorities in MPLS packets
		Mapping from 802.1p priorities to EXP priorities in MPLS packets
	MPLS TE	MPLS TE tunnel
		MPLS TE protection group
	MPLS OAM	LSP ping and LSP traceroute
		Automatic detection of LSP faults
		1+1 protection switchover of LSPs
	VPN	Multi-VPN-Instance CE (MCE)
		VLL in SVC, Martini, CCC, and Kompella modes
		VLL FRR
		VPLS
		MPLS L3VPN
		HVPLS in LSP and QinQ modes
Device reliability	BFD	Basic BFD functions
		BFD for static route/IS-IS/OSPF/BGP
		BFD for PIM
		BFD for VRRP
		BFD for VLL FRR
	CSS	<ul style="list-style-type: none"> Cluster card supporting CSS Service interface supporting CSS
	Others	VRRP
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
	OAM association	Association between 802.1ag and 802.3ah
		Association between 802.3ah and 802.1ag

Feature		Description
	Y.1731	Delay and variation measurement
QoS features	Traffic classifier	Traffic classification based on ACLs
		Traffic classification based on outer 802.1p priorities, inner VLAN IDs, outer VLAN IDs, source MAC addresses, and Ethernet types
		Traffic classification based on inner 802.1p priorities
	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	Weighted Random Early Detection (WRED)
	Congestion management	Priority Queuing (PQ)
		Weighted Deficit Round Robin (WDRR)
		PQ+WDRR
		Weighted Round Robin (WRR)
		PQ+WRR
	HQoS	Hierarchical Quality of Service
Configuration and maintenance	Login and configuration management	Command line configuration
		Messages and help information in English and Chinese
		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
		EasyDeploy (commander)
		Easy deployment and maintenance
		SVF
	File system	File system
		Directory and file management
		File upload and download through FTP, TFTP, SFTP, SCP, and FTPS
	Monitoring and maintenance	Hardware monitoring
		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	ARP security	ARP packet rate limiting based on source MAC addresses
		ARP packet rate limiting based on source IP addresses, interfaces, and VLANs, and global ARP packet rate limiting
		ARP anti-spoofing
		Association between ARP and STP
		ARP gateway anti-collision
		Dynamic ARP Inspection (DAI) and Static ARP Inspection (SAI)
		Egress ARP Inspection (EAI)

Feature		Description
	IP security	ICMP attack defense
		IP source guard
	Local attack defense	CPU attack defense
	MTF	MAC-Forced Forwarding (MTF)
	DHCP Snooping	DHCP snooping
		Option 82 function and dynamically limiting the rate of 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
	User access and authentication	AAA
		NAC
		Policy association
Network management	-	Ping and traceroute
		NQA
		iPCA
		Network Time Protocol (NTP)

Feature		Description
		sFlow
		NetStream
		SNMP v1/v2c/v3
		Standard MIB
		HTTP
		Hypertext Transfer Protocol Secure (HTTPS)
		Remote network monitoring (RMON)
		RMON2
WLAN	-	AP Management Specifications
		Radio Management Specifications
		WLAN Service Management Specifications
		WLAN QoS
		WLAN Security Specifications
		WLAN user management specifications

5.5 Product Features Supported by V200R008C00

The following table lists the features supported by the S7700.

Table 5-5 Features supported by the S7700

Feature		Description
Ethernet features	Ethernet	Operating modes of full-duplex, half-duplex, and auto-negotiation
		Rates of an Ethernet interface: 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, 10 Gbit/s, 40 Gbit/s, 100 Gbit/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)

Feature		Description
		Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)
		Interface isolation
		Broadcast storm suppression
	VLAN	Access modes of access, trunk, hybrid, QinQ, and LNP
		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
		Double VLAN tags insertion based on interfaces
		Super VLAN
		VLAN mapping
		Selective QinQ
		MUX VLAN
		Voice VLAN
		Guest VLAN
	GVRP	Generic Attribute Registration Protocol (GARP)
		GARP VLAN Registration Protocol (GVRP)
	VCMP	VLAN Central Management Protocol (VCMP)
	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
		Configuring MAC address learning priorities for interfaces
		Port bridge
	ARP	Static and dynamic ARP entries
		ARP in a VLAN

Feature		Description
		Aging of ARP entries
		Proxy ARP
		ARP entry with multiple outbound interfaces
Ethernet loop protection	MSTP	STP
		RSTP
		MSTP
		BPDU protection, root protection, and loop protection
		TC-BPDU attack defense
		STP loop detection
		VBST
	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
		VRF
		DHCP client
		DHCP server
		DHCP relay
		URPF check
		Routing policies
		RIPv1/RIPv2

Feature		Description
		OSPF
		BGP
		MBGP
		IS-IS
		PBR (redirection in a traffic policy)
	Multicast routing features	IGMPv1/v2/v3
		PIM-DM
		PIM-SM
		MSDP
		Multicast routing policies
		RPF
	IPv6 features	IPv6 protocol stack
		ND and ND snooping
		DHCPv6 snooping
		RIPng
		DHCPv6 server
		DHCPv6 relay
		OSPFv3
		BGP4+, ISIS for IPv6
		VRRP6
		MLDv1 and MLDv2
		PIM-DM for IPv6
		PIM-SM for IPv6
	IP transition technology	4 over 6 tunnel
		6 over 4 tunnel
		6PE
Layer 2 multicast features	-	IGMPv1/v2/v3 snooping
		Fast leave
		IGMP snooping proxy
		MLD snooping

Feature		Description
MPLS&VPN		Interface-based multicast traffic suppression
		Inter-VLAN multicast replication
		Controllable multicast
	Basic MPLS functions	LDP
		Double MPLS labels
		Mapping from DSCP to EXP priorities in MPLS packets
		Mapping from 802.1p priorities to EXP priorities in MPLS packets
	MPLS TE	MPLS TE tunnel
		MPLS TE protection group
	MPLS OAM	LSP ping and LSP traceroute
		Automatic detection of LSP faults
		1+1 protection switchover of LSPs
	VPN	Multi-VPN-Instance CE (MCE)
		VLL in SVC, Martini, CCC, and Kompella modes
		VLL FRR
		VPLS
		MPLS L3VPN
		HVPLS in LSP and QinQ modes
Device reliability	BFD	Basic BFD functions
		BFD for static route/IS-IS/OSPF/BGP
		BFD for PIM
		BFD for VRRP
		BFD for VLL FRR
	CSS	<ul style="list-style-type: none"> Cluster card supporting CSS Service interface supporting CSS
	Others	VRRP
Ethernet OAM	EFM OAM (802.3ah)	Automatic discovery
		Link fault detection
		Link fault troubleshooting
		Remote loopback

Feature		Description
	CFM OAM (802.1ag)	Software-level CCM
		MAC ping
		MAC trace
	OAM association	Association between 802.1ag and 802.3ah
		Association between 802.3ah and 802.1ag
	Y.1731	Delay and variation measurement
QoS features	Traffic classifier	Traffic classification based on ACLs
		Traffic classification based on outer 802.1p priorities, inner VLAN IDs, outer VLAN IDs, source MAC addresses, and Ethernet types
		Traffic classification based on inner 802.1p priorities
	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	Weighted Random Early Detection (WRED)
	Congestion management	Priority Queuing (PQ)
		Deficit Round Robin (DRR)
		PQ+DRR
		Weighted Round Robin (WRR)
		PQ+WRR
	HQoS	Hierarchical Quality of Service
Configuration and maintenance	Login and configuration management	Command line configuration
		Messages and help information in English and Chinese
		Login through console and Telnet terminals
		SSH1.5/SSH2

Feature		Description
		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)
		EasyDeploy (commander)
		Easy deployment and maintenance
		SVF
	File system	File system
		Directory and file management
		File upload and download through FTP, TFTP, SFTP, SCP, and FTPS
	Monitoring and maintenance	Hardware monitoring
		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	ARP security	ARP packet rate limiting based on source MAC addresses
		ARP packet rate limiting based on source IP addresses, interfaces, and VLANs, and global ARP packet rate limiting

Feature		Description
		ARP anti-spoofing
		Association between ARP and STP
		ARP gateway anti-collision
		Dynamic ARP Inspection (DAI) and Static ARP Inspection (SAI)
		Egress ARP Inspection (EAI)
	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 dynamically limiting the rate of 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
User access and authentication	AAA	Local authentication and authorization
		RADIUS authentication, authorization, and accounting
		HWTACACS authentication, authorization, and accounting
		Destination Address Accounting (DAA)
	NAC	802.1X authentication
		MAC address authentication
		Portal authentication
		MAC address bypass authentication
		PPP over Ethernet (PPPoE)

Feature		Description
	Policy association	Policy association
Network management	-	Ping and traceroute
		NQA
		iPCA
		Network Time Protocol (NTP)
		sFlow
		NetStream
		SNMP v1/v2c/v3
		Standard MIB
		HTTP
		Hypertext Transfer Protocol Secure (HTTPS)
		Remote network monitoring (RMON)
		RMON2
WLAN	-	AP Management Specifications
		Radio Management Specifications
		WLAN Service Management Specifications
		WLAN QoS
		WLAN Security Specifications
		WLAN user management specifications

5.6 Product Features Supported by V200R007C00

The following table lists the features supported by the S7700.

NOTE

Features marked with * are added in V200R007C00.

Table 5-6 Features supported by the S7700

Feature		Description
Ethernet features	Ethernet	Operating modes of full-duplex, half-duplex, and auto-negotiation

Feature		Description
		Rates of an Ethernet interface: 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, 10 Gbit/s, 40 Gbit/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
		Broadcast storm suppression
	VLAN	Access modes of access, trunk, hybrid, QinQ, and LNP
		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● DHCP policies
		Double VLAN tags insertion based on interfaces
		Super VLAN
		VLAN mapping
		Selective QinQ
		MUX VLAN
		Voice VLAN
		Guest VLAN
	GVRP	Generic Attribute Registration Protocol (GARP)
		GARP VLAN Registration Protocol (GVRP)
	VCMP	VLAN Central Management Protocol (VCMP)
	MAC	Automatic learning and aging of MAC addresses

Feature		Description
		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
		Configuring MAC address learning priorities for interfaces
		Port bridge
	ARP	Static and dynamic ARP entries
		ARP in a VLAN
		Aging of ARP entries
		Proxy ARP
		ARP entry with multiple outbound interfaces
Ethernet loop protection	MSTP	STP
		RSTP
		MSTP
		BPDU protection, root protection, and loop protection
		TC-BPDU attack defense
		STP loop detection
		VBST
	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

Feature		Description
		Subring
IPv4/IPv6 forwarding	IPv4 and unicast routes	Static IPv4 routes
		VRF
		DHCP client
		DHCP server
		DHCP relay
		URPF check
		Routing policies
		RIPv1/RIPv2
		OSPF
		BGP
		MBGP
		IS-IS
		PBR (redirection in a traffic policy)
	Multicast routing features	IGMPv1/v2/v3
		PIM-DM
		PIM-SM
		MSDP
		Multicast routing policies
		RPF
	IPv6 features	IPv6 protocol stack
		ND and ND snooping
		DHCPv6 snooping
		RIPng
		DHCPv6 server
		DHCPv6 relay
		OSPFv3
		BGP4+, ISIS for IPv6
		VRRP6
		MLDv1 and MLDv2

Feature		Description
		PIM-DM for IPv6
		PIM-SM for IPv6
	IP transition technology	4 over 6 tunnel
		6 over 4 tunnel
		6PE
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
MPLS&VPN	Basic MPLS functions	LDP
		Double MPLS labels
		Mapping from DSCP to EXP priorities in MPLS packets
		Mapping from 802.1p priorities to EXP priorities in MPLS packets
	MPLS TE	MPLS TE tunnel
		MPLS TE protection group
	MPLS OAM	LSP ping and LSP traceroute
		Automatic detection of LSP faults
		1+1 protection switchover of LSPs
	VPN	Multi-VPN-Instance CE (MCE)
		VLL in SVC, Martini, CCC, and Kompella modes
		VLL FRR
		VPLS
		MPLS L3VPN
		HVPLS in LSP and QinQ modes
Device reliability	BFD	Basic BFD functions
		BFD for static route/IS-IS/OSPF/BGP

Feature		Description
		BFD for PIM
		BFD for VRRP
		BFD for VLL FRR
	CSS	<ul style="list-style-type: none"> Cluster card supporting CSS Service interface supporting CSS
	Others	VRRP
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
	OAM association	Association between 802.1ag and 802.3ah
		Association between 802.3ah and 802.1ag
	Y.1731	Delay and variation measurement
QoS features	Traffic classifier	Traffic classification based on ACLs
		Traffic classification based on outer 802.1p priorities, inner VLAN IDs, outer VLAN IDs, source MAC addresses, and Ethernet types
		Traffic classification based on inner 802.1p priorities
	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	Weighted Random Early Detection (WRED)
	Congestion management	Priority Queuing (PQ)

Feature		Description
		Deficit Round Robin (DRR)
		PQ+DRR
		Weighted Round Robin (WRR)
		PQ+WRR
	HQoS	Hierarchical Quality of Service
Configuration and maintenance	Login and configuration management	Command line configuration
		Messages and help information in English and Chinese
		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)
		EasyDeploy (commander)
		Easy deployment and maintenance
		SVF*
	File system	File system
		Directory and file management
		File upload and download through FTP, TFTP, SFTP, SCP, and FTPS
	Monitoring and maintenance	Hardware monitoring
		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

Feature		Description
		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	ARP security	ARP packet rate limiting based on source MAC addresses
		ARP packet rate limiting based on source IP addresses, interfaces, and VLANs, and global ARP packet rate limiting
		ARP anti-spoofing
		Association between ARP and STP
		ARP gateway anti-collision
		Dynamic ARP Inspection (DAI) and Static ARP Inspection (SAI)
		Egress ARP Inspection (EAI)
	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 dynamically limiting the rate of 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
User access and authentication	AAA	Local authentication and authorization
		RADIUS authentication, authorization, and accounting
		HWTACACS authentication, authorization, and accounting
		Destination Address Accounting (DAA)
	NAC	802.1X authentication
		MAC address authentication
		Portal authentication
		MAC address bypass authentication
		PPP over Ethernet (PPPoE)
	Policy association	Policy association
Network management	-	Ping and traceroute
		NQA
		iPCA
		Network Time Protocol (NTP)
		sFlow
		NetStream
		NAT (SPU)
		Load Balance (SPU)
		SNMP v1/v2c/v3
		Standard MIB
		HTTP
		Hypertext Transfer Protocol Secure (HTTPS)
		Remote network monitoring (RMON)
		RMON2
WLAN	-	AP Management Specifications
		Radio Management Specifications
		WLAN Service Management Specifications
		WLAN QoS
		WLAN Security Specifications

Feature		Description
		WLAN user management specifications

5.7 Product Features Supported by V200R006C00

The following table lists the features supported by the S7700.

Table 5-7 Features supported by the S7700

Feature		Description
Ethernet features	Ethernet	Operating modes of full-duplex, half-duplex, and auto-negotiation
		Rates of an Ethernet interface: 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, 10 Gbit/s, 40 Gbit/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
		Broadcast storm suppression
	VLAN	Access modes of access, trunk, hybrid, QinQ, and LNP
		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● DHCP policies
		Double VLAN tags insertion based on interfaces
		Super VLAN

Feature		Description
		VLAN mapping
		Selective QinQ
		MUX VLAN
		Voice VLAN
		Guest VLAN
	GVRP	Generic Attribute Registration Protocol (GARP)
		GARP VLAN Registration Protocol (GVRP)
	VCMP	VLAN Central Management Protocol (VCMP)
	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
		Configuring MAC address learning priorities for interfaces
		Port bridge
	ARP	Static and dynamic ARP entries
		ARP in a VLAN
		Aging of ARP entries
		Proxy ARP
		ARP entry with multiple outbound interfaces
Ethernet loop protection	MSTP	STP
		RSTP
		MSTP
		BPDU protection, root protection, and loop protection
		TC-BPDU attack defense
		STP loop detection
		VBST
	Loopback-detect	Loop detection on an interface

Feature		Description
	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
		VRF
		DHCP client
		DHCP server
		DHCP relay
		URPF check
		Routing policies
		RIPv1/RIPv2
		OSPF
		BGP
		MBGP
		IS-IS
		PBR (redirection in a traffic policy)
	Multicast routing features	IGMPv1/v2/v3
		PIM-DM
		PIM-SM
		MSDP
		Multicast routing policies
		RPF

Feature		Description
	IPv6 features	IPv6 protocol stack
		ND and ND snooping
		DHCPv6 snooping
		RIPng
		DHCPv6 server
		DHCPv6 relay
		OSPFv3
		BGP4+, ISIS for IPv6
		VRRP6
		MLDv1 and MLDv2
		PIM-DM for IPv6
		PIM-SM for IPv6
	IP transition technology	4 over 6 tunnel
		6 over 4 tunnel
		6PE
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
MPLS&V PN	Basic MPLS functions	LDP
		Double MPLS labels
		Mapping from DSCP to EXP priorities in MPLS packets
		Mapping from 802.1p priorities to EXP priorities in MPLS packets
	MPLS TE	MPLS TE tunnel
		MPLS TE protection group
	MPLS OAM	LSP ping and LSP traceroute

Feature		Description
		Automatic detection of LSP faults
		1+1 protection switchover of LSPs
	VPN	Multi-VPN-Instance CE (MCE)
		VLL in SVC, Martini, CCC, and Kompella modes
		VLL FRR
		VPLS
		MPLS L3VPN
		HVPLS in LSP and QinQ modes
Device reliability	BFD	Basic BFD functions
		BFD for static route/IS-IS/OSPF/BGP
		BFD for PIM
		BFD for VRRP
		BFD for VLL FRR
	CSS	<ul style="list-style-type: none">● Cluster card supporting CSS● Service interface supporting CSS
Ethernet OAM	Others	VRRP
	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
	OAM association	Association between 802.1ag and 802.3ah
		Association between 802.3ah and 802.1ag
	Y.1731	Delay and variation measurement
QoS features	Traffic classifier	Traffic classification based on ACLs
		Traffic classification based on outer 802.1p priorities, inner VLAN IDs, outer VLAN IDs, source MAC addresses, and Ethernet types
		Traffic classification based on inner 802.1p priorities

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	Weighted Random Early Detection (WRED)
	Congestion management	Priority Queuing (PQ)
		Deficit Round Robin (DRR)
		PQ+DRR
		Weighted Round Robin (WRR)
		PQ+WRR
	HQoS	Hierarchical Quality of Service
Configuration and maintenance	Login and configuration management	Command line configuration
		Messages and help information in English and Chinese
		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)
		EasyDeploy (commander)
		Easy deployment and maintenance
	File system	File system
		Directory and file management
		File upload and download through FTP, TFTP, SFTP, SCP, and FTPS

Feature		Description
	Monitoring and maintenance	Hardware monitoring
		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
		Destination Address Accounting (DAA)
	NAC	802.1X authentication
		MAC address authentication
		Portal authentication
		MAC address bypass authentication
		PPP over Ethernet (PPPoE)
	ARP security	ARP packet rate limiting based on source MAC addresses
		ARP packet rate limiting based on source IP addresses, interfaces, and VLANs, and global ARP packet rate limiting
		ARP anti-spoofing
		Association between ARP and STP
		ARP gateway anti-collision

Feature		Description
		Dynamic ARP Inspection (DAI) and Static ARP Inspection (SAI)
		Egress ARP Inspection (EAI)
	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 dynamically limiting the rate of 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
		iPCA
		Network Time Protocol (NTP)
		sFlow
		NetStream
		NAT (SPU)
		Load Balance (SPU)
		SNMP v1/v2c/v3
		Standard MIB
		HTTP
		Hypertext Transfer Protocol Secure (HTTPS)

Feature		Description
		Remote network monitoring (RMON)
		RMON2
WLAN	-	AP Management Specifications
		Radio Management Specifications
		WLAN Service Management Specifications
		WLAN QoS
		WLAN Security Specifications
		WLAN user management specifications

5.8 Product Features Supported by V200R005C00

The following table lists the features supported by the S7700.

NOTE

Features marked with * are added in V200R005C00.

Table 5-8 Features supported by the S7700

Feature		Description
Ethernet features	Ethernet	Operating modes of full-duplex, half-duplex, and auto-negotiation
		Rates of an Ethernet interface: 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, 10 Gbit/s, 40 Gbit/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
		Broadcast storm suppression

Feature		Description
	VLAN	Access modes of access, trunk, hybrid, QinQ, and LNP*
		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 ● DHCP policies
		Double VLAN tags insertion based on interfaces
		Super VLAN
		VLAN mapping
		Selective QinQ
		MUX VLAN
		Voice VLAN
		Guest VLAN
	GVRP	Generic Attribute Registration Protocol (GARP)
		GARP VLAN Registration Protocol (GVRP)
	VCMP*	VLAN Central Management Protocol (VCMP)
	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
		Configuring MAC address learning priorities for interfaces
		Port bridge
	ARP	Static and dynamic ARP entries
		ARP in a VLAN
		Aging of ARP entries
		Proxy ARP
		ARP entry with multiple outbound interfaces

Feature		Description
Ethernet loop protection	MSTP	STP
		RSTP
		MSTP
		BPDU protection, root protection, and loop protection
		TC-BPDU attack defense
		STP loop detection
		VBST*
	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
		VRF
		DHCP client
		DHCP server
		DHCP relay
		URPF check
		Routing policies
		RIPv1/RIPv2
		OSPF
		BGP
		MBGP

Feature		Description
		IS-IS
		PBR (redirection in a traffic policy)
	Multicast routing features	IGMPv1/v2/v3
		PIM-DM
		PIM-SM
		MSDP
		Multicast routing policies
		RPF
	IPv6 features	IPv6 protocol stack
		ND and ND snooping
		DHCPv6 snooping
		RIPng
		DHCPv6 server
		DHCPv6 relay
		OSPFv3
		BGP4+, ISIS for IPv6
		VRRP6
		MLDv1 and MLDv2
		PIM-DM for IPv6
		PIM-SM for IPv6
	IP transition technology	4 over 6 tunnel
		6 over 4 tunnel
		6PE
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
MPLS&VPN	Basic MPLS functions	LDP
		Double MPLS labels
		Mapping from DSCP to EXP priorities in MPLS packets
		Mapping from 802.1p priorities to EXP priorities in MPLS packets
	MPLS TE	MPLS TE tunnel
		MPLS TE protection group
	MPLS OAM	LSP ping and LSP traceroute
		Automatic detection of LSP faults
		1+1 protection switchover of LSPs
	VPN	Multi-VPN-Instance CE (MCE)
		VLL in SVC, Martini, CCC, and Kompella modes
		VLL FRR
		VPLS
		MPLS L3VPN
		HVPLS in LSP and QinQ modes
Device reliability	BFD	Basic BFD functions
		BFD for static route/IS-IS/OSPF/BGP
		BFD for PIM
		BFD for VRRP
		BFD for VLL FRR
	CSS	<ul style="list-style-type: none"> Cluster card supporting CSS Service interface supporting CSS
	Others	VRRP
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

Feature		Description
	OAM association	Association between 802.1ag and 802.3ah
		Association between 802.3ah and 802.1ag
	Y.1731	Delay and variation measurement
QoS features	Traffic classifier	Traffic classification based on ACLs
		Traffic classification based on outer 802.1p priorities, inner VLAN IDs, outer VLAN IDs, source MAC addresses, and Ethernet types
		Traffic classification based on inner 802.1p priorities
	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	Weighted Random Early Detection (WRED)
	Congestion management	Priority Queuing (PQ)
		Deficit Round Robin (DRR)
		PQ+DRR
		Weighted Round Robin (WRR)
		PQ+WRR
	HQoS*	Hierarchical Quality of Service
Configuration and maintenance	Login and configuration management	Command line configuration
		Messages and help information in English and Chinese
		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)

Feature		Description
		Web page-based configuration and management
		EasyDeploy (client)
		EasyDeploy (commander)
		Easy deployment and maintenance
	File system	File system
		Directory and file management
		File upload and download through FTP, TFTP, SFTP, SCP, and FTPS
	Monitoring and maintenance	Hardware monitoring
		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
		Destination Address Accounting (DAA*)
	NAC	802.1X authentication
		MAC address authentication
		Portal authentication

Feature		Description
		MAC address bypass authentication
		PPP over Ethernet (PPPoE*)
	ARP security	ARP packet rate limiting based on source MAC addresses
		ARP packet rate limiting based on source IP addresses, interfaces, and VLANs, and global ARP packet rate limiting
		ARP anti-spoofing
		Association between ARP and STP
		ARP gateway anti-collision
		Dynamic ARP Inspection (DAI) and Static ARP Inspection (SAI)
		Egress ARP Inspection (EAI)
	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 dynamically limiting the rate of 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
		iPCA*
		Network Time Protocol (NTP)
		sFlow

Feature		Description
		NetStream
		NAT (SPU)
		Load Balance (SPU)
		SNMP v1/v2c/v3
		Standard MIB
		HTTP
		Hypertext Transfer Protocol Secure (HTTPS)
		Remote network monitoring (RMON)
		RMON2
WLAN*	-	AP Management Specifications
		Radio Management Specifications
		WLAN Service Management Specifications
		WLAN QoS
		WLAN Security Specifications
		WLAN user management specifications

5.9 Product Features Supported by V200R003C00

The following table lists the features supported by the S7700.

Table 5-9 Features supported by the S7700

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, 10 Gbit/s, 40 Gbit/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
		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 ● DHCP policies
		Double VLAN tags insertion based on interfaces
		Super VLAN
		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
		Configuring MAC address learning priorities for interfaces
	ARP	Port bridge
		Static and dynamic ARP entries

Feature		Description
		ARP in a VLAN
		Aging of ARP entries
		Proxy ARP
		ARP entry with multiple outbound interfaces
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
		VRF
		DHCP client
		DHCP server
		DHCP relay
		URPF check
		Routing policies
		RIPv1/RIPv2

Feature		Description
		OSPF
		BGP
		MBGP
		IS-IS
		PBR (redirection in a traffic policy)
	Multicast routing features	IGMPv1/v2/v3
		PIM-DM
		PIM-SM
		MSDP
		Multicast routing policies
		RPF
	IPv6 features	IPv6 protocol stack
		ND and ND snooping
		DHCPv6 snooping
		RIPng
		DHCPv6 server
		DHCPv6 relay
		OSPFv3
		BGP4+, ISIS for IPv6
		VRRP6
		MLDv1 and MLDv2
		PIM-DM for IPv6
		PIM-SM for IPv6
	IP transition technology	4 over 6 tunnel
		6 over 4 tunnel
		6PE
Layer 2 multicast features	-	IGMPv1/v2/v3 snooping
		Fast leave
		IGMP snooping proxy
		MLD snooping

Feature		Description
		Interface-based multicast traffic suppression
		Inter-VLAN multicast replication
		Controllable multicast
MPLS&VPN	Basic MPLS functions	LDP
		Double MPLS labels
		Mapping from DSCP to EXP priorities in MPLS packets
		Mapping from 802.1p priorities to EXP priorities in MPLS packets
	MPLS TE	MPLS TE tunnel
		MPLS TE protection group
	MPLS OAM	LSP ping and LSP traceroute
		Automatic detection of LSP faults
		1+1 protection switchover of LSPs
	VPN	Multi-VPN-Instance CE (MCE)
		VLL in SVC, Martini, CCC, and Kompella modes
		VLL FRR
		VPLS
		MPLS L3VPN
		HVPLS in LSP and QinQ modes
Device reliability	BFD	Basic BFD functions
		BFD for static route/IS-IS/OSPF/BGP
		BFD for PIM
		BFD for VRRP
		BFD for VLL FRR
	CSS	<ul style="list-style-type: none"> Cluster card supporting CSS Service interface supporting CSS
	Others	VRRP
Ethernet OAM	EFM OAM (802.3ah)	Automatic discovery
		Link fault detection
		Link fault troubleshooting
		Remote loopback

Feature		Description
	CFM OAM (802.1ag)	Software-level CCM
		MAC ping
		MAC trace
	OAM association	Association between 802.1ag and 802.3ah
		Association between 802.3ah and 802.1ag
	Y.1731	Delay and variation measurement
QoS features	Traffic classifier	Traffic classification based on ACLs
		Traffic classification based on outer 802.1p priorities, inner VLAN IDs, outer VLAN IDs, source MAC addresses, and Ethernet types
		Traffic classification based on inner 802.1p priorities
	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	Weighted Random Early Detection (WRED)
	Congestion management	Priority Queuing (PQ)
		Deficit Round Robin (DRR)
		PQ+DRR
		Weighted Round Robin (WRR)
		PQ+WRR
Configuration and maintenance	Login and configuration management	Command line configuration
		Messages and help information in English and Chinese
		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)
		EasyDeploy (commander)
		Easy deployment and maintenance
	File system	File system
		Directory and file management
		File upload and download through FTP, TFTP, SFTP, SCP, and FTPS
	Monitoring and maintenance	Hardware monitoring
		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

Feature		Description
		Portal authentication
		MAC address bypass authentication
	ARP security	ARP packet rate limiting based on source MAC addresses
		ARP packet rate limiting based on source IP addresses, interfaces, and VLANs, and global ARP packet rate limiting
		ARP anti-spoofing
		Association between ARP and STP
		ARP gateway anti-collision
		Dynamic ARP Inspection (DAI) and Static ARP Inspection (SAI)
		Egress ARP Inspection (EAI)
	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 dynamically limiting the rate of 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
		NetStream

Feature		Description
		NAT (SPU)
		Load Balance (SPU)
		SNMP v1/v2c/v3
		Standard MIB
		HTTP
		Hypertext Transfer Protocol Secure (HTTPS)
		Remote network monitoring (RMON)
		RMON2

6 Hardware Information

For the version mappings, appearance and structure, slot configuration, power supply slot configuration, heat dissipation, and specifications of S7700, see the *S7700 Hardware Description - Chassis*.

7 References

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