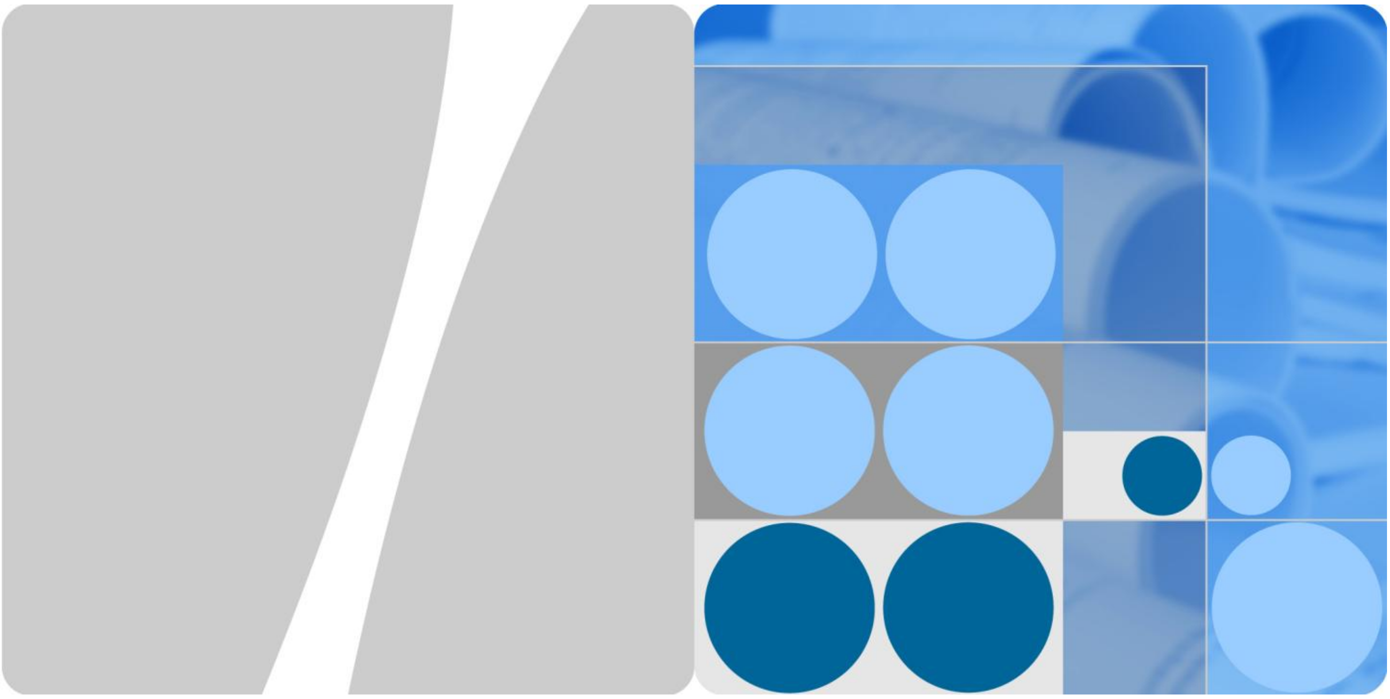


S1700 Managed Series Ethernet Switches V100R007C00

Product Description

Issue	**03**
Date	**2012-10-25**

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: http://enterprise.huawei.com

About This Document

Intended Audience

This document describes the product position, product characteristics, product architecture, link features, service features, networking and applications, operation, maintenance and system technical specifications of S1700.

This document provides guides to get the information about how to construct a network.

This document is intended for:

- Policy planning engineers
- Installation and commissioning engineers
- NM configuration engineers
- Technical support engineers
- FAE
- Network monitoring engineers
- System maintain engineers

Conventions

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

Symbol	Description
⚠ DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injury.
⚠ CAUTION	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
TIP	Indicates a tip that may help you solve a problem or save time.
NOTE	Provides additional information to emphasize or supplement important points of the main text.

Change History

Changes between document issues are cumulative. Therefore, the latest document issue contains all changes made in previous issues.

Issue 03（2012-10-25）

Compare to Issue 02 (2012-05-24) :

Optimize some pictures in version 02.

Issue 02 (2012-05-24)

Compare to Issue 01 (2012-03-05):

Revise Contact Information.

Issue 01(2012-03-05)

Initial release.

Contents

About This Document ii

1 Product Positioning and Features 1

1.1 Product Positioning 1

1.2 Product Characteristics 1

1.2.1 Flexible Networking Capability 2

1.2.2 Comprehensive Security Measures 2

1.2.3 Convenient Operation and Maintenance 2

1.2.4 Energy-Saving Design 2

1.2.5 Advanced Lightning Protection Technologies 3

2 Product Architecture 4

2.1 Overview 4

2.2 Device Structure 4

2.3 Hardware Modules 7

2.3.1 SCU 8

2.3.2 Power Supply 9

3 Link Features 10

3.1 Ethernet Features 10

3.1.1 Flow Control on an Interface 10

3.1.2 Interface Speed 11

3.1.3 Duplex 11

3.1.4 Auto-negotiation 11

3.1.5 Jumbo Frame 11

3.1.6 Link Aggregation 11

3.1.7 VLAN 12

3.1.8 MAC 12

3.2 STP 13

3.2.1 STP,RSTP and MSTP 13

3.3 Multicast 13

3.3.1 IGMP Snooping 13

3.3.2 Fast Leave of Multicast Member Interface 13

3.4 Link Detection 13

4 Service Features 15
4.1 ACL Control 15
4.2 QoS 15
4.2.1 QoS Interface 16
4.2.2 Priority Mapping 16
4.2.3 DSCP Mapping 16
4.2.4 IP Precedence Mapping 16
4.2.5 Service Level Mapping 16
4.2.6 QoS Scheduling 16
4.2.7 Traffic Management 17
4.2.8 SERD 17
4.2.9 Traffic Shaping 17
4.3 Security 18
4.3.1 Hierarchical Web Protection 18
4.3.2 AAA 19
4.3.3 RADIUS 19
4.3.4 SSL Connection 19
4.3.5 VLAN 19
4.3.6 MAC Table Searching Based on VLAN+MAC 19
4.3.7 Guest VLAN 19
4.3.8 Port Security 19
4.3.9 DoS Attack Prevetion 20
4.3.10 Worm Prevention 20
4.3.11 MAC Attack 20
4.3.12 Port Isolation 20
4.3.13 Storm Control 20
4.3.14 Storm Suppression 20
4.3.15 802.1X Authentication 20
4.3.16 Acess control based on MAC adress 21
4.3.17 MAC Authentication 21
4.3.18 DHCP Snooping 21
4.3.19 IPSG 21
4.3.20 DAI 21
4.4 Network Management 21
4.4.1 SNMP 22
4.4.2 RMON 22
4.4.3 LLDP 22
4.4.4 LLDP-MED 22
4.5 Routing 23
5 Networking and Applications 24
5.1 Access on an Enterprise Network or a Campus Network 24

5.2 Desktop Access 25

6 Maintenance and Network Management System 26

6.1 Maintenance and Management 26

6.1.1 Configuration Methods 26

6.1.2 Monitoring and Maintenance 27

6.1.3 Diagnosis and Debugging 27

6.1.4 Software Upgrade 28

7 System Technical Specifications 29

7.1 Physical Parameters 29

7.2 Optical Module Attributes 30

7.3 System Configuration 31

7.4 List of Software Features 32

1 Product Positioning and Features

About This Chapter

1.1 Product Positioning

1.2 Product Characteristics

1.1 Product Positioning

CAUTION

The S1700 Managed Series Ethernet Switches are class A products. The switches that are operating may cause radio interference. Customers need to take prevention measures.

The S1700 Managed Series Ethernet Switches (hereinafter referred to as the S1700) provide the connection and transmission functions. They are developed by Huawei to meet the requirements for reliable access and high-quality transmission of multiple services on the enterprise network.

Positioned for the access layer of the enterprise network, the S1700 provides large capacity, high port density, and cost-effective packet forwarding capabilities. In addition, the S1700 provides multi-service access capabilities, excellent extensibility, quality of service (QoS) guarantee, powerful multicast replication, and carrier-class security, and can be used to build ring topologies of high reliability.

The S1700 Series include S1700-28FR-2T2P-AC, S1700-28GFR-4P-AC, S1700-52FR-2T2P-AC and S1700-52GFR-4P-AC.

1.2 Product Characteristics

1.2.1 Flexible Networking Capability

1.2.2 Comprehensive Security Measures

1.2.3 Convenient Operation and Maintenance

1.2.4 Energy-Saving Design

1.2.5 Advanced Lightning Protection Technologies

1.2.1 Flexible Networking Capability

The S1700 provides 10/100/1000BASE-T Ethernet electrical interfaces, and 1000BASE-X Ethernet optical interfaces. It supports multiple interface types such as access, Trunk, and hybrid.

The S1700 supports swappable Small Form-Factor Pluggable (SFP) optical modules for optical fiber connections. The length of optical fibers can be selected according to the transmission distance.

The S1700 can be used to construct a tree, star, or ring Ethernet network. For the ring Ethernet, the S1700 supports the STP/RSTP/MSTP to prevent loops and provide rapid switchover.

1.2.2 Comprehensive Security Measures

The S1700 guarantees the security of network devices and data transmission. It provides the following security measures to protect the network against attacks initiated by malicious users:

- Mechanism of searching the forwarding table based on VLAN IDs and MAC addresses
- Support traffic suppression

In addition, the S1700 provides the following functions to ensure secure login of users:

- Providing login passwords and password encryption for login users
- Protecting commands through users levels
- Displaying confirm or prompt information for important commands that affect system performance

1.2.3 Convenient Operation and Maintenance

S1700 provides an interface based traffic statistic function, and supports Ping fault detection and locating technique on an IP network.

1.2.4 Energy-Saving Design

The S1700 adopts the following measures to save energy:

- S1700-28FR-2T2P-AC, S1700-28GFR-4P-AC and S1700-52FR-2T2P-AC adopt natural heat dissipation so that power consumed by fans is saved.
- The chip switches to the power saving mode when no connected device is detected on a service interface, that is, the interface is idle.
- It uses highly-integrated and energy-saving chips produced through advanced processing techniques. With the help of the intelligent device management system, the chips not only improve system performance but also greatly reduce power consumption of the entire system.
- 1700-28GFR-4P-AC and S1700-52gfr-4P-AC support Power Saving and IEEE 802.3az function.

Natural heat dissipation has the following advantages:

- The product reliability is high.

- There is no noise pollution.
- You do not need to maintain the fans, which saves the maintenance cost.
- The system does not have additional power consumption generated by fans, which improves the power efficiency.
- Boards are prevented from being eroded.

1.2.5 Advanced Lightning Protection Technologies

The S1700 adopts the built-in lightning protection technologies, which reduce the probability of damages and greatly improve the device reliability.

2 Product Architecture

About This Chapter

2.1 Overview

2.2 Device Structure

2.3 Hardware Modules

2.1 Overview

The S1700 Managed Series Ethernet Switches adopt an integrated hardware platform. The hardware system consists of the chassis, power supply panel, switch control unit (SCU). The width of overall system complies with industry standards, and can be installed in cabinet complying with IEC297 standard or cabinet complying with ETSI standard.

Currently the S1700 Managed Series Ethernet Switches include:

1700-28FR-2T2P-AC

S1700-28GFR-4P-AC

S1700-52FR-2T2P-AC

S1700-52GFR-4P-AC

2.2 Device Structure

The S1700 Managed Series Ethernet Switches adopt an integrated hardware platform. An S1700 consists of the chassis, power supply unit and switch control unit (SCU). The width of an S1700 complies with industry standards, and the S1700 can be installed in an IEC297 cabinet or an ETSI cabinet.

NOTE

The S1700 is 1 U (1 U = 44.45 mm) high.

The dimensions of the device are 442mm x 219.85mm x 43.8 mm (width x depth x height).

S1700 Appearances

Table 2-1shows the front views of S1700.

Table 2-1 S1700 Front Views

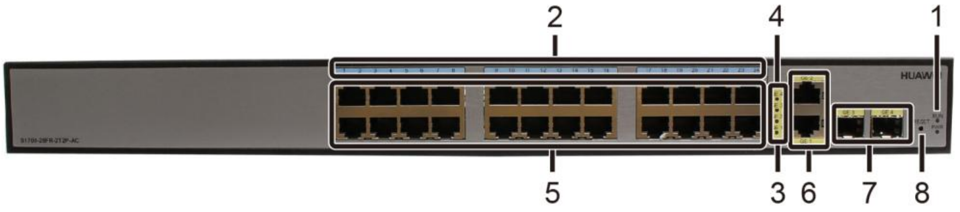
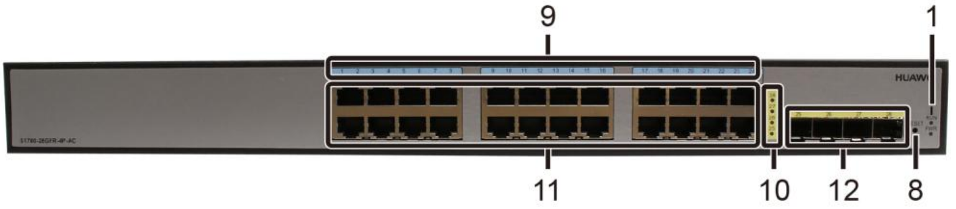
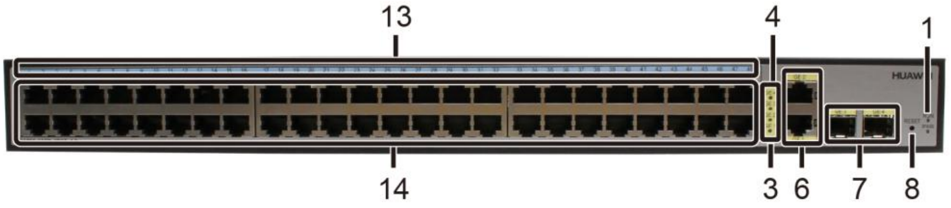
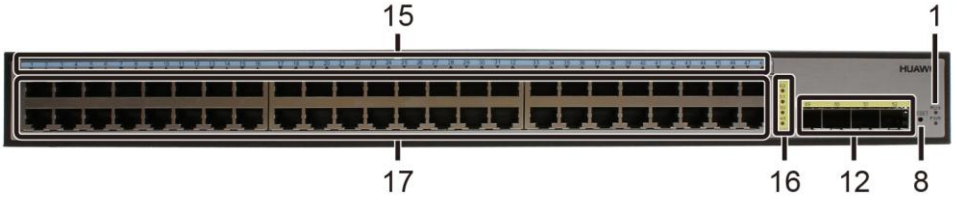
Model	Image
S1700-28FR-2T2P-AC	
S1700-28GFR-4P-AC	
S1700-52FR-2T2P-AC	
S1700-52GFR-4P-AC	

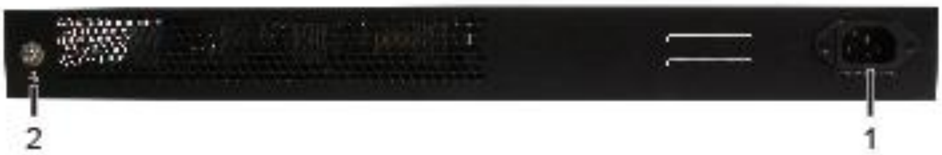
Table 2-2 showsThe interfaces and LEDs of S1700 are as follows.

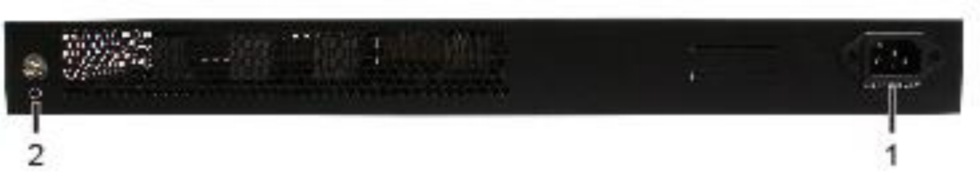
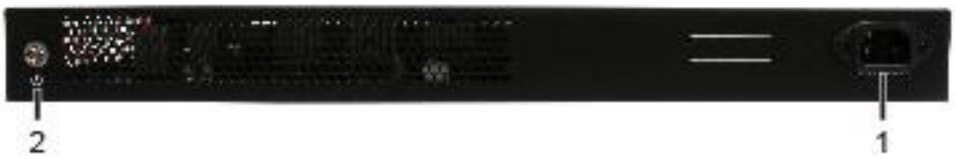
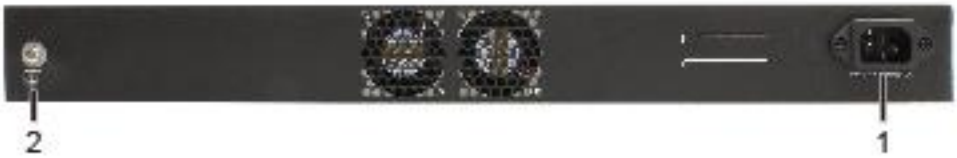
Table 2-2 S1700 Interfaces and LEDs

1. Power/Run LEDs	2. 1-24 10/100BASE-T Ethernet interfaces LEDs	3. GE1-GE2 10/100/1000BASE-T Ethernet interfaces LEDs	4. GE3-GE4 1000BASE-T Ethernet optical interfaces LEDs
5. 24 10/100BASE-T Ethernet interfaces	6. 2 10/100/1000BASE-T Ethernet interfaces	7. 2 1000BASE-X Ethernet optical interfaces	8. Reset button
9. 1-24 10/100/1000 BASE-T Ethernet interfaces LEDs	10. 25-28 1000BASE-X Ethernet optical interfaces LEDs	11. 24 10/100BASE-T Ethernet interfaces	12. 4 1000BASE-X Ethernet optical interfaces
13. 1-48 10/100BASE-T Ethernet interfaces LEDs	14. 48 10/100BASE-T Ethernet interfaces	15. 1-48 10/100/1000 BASE-T Ethernet interfaces LEDs	16. 49-52 1000BASE-X Ethernet optical interfaces LEDs
17. 48 10/100/1000BASE-T Ethernet interfaces	-	-	-

Table 2-3 shows the rear views of S1700.

Table 2-3 S1700 Rear Views

Model	Image
S1700-28 FR-2T2P-AC	

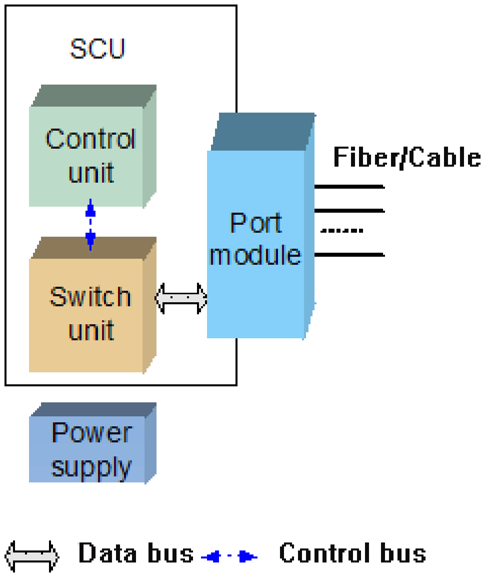
Model	Image
S1700-28 GFR-4P-AC	
S1700-52 FR-2T2P-AC	
S1700-52 GFR-4P-AC	

1. AC jack	2. Ground screw	-	-

2.3 Hardware Modules

Figure 2-1shows the logical structure of hardware modules of the S1700.

Figure 2-1 Logical Structure of Hardware Modules for S1700



Hardware modules of S1700 includes SCU and power supply

2.3.1 SCU

2.3.2 Power Supply

2.3.1 SCU

SCU is the switch control unit of S1700 and fixed on it. Each S1700 has one SCU.

The SCU is responsible for message switching and device management. It integrates multiple functional modules, namely, the main control module, switching module, and interface module.

Main Control Module

The main control module provides the following functions:

- Processing protocols
- Functioning as an agent of the user to manage the system and monitor the system performance according to instructions of the user, and report the running status of the device to the user
- Monitoring and maintaining the interface module and switching module on the SCU.

Switching Module

The switching module, also called the switching fabric, is responsible for message switching, multicast replication, QoS scheduling, and access control on the interface module of the SCU.

The switching module adopts high performance ASIC chips to implement line-speed forwarding and fast switching of data with different priorities.

Interface Module

The interface module provides Ethernet interfaces for accessing Ethernet services.

2.3.2 Power Supply

The S1700 can use the AC power supply.

Table 2-4 Power Supply

Device Name	AC	DC
S1700-28FR-2T2P-AC	Y	N
S1700-28GFR-4P-AC	Y	N
S1700-52FR-2T2P-AC	Y	N
S1700-52GFR-4P-AC	Y	N

3 Link Features

About This Chapter

3.1 Ethernet Features

3.2 STP

3.3 Multicast

3.4 Link Detection

3.1 Ethernet Features

3.1.1 Flow Control on an Interface

3.1.2 Interface Speed

3.1.3 Duplex

3.1.4 Auto-negotiation

3.1.5 Jumbo Frame

3.1.6 Link Aggregation

3.1.7 VLAN

3.1.8 MAC

3.1.1 Flow Control on an Interface

Flow control on an interface is a method of congestion management. It applies to all types of flows. The S1700 implements flow control on an interface by using the hardware backpressure mechanism. When an interface works in full duplex mode, the S1700 implements flow control complying with IEEE 802.3x. When the interface works in half duplex mode, the S1700 implements flow control through the backpressure mechanism (peer side device needs to enable the function of flow control auto-negotiation).

When congestion occurs, the S1700 sends continuous Pause frames to the upstream device, requesting it to stop sending data for a specified period of time. When the upstream device receives the pause frames, it reduces the total volume of traffic sent from its egress interface.

This interface flow control mechanism does not differentiate flow types and is effective to all types of flows.

3.1.2 Interface Speed

Usually interface of switch are all multi-speed adaptive, FastEthernet interface having two speeds of 10/100M, and GigabitEthernet interface having three speeds of 10/100/1000M. By default, operating speed of interface is determined by way of auto-negotiation. Interface can be assigned with only one fixed speed by manual configuration.

3.1.3 Duplex

Interface of switch can operate in half-duplex or duplex mode, and operating speed of interface is determined by way of auto-negotiation by default. Interface can be assigned with only one fixed speed by manual configuration.

3.1.4 Auto-negotiation

Auto-negotiation indicates that interface adjust its speed to the highest public level automatically according to the connection speed and duplex mode the device of the other end, thus both ends can obtain the highest speed and duplex mode.

3.1.5 Jumbo Frame

Jumbo frame is a manufacturer standard jumbo frame format, specially designed for GigabitEthernet. Using Jumbo frame can enable Gigabitethernet to perform fully, and improve the efficiency of data transmission for 50%-100%. Jumbo frame needs a support on two intercommunicated ports at the same time.

3.1.6 Link Aggregation

Link aggregation is a function that binds multiple physical interfaces on one device into a logical interface (such as an Eth-Trunk). This logical interface is also called a load balancing group or a link aggregation group.

After multiple physical interfaces are bound into a logical interface, the S1700 load balances the traffic passing through the logical interface among the member interfaces. When a member interface fails, the traffic on this interface is shared by the other member interfaces without interrupting services. When the faulty interface recovers, the traffic is balanced among all interfaces again.

Currently, the S1700 supports binding between FE interfaces (a mixed binding can be implemented to FE and GE interfaces) or GE interfaces. Load balancing can be implemented based on the following information:

- Source MAC address
- Destination MAC address
- Source MAC address and destination MAC address
- Source IP address
- Destination IP address
- Source IP address and destination IP address

Using the link aggregation technology, you can increase the bandwidth and improve link reliability without upgrading the hardware, thus saving costs.

3.1.7 VLAN

A local area network (LAN) can be divided into several logical LANs. Each logical LAN is a broadcast domain, which is called a virtual LAN (VLAN). To put it simply, devices on a LAN are logically grouped into different LAN segments, irrespective of their physical locations. In this manner, VLANs isolate broadcast domains on a LAN.

Methods to Divide VLANs

A physical LAN can be divided into several VLANs, and several physical LANs can be grouped into a VLAN. Devices on a VLAN belong to the same broadcast domain and can communicate with each other. Different VLANs are isolated from each other, so devices on different VLANs cannot communicate with each other.

S1700 supports the following methods to divide VLANs:

- Based on interfaces

  VLAN members are defined according to device interfaces, and the specified interfaces on device are added into different VLANs, thus messages received by the interface can be transmitted only on corresponding VLAN.

- Based on MAC

  VLAN members are defined according to MAC addresses, and the specified MAC addresses are added into different VLANs, thus messages received by the MAC addresses can be transmitted only on corresponding VLAN.

Voice VLAN

A voice VLAN is used to transmit voice data flows. You can create a voice VLAN and add the interface connected to the voice device to the voice VLAN. Then voice data flows can be transmitted on the voice VLAN.

A way of Voice VLAN is applied, convenient for voice data flow to implement targeted QoS configuration, resulting in priority improving of voice data flow, thus quality of voice connection is ensured.

3.1.8 MAC

Switch uses MAC address table information to quickly address and forward the message on data-link layer. The MAC address table can be viewed on MAC address table information page. MAC address aging time is used to set the time of saving the MAC addresses learned by switch in MAC addresses forwarding list. The specified MAC address is bound to certain interface, and the generated static MAC table item will not be aged in the address table. Black hole MAC is a kind of specific MAC address configured manually by user; when the switch receives the message sent by source MAC address and destination MAC address listed as black hole MAC address, the message will be dropped. When MAC filter is enabled, only the data of computer in static MAC address can pass through the switch.Security MAC is the MAC address securely generated from the port, and its aging depends on port security, instead of MAC address list. Address migration will not occur to security MAC. The MAC filter function is invalid to security MAC. Address migration table lists the changing information for the same MAC address among the switch interfaces.

3.2 STP

3.2.1 STP,RSTP and MSTP

3.2.1 STP,RSTP and MSTP

The Spanning Tree Protocol (STP), the Rapid Spanning Tree Protocol (RSTP) and the Multiple Spanning Tree Protocol (MSTP) are link-layer management protocols and are mainly applied to LANs to prevent loops. STP blocks redundant links and trims a network into a tree topology free from loops. RSTP enhances STP. It provides fast transition of interfaces status to speed up network convergence. MSTP maps VLANs to different Instances; each instance only runs one spanning tree (RSTP) so as to improve the expandability of RSTP.

STP, RSTP and MSTP technologies are adopted to prevent broadcast storms caused by loops and provide backup links for data forwarding.

3.3 Multicast

The Internet Group Management Protocol (IGMP) is a protocol used to manage IP multicast members in the TCP/IP suite. It sets up and maintains the member relationship between IP hosts and their directly connected multicast routers.

3.3.1 IGMP Snooping

3.3.2 Fast Leave of Multicast Member Interface

3.3.1 IGMP Snooping

Located between hosts and a multicast router, the S1700 supports static multicast forwarding entries and generates a dynamic Layer 2 multicast forwarding table with multicast groups, VLANs, and egress interfaces by listening to IGMP messages.

When the S1700 receives a multicast packet, it forwards the packet only to the members on the VLAN corresponding to the multicast group. The multicast message is transmitted in multicast mode on the VLAN according to the Layer 2 forwarding table. This saves bandwidth and enhances the security of information transfer.

3.3.2 Fast Leave of Multicast Member Interface

When multicast member leaves, the host will be triggered to send an IGMP leave message. For the S1700 interface connected to only one host, the item of multicast forwarding list corresponding to the interface will be deleted immediately when S1700 receives the IGMP leave message. This can save bandwidth and system resource, also realize rapid service switching.

3.4 Link Detection

Link detection includes loopback test and virtual cable test (VCT). They provide users with two means to detect the switch port and link faults on LANs.

- Port loopback test is a very common way to check and analyze the port and chip issues ,by checking whether the test packet which is sent by switch to port is back to the device from the port.
- VCT is mainly used to estimate the length of a network cable and locate the failure point of the cable. The S-switch simulates radar to detect cable faults and locate the failure points on the basis of a single link.

4 Service Features

About This Chapter

4.1 ACL Control

4.2 QoS

4.3 Security

4.4 Network Management

4.5 Routing

4.1 ACL Control

S1700 supports to create ACL rules to decide whether forward packets according to the contents contained in each packet's header. The ACL rules can be based on "Standard IP", "Extended IP", "Extended IPv6", "Extended MAC", and "User Define" standards to filter frames. HTTP ACL can apply ACL rules to HTTP protocol data accessing the switch.

4.2 QoS

The S1700 supports priority mapping, DSCP mapping, IP Precedence mapping and service level mapping, QoS scheduling and can avoid SRED and traffic shaping. It also supports traffic management based on traffic.

4.2.1 QoS Interface

4.2.2 Priority Mapping

4.2.3 DSCP Mapping

4.2.4 IP Precedence Mapping

4.2.5 Service Level Mapping

4.2.6 QoS Scheduling

4.2.7 Traffic Management

4.2.8 SERD

4.2.9 Traffic Shaping

4.2.1 QoS Interface

Trust mode of QoS interface can be chosen, and is used to select the mode of mapping the priority of message to that of device. Selectable trust modes include following three: trust 802.1p, trust DSCP and trust IP precedence. In CFI mapping, when the port is enabled and the trust mode is 802.1p, different colors will be mapped to the internal based on the CFI value of the tag message, that is, CFI0 is mapped as green, and CFI1 mapped as yellow. If the message is sent through the port that enables this option, CFI value of red message is 1, and the CFI value of other red messages is 0.

4.2.2 Priority Mapping

The priority mapping uses 3 bits priority field (CoS, Class of Service) in IEEE 802.1Q label to divide the packet into different traffic types. S1700 supports marking ingress Untagged packets with the specified CoS priority value and to conduct service level mapping.

4.2.3 DSCP Mapping

The Differentiated Services Code Point (DSCP) uses the used 6 bits and not used 2 bit to define priority by coding value in TOS identification byte of service type of the IP head of each packet. DSCP mapping can map the DSCP value to service level, then determine the forwarded priority queue by service level mapping.

4.2.4 IP Precedence Mapping

IP Precedence is a 3 bits value and distributes precedence to IP groups according to the TOS type of IP head. With IP Precedence configuration, network grouping will pass through IP precedence device according to the user-set precedence. IP Precedence mapping can map IP Precedence mapping to priority queue, then determine the forwarded priority queue by service level mapping.

4.2.5 Service Level Mapping

The device supports the mapping from service level mapping to priority queue, to determine the corresponding forwarded queue for the message specified with service level.

4.2.6 QoS Scheduling

The S1700 manages traffic congestion through queue scheduling. Each egress interface on the S1700 is configured with eight queues. Queue scheduling manage the resource for each priority queue. Through the control of link bandwidth usage for each queue, the different data streams will be defined as different levels of service.

The S1700 provides the following queue scheduling policies:

- SP（Strict Priority）
- WRR（Weight Round Robin）

4.2.7 Traffic Management

Traffic management is used to match the contents encapsulated in packet header with the specified rules to achieve the classification of varies kind of business packets.

Traffic Classifier

S1700 supports simple flow classification based on 802.1p priority, VLAN ID, MAC address, Ethernet type, and ACL. You can choose “match all the packets” to match the preset rules in all packets.

Traffic Behavior

After traffic is classified, the S1700 performs access control on the packets, that is, permits or denies the packets forwarding. Then, the S1700 re-marks the following fields in the packets:

- 802.1p Priority
- DSCP
- IP Precedence
- Local Priority

In addition, S1700 also supports to carry out the following actions for the appropriate classified packets:

- Traffic statistics
- Flow supervision
- Re-tag 802.1p
- Re-tag DSCP
- Re-tag IP priority
- Specify local queue
- Redirection

Traffic Policy

Traffic policy binds Traffic Classifier and Traffic Behavior, and then applies to the specified Ethernet interface/VLAN/Trunk.

4.2.8 SERD

SRED support congestion avoidance mechanism based on SRED. SRED (Simple Random Early Detection) is a simple mechanism of congestion avoidance, in which active management is realized for queue by random discard of some packets with specified colors, resulting in that the size of queue is kept at a reasonable level, thereby avoiding congestion. S1700 uses SRED template to analyze data packet and QoS queue thereof, and predicts network congestion by means of SRED algorithm, so as to avoid network congestion by action of packet loss in advance.

4.2.9 Traffic Shaping

Traffic shaping indicates that network administrator is allowed to allocate the minimal assured bandwidth and the maximal bandwidth limit to each queue, resulting in reasonable allocation of resources based on network environment thereby improving the quality of network service.

Through traffic shaping, S1700 can control the flow for each service, and perform any specific bandwidth allocation and configuration, so that the service quality of network can be ensured.

4.3 Security

The S1700 guarantees both device security and transmission service security.

4.3.1 Hierarchical Web Protection

4.3.2 AAA

4.3.3 RADIUS

4.3.4 SSL Connection

4.3.5 VLAN

4.3.6 MAC Table Searching Based on VLAN+MAC

4.3.7 Guest VLAN

4.3.8 Port Security

4.3.9 DoS Attack Prevetion

4.3.10 Worm Prevention

4.3.11 MAC Attack

4.3.12 Port Isolation

4.3.13 Storm Control

4.3.14 Storm Suppression

4.3.15 802.1X Authentication

4.3.16 Acess control based on MAC adress

4.3.17 MAC Authentication

4.3.18 DHCP Snooping

4.3.19 IPSG

4.3.20 DAI

4.3.1 Hierarchical Web Protection

When a user logs in to the S1700 from an Ethernet interface through Web, the S1700 authenticates the user to ensure security. The user can configure and maintain the S1700 only after passing the authentication.

The S1700 adopts a hierarchical protection mode. After logging in to the S1700, a user can run only the commands at the same or lower level. This mode effectively controls the user authority.

4.3.2 AAA

The S1700 supports full Authentication, Authorization, and Accounting (AAA) mechanism. Using AAA and hierarchical command protection, the S1700 can authenticate and authorize login users. In addition, it can authenticate the NMS administrator. AAA effectively prevents unauthorized users from logging in to the S1700.

The S1700 supports authentication methods such as local authentication, RADIUS authentication.

4.3.3 RADIUS

RADIUS is a distributed client / server systems which used to secure networks and aviod unauthorized access. RADIUS clients runs on the switch and send authentication requests to a central RADIUS server which contains all user authentication and network service access information. S1700 support RADIUS authentication and accounting function for users and also supports RADIUS sever to distribute VLAN and ACL attributes. It supoort RADIUS dynamic authorization function to change access users' VLAN or ACL authorization .

4.3.4 SSL Connection

Secure Sockets Layer (SSL) is a security function. It provides hosts and clients a secure communication path through authentication, digital signature and encryption. The SSL protocol mainly provides the following services: 1, authenticate user and server, ensure packets transmitting to the specified clients and server; 2, encrypt packets to prevent packets capturing in process; 3, maintain packets integrity to ensure the packets not be changed in transmission.

4.3.5 VLAN

The S1700 supports the division of a LAN into multiple VLANs. Devices on different VLANs cannot communicate with each other. This isolates broadcast domains and improves service security.

4.3.6 MAC Table Searching Based on VLAN+MAC

The S1700 uses MAC table searching based on VLANs and MAC addresses to improve interface security. Network administrator can add static table entries in the MAC address to record the mapping relationship between specific MAC addresses to interfaces. In this way, devices are bound to interfaces so that it prevents attack using fake MAC addresses.

4.3.7 Guest VLAN

Configure Guest VLAN under 802.1X authentication and MAC authentication. When the authentication requirements are not responded by terminal or user authentication is failure, user will gain limited access to the network. User who belongsto the Guest VLAN accessing resource of the Guest VLAN will not be authenticated, and the user will be authenticated when accesses the external resource. Thus this satisfies the requirements of the unauthenticated user accessing certain resource.

4.3.8 Port Security

Port security can remember Ethernet MAC address, connected to switch's port so as to only permit certain MAC address to pass the port communication. If any other MAC address tries to pass the port communication, the port security will prevent it. Using port security can prevent some devices access network and improve security.

4.3.9 DoS Attack Prevetion

DoS attack uses up server resources (including server’s computation, memory resource, network bandwidth) by sending many service requests, causes unusual working of server by triggering some error code, and then make the server cannot send proper responses to the service requests. S1700 can prevent DoS attack.

4.3.10 Worm Prevention

S1700 can add the features of passed worm to the worm list to achieve worm prevention.

4.3.11 MAC Attack

S1700 can prevent the MAC attack from the network.

4.3.12 Port Isolation

Port isolation prevents ports on the same S1700 from sending Layer 2 packets to each other. The S1700 supports unidirectional and bidirectional port isolation. Port isolation ensures security of user networks and helps to construct low-cost intelligent community networks. Port isolation also limits unnecessary broadcast packets and thus increases network throughput.

4.3.13 Storm Control

When excessive broadcast, multicast and unspecified unicast present in network, storm may occur, resulting in slow-down of network and irregular network activities. Storm control applies flow control mechanism to solve storm. When some class of packet is excessive, switch will prohibit forwarding of this class of data packet temporarily, until data flow returns to normal. Interface of S1700 series of switch supports the setting of storm control.

4.3.14 Storm Suppression

Storm suppression limits the number of unknown unicast packets, multicast packets, and broadcast packets within a proper range to ensure network efficiency.

The S1700 can suppress the packets based on interfaces. When traffic suppression is enabled on an interface, the interface monitors received unknown unicast packets, multicast packets, and broadcast packets to check whether their traffic exceeds the threshold. If traffic exceeds the threshold, the S1700 discards excessive packets to keep the traffic volume within the limit and thus services on the network run normally.

4.3.15 802.1X Authentication

The IEEE 802.1X standard is a port-based network access control protocol. It is a security measure for authorizing and authenticating users to gain access to a specified Local Area Network by using a Client and Server based access control model. Unauthorized devices are restricted from connecting to a LAN through a port to which the user is connected.

4.3.16 Acess control based on MAC adress

To take full advantage of 802.1X authentication advantages, it is necessary to create "logical" interface for each connected device accessing the switch, that means the switch will manage the shared network segment of physical interface connected on switch as as a series of logical interface, each logical interfaces must be authenticated and authorizated by a separate authentication server. Switch learns the MAC address of each connected device, and create a logical interface, so that connected equipment will communicate with the switch through this logical interface.

4.3.17 MAC Authentication

MAC-Based Network Access Control is a security measure for authorizing and authenticating users to gain access to a specified network based on port and MAC address control, which does not require the installation of any client authentication software. The authentication starts after the switch detects the MAC address at the first time. The authentication process does not require any user name or password.

4.3.18 DHCP Snooping

DHCP Snooping is used to listen for DHCP packets, then extract and record VLAN, the IP address, the interface number and MAC address information from the received DHCP Ack or DHCP Request packets, then dynamically create a binding entry to DHCP Snooping binding table. Other security moudles, such as IPSG, will use this binding table to restrict the access of specified users.

DHCP Snooping allows you to configure trusted ports and Untrusted ports. Untrusted ports can not process the DHCP response packets.

4.3.19 IPSG

IPSG - IP SOURCE GUARD is a interface traffic filter technology based on IP/MAC/VLAN. It can prevent the LAN IP address spoofing attacks. There is a IP source binding table in switch that is detection standards for each received packet.

When the received IP packets meet the IP / MAC / VLAN correspondence in IP source binding table, the switch will forward this packets. The remaining packets will be discarded by switche.

IP source binding table can be added by user in static or binding acquired after ARP learning, and automatically learning from DHCP Snooping binding table.

4.3.20 DAI

DAI is also based on the binding table. DAI only detects the ARP packets from the Untrusted ports. It records and discards the packets which do not match the MAC address and IP address mapping entry in the binding table. Meanwhile ARP packet speed of interface can be restricted at speed limit state, to enable or disable speed limit of over-speed ARP packet.

4.4 Network Management

Through network management, user can manage devices conveniently by GUI, to reduce the requirements to maintenance personnel.

4.4.1 SNMP

4.4.2 RMON

4.4.3 LLDP

4.4.4 LLDP-MED

4.4.1 SNMP

SNMP is designated to manage and monitor network devices. SNMP allows network management sites to read and change settings of gateway, router, switch and other network devices. SNMP is applied to ensuring the regular operation of switch, switch set or network, the performance monitoring and detection of potential problems.

Network-manageable device of supporting SNMP includes a set of software (called agent herein) operating on local devices. SNMP agent uses a set of predefined variables (manageable objects) to maintain and manage devices. These objects are defined by management information base (MIB), and standard control information is provided by built-in SNMP agent. At the same time, SNMP defined MIB size and protocols for accessing the information.

S1700 supports SNMPv1, v2c and v3. These three different versions of SNMP provide management sites and network devices with security at different levels.

4.4.2 RMON

RMON is the monitoring standard of Internet Engineering Task Force (IETF), enabling various network monitors and console system to exchange network monitoring data each other. RMON sets detectors on network nodes, and network management platform decides what these detectors report, such as the monitored statistics information, time used in collection of history information and so on. For example, such network devices as switches and routers are equivalent to a network node on network, which can monitor the information of currently stated node through RMON function.

4.4.3 LLDP

The S1700 supports the Link Layer Discovery Protocol (LLDP) that conforms to IEEE 802.1ab. LLDP is a link layer protocol used for interconnected devices to obtain the connection information of each other.

Using LLDP, the local NMS can obtain the link layer information of all devices on the local network and details about the network topology. Thus the NMS can manage a larger area on the network.

The LLDP-enabled interfaces on the S1700 periodically notify the neighbors of its own status. If the status of an interface changes, interface sends status update messages to the directly connected neighboring device.

4.4.4 LLDP-MED

LLDP-MED provides the extention applications, including basic configuration, network policy configuration, address information and content management, etc.

4.5 Routing

Static routing is achieved by manual configuration of administrator. After the configuration, the messages to specified destination are forwarded according to the path specified by administrator. For the network with simple networking architecture, network intercommunication can be realized with only need of static routing configuration.

5 Networking and Applications

About This Chapter

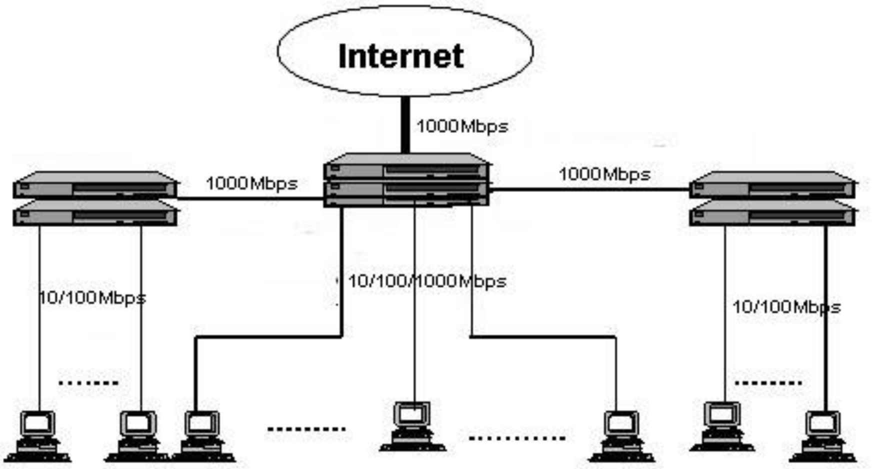
5.1 Access on an Enterprise Network or a Campus Network

5.2 Desktop Access

5.1 Access on an Enterprise Network or a Campus Network

In an enterprise network and a campus network, the S1700 access to end users through the Fast/Gigabit copper port, uplink through Gigabit optical port or gigabit copper port to aggregation layer switch, then tied through Link Aggregation or 10 Gigabit uplink to the backbone networks, in order to constitute the 10 Gigabit backbone, Fast/Gigabit to desktop total solution to meet customers high-bandwidth, multi-service requirements.

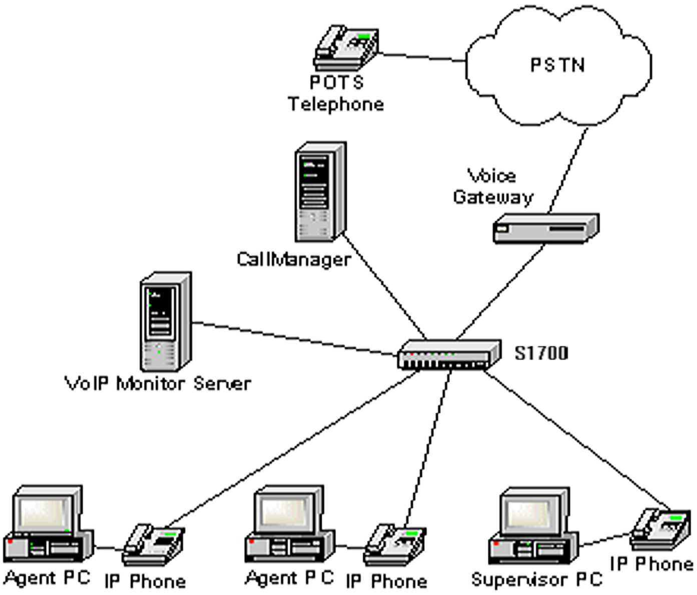
Figure 5-1 Campus Topology



5.2 Desktop Access

The S1700 provides the function such as Voice VLAN, with the S1700 compact design; it is easily to provide a variety of desktop access.

Figure 5-2 Voice VLAN



6 Maintenance and Network Management System

About This Chapter

6.1 Maintenance and Management

6.1 Maintenance and Management

6.1.1 Configuration Methods

6.1.2 Monitoring and Maintenance

6.1.3 Diagnosis and Debugging

6.1.4 Software Upgrade

6.1.1 Configuration Methods

Configuration Modes

The S1700 supports the following configuration and management modes:

- Web management

  User can configure features and parameters by login the S1700 through the Web browser.
- SNMP management

  User configures and manages features and parameters of the S1700 through the network management station.

Various Login and authentication Modes

User can take various authentications like local authentication and RADIUS authentication according to the needs during the login process.

6.1.2 Monitoring and Maintenance

Device Management and Maintenance

The S1700 provides various management and maintenance functions:

- Apart from providing flexible online help, supporting two way operations “user management”, Chinese and English, all the pages in the two level account methods are the same and without classifications. In the page of “user management”, zero level user cannot see the account of 15 level user.
- Supports an information center, user can check log information and transmit log information to specified hosts.
- Supports various information search, including version and temperature.

Board Status

From here, user can check whether S1700 is in cold start with power off or warm start with manual commands.

E-label

E-label is also called permanent configuration data or profile information which includes name, serial number, and module information such as production or custom manufacturers. It's written to the memory in the process of device production.

DDM

Optical power diagnostics is used to test the optical module of switch, and display the temperature, voltage, receive optical power and transmit optical power and other parameters.

Information Center

Information Center is the hub of information systems which classifies and manages all the system information. Through combination with the debugger, information center provides network administrators and developers a strong support for the capability of monitoring network performance and network fault diagnosis.

Power Saving Management

S1700-28GFR-4P-AC and S1700-52GFR-4P-AC support Power Saving and IEEE 802.3az EEE standard. S1700-28FR-2T2P-AC and S1700-52FR-2T2P-AC support Power Saving standard.

6.1.3 Diagnosis and Debugging

Ping and Tracert

On traditional IP networks, the S1700 provides the following tools to check network connectivity:

- Ping
- Tracert

Mirroring

The S1700 supports interface-based mirroring on a single switch.

- Port mirroring

  The incoming traffic, outgoing traffic, or both incoming and outgoing traffic at an observed interface is completely copied to an observing interface.

  By connecting a monitoring host to an observing interface on the S1700, a network administrator can easily observe the packets that pass through the S1700 in real time. The mirroring result serves as a basis for traffic detection, fault location, and data analysis.

6.1.4 Software Upgrade

Software Upgrade

The S1700 can detect the integrity and validity of the system software before the upgrade and provides various methods of upgrading the software:

- Remote in-service upgrade

  When the S1700 runs normally, it can download the software through Web. The new software is run when the S1700 is restarted. This realizes the remote seamless software upgrade.

- FTP upgrade

  S1700 can be upgraded by FTP. The FTP server IP address, user name / password, TCP port number, firmware file full path and file name are needed when upgrading S1700.

7 System Technical Specifications

About This Chapter

7.1 Physical Parameters

7.2 Optical Module Attributes

7.3 System Configuration

7.4 List of Software Features

7.1 Physical Parameters

Table 7-1 Physical Parameters

Item		Description
Dimensions (width x depth x height)		442mm x 219.85mm x 43.8mm
Maximum power (full configuration)		• S1700-28FR-2T2P-AC: 20.2W • S1700-28GFR-4P-AC: 31.1W • S1700-52FR-2T2P-AC: 32.0W • S1700-52GFR-4P-AC: 55.0W
Weight		• S1700-28GFR-4P-AC:2.35kg • S1700-52GFR-4P-AC: 3.2kg • S1700-28FR-2T2P-AC: 2.3kg • S1700-52FR-2T2P-AC: 2.66kg
AC input voltage	Rated voltage	100V AC to 240V AC
	Maximum voltage	90V AC to 264V AC
Temperature	operating temperature	0 ℃ to 45 ℃

Item		Description
	Storage temperature	-20 ℃ to 70 ℃
Relative humidity		10%RH to 95%RH
Altitude	Long-term operation altitude	0 m to 2000 m
	Storage altitude	0 m to 3500 m

7.2 Optical Module Attributes

Table 7-2 Attributes of the ESFP (GE) Optical Module

Attribute	Specification							
Transmission distance	0.5km	10km	10km(single-mode bidirectional fiber)	10km(single-mode bidirectional fiber)	40km	40km	80km	100km
Center wavelength	850nm	1310nm	Sending: 1310nm Receiving: 1490nm	Sending: 1490nm Receiving: 1310nm	1550nm	1310 nm	1550nm	1550 nm
Transmitting power	-9.5dBm ～ -2.5dBm	-9.0dBm ～ -3.0dBm	-9.0dBm ～ -3.0dBm	-9.0dBm ～ -3.0dBm	-5.0dBm～0dBm	-5.0dBm～0dBm	-2.0dBm ～ 5.0dBm	0dBm ～ 5.0dBm
Receiver sensitivity	-17.0dBm	-20.0dBm	-19.5dBm	-19.5dBm	-22.0dBm	-22.0 dBm	-22.0dBm	-30.0 dBm
Overload power	0dBm	-3.0dBm	-3.0dBm	-3.0dBm	-3.0dBm	-3.0dBm	-3.0dBm	-9.0dBm
Extinction ratio	9.0dB	9.0dB	6.0dB	6.0dB	8.5dB	9.0dB	9.0dB	8.0dB
Type of the optical connector	LC	LC	LC	LC	LC	LC	LC	LC

Attribute	Specification							
Fiber type	Multi-mode	Single mode	Single mode	Single mode	Single mode	Single mode	Single mode	Single mode

Table 7-3 Attributes of the ESFP (CWDM) Optical Module

Attribute	Specification							
Transmission distance	80km	80km	80km	80km	80km	80km	80km	80km
Center wavelength	1571nm	1591nm	1551nm	1511nm	1611nm	1491nm	1531nm	1471nm
Transmitting power	0dBm ～ 5.0dBm	0dBm ～ 5.0dBm	0dBm ～ 5.0dBm	0dBm ～ 5.0dBm	0dBm ～ 5.0dBm	0dBm ～ 5.0dBm	0dBm ～ 5.0dBm	0dBm ～ 5.0dBm
Receiver sensitivity	-28.0dBm	-28.0dBm	-28.0dBm	-28.0dBm	-28.0dBm	-28.0dBm	-28.0dBm	-28.0dBm
Overload power	-9.0dBm	-9.0dBm	-9.0dBm	-9.0dBm	-9.0dBm	-9.0dBm	-9.0dBm	-9.0dBm
Extinction ratio	8.5dB	8.5dB	8.5dB	8.5dB	8.5dB	8.5dB	8.5dB	8.5dB
Type of the optical connector	LC	LC	LC	LC	LC	LC	LC	LC
Fiber type	Single mode							

7.3 System Configuration

Table 7-4 System Configuration

Item	Parameter
Processor	Dominant frequency: 400 MHz
Switching capacity	• S1700-28FR-2T2P-AC: 12.8Gbit/s • S1700-28GFR-4P-AC: 56Gbit/s • S1700-52FR-2T2P-AC: 17.6Gbit/s • S1700-52GFR-4P-AC: 104Gbit/s

Item	Parameter
Packet forwarding capacity	- S1700-28FR-2T2P-AC: 9.52 Mpps - S1700-28GFR-4P-AC: 41.66 Mpps - S1700-52FR-2T2P-AC: 13.09 Mpps - S1700-52GFR-4P-AC: 77.376 Mpps
SDRAM memory	128 MB
Flash Memory	16 MB

7.4 List of Software Features

Table 7-5 List of Software Features

Software features		Description
System management	Basic management	- Software function reset: recover default setting of device. - Restart of command management device. - Software version upgrade and file management. - Operation and management of management interface. - Configuration saving.

Software features		Description
Ethernet features	LLDP	The S1700 supports the Link Layer Discovery Protocol (LLDP) that conforms to IEEE 802.1ab. LLDP is a link layer protocol used for interconnected devices to obtain the connection information of each other. Using LLDP, the local NMS can acquire the link layer information of all devices on the local network and the details about the network topology. This expands the management scope of the NMS. The LLDP-enabled interfaces on the S1700 regularly notify the neighbors of the local status. If the status of an interface changes, the interface notifies the directly connected device that its status is changed. LLDP-MED provides VoIP (Voice over IP) with many advanced applications, including basic configuration, network policy configuration, address information and content management, etc., thus meeting such requirements as cost effectiveness, easy deployment and easy management of different voice device manufacturers, and solving the problem of deploying voice device in Ethernet, convenient for voice device manufacturers, sellers and users.
	Link aggregation	The S1700 supports link aggregation in manual mode or in static LACP mode.
	Spanning tree	The S1700 supports STP, RSTP and MSTP. The S1700s running the preceding protocols discover loops on the network by exchanging information with each other, and block certain interfaces to eliminate loops. Then the network with loops is pruned as a loop-free network. Thus this prevents the increase and infinite circulation of packets on the network with loops and avoids handling ability fall caused by repeated receiving of messages.
	VLAN	• Support the interface-based VLANs. An interface can be an access interface, a trunk, or a hybrid interface. The VLAN IDs range from 1 to 4094. • Support the voice VLAN. • Support the MAC-based VLAN.
Interface and link management	Interface configuration	• Logical interfaces: Trunks. • Physical interfaces: FE/GE interfaces.
	Port traffic limit	Support port traffic limit based on egress and ingress.

Software features		**Description**
	Link protocol	Ethernet
	Management and Maintenance	• Support user authentication management.
	Web management	• Support the web browser management.
Multicast	IGMP	• IGMP V1/V2/V3 Snooping
QoS	QoS interface	• Trust mode (trust 802.1p, trust DSCP, trust IP precedence) and CFI mapping.
	Mapping	• Support the mapping of sevice level to queue . • Support mapping based on 802.1p . • Support mapping based on DSCP. • Support mapping based on IP Precedence.
	Scheduling mode	• Support Strict-Priority + Weighted Round Robin (WRR) scheduling algorithms. • Support 8 queues per port.
	Congestion Avoidance	Support congestion avoidance based on SRED.
	Traffic Shaping	Support traffic shaping.
	Traffic Management	Support management to QoS based on traffic policy.
ACL	Effective Period	Support ACL based on effective period.
	ACL Template Application	Support ACL template configuration setup and delete. Support application in physical interface and specific VLAN.
	HTTP ACL	Support regular ACL application in HTTP protocol data of network.
Routing	Routing	Support IPv4/IPv6 static routing management.
Security	User Management	Support two types of user management (general user and privileged user) and view onlie user.
	802.1X	Support 802.1X.
	Guest VLAN	Support Guest VLAN.
	Port Security	Support port security.
	MAC Authentication	Support MAC authentication.
	DOS Anti-attack	Prevent DOS from being attacked.
	DHCP Snooping	Support DHCP Snooping.

Software features		Description
	IPSG	Support IPSG.
	DAI	Support DAI.
	MAC Attack	Support MAC Attack.
	Port Isolation	Achieve layer 2 isolation between hosts and clients in the broadcast domain.
	Authentication	Support local authentication and RADIUS server authentication.
		Support port-based 802.1X authentication.
	AAA	Supports local authentication and RADIUS server authentication. Supports RADIUS accounting fuction
	RADIUS	Support RADIUS authentication, accounting and dynamic authorization.
	SSL	Support SSL.
	Broadcast Storm Suppression	Support broadcast, multicast, unknown unicast storm suppression.
Network Managment	SNMP	Support SNMP.
	RMON	Support RMON.
Device Managment	Board Status	Support board status.
	E-label	Support E-label.
	Loop-back Diagnostics	Support loop-back diagnostics.
	Cable Diagnostics	Support cable diagnostics.
	Optical Power Diagnostics	Support optical power diagnostics.
	Information center	Support information center.
	Power-saving Management	• S1700-28GFR-4P-AC and S1700-52GFR-4P-AC support IEEE 802.3az EEE and Power Saving • S1700-28FR-2T2P-AC and S1700-52FR-2T2P-AC support Power Saving
	Mirror Management	• Support port ingress traffic mirror. • Support port egress traffic mirror.
	Tools	• Support ping, tracert, one-key information gathering.