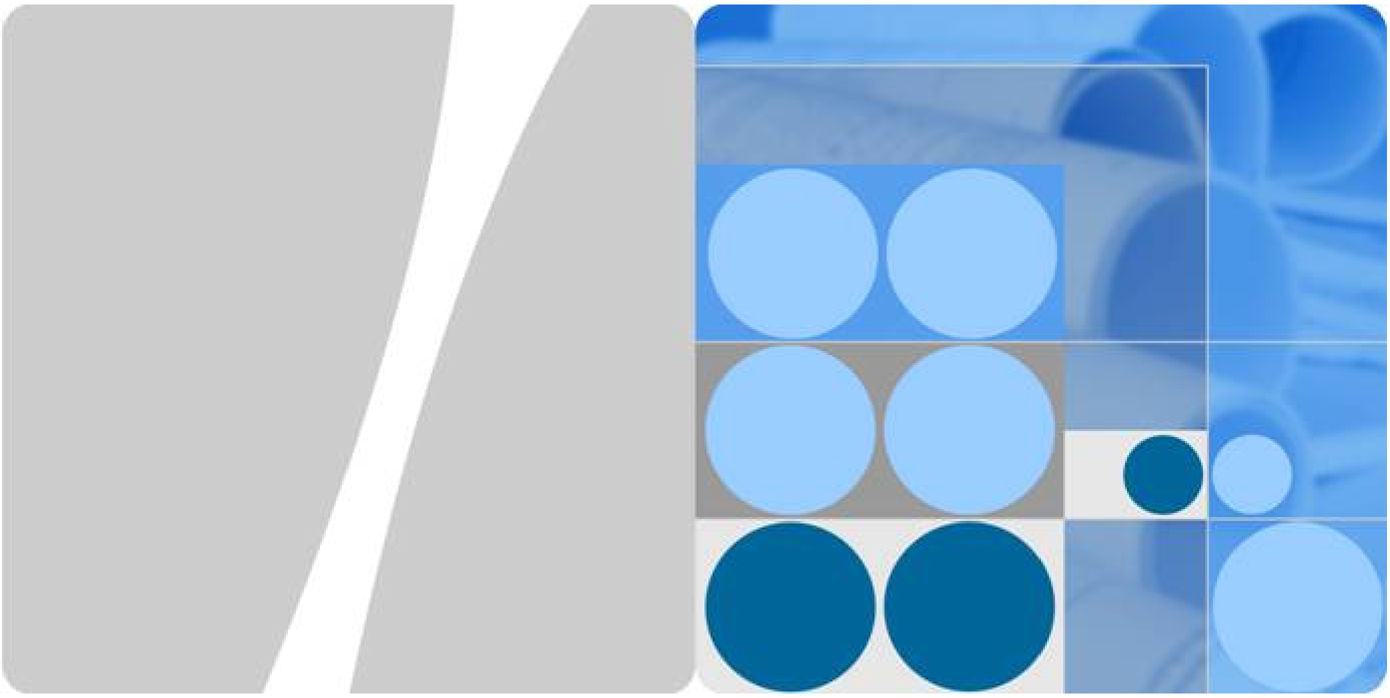

S12700 Agile Switch

Product Description

Issue	**21**
Date	**2018-05-14**

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: http://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

1 Mapping Between the S12700 Series Switches and Software Versions

Table 1-1 lists the mapping between S12700 series switches and software versions.

Table 1-1 Mapping between the S12700 series switches and software versions

Device Series	Device Model	Software Version
S12700	S12704	V200R008C00 and later versions
	S12708	V200R005C00 and later versions
	S12710	V200R010C00 and later versions
	S12712	V200R005C00 and later versions

2 Product Overview

About This Chapter

2.1 Introduction

Huawei S12700 series agile switches are core switches designed for next-generation campus networks. Using a fully programmable switching architecture, the S12700 series allows for fast, flexible function customization and supports a smooth evolution to software-defined networking (SDN). The S12700 series uses Huawei Ethernet Network Processor (ENP) and provides the native wireless access controller (AC) capability to help build a wired and wireless converged network. Its uniform user management capabilities deliver refined user and service management. The S12700 series runs Huawei Versatile Routing Platform (VRP), which provides high-performance L2/L3 switching services as well as a variety of network services, such as MPLS VPN, hardware IPv6, desktop cloud, and video conferencing. In addition, the S12700 series offers a range of reliability technologies including in-service software upgrade, non-stop forwarding, CSS2 switch fabric hardware clustering that allows 1+N backup of MPUs, hardware Eth-OAM/BFD, and ring network protection. These help you improve productivity and maximize network operation time, and therefore reduce the total cost of ownership (TCO).

The S12700 comes in four models: S12704, S12708, S12710, and S12712. The maximum numbers of line processing units and switch fabric units supported by these models are:

- S12704: 4 LPUs and 2 SFUs
- S12708: 8 LPUs and 4 SFUs
- S12710: 10 LPUs and 2 SFUs
- S12712: 12 LPUs and 4 SFUs

2.2 Product Characteristics

Make Your Network More Agile and Service-oriented

The S12700 series switches have built-in Ethernet Network Processor (ENP) chips, provide fully programmable interfaces, and support forwarding process customization.

- The high-speed ENP chip is tailored for Ethernet. Its flexible packet processing and traffic control capabilities help to build a highly scalable network that meets current and future service requirements.
- In addition to all the capabilities of common switches, the S12700 series provides fully programmable open interfaces and supports programmable forwarding behaviors. Enterprises can use the open interfaces to develop new protocols and functions independently or jointly with other vendors to satisfy their needs.
- The ENP chip uses a fully programmable architecture, on which enterprises can define their own forwarding models, forwarding behaviors, and lookup algorithms. This architecture speeds up service innovation and makes it possible to provision a customized service within several months, without replacing hardware. Therefore, the ENP chip provides much higher flexibility than traditional ASIC chips with fixed forwarding architecture and fixed forwarding process (1-3 years taken for provisioning a new service).

Deliver Extensive Services More Efficiently

The S12700 series provides hardware native T-bit AC and unified user management functions, allowing for more agile service features.

- The native AC 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 helps you better cope with challenges in the high-speed wireless access era.
- The S12700 provides the unified user management function that shields the differences of access devices in capacity and access methods. It supports PPPoE, 802.1X, MAC, and Portal authentication, and can manage users based on user groups, domains, and time ranges. These functions facilitate user and service management and enable a transformation from device-centered to user-centered 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 the physical locations. The service chaining function allows for more flexible value-added service deployment, which reduces equipment and maintenance costs.

Provide Fine Granular Management More Efficiently

The S12700 series supports Packet Conservation Algorithm for Internet (iPCA) and super virtual fabric (SVF), and can manage access switches, allowing for fine-granular network management.

- 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.

- SVF technology can virtualize fixed switches into line cards of an S12700 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.
- The S12700 series manages access switches in a similar way an AC manages APs, saving the configuration workload on access switches. It manages access switches and APs uniformly over CAPWAP tunnels, allowing access switches and APs to connect to the network with zero configuration.

Industry-Leading Line Cards

Industry-leading line cards of the S12700 series switches support large table sizes and provide low-latency forwarding of heavy traffic.

- Using Huawei advanced ENP chips, the S12700 series supports several million hardware entries, leaving traditional switches far behind. The S12700 series provides large routing tables for metro core layer of television broadcasting or education network and fine granular traffic statistics collection for education campus networks and large-scale enterprise campus networks.
- Compared to the 4 MB buffer size on line cards of traditional switches, the S12700 series provides a large buffer size on each line card to prevent packet loss upon traffic bursts, delivering high-quality video services.
- The S12700 series supports high-density line-speed cards, such as 48*10GE and 8*40GE line cards. These large port capacities meet the requirements of bandwidth-consuming applications, such as multimedia video conferencing, and provide investment protection for customers.

Device-Level End-to-End Reliability Design: CSS2 Switch Fabric Hardware Clustering

The S12700 series switches use CSS2 switch fabric hardware clustering, a second-generation CSS technology.

- CSS2 technology connects member switches through hardware channels of switch fabric units. Therefore, control packets and data packets of a cluster only need to be forwarded once by the switch fabric units and do not go through line cards. Compared to traditional service port clustering, CSS2 minimizes the impact of software failures, reduces the risks of service interruption caused by line cards, and significantly shortens the transmission latency.
- CSS2 supports 1+N backup of MPUs. This means a cluster can run stably as long as one MPU in either member chassis is working normally. In a cluster connected by service ports, each chassis must have at least one MPU working normally. Therefore, CSS2 is more reliable than traditional service port clustering technology.

Network-Level Reliability Design: End-to-End Hardware Protection Switching

The S12700 uses a series of link detection and protection switching technologies, such as hardware Eth-OAM, BFD, G.8032, and Smart Ethernet Protection (SEP). These technologies help build a campus network that responds quickly to topology changes and provides the most reliable services.

Related Content

Support Community

Introduction to Modular Switches

Videos

Huawei S12700 Series Switches Introduction

3 Usage Scenarios

About This Chapter

3.1 S12700 Typical Applications (Enterprise)

In an Enterprise Campus Network

The S12700 series switches are deployed on the core layer of an enterprise campus network. ACs are built in to the S12700 switches so that wireless networks can be constructed without any additional AC devices, reducing network construction costs. The T-bit AC capability avoids performance bottlenecks on independent ACs and enables a migration to 802.11ac networks. With the native AC capability, the S12700 series realizes wired and wireless convergence and delivers a consistent experience to wired and wireless users through uniform device management, user management, and service management.

In an Education Campus Network

The S12700 series switches are deployed on the core layer of a college campus network. As they support unified user management, you do not need to buy additional hardware components, reducing network construction costs. Each S12700 switch allows for a large number of concurrent access users. The H-QoS feature implements fine granular user and service management. With the wired and wireless convergence capability, the S12700 switches deliver a consistent experience to wired and wireless users through uniform device management, user management, and service management.

In a Bearer Network for Video Conferencing, Desktop Cloud, and Video Surveillance Applications

The S12700 series has a large buffer to prevent packet loss when traffic bursts occur, delivering high-quality video streams. Each S12700 switch supports millions of hardware entries, which allow for a large number of terminals and facilitate evolution to IPv6 and the

Internet of Things. Employing end-to-end hardware reliability technologies and iPCA, the S12700 series offers a highly reliable, high-quality, scalable video conferencing and surveillance solution.

On the MAC Core/Aggregation Layer

The S12700 series switches can be used as core or aggregation switches on a metro television broadcasting or education network. Each S12700 switch supports millions of FIB entries for large-scale routing on the network. CSS2 switch fabric hardware clustering technology delivers carrier-grade reliability. Additionally, the S12700 series supports comprehensive L2/L3 MPLS VPN features, ensuring high reliability, security, and scalability on the metropolitan bearer network.

In an Enterprise Data Center

The S12700 series switches can be deployed on the core or aggregation layer of an enterprise data center network, and provide large throughput using high-density line cards, such as 8*40GE, 48*10GE, and 4*100GE cards. CSS2 switch fabric hardware clustering technology shortens the inter-chassis forwarding latency to 4 microseconds. This technology helps to build a data center network with high performance, high reliability, and low latency.

3.2 S12700 Typical Applications (Carrier)

In a Campus Network

The S12700 series switches are deployed on the core layer of a campus network. Native ACs provided by the S12700 enable customers to build wireless networks without additional AC hardware, reducing network construction costs. It is a core switch that provides T-bit AC capabilities, avoiding the performance bottleneck on independent ACs. The native AC capabilities help customers migrate their wireless networks to 802.11ac. The S12700 series realizes wired and wireless convergence and delivers consistent experience to wired and wireless users through uniform device, user, and service management.

In a Bearer Network for Video Conferencing, Desktop Cloud, and Video Surveillance Applications

The S12700 series has a large buffer to prevent packet loss when traffic bursts occur, delivering high-quality video streams. Each S12700 switch supports millions of hardware entries, which allow for a large number of terminals and facilitate evolution to IPv6 and the Internet of Things. Employing end-to-end hardware reliability technologies and iPCA, the S12700 series offers a highly reliable, high-quality, scalable video conferencing and surveillance solution.

On the MAC Core/Aggregation Layer

The S12700 series switches can be used as core or aggregation switches on a metro television broadcasting or education network. Each S12700 switch supports millions of FIB entries for large-scale routing on the network. CSS2 switch fabric hardware clustering technology delivers carrier-grade reliability. Additionally, the S12700 series supports comprehensive L2/L3 MPLS VPN features, ensuring high reliability, security, and scalability on the metropolitan bearer network.

In a Data Center

The S12700 series switches can be deployed on the core or aggregation layer of a center network, and provide large throughput using high-density line cards, such as 8*40GE, 48*10GE, and 4*100GE cards. CSS2 switch fabric hardware clustering technology shortens the inter-chassis forwarding latency to 4 microseconds. This technology helps to build a data center network with high performance, high reliability, and low latency.

4 Performance Specifications

The features mentioned in the "Introduction", "Product Characteristics", and "Usage Scenarios" sections are not supported on all S12700 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

The following table lists features supported by the S12700.

Table 5-1 Features supported by the S12700

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, 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: ● 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	CSS2
	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
	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
User access and authentica tion	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 S12700.

Table 5-2 Features supported by the S12700

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, 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: ● 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
	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
	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	CSS2
	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)

Feature		Description
	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
		Virtual cable test (VCT)
		User operation logs

Feature		Description
		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
		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
		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)

5.3 Product Features Supported by V200R010C00

The following table lists the features supported by the S12700.

Table 5-3 Features supported by the S12700

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, 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: ● 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

Feature		Description
		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
	SEP	Smart Ethernet Protection (SEP)
	Smart Link	Smart Link
		Smart Link multi-instance
		Monitor Link

Feature		Description
	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 forwardin g	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

Feature		Description
		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&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

Feature		Description
		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	CSS2
	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

Feature		Description
	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
		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

Feature		Description
		Version matching check
		Information center and unified management over logs, alarms, and debugging information
		Electronic labels, and command line query and backup
		Virtual cable test (VCT)
		User operation logs
		Detailed debugging information for network fault diagnosis
		Network test tools such as traceroute and ping commands
		Port mirroring, flow mirroring, and remote mirroring
		Energy saving
	Version upgrade	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

Feature		Description
		Defense against attacks from many fragments, attacks from many packets with offsets, attacks from repeated packet fragments, Tear Drop attacks, Syndrop attacks, NewTear attacks, Bonk attacks, Nesta attacks, Rose attacks, Fawx attacks, Ping of Death attacks, and Jolt attacks
		Defense against TCP SYN flood attacks, UDP flood attacks (including Fraggle attacks and UDP diagnosis port attacks), and ICMP flood attacks
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

Feature		Description
		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 S12700.

Table 5-4 Features supported by the S12700

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, 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: ● MAC address + IP address ● MAC address + IP address + interface number

Feature		Description
		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
		MSTP
		BPDU protection, root protection, and loop protection
		TC-BPDU attack defense
		STP loop detection
		VBST

Feature		Description
	Loopback-detect	Loop detection on an interface
	SEP	Smart Ethernet Protection (SEP)
	Smart Link	Smart Link
		Smart Link multi-instance
		Monitor Link
	RRPP	RRPP protective switchover
		Single RRPP ring, tangent RRPP ring, and intersecting RRPP ring
		Hybrid networking of RRPP rings and other ring networks
	ERPS	G.8032 v1/v2
		Single closed ring
		Subring
IPv4/IPv6 forwardin g	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

Feature		Description
		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&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

Feature		Description
	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	CSS2
	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

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

5.5 Product Features Supported by V200R008C00

The following table lists the features supported by the S12700.

Table 5-5 Features supported by the S12700

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, 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: ● 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	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)

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&VPN	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	CSS2
	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)
		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)

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
	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)
	Policy association	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

5.6 Product Features Supported by V200R007C00

The following table lists the features supported by the S12700.

NOTE

Features marked with * are added in V200R007C00.

Table 5-6 Features supported by the S12700

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

Feature		Description
		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: ● 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

Feature		Description
		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 forwardin g	IPv4 and unicast routes	Static IPv4 routes
		VRF
		DHCP client
		DHCP server
		DHCP relay

Feature		Description
		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	CSS2
	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)
		Deficit Round Robin (DRR)
		PQ+DRR
		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*
	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

Feature		Description
		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
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

Feature		Description
		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

5.7 Product Features Supported by V200R006C00

The following table lists the features supported by the S12700.

Table 5-7 Features supported by the S12700

Feature		Description
Ethernet features	Ethernet	Full-duplex, half-duplex, and auto-negotiation modes on Ethernet interfaces

Feature		Description
		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)
		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: ● 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	CSS2
	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)
		Deficit Round Robin (DRR)

Feature		Description
		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
	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

Feature		Description
		Energy saving
	Version upgrade	Device software loading and online software loading
		BootROM online upgrade
		In-service patching
Security	AAA	Local authentication and authorization
		RADIUS authentication, authorization, and accounting
		HWTACACS authentication, authorization, and accounting
		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
		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

Feature		Description
	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
		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

5.8 Product Features Supported by V200R005C00

The following table lists the features supported by the S12700.

NOTE

Features marked with * are added in V200R005C00.

Table 5-8 Features supported by the S12700

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)
		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: ● 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

Feature		Description
		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
	SEP	Smart Ethernet Protection (SEP)
	Smart Link	Smart Link
		Smart Link multi-instance
		Monitor Link

Feature		Description
	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 forwardin g	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

Feature		Description
		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&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

Feature		Description
		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	CSS2
	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

Feature		Description
	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
	Monitoring and maintenance	Hardware monitoring
		Second-time fault detection to prevent detection errors caused by instant interference
		Version matching check

Feature		Description
		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
		Dynamic ARP Inspection (DAI) and Static ARP Inspection (SAI)
		Egress ARP Inspection (EAI)
	IP security	ICMP attack defense

Feature		Description
		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
		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

Feature		Description
		WLAN Security Specifications
		WLAN user management specifications

6 Hardware Information

For the version mappings, appearance and structure, slot configuration, power supply slot configuration, heat dissipation, and specifications of S12700, see the *S12700 Hardware Description* - Chassis.

7 References

You can download the *Switch Standard and Protocol Compliance List* from the **Huawei official website**.