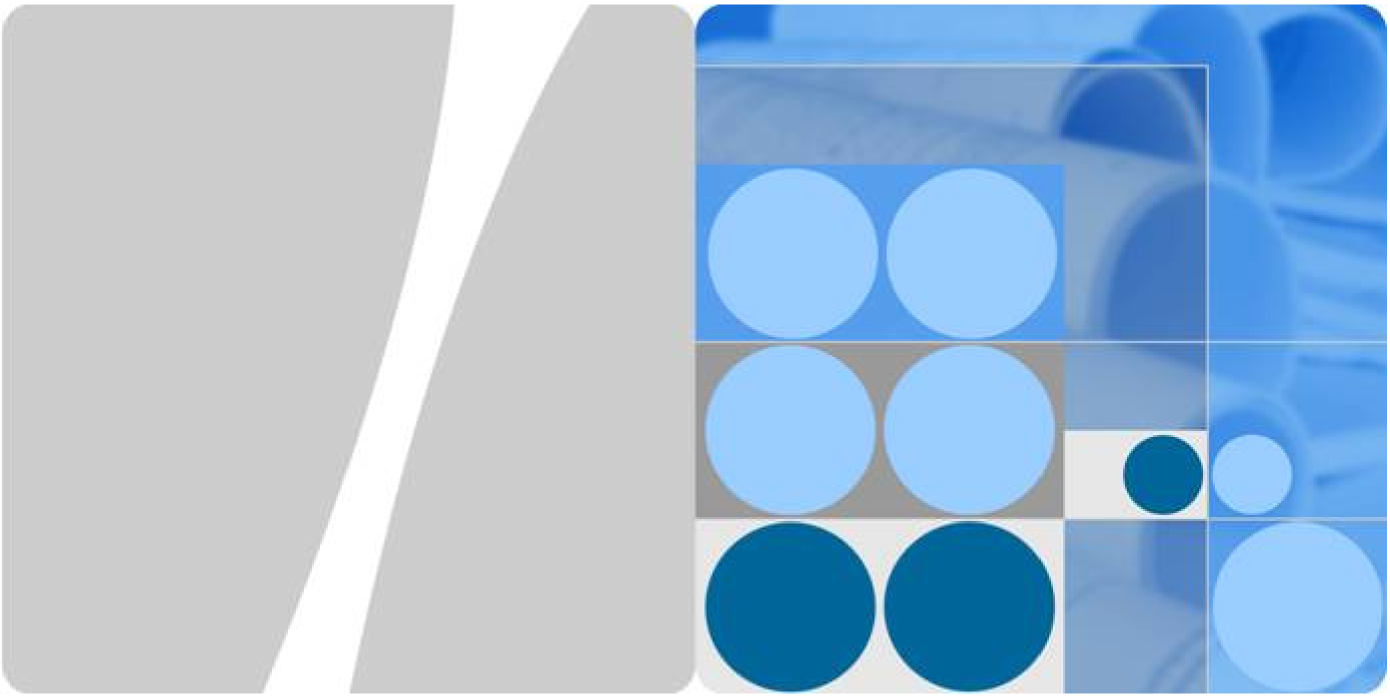


S6700 Series Ethernet Switches

Product Description

Issue 19

Date 2018-05-14

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

1 Product Overview

About This Chapter

1.1 Introduction

The S6700 series Ethernet switches (S6700 for short) are next-generation 10G fixed switches. The S6700 can function as an access switch in an Internet data center (IDC) or a core switch on a campus network.

The S6700 has industry-leading performance and provides line-speed 10GE access ports and line-speed 40GE uplink ports (40GE is supported since V200R008C00). It can be used in a data center to provide 10 Gbit/s access to servers or function as a core switch on a campus network to provide 40 Gbit/s traffic aggregation. In addition, the S6700 provides a wide variety of services, comprehensive security policies, and various QoS features to help customers build scalable, manageable, reliable, and secure data centers.

1.2 Product Characteristics

Enabling networks to be more agile for services

The high-speed Ethernet Network Processor (ENP) embedded in the S6720-HI is tailored for Ethernet. The chip's flexible packet processing and traffic control capabilities can meet current and future service requirements, helping build a highly scalable network.

The ENP has a fully programmable architecture, on which enterprises can define their own forwarding models, forwarding behaviors, and lookup algorithms. Microcode programmability makes it possible to provide new services within six months, without the need of replacing the hardware. In contrast, traditional ASIC chips use a fixed forwarding architecture and follow a fixed forwarding process. For this reason, new services cannot be provisioned until new hardware is developed to support the services one to three years later.

Delivering abundant services more agilely

The S6720-HI integrates the AC function, so customers do not need to buy independent AC devices or hardware components.

With the unified user management function, the S6720-EI, S6720S-EI, and S6720-HI authenticate both wired and wireless users, ensuring a consistent user experience no matter whether they are connected to the network through wired or wireless access devices. The unified user management function supports various authentication methods, including 802.1X, MAC address, and Portal authentication, and is capable of managing users based on user groups, domains, and time ranges. These functions visualize user and service management and boost the transformation from device-centric management to user-centric management.

The S6720 provides excellent quality of service (QoS) capabilities and supports queue scheduling and congestion control algorithms. Additionally, it adopts innovative priority queuing and multi-level scheduling mechanisms to implement fine-grained scheduling of data flows, meeting service quality requirements of different user terminals and services.

Providing fine granular network management more agilely

The S6720-HI uses the Packet Conservation Algorithm for Internet (iPCA) technology that changes the traditional method of using simulated traffic for fault location. iPCA technology can monitor network quality for any service flow anywhere, anytime, without extra costs. It can detect temporary service interruptions in a very short time and can identify faulty ports accurately. This cutting-edge fault detection technology turns "extensive management" to "fine granular management."

The S6720-HI supports Two-Way Active Measurement Protocol (TWAMP) to accurately check any IP link and obtain the entire network's IP performance. This protocol eliminates the need of using a dedicated probe or a proprietary protocol.

The S6720-HI supports SVF and functions as a parent switch. With this virtualization technology, a physical network with the "Small-sized core/aggregation switches + Access switches + APs" structure can be virtualized into a "super switch", offering the industry's simplest network management solution.

Large-Capacity, High-Density, 10 Gbit/s Access and 40 Gbit/s Uplink

To provide sufficient bandwidth for users, many servers use 10G network adapters, especially servers in data centers. The S6700 can be used in data centers to provide high forwarding performance and 10GE ports.

The S6700 has the highest density of 10GE ports and largest switching capacity among counterpart switches. Each S6700 provides a maximum of 52 line-rate 10GE ports. These ports support 1GE and 10GE access and can identify optical module types, maximizing the return on investment and allowing users to deploy service flexibly.

The S6700 has a large buffer capacity and uses advanced buffer scheduling mechanism to ensure non-blocking transmission of high traffic volume in data centers.

Comprehensive Security Control Policies

The S6700 provides multiple security measures to defend against Denial of Service (DoS) attacks (such as SYN, Land, Smurf, and ICMP Flood), attacks to networks (STP BPDU/root attacks), and attacks to users (bogus DHCP server attacks, man-in-the-middle attacks, IP/MAC spoofing attacks, DHCP request flood attacks, and attacks with variable CHADDR field of packets). DHCP snooping discards invalid packets that do not match any binding entries, such as ARP spoofing packets and IP spoofing packets. This prevents man-in-the-middle attacks that hackers initiate using ARP packets. The interface connected to a DHCP server can be configured as a trusted interface to protect the system against bogus DHCP server attacks.

The S6700 supports strict ARP learning, which prevents ARP spoofing from exhausting ARP entries to ensure normal Internet normally access. The switch also provides IP source check to prevent DoS attacks caused by MAC address spoofing, IP address spoofing, and MAC/IP spoofing. The unicast reverse path forwarding (URPF) function protects a network against source address spoofing attacks by reversely checking packet transmission paths.

The S6700 supports centralized MAC address authentication and 802.1X authentication. It authenticates users based on static or dynamic bindings of information such as the user name, IP address, MAC address, VLAN ID, interface number, and antivirus software installation flag. VLANs, QoS policies, and ACLs can be applied to users dynamically. The S6700 can limit the number of MAC addresses learned on an interface to prevent attackers from exhausting MAC address entries using bogus source MAC addresses. This function minimizes packet flooding that occurs when MAC addresses of users cannot be found in the MAC address table.

Comprehensive Reliability Mechanisms

The S6700 supports redundant power supplies. You choose a single power supply or use two power supplies to ensure power reliability. With two swappable fans, the S6700 has a longer MTBF time than counterpart switches. The S6700 supports multi-process MSTP that enhances the existing STP, RSTP, and MSTP implementation by increasing the number of MSTIs supported on a network. It also supports enhanced Ethernet reliability technologies such as Smart Link and RRPP, which implement millisecond-level protection switching to ensure network reliability. Smart Link and RRPP both support multiple instances to implement load balancing among links, improving the bandwidth efficiency.

The S6700 supports enhanced trunk (E-Trunk) that enables a CE to be dual-homed to two PEs using Eth-Trunk links. This implements inter-device link aggregation and link load balancing, and greatly improves reliability of access devices.

The S6700 supports the Smart Ethernet Protection (SEP) protocol, a ring network protocol applied to the link layer of an Ethernet network. SEP features simplicity, high reliability, high switching performance, convenient maintenance, and flexible topology, enabling users to manage and plan networks conveniently.

The S6700 supports G.8032, also called Ethernet Ring Protection Switch (ERPS). ERPS is based on traditional Ethernet MAC and bridging functions and uses mature Ethernet OAM and Ring Automatic Protection Switching (Ring APS or R-APS) technologies to implement fast protection switching on Ethernet networks. ERPS supports multiple services and provides flexible networking, reducing the OPEX and CAPEX. Two S6700s can form a VRRP group to ensure nonstop communication. Multiple equal-cost routes to an upstream device can be configured on the S6700 to provide route redundancy. When an active route is unreachable, traffic is switched to a backup route.

Extensive QoS Control Mechanisms

The S6700 implements complex traffic classification based on packet information such as the 5-tuple, IP preference, ToS, DSCP, IP protocol type, ICMP type, TCP source port, VLAN ID, Ethernet protocol type, and CoS. ACLs can be applied to inbound or outbound direction to filter packets. The S6700 supports a per flow two-rate three-color CAR. Each port supports eight priority queues, multiple queue scheduling algorithms such as WRR, WDRR, PQ, WRR +PQ, and WDRR+PQ, and congestion avoidance algorithm WRED. All of these ensure the quality of voice, video, and data services.

High Scalability

The S6700 supports the intelligent stack (iStack) function that allows switches far from each other to set up a stack. A port of the S6700 can be configured as a stack port for flexible stack deployment. The distance between stacked switches is further increased when the switches are connected with optical fibers. Compared with a single device, iStack provides higher expansibility, reliability, and performance. New member switches can be added to a stack without interrupting services when the system capacity needs to be increased or a member switch fails. Compared with stacking of modular switches, iStack can increase system capacity and port density without restricted by the hardware structure. Multiple stack switches are managed as one logical device with a single IP address, which greatly reduces system expansion, operation, and maintenance costs.

Convenient Management

The S6700 supports automatic configuration, plug-and-play, USB-based deployment, and batch remote upgrade. These capabilities simplify device management and maintenance while reducing maintenance costs. The S6700 supports SNMPv1/v2c/v3 and provides flexible device management methods. You can manage the S6700 using the CLI, Web system, or Telnet. The NQA function helps you with network planning and upgrades. In addition, the S6700 supports NTP, SSH v2, HWTACACS, RMON, log hosts, and port-based traffic statistics collection. The switch supports GVRP, which dynamically distributes, registers, and propagates VLAN attributes to reduce the manual configuration workload of network administrators and ensure correct VLAN configuration.

The S6700 supports MUX VLAN that isolates Layer 2 traffic between interfaces in a VLAN. Interfaces in a subordinate separate VLAN can communicate with interfaces in the principal VLAN but cannot communicate with each other. This function prevents communication between network devices connected to certain interfaces or interface groups but allows the devices to communicate with the default gateway. MUX VLAN is usually used on an enterprise intranet to isolate user interfaces from each other but allow them to communicate with server interfaces.

The S6700 supports BFD, which provides millisecond-level fault detection for protocols such as OSPF, IS-IS, VRRP, and PIM to improve network reliability. Complying with IEEE 802.3ah and 802.1ag, the S6700 supports point-to-point Ethernet fault management and can detect faults in the last mile of an Ethernet link to users. Ethernet OAM improves the Ethernet network management and maintenance capabilities and ensures a stable network.

Various IPv6 Features

The S6700 hardware supports IPv4/IPv6 dual stack and IPv6 over IPv4 tunnels (including manual tunnels, 6to4 tunnels, and ISATAP tunnels). S6700 switches can be deployed on IPv4 networks, IPv6 networks, or networks that run both IPv4 and IPv6. This makes networking flexible and enables smooth network migration from IPv4 to IPv6.

The S6700 supports various IPv6 routing protocols including RIPng and OSPFv3. It uses the IPv6 Neighbor Discovery Protocol (NDP) to manage packets exchanged between neighbors.

It also provides the Path MTU Discovery (PMTU) mechanism to select a proper MTU on the path from the source to the destination, optimizing network resources and obtaining the maximum throughput.

Cloud-based Management

Huawei provides the Cloud Managed Network Solution based on a public cloud. The S6720EI/S6720S-EI/S6720HI/S6720SI/S6720S-SI (since V200R012C00), can be managed by a cloud management platform. In the Huawei Cloud Managed Network solution, cloud-managed switches are plug-and-play. They automatically connect to the cloud management platform and use bidirectional certificate authentication to ensure management channel security. The cloud-managed switches provide the NETCONF and YANG interfaces, through which the cloud management platform delivers configurations to them. In addition, remote maintenance and fault diagnosis can be performed on the cloud-managed switches using the cloud management platform.

VXLAN features

The S6720-EI, S6720S-EI, and S6720-HI support VXLAN L2 and L3 gateway functions, which can be configured using NETCONF/YANG. Based on this feature, multiple service networks or tenant networks can be deployed together on the same physical network. Service networks or tenant networks are isolated from each other, achieving one network for multiple purposes. This helps meet data bearing requirements of different services or customers while reducing network construction costs and improving network resource utilization efficiency.

Clock synchronization

The S6720-HI supports the IEEE 1588v2 protocol, which implements low-cost, high-precision, and high-reliability time and clock synchronization. This feature can meet strict requirements of power and transportation industry customers on time and clock synchronization.

Open Programmability System (OPS)

The S6720 provides open interfaces, and customers can make executable paython scripts based on specified events to implement intelligent device management, lowering O&M costs and simplifying operations.

Related Content

Support Community

- **Introduction to Huawei Fixed Switches**

Videos

- **S6720-EI Series Switches: Overview**
- **Huawei S6720-SI Multi-gigabit Ethernet Switches**
- **Huawei S6720-LI Simplified 10 GE Ethernet Switch**

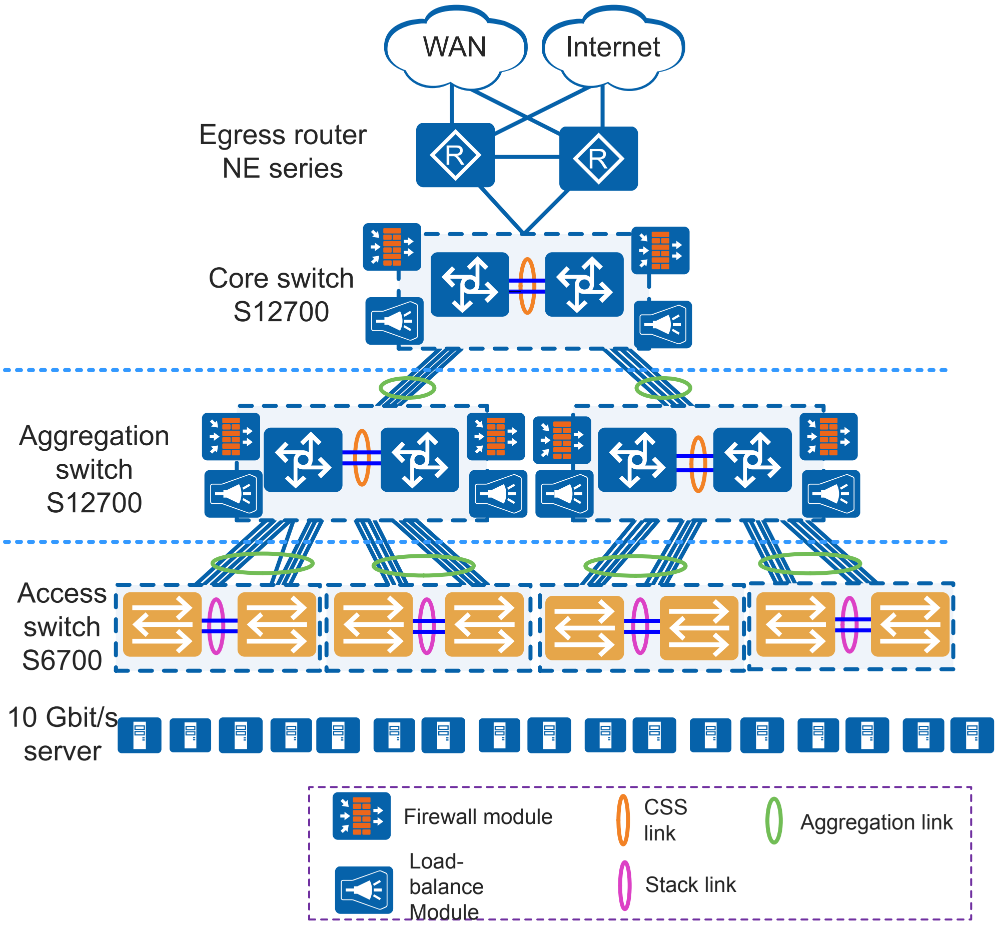
2 Usage Scenarios

About This Chapter

2.1 Data Center

The S6700 switches can be deployed at the access layer build a virtualized, highly reliable, non-blocking, and energy conservative data center network.

Figure 2-1 S6700 in a data center



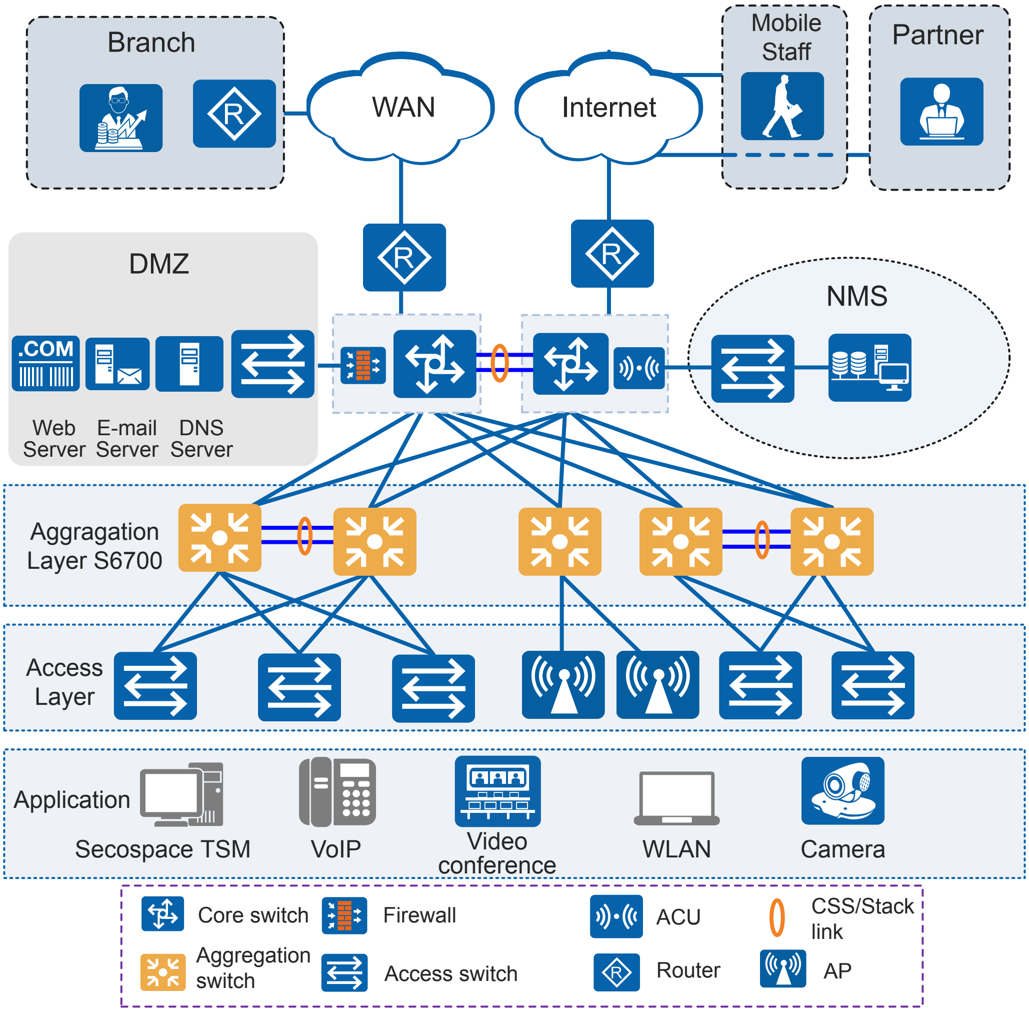
In a data center network shown in **Figure 2-1**, NE routers act as the egress routers. S12700 switches work at the core and aggregation layers to ensure network security and implement load balancing using firewall and load balance modules.

The S6700 switches are deployed at the access layer to provide 10 Gbit/s access. They set up stacks to ensure high reliability. When a stack member switch fails, the other switch in the stack takes over services. Eth-Trunk is used to achieve link-level reliability, without a need for STP or VRRP, thereby simplifying configuration and maintenance, and reducing configuration errors.

2.2 Large-scale Enterprise Campus Network

As shown in **Figure 2-2**, S6700 switches are deployed at the aggregation layer of a large-scale enterprise campus network, creating a highly reliable, scalable, and manageable enterprise campus network.

Figure 2-2 S6700 in an enterprise campus network



In an enterprise network or campus network, S6700 switches connect to access switches through 100M/1000M interfaces to provide high-performance switching and connect to core switches through 10GE optical interfaces. The network provides a 10G backbone layer and 100M-to-the-desktop capability, meeting requirements for high bandwidth and multi-service operation.

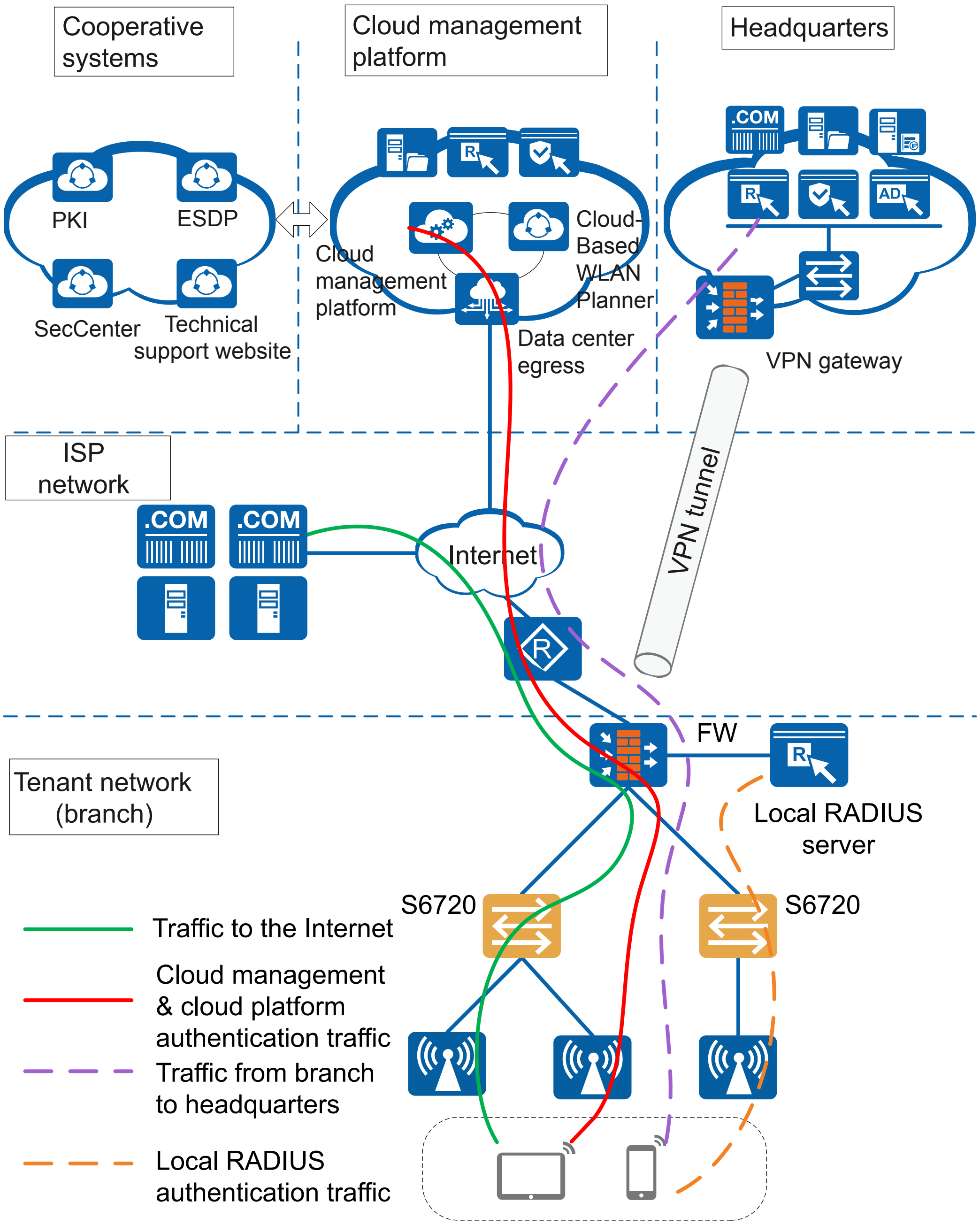
The S6700 switches support SEP and RRPP to implement millisecond-level protection switching. Multiple S6700 switches set up a stack using iStack technology to provide a distributed forwarding structure and fast fault recovery. The stack increases the number of user interfaces and improves packet processing capability. The stack member switches can be managed as one device to facilitate network management and maintenance.

2.3 Application in Public Cloud

Agile Cloud Network is a network solution suite based on Huawei public cloud. The S6720EI/S6720S-EI/S6720HI/S6720SI/S6720S-SI (since V200R012C00) can be located at the access layer of an agile cloud network as a cloud-managed device, as shown in **Figure 2-3**.

Cloud-managed devices are plug-and-play. They go online automatically after being powered on and connected with network cables, without the need for complex configurations. A cloud-managed device can connect to the cloud management platform and use bidirectional certificate authentication to ensure management channel security. The cloud-managed device provides the NETCONF and YANG interfaces, through which the cloud management platform delivers configurations to it. In addition, remote maintenance and fault diagnosis can be performed on the cloud management platform.

Figure 2-3 Application of S6720 in public cloud



3 Performance Specifications

The features mentioned in the "Introduction", "Product Characteristics", and "Usage Scenarios" sections are not supported on all S6700 models. For the feature support of specific product models, download their brochures or feature lists from **Huawei official website**. (If your account is unauthorized, contact Huawei's support team).

4 Product Performance

About This Chapter

4.1 Product Features Supported by V200R012C00

Table 4-1 lists the features supported by the S6720.

Table 4-1 Features supported by the S6720

Feature		Description	Supplementary Information
Ethernet features	Ethernet	Operating modes of full-duplex, half-duplex, and auto-negotiation	The S6720EI, S6720S-EI, and S6720HI do not support the duplex mode configuration.

Feature		Description	Supplementary Information
		Rates of an Ethernet interface: 2.5 Gbit/s, 10 Gbit/s, 40 Gbit/s, 100 Gbit/s, and auto-negotiation	● S6720EI/S6720S-EI: Do not support the 2.5 Gbit/s or 100 Gbit/s Ethernet interface. ● S6720LI/S6720S-LI: Do not support the 2.5 Gbit/s or 100 Gbit/s Ethernet interface. Some S6720LI/S6720S-LI models do not support the 40 Gbit/s Ethernet interface. ● S6720SI/S6720S-SI: Do not support the 100 Gbit/s Ethernet interface. Some S6720SI/S6720S-SI models do not support the 2.5 Gbit/s or 40 Gbit/s Ethernet interface. ● S6720HI: Does not support the 2.5 Gbit/s Ethernet interface.
		Flow control on interfaces	None
		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 LNP (link type negotiation protocol), access, trunk, hybrid, and QinQ	None
		Default VLAN	
		VLAN assignment based on interfaces, MAC addresses, protocols, and IP subnets	

Feature		Description	Supplementary Information
		VLAN assignment based on the following policies: ● MAC address + IP address ● MAC address + IP address + interface number	
		Adding double VLAN tags to packets based on interface	
		Super VLAN	The S6720LI and S6720S-LI do not support this function.
		VLAN mapping	None
		Selective QinQ	
		MUX VLAN	
		Voice VLAN	
		Guest VLAN	
	GVRP	Generic Attribute Registration Protocol (GARP)	None
		GARP VLAN Registration Protocol (GVRP)	
	VCMP	VCMP (VLAN centralized management protocol)	None
	MAC	Automatic learning and aging of MAC addresses	None
		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	Only the S6720HI, S6720EI, and S6720S-EI support this function.
		MAC address spoofing defense	The S6720HI, S6720EI, and S6720S-EI do not support this function.
		Port bridge	None

Feature		Description	Supplementary Information
	ARP	Static and dynamic ARP entries	None
		ARP in a VLAN	
		Aging of ARP entries	
		Proxy ARP	The S6720LI and S6720S-LI do not support inter-VLAN proxy ARP.
		Multi-port ARP for connecting to the NLB cluster server	The S6720LI and S6720S-LI do not support this function.
Ethernet loop protection	MSTP	STP	None
		RSTP	
		MSTP	
		VBST	
		BPDU protection, root protection, and loop protection	
		TC-BPDU attack defense	
	Loopback-detect	Loop detection on an interface	
	SEP	Smart Ethernet Protection (SEP)	
	Smart Link	Smart Link	
		Smart Link multi-instance	
		Monitor Link	
	RRPP	RRPP protective switchover	
		Single RRPP ring, tangent RRPP ring, and intersecting RRPP ring	
		Hybrid networking of RRPP rings and other ring networks	
	ERPS	G.8032 v1/v2	
		Single closed ring	
		Subring	
IPv4/ IPv6 forwarding	IPv4 and unicast routes	Static IPv4 routes	None
		VRF	None
		DHCP client	None

Feature		Description	Supplementary Information
		DHCP server	
		DHCP relay	
		DHCP policy VLAN	
		URPF check	The S6720LI and S6720S-LI do not support this function.
		Routing policies	None
		RIPv1/RIPv2	
		OSPF	
		BGP	The S6720LI and S6720S-LI do not support this function.
		MBGP	Only the S6720HI, S6720EI, and S6720S-EI support this function.
		IS-IS	The S6720LI and S6720S-LI do not support this function.
		PBR (redirection in a traffic policy)	None
	Multicast routing features	IGMPv1/v2/v3	None
		PIM-DM	
		PIM-SM	
		MSDP	
		Multicast routing policies	
		RPF	
	IPv6 features	IPv6 protocol stack	None
		ND and ND snooping	
		DHCPv6 snooping	
		RIPng	
		DHCPv6 server	
		DHCPv6 relay	
		OSPFv3	
		BGP4+ & ISIS for IPv6	The S6720LI and S6720S-LI do not support this function.
		VRRP6	None

Feature		Description	Supplementary Information
		MLDv1 and MLDv2	None
		PIM-DM for IPv6	
		PIM-SM for IPv6	
	Transition technology	6 over 4 tunnel	The S6720LI and S6720S-LI do not support this function.
Layer 2 multicast features	-	IGMPv1/v2/v3 snooping	None
		Fast leave	
		IGMP snooping proxy	
		MLD snooping	
		Interface-based multicast traffic suppression	
		Inter-VLAN multicast replication	
		Controllable multicast	
MPLS &VPN	Basic MPLS functions	LDP	The S6720LI, S6720S-LI, S6720SI, and S6720S-SI do not support this function.
		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	
	VPN	Multi-VPN-Instance CE (MCE)	None
		VLL in SVC, Martini, CCC, and Kompella modes	The S6720LI, S6720S-LI, S6720SI, and S6720S-SI do not support this function.
		VLL FRR	
		VPLS	
		MPLS L3VPN	
		IPSec Efficient VPN	None
Device reliability	BFD	Basic BFD functions	The S6720LI and S6720S-LI do not support this function.
		BFD for static route/IS-IS/OSPF/BGP	

Feature		Description	Supplementary Information
		BFD for PIM	
		BFD for VRRP	
	Stacking	Service interface supporting the stacking function	None
	Others	VRRP	
Ethernet OAM	EFM OAM(802.3ah)	Automatic discovery	None
		Link fault detection	
		Link fault troubleshooting	
		Remote loopback	
	CFM OAM (802.1ag)	Software-level CCM	
		MAC ping	
		MAC trace	
	Y.1731	Delay and variation measurement	
QoS features	Traffic classifier	Traffic classification based on ACLs	None
		Traffic classification based on outer 802.1p priorities, inner VLAN IDs, outer VLAN IDs, source MAC addresses, and Ethernet types	The S6720LI and S6720S-LI do not support this function.
		Traffic classification based on inner 802.1p priorities	The S6720LI, S6720S-LI, S6720SI, and S6720S-SI do not support this function.
	Traffic behavior	Access control after traffic classification	None
		Traffic policing based on traffic classification	
		Re-marking based on traffic classification	
		Adding classified packets into the specified queue	
		Associating traffic classifiers with traffic behaviors	
	Traffic policing	Rate limiting on inbound and outbound interfaces	

Feature		Description	Supplementary Information
	Traffic shaping	Traffic shaping on interfaces and queues	
	Congestion avoidance	Weighted Random Early Detection (WRED)	The S6720LI, S6720S-LI, S6720SI, and S6720S-SI do not support this function.
		Tail drop	None
	Congestion management	Priority Queuing (PQ)	The S6720HI does not support Weighted Round Robin (WRR) or PQ+WRR.
		Weighted Deficit Round Robin (WDRR)	
		PQ+WDRR	
		WRR	
		PQ+WRR	
Configuration and maintenance	Login and configuration management	Command line configuration	None
		Error message and help information in English	
		Login through console and Telnet terminals	
		SSH1.5/SSH2	
		Send function and data communication between terminal users	
		Hierarchical user authority management and commands	
		SNMP-based NMS management (eSight)	
		Web page-based configuration and management	
		EasyDeploy (client)	
		EasyDeploy (commander)	The S6720LI, S6720S-LI, S6720SI, and S6720S-SI do not support this function.
		Easy deployment and maintenance	None

Feature		Description	Supplementary Information
		SVF	Only the S6720EI, S6720S-EI, S6720SI, and S6720S-SI can function as parents. The S6720HI can only function as a parent and cannot serve as an AS.
		Cloud-based management	The S6720LI and S6720S-LI do not support this function.
		Open Programmability System (OPS)	None
	File system	File system	None
		Directory and file management	
		File upload and download through FTP, TFTP, SFTP, SCP, and FTPS	
	Monitoring and maintenance	Hardware monitoring	
		Reporting alarms on abnormal device temperature	
		Second-time fault detection to prevent detection errors caused by instant interference	
		Version matching check	
		Information center and unified management over logs, alarms, and debugging information	
		Electronic labels, and command line query and backup	
		Virtual cable test (VCT)	
		User operation logs	
		Detailed debugging information for network fault diagnosis	
		Network test tools such as traceroute and ping commands	
		Port mirroring, flow mirroring, and remote mirroring	
		Energy saving	
	Version	Device software loading and online software loading	

Feature		Description	Supplementary Information
	upgrade	BootLoad online upgrade	
		In-service patching	
Security	ARP security	ARP packet rate limiting based on source MAC addresses	The S6720LI, S6720S-LI, S6720SI, and S6720S-SI do not support this function.
		ARP packet rate limiting based on source IP addresses, interfaces, and VLANs, and global ARP packet rate limiting	None
		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	None
		IP source guard	
	Local attack defense	CPU attack defense	
	MFF	MAC-Forced Forwarding (MFF)	
	DHCP snooping	DHCP snooping	
		Option 82 function and dynamic rate limiting for DHCP packets	
	Attack defense	Defense against flood attacks without IP payloads, attacks from IGMP null payload packets, LAND attacks, Smurf attacks, and attacks from packets with invalid TCP flag bits	

Feature		Description	Supplementary Information
		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	None
		RADIUS authentication, authorization, and accounting	
		HWTACACS authentication, authorization, and accounting	
	NAC	802.1X authentication	
		MAC address authentication	
		Portal authentication	
		Hybrid authentication	
	Policy association	-	The S6720SI, S6720S-SI, S6720EI, and S6720S-EI can function as access devices or control devices. The S6720LI and S6720S-SI can function as access devices. The S6720HI can function as control device.
Network management	-	Ping and traceroute	The S6720HI does not support sFlow.
		NQA	
		Network Time Protocol (NTP)	
		sFlow	
		SNMP v1/v2c/v3	
		Standard MIB	
		HTTP	

Feature		Description	Supplementary Information
		Hypertext Transfer Protocol Secure (HTTPS)	
		Remote network monitoring (RMON)	
		RMON2	Only the S6720HI, S6720EI, and S6720S-EI support this function.
WLAN	-	AP Management Specifications	Only the S6720HI supports this function.
		Radio Management Specifications	
		WLAN Service Management Specifications	
		QoS	
		WLAN Security Specifications	
		WLAN user management specifications	
VXLAN	-	Virtual eXtensible Local Area Network (VXLAN)	Only the S6720HI, S6720EI, and S6720S-EI support this function.

4.2 Product Features Supported by V200R011C10

Table 4-2 lists the features supported by the S6720.

Table 4-2 Features supported by the S6720

Feature		Description	Supplementary Information
Ethernet features	Ethernet	Operating modes of full-duplex, half-duplex, and auto-negotiation	None
		Rates of an Ethernet interface: 2.5 Gbit/s, 10 Gbit/s, 40 Gbit/s, and auto-negotiation	The S6720EI and S6720S-EI do not support the 2.5 Gbit/s Ethernet interface. The S6720LI and S6720S-LI do not support the 2.5 Gbit/s Ethernet interface, and only some S6720LI/S6720S-LI models support the 40 Gbit/s Ethernet interface. Only some S6720SI/S6720S-SI models support the 2.5 Gbit/s and 40 Gbit/s Ethernet interfaces.
		Flow control on interfaces	None

Feature		Description	Supplementary Information
		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 LNP (link type negotiation protocol), access, trunk, hybrid, and QinQ	None
		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	
		Adding double VLAN tags to packets based on interface	
		Super VLAN	The S6720LI and S6720S-LI do not support this function.
		VLAN mapping	None
		Selective QinQ	
		MUX VLAN	
		Voice VLAN	
		Guest VLAN	

Feature		Description	Supplementary Information
	GVRP	Generic Attribute Registration Protocol (GARP)	None
		GARP VLAN Registration Protocol (GVRP)	
	VCMP	VCMP (VLAN centralized management protocol)	None
	MAC	Automatic learning and aging of MAC addresses	None
		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	Only the S6720EI and S6720S-EI support this function.
		MAC address spoofing defense	The S6720EI and S6720S-EI do not support this function.
		Port bridge	None
	ARP	Static and dynamic ARP entries	None
		ARP in a VLAN	
		Aging of ARP entries	
		Proxy ARP	The S6720LI and S6720S-LI do not support inter-VLAN proxy ARP.
		Multi-port ARP for connecting to the NLB cluster server	The S6720LI and S6720S-LI do not support this function.
Ethernet loop protection	MSTP	STP	None
		RSTP	
		MSTP	
		VBST	
		BPDU protection, root protection, and loop protection	

Feature		Description	Supplementary Information
		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	None
		VRF	None
		DHCP client	None
		DHCP server	
		DHCP relay	
		DHCP policy VLAN	
		URPF check	The S6720LI and S6720S-LI do not support this function.
		Routing policies	None
		RIPv1/RIPv2	
		OSPF	
		BGP	The S6720LI and S6720S-LI do not support this function.
		MBGP	Only the S6720EI and S6720S-EI support this function.

Feature		Description	Supplementary Information
		IS-IS	The S6720LI and S6720S-LI do not support this function.
		PBR (redirection in a traffic policy)	None
	Multicast routing features	IGMPv1/v2/v3	None
		PIM-DM	
		PIM-SM	
		MSDP	
		Multicast routing policies	
		RPF	
	IPv6 features	IPv6 protocol stack	None
		ND and ND snooping	
		DHCPv6 snooping	
		RIPng	
		DHCPv6 server	
		DHCPv6 relay	
		OSPFv3	
		BGP4+ & ISIS for IPv6	The S6720LI and S6720S-LI do not support this function.
		VRRP6	None
		MLDv1 and MLDv2	None
		PIM-DM for IPv6	
		PIM-SM for IPv6	
	Transition technology	6 over 4 tunnel	The S6720LI and S6720S-LI do not support this function.
Layer 2 multicast features	-	IGMPv1/v2/v3 snooping	None
		Fast leave	
		IGMP snooping proxy	
		MLD snooping	
		Interface-based multicast traffic suppression	

Feature		Description	Supplementary Information
		Inter-VLAN multicast replication	
		Controllable multicast	
MPLS &VPN	Basic MPLS functions	LDP	The S6720LI, S6720S-LI, S6720SI, and S6720S-SI do not support this function.
		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	
	VPN	Multi-VPN-Instance CE (MCE)	None
		VLL in SVC, Martini, CCC, and Kompella modes	The S6720LI, S6720S-LI, S6720SI, and S6720S-SI do not support this function.
		VLL FRR	
		VPLS	
		MPLS L3VPN	
		IPSec Efficient VPN	The S6720LI and S6720S-LI do not support this function.
Device reliability	BFD	Basic BFD functions	The S6720LI and S6720S-LI do not support this function.
		BFD for static route/IS-IS/ OSPF/BGP	
		BFD for PIM	
		BFD for VRRP	
	Stacking	Service interface supporting the stacking function	None
	Others	VRRP	
Ethernet OAM	EFM OAM(802.3ah)	Automatic discovery	None
		Link fault detection	
		Link fault troubleshooting	
		Remote loopback	
	CFM OAM (802.1ag)	Software-level CCM	
		MAC ping	

Feature		Description	Supplementary Information
		MAC trace	
	Y.1731	Delay and variation measurement	
QoS features	Traffic classifier	Traffic classification based on ACLs	None
		Traffic classification based on outer 802.1p priorities, inner VLAN IDs, outer VLAN IDs, source MAC addresses, and Ethernet types	The S6720LI and S6720S-LI do not support this function.
		Traffic classification based on inner 802.1p priorities	The S6720LI, S6720S-LI, S6720SI, and S6720S-SI do not support this function.
	Traffic behavior	Access control after traffic classification	None
		Traffic policing based on traffic classification	
		Re-marking based on traffic classification	
		Adding classified packets into the specified queue	
		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)	The S6720LI, S6720S-LI, S6720SI, and S6720S-SI do not support this function.
		Tail drop	None
	Congestion management	Priority Queuing (PQ)	None
		Weighted Deficit Round Robin (WDRR)	
		PQ+WDRR	
		Weighted Round Robin (WRR)	
		PQ+WRR	

Feature		Description	Supplementary Information
Configuration and maintenance	Login and configuration management	Command line configuration	None
		Error message and help information in English	
		Login through console and Telnet terminals	
		SSH1.5/SSH2	
		Send function and data communication between terminal users	
		Hierarchical user authority management and commands	
		SNMP-based NMS management (eSight)	
		Web page-based configuration and management	
		EasyDeploy (client)	
		EasyDeploy (commander)	The S6720LI, S6720S-LI, S6720SI, and S6720S-SI do not support this function.
		Easy deployment and maintenance	None
		SVF	Only the S6720EI, S6720S-EI, S6720SI, and S6720S-SI can function as parents.
	File system	File system	None
		Directory and file management	
		File upload and download through FTP, TFTP, SFTP, SCP, and FTPS	
	Monitoring and maintenance	Hardware monitoring	
		Reporting alarms on abnormal device temperature	
		Second-time fault detection to prevent detection errors caused by instant interference	
		Version matching check	
		Information center and unified management over logs, alarms, and debugging information	

Feature		Description	Supplementary 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	The S6720LI, S6720S-LI, S6720SI, and S6720S-SI do not support this function.
		ARP packet rate limiting based on source IP addresses, interfaces, and VLANs, and global ARP packet rate limiting	None
		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	None
		IP source guard	
	Local attack defense	CPU attack defense	
	MFF	MAC-Forced Forwarding (MFF)	

Feature		Description	Supplementary Information
	DHCP snooping	DHCP snooping	
		Option 82 function and dynamic rate limiting for DHCP packets	
	Attack defense	Defense against flood attacks without IP payloads, attacks from IGMP null payload packets, LAND attacks, Smurf attacks, and attacks from packets with invalid TCP flag bits	
		Defense against attacks from many fragments, attacks from many packets with offsets, attacks from repeated packet fragments, Tear Drop attacks, Syndrop attacks, NewTear attacks, Bonk attacks, Nesta attacks, Rose attacks, Fawx attacks, Ping of Death attacks, and Jolt attacks	
		Defense against TCP SYN flood attacks, UDP flood attacks (including Fraggle attacks and UDP diagnosis port attacks), and ICMP flood attacks	
User access and authentication	AAA	Local authentication and authorization	None
		RADIUS authentication, authorization, and accounting	
		HWTACACS authentication, authorization, and accounting	
	NAC	802.1X authentication	
		MAC address authentication	
		Portal authentication	
		Hybrid authentication	
	Policy association	-	Only the S6720SI, S6720S-SI, S6720EI, and S6720S-EI can function as control devices.
Network management	-	Ping and traceroute	None
		NQA	
		Network Time Protocol (NTP)	

Feature		Description	Supplementary Information
		sFlow	
		SNMP v1/v2c/v3	
		Standard MIB	
		HTTP	
		Hypertext Transfer Protocol Secure (HTTPS)	
		Remote network monitoring (RMON)	
		RMON2	Only the S6720EI and S6720S-EI support this function.
VXLAN	-	Virtual eXtensible Local Area Network (VXLAN)	Only the S6720EI and S6720S-EI support this function.

4.3 Product Features Supported by V200R011C00

Table 4-3 lists the features supported by the S6720.

Table 4-3 Features supported by the S6720

Feature		Description	Supplementary Information
Ethernet features	Ethernet	Operating modes of full-duplex, half-duplex, and auto-negotiation	None
		Rates of an Ethernet interface: 2.5 Gbit/s, 10 Gbit/s, 40 Gbit/s, and auto-negotiation	The S6720EI and S6720S-EI do not support the 2.5 Gbit/s Ethernet interface. The S6720LI and S6720S-LI do not support the 2.5 Gbit/s Ethernet interface, and only some S6720LI/S6720S-LI models support the 40 Gbit/s Ethernet interface. Only some S6720SI/S6720S-SI models support the 2.5 Gbit/s and 40 Gbit/s Ethernet interfaces.
		Flow control on interfaces	None
		Jumbo frames	
		Link aggregation	
		Load balancing among links of a trunk	

Feature		Description	Supplementary Information
		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 LNP (link type negotiation protocol), access, trunk, hybrid, and QinQ	None
		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	
		Adding double VLAN tags to packets based on interface	
		Super VLAN	The S6720LI and S6720S-LI do not support this function.
		VLAN mapping	None
		Selective QinQ	
		MUX VLAN	
		Voice VLAN	
		Guest VLAN	
	GVRP	Generic Attribute Registration Protocol (GARP)	None
		GARP VLAN Registration Protocol (GVRP)	

Feature		Description	Supplementary Information
	VCMP	VCMP (VLAN centralized management protocol)	None
	MAC	Automatic learning and aging of MAC addresses	None
		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	Only the S6720EI and S6720S-EI support this function.
		MAC address spoofing defense	The S6720EI and S6720S-EI do not support this function.
		Port bridge	None
	ARP	Static and dynamic ARP entries	None
		ARP in a VLAN	
		Aging of ARP entries	
		Proxy ARP	The S6720LI and S6720S-LI do not support inter-VLAN proxy ARP.
		Multi-port ARP for connecting to the NLB cluster server	The S6720LI and S6720S-LI do not support this function.
Ethernet loop protection	MSTP	STP	None
		RSTP	
		MSTP	
		VBST	
		BPDU protection, root protection, and loop protection	
		TC-BPDU attack defense	
		STP loop detection	

Feature		Description	Supplementary Information
	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	None
		VRF	None
		DHCP client	None
		DHCP server	
		DHCP relay	
		DHCP policy VLAN	
		URPF check	The S6720LI and S6720S-LI do not support this function.
		Routing policies	None
		RIPv1/RIPv2	
		OSPF	
		BGP	The S6720LI and S6720S-LI do not support this function.
		MBGP	Only the S6720EI and S6720S-EI support this function.
		IS-IS	The S6720LI and S6720S-LI do not support this function.
		PBR (redirection in a traffic policy)	None

Feature		Description	Supplementary Information
	Multicast routing features	IGMPv1/v2/v3	The S6720LI and S6720S-LI do not support this function.
		PIM-DM	
		PIM-SM	
		MSDP	
		Multicast routing policies	
		RPF	
	IPv6 features	IPv6 protocol stack	None
		ND and ND snooping	
		DHCPv6 snooping	
		RIPng	
		DHCPv6 server	
		DHCPv6 relay	
		OSPFv3	
		BGP4+ & ISIS for IPv6	The S6720LI and S6720S-LI do not support this function.
		VRRP6	None
		MLDv1 and MLDv2	The S6720LI and S6720S-LI do not support this function.
		PIM-DM for IPv6	The S6720LI and S6720S-LI do not support this function.
		PIM-SM for IPv6	The S6720LI and S6720S-LI do not support this function.
	Transition technology	6 over 4 tunnel	The S6720LI and S6720S-LI do not support this function.
Layer 2 multicast features	-	IGMPv1/v2/v3 snooping	None
		Fast leave	
		IGMP snooping proxy	
		MLD snooping	
		Interface-based multicast traffic suppression	
		Inter-VLAN multicast replication	

Feature		Description	Supplementary Information
		Controllable multicast	
MPLS &VPN	Basic MPLS functions	LDP	The S6720LI, S6720S-LI, S6720SI, and S6720S-SI do not support this function.
		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	
	VPN	Multi-VPN-Instance CE (MCE)	None
		VLL in SVC, Martini, CCC, and Kompella modes	The S6720LI, S6720S-LI, S6720SI, and S6720S-SI do not support this function.
		VLL FRR	
		VPLS	
		MPLS L3VPN	
		IPSec Efficient VPN	The S6720LI and S6720S-LI do not support this function.
Device reliability	BFD	Basic BFD functions	The S6720LI and S6720S-LI do not support this function.
		BFD for static route/IS-IS/ OSPF/BGP	
		BFD for PIM	
		BFD for VRRP	
	Stacking	Service interface supporting the stacking function	None
	Others	VRRP	
Ethernet OAM	EFM OAM(802.3ah)	Automatic discovery	None
		Link fault detection	
		Link fault troubleshooting	
		Remote loopback	
	CFM OAM (802.1ag)	Software-level CCM	
		MAC ping	
		MAC trace	

Feature		Description	Supplementary Information
	Y.1731	Delay and variation measurement	
QoS features	Traffic classifier	Traffic classification based on ACLs	None
		Traffic classification based on outer 802.1p priorities, inner VLAN IDs, outer VLAN IDs, source MAC addresses, and Ethernet types	The S6720LI and S6720S-LI do not support this function.
		Traffic classification based on inner 802.1p priorities	The S6720LI, S6720S-LI, S6720SI, and S6720S-SI do not support this function.
	Traffic behavior	Access control after traffic classification	None
		Traffic policing based on traffic classification	
		Re-marking based on traffic classification	
		Adding classified packets into the specified queue	
		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)	Only the S6720EI and S6720S-EI support this function.
		Tail drop	Only the S6720LI, S6720S-LI, S6720SI, and S6720S-SI support this function.
	Congestion management	Priority Queuing (PQ)	None
		Weighted Deficit Round Robin (WDRR)	
		PQ+WDRR	
		Weighted Round Robin (WRR)	
		PQ+WRR	

Feature		Description	Supplementary Information
Configuration and maintenance	Login and configuration management	Command line configuration	None
		Error message and help information in English	
		Login through console and Telnet terminals	
		SSH1.5/SSH2	
		Send function and data communication between terminal users	
		Hierarchical user authority management and commands	
		SNMP-based NMS management (eSight)	
		Web page-based configuration and management	
		EasyDeploy (client)	
		EasyDeploy (commander)	The S6720LI, S6720S-LI, S6720SI, and S6720S-SI do not support this function.
		Easy deployment and maintenance	None
		SVF	Only the S6720EI and S6720S-EI can function as parents.
	File system	File system	None
		Directory and file management	
		File upload and download through FTP, TFTP, SFTP, SCP, and FTPS	
	Monitoring and maintenance	Hardware monitoring	
		Reporting alarms on abnormal device temperature	
		Second-time fault detection to prevent detection errors caused by instant interference	
		Version matching check	
		Information center and unified management over logs, alarms, and debugging information	

Feature		Description	Supplementary 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	The S6720LI, S6720S-LI, S6720SI, and S6720S-SI do not support this function.
		ARP packet rate limiting based on source IP addresses, interfaces, and VLANs, and global ARP packet rate limiting	None
		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	None
		IP source guard	
	Local attack defense	CPU attack defense	
	MFF	MAC-Forced Forwarding (MFF)	

Feature		Description	Supplementary Information
	DHCP snooping	DHCP snooping	
		Option 82 function and dynamic rate limiting for DHCP packets	
	Attack defense	Defense against flood attacks without IP payloads, attacks from IGMP null payload packets, LAND attacks, Smurf attacks, and attacks from packets with invalid TCP flag bits	
		Defense against attacks from many fragments, attacks from many packets with offsets, attacks from repeated packet fragments, Tear Drop attacks, Syndrop attacks, NewTear attacks, Bonk attacks, Nesta attacks, Rose attacks, Fawx attacks, Ping of Death attacks, and Jolt attacks	
		Defense against TCP SYN flood attacks, UDP flood attacks (including Fraggle attacks and UDP diagnosis port attacks), and ICMP flood attacks	
User access and authentication	AAA	Local authentication and authorization	None
		RADIUS authentication, authorization, and accounting	
		HWTACACS authentication, authorization, and accounting	
	NAC	802.1X authentication	
		MAC address authentication	
		Portal authentication	
		Hybrid authentication	
	Policy association	-	Only the S6720EI and S6720S-EI can function as control devices.
Network management	-	Ping and traceroute	None
		NQA	
		Network Time Protocol (NTP)	

Feature		Description	Supplementary Information
		sFlow	
		SNMP v1/v2c/v3	
		Standard MIB	
		HTTP	
		Hypertext Transfer Protocol Secure (HTTPS)	
		Remote network monitoring (RMON)	
		RMON2	Only the S6720EI and S6720S-EI support this function.

4.4 Product Features Supported by V200R010C00

Table 4-4 lists the features supported by the S6720.

Table 4-4 Features supported by the S6720

Feature		Description
Ethernet features	Ethernet	Full-duplex, half-duplex, and auto-negotiation modes on Ethernet interfaces
		Ethernet interface rates: 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 LNP (link type negotiation protocol), access, trunk, hybrid, and QinQ

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
		Adding double VLAN tags to packets based on interface
		Super VLAN
		VLAN mapping
		Selective QinQ
		MUX VLAN
		Voice VLAN
		Guest VLAN
	GVRP	Generic Attribute Registration Protocol (GARP)
		GARP VLAN Registration Protocol (GVRP)
	VCMP	VCMP (VLAN centralized management protocol)
	MAC	Automatic learning and aging of MAC addresses
		Static, dynamic, and blackhole MAC address entries
		Packet filtering based on source MAC addresses
		Interface-based MAC learning limiting
		Sticky MAC address entries
		MAC address flapping detection
		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
		Multi-port ARP for connecting to the NLB cluster server
Ethernet loop protection	MSTP	STP
		RSTP

Feature		Description
		MSTP
		VBST
		BPDU protection, root protection, and loop protection
		TC-BPDU attack defense
		STP loop detection
	Loopback-detect	Loop detection on an interface
	SEP	Smart Ethernet Protection (SEP)
	Smart Link	Smart Link
		Smart Link multi-instance
		Monitor Link
	RRPP	RRPP protective switchover
		Single RRPP ring, tangent RRPP ring, and intersecting RRPP ring
		Hybrid networking of RRPP rings and other ring networks
	ERPS	G.8032 v1/v2
		Single closed ring
		Subring
IPv4/IPv6 forwarding	IPv4 and unicast routes	Static IPv4 routes
		VRF
		DHCP client
		DHCP server
		DHCP relay
		DHCP policy VLAN
		URPF check
		Routing policies
		RIPv1/RIPv2
		OSPF
		BGP
		MBGP
		IS-IS

Feature		Description
		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
	Transition technology	6 over 4 tunnel
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
	VPN	Multi-VPN-Instance CE (MCE)
		VLL in SVC, Martini, CCC, and Kompella modes
		VLL FRR
		VPLS
		MPLS L3VPN
Device reliability	BFD	Basic BFD functions
		BFD for static route/IS-IS/OSPF/BGP
		BFD for PIM
		BFD for VRRP
	Stacking	Service interface supporting the stacking function
	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
	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

Feature		Description
		Re-marking based on traffic classification
		Adding classified packets into the specified queue
		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
Configuration and maintenance	Login and configuration management	Command line configuration
		Error message and help information in English
		Login through console and Telnet terminals
		SSH1.5/SSH2
		Send function and data communication between terminal users
		Hierarchical user authority management and commands
		SNMP-based NMS management (eSight)
		Web page-based configuration and management
		EasyDeploy (client)
		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

Feature		Description
	Monitoring and maintenance	Hardware monitoring
		Reporting alarms on abnormal device temperature
		Second-time fault detection to prevent detection errors caused by instant interference
		Version matching check
		Information center and unified management over logs, alarms, and debugging information
		Electronic labels, and command line query and backup
		Virtual cable test (VCT)
		User operation logs
		Detailed debugging information for network fault diagnosis
		Network test tools such as traceroute and ping commands
		Port mirroring, flow mirroring, and remote mirroring
		Energy saving
	Version upgrade	Device software loading and online software loading
		BootROM online upgrade
		In-service patching
Security	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 dynamic rate limiting for DHCP packets
	Attack defense	Defense against flood attacks without IP payloads, attacks from IGMP null payload packets, LAND attacks, Smurf attacks, and attacks from packets with invalid TCP flag bits
		Defense against attacks from many fragments, attacks from many packets with offsets, attacks from repeated packet fragments, Tear Drop attacks, Syndrop attacks, NewTear attacks, Bonk attacks, Nesta attacks, Rose attacks, Fawx attacks, Ping of Death attacks, and Jolt attacks
		Defense against TCP SYN flood attacks, UDP flood attacks (including Fraggle attacks and UDP diagnosis port attacks), and ICMP flood attacks
User access and authentication	AAA	Local authentication and authorization
		RADIUS authentication, authorization, and accounting
		HWTACACS authentication, authorization, and accounting
	NAC	802.1X authentication
		MAC address authentication
		Portal authentication
		Hybrid authentication
	Policy association	-
Network management	-	Ping and traceroute
		NQA
		Network Time Protocol (NTP)
		sFlow
		SNMP v1/v2c/v3
		Standard MIB
		HTTP
		Hypertext Transfer Protocol Secure (HTTPS)
		Remote network monitoring (RMON)
		RMON2

4.5 Product Features Supported by V200R009C00

Table 4-5 lists the features supported by the S6720.

Table 4-5 Features supported by the S6720

Feature		Description
Ethernet features	Ethernet	Full-duplex, half-duplex, and auto-negotiation modes on Ethernet interfaces
		Ethernet interface rates: 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 LNP (link type negotiation protocol), access, trunk, hybrid, and QinQ
		Default VLAN
		VLAN assignment based on interfaces, MAC addresses, protocols, and IP subnets
		VLAN assignment based on the following policies: ● MAC address + IP address ● MAC address + IP address + interface number
		Adding double VLAN tags to packets based on interface
		Super VLAN
		VLAN mapping
		Selective QinQ

Feature		Description
		MUX VLAN
		Voice VLAN
		Guest VLAN
	GVRP	Generic Attribute Registration Protocol (GARP)
		GARP VLAN Registration Protocol (GVRP)
	VCMP	VCMP (VLAN centralized management protocol)
	MAC	Automatic learning and aging of MAC addresses
		Static, dynamic, and blackhole MAC address entries
		Packet filtering based on source MAC addresses
		Interface-based MAC learning limiting
		Sticky MAC address entries
		MAC address flapping detection
		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
		Multi-port ARP for connecting to the NLB cluster server
Ethernet loop protection	MSTP	STP
		RSTP
		MSTP
		VBST
		BPDU protection, root protection, and loop protection
		TC-BPDU attack defense
		STP loop detection
	Loopback-detect	Loop detection on an interface
	SEP	Smart Ethernet Protection (SEP)
	Smart Link	Smart Link

Feature		Description
		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
		DHCP policy VLAN
		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

Feature		Description
		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
	Transition technology	6 over 4 tunnel
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
	VPN	Multi-VPN-Instance CE (MCE)
		VLL in SVC, Martini, CCC, and Kompella modes
		VLL FRR
		VPLS

Feature		Description
		MPLS L3VPN
Device reliability	BFD	Basic BFD functions
		BFD for static route/IS-IS/OSPF/BGP
		BFD for PIM
		BFD for VRRP
	Stacking	Service interface supporting the stacking function
	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
	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
		Adding classified packets into the specified queue
		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
Configuration and maintenance	Login and configuration management	Command line configuration
		Error message and help information in English
		Login through console and Telnet terminals
		SSH1.5/SSH2
		Send function and data communication between terminal users
		Hierarchical user authority management and commands
		SNMP-based NMS management (eSight)
		Web page-based configuration and management
		EasyDeploy (client)
		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
		Reporting alarms on abnormal device temperature
		Second-time fault detection to prevent detection errors caused by instant interference
		Version matching check
		Information center and unified management over logs, alarms, and debugging information
		Electronic labels, and command line query and backup
		Virtual cable test (VCT)
		User operation logs

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 dynamic rate limiting for DHCP packets
	Attack defense	Defense against flood attacks without IP payloads, attacks from IGMP null payload packets, LAND attacks, Smurf attacks, and attacks from packets with invalid TCP flag bits
		Defense against attacks from many fragments, attacks from many packets with offsets, attacks from repeated packet fragments, Tear Drop attacks, Syndrop attacks, NewTear attacks, Bonk attacks, Nesta attacks, Rose attacks, Fawx attacks, Ping of Death attacks, and Jolt attacks

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
	NAC	802.1X authentication
		MAC address authentication
		Portal authentication
		Hybrid authentication
	Policy association	-
Network management	-	Ping and traceroute
		NQA
		Network Time Protocol (NTP)
		sFlow
		SNMP v1/v2c/v3
		Standard MIB
		HTTP
		Hypertext Transfer Protocol Secure (HTTPS)
		Remote network monitoring (RMON)
		RMON2

4.6 Product Features Supported by V200R008C00

Table 4-6 lists the features supported by the S6720.

Table 4-6 Features supported by the S6720

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

Feature		Description
		Ethernet interface rates: 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 LNP (link type negotiation protocol), access, trunk, hybrid, and QinQ
		Default VLAN
		VLAN assignment based on interfaces, MAC addresses, protocols, and IP subnets
		VLAN assignment based on the following policies: ● MAC address + IP address ● MAC address + IP address + interface number
		Adding double VLAN tags to packets based on interface
		Super VLAN
		VLAN mapping
		Selective QinQ
		MUX VLAN
		Voice VLAN
		Guest VLAN
	GVRP	Generic Attribute Registration Protocol (GARP)
		GARP VLAN Registration Protocol (GVRP)
	VCMP	VCMP (VLAN centralized management protocol)
	MAC	Automatic learning and aging of MAC addresses

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
		Multi-port ARP for connecting to the NLB cluster server
Ethernet loop protection	MSTP	STP
		RSTP
		MSTP
		VBST
		BPDU protection, root protection, and loop protection
		TC-BPDU attack defense
		STP loop detection
	Loopback-detect	Loop detection on an interface
	SEP	Smart Ethernet Protection (SEP)
	Smart Link	Smart Link
		Smart Link multi-instance
		Monitor Link
	RRPP	RRPP protective switchover
		Single RRPP ring, tangent RRPP ring, and intersecting RRPP ring
		Hybrid networking of RRPP rings and other ring networks
	ERPS	G.8032 v1/v2
		Single closed ring

Feature		Description
		Subring
IPv4/IPv6 forwarding	IPv4 and unicast routes	Static IPv4 routes
		VRF
		DHCP client
		DHCP server
		DHCP relay
		DHCP policy VLAN
		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

Feature		Description
		MLDv1 and MLDv2
		PIM-DM for IPv6
		PIM-SM for IPv6
	Transition technology	6 over 4 tunnel
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
	VPN	Multi-VPN-Instance CE (MCE)
		VLL in SVC, Martini, CCC, and Kompella modes
		VLL FRR
		VPLS
		MPLS L3VPN
Device reliability	BFD	Basic BFD functions
		BFD for static route/IS-IS/OSPF/BGP
		BFD for PIM
		BFD for VRRP
	Stacking	Service interface supporting the stacking function
	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
	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
		Adding classified packets into the specified queue
		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
Configuration and maintenance	Login and configuration management	Command line configuration
		Error message and help information in English
		Login through console and Telnet terminals

Feature		Description
		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
		Reporting alarms on abnormal device temperature
		Second-time fault detection to prevent detection errors caused by instant interference
		Version matching check
		Information center and unified management over logs, alarms, and debugging information
		Electronic labels, and command line query and backup
		Virtual cable test (VCT)
		User operation logs
		Detailed debugging information for network fault diagnosis
		Network test tools such as traceroute and ping commands
		Port mirroring, flow mirroring, and remote mirroring
		Energy saving
	Version upgrade	Device software loading and online software loading
		BootROM online upgrade
		In-service patching
Security	AAA	Local authentication and authorization

Feature		Description
		RADIUS authentication, authorization, and accounting
		HWTACACS authentication, authorization, and accounting
	NAC	802.1X authentication
		MAC address authentication
		Portal authentication
		Hybrid 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 dynamic rate limiting for DHCP packets
	Attack defense	Defense against flood attacks without IP payloads, attacks from IGMP null payload packets, LAND attacks, Smurf attacks, and attacks from packets with invalid TCP flag bits
		Defense against attacks from many fragments, attacks from many packets with offsets, attacks from repeated packet fragments, Tear Drop attacks, Syndrop attacks, NewTear attacks, Bonk attacks, Nesta attacks, Rose attacks, Fawx attacks, Ping of Death attacks, and Jolt attacks

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

4.7 Product Features Supported by V200R005C00

NOTE

Features marked with * are added in V200R005C00.

Table 4-7 lists the features supported by the S6700.

Table 4-7 Features supported by the S6700

Feature		Description
Ethernet features	Ethernet	Full-duplex, half-duplex, and auto-negotiation modes on Ethernet interfaces
		Ethernet interface rates: 1000 Mbit/s, 10 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 and forwarding restriction
		Broadcast storm suppression
	VLAN	Access modes of LNP* (link type negotiation protocol), access, trunk, hybrid, and QinQ
		Default VLAN
		VLAN assignment based on interfaces, MAC addresses, protocols, and IP subnets
		VLAN assignment based on the following policies: ● MAC address + IP address ● MAC address + IP address + interface number
		Adding double VLAN tags to packets based on interface
		Super VLAN
		VLAN mapping
		Selective QinQ
		MUX VLAN
		Voice VLAN
		Guest VLAN
	GVRP	Generic Attribute Registration Protocol (GARP)
		GARP VLAN Registration Protocol (GVRP)
	VCMP*	VCMP (VLAN centralized management protocol)
	MAC	Automatic learning and aging of MAC addresses
		Static, dynamic, and blackhole MAC address entries
		Packet filtering based on source MAC addresses
		Interface-based MAC learning limiting
		Sticky MAC address entries
		MAC address flapping detection
		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
		Multi-port ARP for connecting to the NLB cluster server
Ethernet loop protection	MSTP	STP
		RSTP
		MSTP
		VBST*
		BPDU protection, root protection, and loop protection
		TC-BPDU attack defense
		STP loop detection
	Loopback-detect	Loop detection on an interface
	SEP	Smart Ethernet Protection (SEP)
	Smart Link	Smart Link
		Smart Link multi-instance
		Monitor Link
	RRPP	RRPP protective switchover
		Single RRPP ring, tangent RRPP ring, and intersecting RRPP ring
		Hybrid networking of RRPP rings and other ring networks
	ERPS	G.8032 v1/v2
		Single closed ring
		Subring
IPv4/IPv6 forwarding	IPv4 and unicast routes	Static IPv4 routes
		VRF
		DHCP client
		DHCP server
		DHCP relay
		DHCP policy VLAN
		URPF check
		Routing policies

Feature		Description
		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
	Transition technology	6 over 4 tunnel
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
	VPN	Multi-VPN-Instance CE (MCE)
		VLL* in SVC, Martini, CCC, and Kompella modes
		VLL FRR*
		VPLS*
		MPLS L3VPN*
Device reliability	BFD	Basic BFD functions
		BFD for static route/IS-IS/OSPF/BGP
		BFD for PIM
		BFD for VRRP
	Stacking	Service interface supporting the stacking function
	Others	VRRP
Ethernet OAM	EFM OAM(802.3ah)	Automatic discovery
		Link fault detection
		Link fault troubleshooting
		Remote loopback
	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
		Adding classified packets into the specified queue
		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
Configuration and maintenance	Login and configuration management	Command line configuration
		Error message and help information in English
		Login through console and Telnet terminals
		SSH1.5/SSH2
		Send function and data communication between terminal users
		Hierarchical user authority management and commands
		SNMP-based NMS management (eSight)
		Web page-based configuration and management
		EasyDeploy (client)
		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
		Reporting alarms on abnormal device temperature
		Second-time fault detection to prevent detection errors caused by instant interference
		Version matching check
		Information center and unified management over logs, alarms, and debugging information
		Electronic labels, and command line query and backup
		Virtual cable test (VCT)
		User operation logs
		Detailed debugging information for network fault diagnosis
		Network test tools such as traceroute and ping commands
		Port mirroring, flow mirroring, and remote mirroring
		Energy saving
	Version upgrade	Device software loading and online software loading
		BootROM online upgrade
		Remote in-service upgrade
		In-service patching
Security	AAA	Local authentication and authorization
		RADIUS authentication, authorization, and accounting
		HWTACACS authentication, authorization, and accounting
	NAC	802.1X authentication
		MAC address authentication
		Portal authentication
		Hybrid authentication
	ARP security	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

Feature		Description
		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 dynamic rate limiting for DHCP packets
	Attack defense	Defense against flood attacks without IP payloads, attacks from IGMP null payload packets, LAND attacks, Smurf attacks, and attacks from packets with invalid TCP flag bits
		Defense against attacks from many fragments, attacks from many packets with offsets, attacks from repeated packet fragments, Tear Drop attacks, Syndrop attacks, NewTear attacks, Bonk attacks, Nesta attacks, Rose attacks, Fawx attacks, Ping of Death attacks, and Jolt attacks
		Defense against TCP SYN flood attacks, UDP flood attacks (including Fraggle attacks and UDP diagnosis port attacks), and ICMP flood attacks
Network management	-	Ping and traceroute
		NQA
		Network Time Protocol (NTP)
		sFlow
		SNMP v1/v2c/v3
		Standard MIB
		HTTP
		Hypertext Transfer Protocol Secure (HTTPS)
		Remote network monitoring (RMON)
		RMON2*

4.8 Product Features Supported by V200R003C00

Table 4-8 lists the features supported by the S6700.

Table 4-8 Features supported by the S6700

Feature		Description
Ethernet features	Ethernet	Full-duplex, half-duplex, and auto-negotiation modes on Ethernet interfaces
		Ethernet interface rates: 1000 Mbit/s, 10 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 and forwarding restriction
		Broadcast storm suppression
	VLAN	Access modes of LNP (link type negotiation protocol), access, trunk, hybrid, and QinQ
		Default VLAN
		VLAN assignment based on interfaces, MAC addresses, protocols, and IP subnets
		VLAN assignment based on the following policies: ● MAC address + IP address ● MAC address + IP address + interface number
		Adding double VLAN tags to packets based on interface
		Super VLAN
		VLAN mapping
		Selective QinQ

Feature		Description
		MUX VLAN
		Voice VLAN
		Guest VLAN
	GVRP	Generic Attribute Registration Protocol (GARP)
		GARP VLAN Registration Protocol (GVRP)
	VCMP	VCMP (VLAN centralized management protocol)
	MAC	Automatic learning and aging of MAC addresses
		Static, dynamic, and blackhole MAC address entries
		Packet filtering based on source MAC addresses
		Interface-based MAC learning limiting
		Sticky MAC address entries
		MAC address flapping detection
		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
		Multi-port ARP for connecting to the NLB cluster server
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

Feature		Description
		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
		DHCP policy VLAN
		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

Feature		Description
		DHCPv6 snooping
		RIPng
		DHCPv6 server
		DHCPv6 relay
		OSPFv3
		BGP4+ & ISIS for IPv6
		VRRP6
		MLDv1 and MLDv2
		PIM-DM for IPv6
		PIM-SM for IPv6
	Transition technology	6 over 4 tunnel
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
MCE	-	Multi-VPN-Instance CE (MCE)
Device reliability	BFD	Basic BFD functions
		BFD for static route/IS-IS/OSPF/BGP
		BFD for PIM
		BFD for VRRP
	Stacking	Service interface supporting the stacking function
	Others	VRRP
Ethernet OAM	EFM OAM(802.3ah)	Automatic discovery
		Link fault detection
		Link fault troubleshooting
		Remote loopback

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
		Adding classified packets into the specified queue
		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
Configuration and maintenance	Login and configuration management	Command line configuration
		Error message and help information in English
		Login through console and Telnet terminals
		SSH1.5/SSH2
		Send function and data communication between terminal users
		Hierarchical user authority management and commands
		SNMP-based NMS management (eSight)
		Web page-based configuration and management
		EasyDeploy (client)

Feature		Description
		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
		Reporting alarms on abnormal device temperature
		Second-time fault detection to prevent detection errors caused by instant interference
		Version matching check
		Information center and unified management over logs, alarms, and debugging information
		Electronic labels, and command line query and backup
		Virtual cable test (VCT)
		User operation logs
		Detailed debugging information for network fault diagnosis
		Network test tools such as traceroute and ping commands
		Port mirroring, flow mirroring, and remote mirroring
		Energy saving
	Version upgrade	Device software loading and online software loading
		BootROM online upgrade
		Remote in-service upgrade
		In-service patching
Security	AAA	Local authentication and authorization
		RADIUS authentication, authorization, and accounting
		HWTACACS authentication, authorization, and accounting
	NAC	802.1X authentication
		MAC address authentication
		Portal authentication

Feature		Description
		Hybrid authentication
	ARP security	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 dynamic rate limiting for DHCP packets
	Attack defense	Defense against flood attacks without IP payloads, attacks from IGMP null payload packets, LAND attacks, Smurf attacks, and attacks from packets with invalid TCP flag bits
		Defense against attacks from many fragments, attacks from many packets with offsets, attacks from repeated packet fragments, Tear Drop attacks, Syndrop attacks, NewTear attacks, Bonk attacks, Nesta attacks, Rose attacks, Fawx attacks, Ping of Death attacks, and Jolt attacks
		Defense against TCP SYN flood attacks, UDP flood attacks (including Fraggle attacks and UDP diagnosis port attacks), and ICMP flood attacks
Network management	-	Ping and traceroute
		NQA
		Network Time Protocol (NTP)
		sFlow
		SNMP v1/v2c/v3

Feature		Description
		Standard MIB
		HTTP
		Hypertext Transfer Protocol Secure (HTTPS)
		Remote network monitoring (RMON)

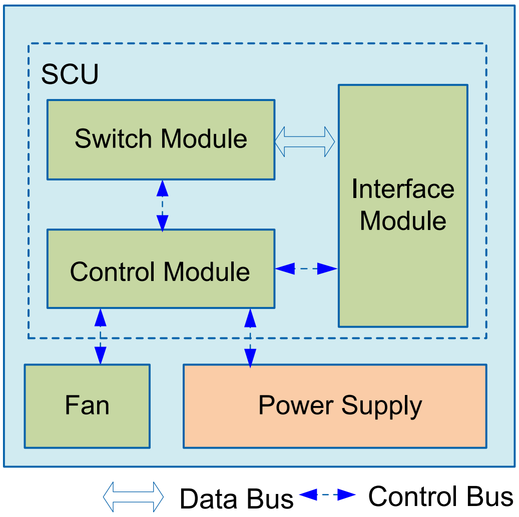
5 Hardware Information

For the version mappings, appearance and structure, port description, indicator description, power supply configuration, heat dissipation, and specifications of the S6700, see the Chassis section in the *S6700 Hardware Description*.

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

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

Figure 5-1 Logical structure of hardware modules



SCU

The SCU is built in the S6700. Each switch has one SCU.

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

Main Control Module

The main control module provides the following functions:

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

Switching Module

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

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

Interface Module

The interface module provides Ethernet interfaces for Ethernet service transmission.

Power Supply

For details about S6700 power supply configuration, see the Power Modules section in the *S6700 Hardware Description*.

Cards

The S6700 supports service cards. Service cards allow for flexible networking and provide cost-effective customized solutions.

For details about cards supported by the S6700, see the Cards section in the *S6700 Hardware Description*.

Fan Modules

For details about fan modules in different models, see "Heat Dissipation" under Chassis in the *S6700 Hardware Description*.

Pluggable Modules for Interfaces

For specifications of various pluggable modules for interfaces, see the Pluggable Modules for Interfaces section in the *S6700 Hardware Description*.

6 References

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