

**Quidway S1700 Series Switches
V100R006C00**

Product Description

Issue **02**
Date **2012-07-25**

Copyright © Huawei Technologies Co., Ltd. 2012. All rights reserved.

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

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Product Version

The following table lists the product versions associated with this document.

Product Name	Product Version
S1700	V100R006C00

Intended Audience

This document describes the product positioning , 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.

Symbol	Description
 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.

Command Conventions

Format	Description
Boldface	The keywords of a command line are in Boldface .
<i>Italic</i>	Command arguments are in <i><Italic></i> .
[]	Items (keywords or arguments) in brackets [] are optional.
{ x y ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x y ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x y ... } *	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x y ...] *	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.

GUI Conventions

Format	Description
“”	Buttons, menus, parameters, tabs, window, and dialog titles are in boldface. For example, click OK .
>	Multi-level menus are in boldface and separated by the ">" signs. For example, choose File > Create Folder .

Change History

Changes between document issues are cumulative. The latest document issue contains all the changes made in earlier issues.

Issue 02 (2012-07-25)

Relative to the version 01(2011-11-17) of the changes are as follows:

[Updated website.](#)

Issue 01 (2011-11-17)

Initial field final 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	5
2.3.2 SCU.....	6
2.3.3 Power Supply	7
3 Link Features	8
3.1 Ethernet Features.....	8
3.1.1 Link Aggregation	8
3.1.2 Flow Control on an Interface	8
3.1.3 Traffic Suppression	9
3.1.4 VLAN	9
3.2 STP.....	10
3.2.1 STP and RSTP	10
3.3 Link Detection.....	10
4 Service Features	11
4.1 Multicast.....	11
4.1.1 IGMP Snooping	11
4.1.2 Multicast Traffic Control.....	11
4.1.3 Controllable Multicast.....	12
4.2 QoS.....	12
4.2.1 Traffic Classification.....	12

4.2.2 Access Control and Re-marking.....	12
4.2.3 Traffic Policing	13
4.2.4 Congestion Management.....	13
4.2.5 Rate Limit on an Interface	13
4.3 Security	13
4.3.1 Device Security	13
4.3.2 Service Security	14
4.3.3 Security Authentication.....	14
4.4 Reliability.....	15
4.5 LLDP.....	15
4.6 Web Server	15
5 Networking and Applications.....	16
5.1 Access on an Enterprise Network or a Campus Network.....	16
5.2 Desktop Access	16
6 Maintenance and Network Management System	17
6.1 Maintenance and Management.....	17
6.1.1 Various Configuration Methods	17
6.1.2 Monitoring and Maintenance	17
6.1.3 Diagnosis and Debugging	18
6.1.4 Software Upgrade and In-Service Patching	18
6.1.5 Hardware Fault Handling.....	19
7 System Technical Specifications.....	20
7.1 Physical Specifications.....	20
7.2 Optical Module Attributes	21
7.3 System Configuration.....	22
7.4 List of Software Features	23

1 Product Positioning and Features

About This Chapter

[1.1 Product Positioning](#)

[1.2 Product Characteristics](#)

1.1 Product Positioning



CAUTION

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

The Quidway S1700 Series series Ethernet switches (hereinafter referred to as the S1700) provide the access and data transport 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 switches are classified into S1724G unmanaged switch and S1728GWR-4P managed switch. The S1728GWR-4P switch provide more powerful VLAN, QoS, multicast, security, authentication, and reliability functions than S1724G switch.

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, 1Q Trunk, and hybrid.

The S1700 provides 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 Spanning Tree Protocol (STP) 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
- 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

In addition to collecting traffic statistics based on interfaces, the S1700 provides fault detection and location tools such as ping on an IP network.

1.2.4 Energy-Saving Design

The S1700 adopts the following measures to save energy:

- It adopts 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.

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 Huawei patented lightning protection technologies to protect the equipment. The lightning protection technologies reduce the probability of damages caused by lightning and increase the safety factor by 30 times, thus greatly improving 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 Ethernet switches adopt an integrated hardware platform. An S1700 consists of the chassis, power supply unit, 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.

The S1700 Ethernet switches includes S1724G, S1728GWR-4P.

2.2 Device Structure

This section describes the structure of the S1700.

The S1700 Ethernet switches adopt an integrated hardware platform. An S1700 consists of the chassis, power supply unit, switch control unit (SCU), and interface subcard. 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 S1724G are 320.0 mm x 208.0 mm x 43.6 mm (width x depth x height).
- The dimensions of S1728GWR-4P are 442.0 mm x 220.0 mm x 43.6 mm (width x depth x height).

S1700 Appearances

[Table 2-1](#) shows the front views of S1700.

Table 2-1 S1700 front views

Model	Image
S1724G	
S1728GWR-4P	

5. Twenty-four 10/100B/1000ASE-T Ethernet interfaces	8. Four 1000BASE-X Ethernet optical interfaces
--	--

Table 2-2 shows the rear views of S1700.

Table 2-2 S1700 rear views

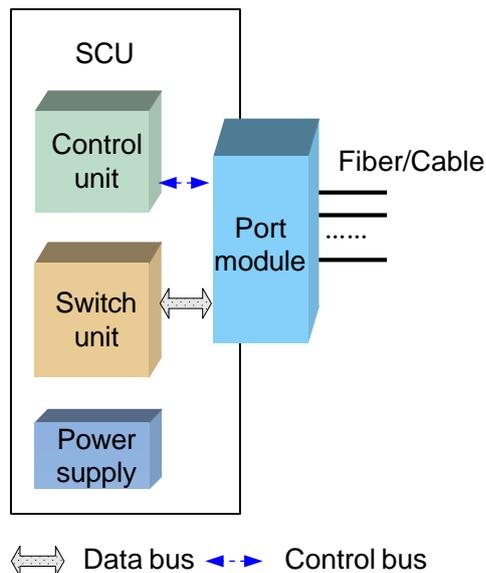
Model	Image
S1724G	
S1728GWR-4P	

1. AC jack	2. Ground screw
------------	-----------------

2.3 Hardware Modules

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

Figure 2-1 Logical structure of hardware modules of the S1700



Hardware modules of the S1700 refer to the SCU, power supply.

2.3.1 SCU

The SCU is fixed on the S1700. Each S1700 has one SCU.

The SCU is responsible for packet 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 implements 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 packet exchange, 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 2-3 Power supply

Device Name	AC	DC	1:1 Backup power supplies
S1724G	Y	N	N
S1728GWR-4P	Y	N	N

3 Link Features

About This Chapter

[3.1 Ethernet Features](#)

[3.2 STP](#)

[3.3 Link Detection](#)

3.1 Ethernet Features

3.1.1 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 implements link aggregation between GE interfaces or FE interfaces. Load balancing can be implemented based on the following information:

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

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

3.1.2 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.

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 volume of traffic sent from its outbound interface. Flow control on an interface does not identify flow types.

3.1.3 Traffic Suppression

Traffic 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.

3.1.4 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 Define 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.

The S1700 supports the following methods to define VLANs:

- Based on interfaces
After an interface is added to a VLAN, packets received by the interface are sent on the 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.

You can apply special QoS configuration to the voice data packets transmitted on the voice VLAN so that voice data packets are transmitted with high priority. The quality of the voice service is ensured.

3.2 STP

3.2.1 STP and RSTP

The Spanning Tree Protocol (STP) and the Rapid Spanning Tree Protocol (RSTP) 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.

STP and RSTP prevent broadcast storms caused by loops and provides backup links for data forwarding.

3.3 Link Detection

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

- 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 Multicast](#)
- [4.2 QoS](#)
- [4.3 Security](#)
- [4.4 Reliability](#)
- [4.5 LLDP](#)
- [4.6 Web Server](#)

4.1 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.

4.1.1 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 outbound 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 packet 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.

4.1.2 Multicast Traffic Control

Unknown multicast packets refer to the multicast packets that do not have forwarding entries in the multicast forwarding table. When receiving unknown multicast packets, the S1700 discards the packets or broadcasts them on the VLAN that the inbound interface belongs to.

The S1700 can also control inbound multicast traffic volume by limiting the percentage of multicast packets on an Ethernet interface.

4.1.3 Controllable Multicast

Multicast protocols do not provide user authentication. Therefore, a user can join or leave a multicast group freely. The multicast source does not know when a user joins or leaves a multicast group, so the number of users receiving multicast traffic on a network in a certain period is unknown. Therefore, the carrier cannot perform accounting for the users. The controllable multicast technology is introduced to solve these problems. Users have to pass authentication before receiving multicast traffic. Furthermore, only authorized multicast traffic can be received by users. Users who pass authentication are allowed to preview unauthorized multicast traffic and can receive multicast traffic in specified periods within a day. Controllable multicast does not apply to static multicast.

4.2 QoS

The S1700 provides the class-based QoS mechanism and supports the 802.1p priority. It provides guarantee of low end-to-end delay, jitter, and high bandwidth.

The S1700 classifies traffic according to certain rules and then performs corresponding actions on the packets such as priority re-marking, traffic policing, congestion management, congestion avoidance, and rate limit on the interface. In this way, value-added services such as NGN services, IPTV, and broadband access are provided with better network service.

4.2.1 Traffic Classification

Traffic classification is a function of identifying the packets of a certain type by matching information in the packet header. For example, the 802.1p priority of the packets sent by the Operating Support System (OSS) and NMS is set to 7; the 802.1p priority of VoIP packets is set to 6; the 802.1p priority of BTM packets and VOD packets is set to 5 or 4; the 802.1p priority of packets sent by VPN users is set to 3, 2, or 1 according to the level of VPN users; the 802.1p priority of packets of the Internet access service is set to 0. Then the packets can be classified based on their 802.1p priorities.

The S1700 adopts a hardware classifier to guarantee line-speed transmission of services data on interfaces.

Simple Traffic Classification

On the S1700, you can perform simple traffic classification for packets according to the mapping between priorities of packets and Per-Hop Behaviors (PHBs). If packets come from an upstream device, the S1700 maps priorities of the packets to PHBs and colors. On the S1700, congestion management is performed for packets according to PHBs of packets and congestion avoidance is performed for packets according to colors of packets. The downstream device provides QoS services according to the priorities of packets.

The S1700 only supports simple traffic classification according to the 802.1p priority of VLAN packets.

4.2.2 Access Control and Re-marking

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

- 802.1p field, that is, the PRI field in a VLAN tag
- DSCP field

- Local precedence

4.2.3 Traffic Policing

The S1700 uses the token bucket algorithm to control the Committed Access Rate (CAR) of network traffic.

The S1700 controls the rate of traffic by adjusting the rate of placing tokens. Each token equals a forwarding rate of 64 kbit/s. The S1700 "punishes" the excessive traffic to limit the incoming traffic within a proper range and to protect the network resources.

4.2.4 Congestion Management

The S1700 manages traffic congestion through queue scheduling. Each outbound interface on the S1700 is configured with four queues. After traffic classification, packets are sent to the corresponding queues based on their priorities.

The S1700 provides the following queue scheduling policies:

- Priority Queuing(PQ)
- Weight Round Robin(WRR)

4.2.5 Rate Limit on an Interface

Rate limit on an interface is used to adjust the rate of traffic on an outbound interface or inbound interface to prevent burst traffic. The S1700 uses the token bucket and a buffer to limit the traffic rate on an outbound interface, implementing traffic shaping. When the rate of packets exceeds the rate limit, the S1700 buffers excessive packets and sends them when the traffic rate falls below the limit. In this manner, the transmission rate is smoothed.

4.3 Security

The S1700 guarantees both device security and service security.

4.3.1 Device Security

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 for commands. Commands are classified into the visit level, configuration level, with their levels in ascending order. Login users are also classified into four levels, corresponding to the four levels of commands. 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.

The S1700 extends command levels and user levels to 16 levels so that users are managed more refinedly.

AAA

The S1700 supports the Authentication, Authorization, and Accounting (AAA). 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.

Limit of MAC Address Learning on Interfaces

You can set the maximum number of MAC addresses learned by an interface on the S1700 to prevent hackers from initiating source MAC address attack from the interface. This ensures that the MAC address entries of the S1700 will not be used up.

4.3.2 Service Security

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.

MAC Table Searching Based on VLAN+MAC

The S1700 supports MAC table searching based on VLANs and MAC addresses to improve interface security. You can add static MAC address entries in the MAC table to map specific MAC addresses to interfaces. In this way, specific devices are bound to interfaces so that hackers cannot attack the S1700 by using fake MAC addresses.

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.

4.3.3 Security Authentication

The 802.1x protocol is a port-based network access control protocol. It authenticates and controls access devices on a LAN based on interfaces. A user device can access resources on the LAN only after it passes the authentication on the access interface.

MAC address-based authentication controls the network access authority of a user based on the access interface and MAC address of the user. The user does not need to install any authentication client software. After detecting the MAC address of the user for the first time, the device starts authenticating the user. During the authentication, the user does not need to enter the user name or password.

4.4 Reliability

The S1700 supports RSTP to provide backup links for data transmission.

The S1700 provides the loop protection function. When the root port cannot receive any BPDU from the upstream device, it enters the Blocking state and stops forwarding packets. At the same time, no new root port is elected. This prevents loops on the network.

4.5 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, the interface sends status update messages to the directly connected neighboring device.

4.6 Web Server

Users can manage network devices through the GUI provided by the Web Server. This reduces requirements for junior maintenance personnel.

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 the Gigabit or 10Gigabit uplink to the backbone networks, in order to constitute the 10Gigabit backbone, 100M to desktop total solution to meet customers high-bandwidth, multi-service requirements.

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.

6 Maintenance and Network Management System

About This Chapter

[6.1 Maintenance and Management](#)

6.1 Maintenance and Management

6.1.1 Various Configuration Methods

Configuration Modes

The S1700 supports the following configuration and management modes:

- Network management station
A user configures and manages the S1700 through the Web browser.

Login Modes

The user can login to the service interface of the S1700 for configuration and management.

The S1700 supports multiple authentication modes, including local authentication, and AAA.

6.1.2 Monitoring and Maintenance

Hardware Monitoring

The S1700 provides the following hardware monitoring functions:

- Provides the re-detection function to prevent incorrect detection because of instant interference.
- Checks version matching automatically when the system is running.

Device Management and Maintenance

The S1700 provides various management and maintenance functions:

- Provides flexible online help for the command line in Chinese or English.
- Provides hierarchical commands and user authority management.
- Provides an information center to uniformly manage logs, traps, and debugging information and redirects information as required.
- Supports the display of the software version, module status, CPU usage, and memory usage.

6.1.3 Diagnosis and Debugging

Ping and TraceRoute

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

- Ping

Debugging

The S1700 provides various debugging commands for each software feature. Each debugging command supports multiple parameters and can be flexibly controlled. The debugging commands display the detailed information about processes, packet receiving and sending, and error check during the running of a feature.

Black Box

The S1700 provides the black box function to record information on the feature modules, tasks, and events. In addition, the black box records the final results, process status, and function calling track to facilitate fault location.

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 and In-Service Patching

Software Upgrade

The S1700 controls the use of features through the license file and 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.

6.1.5 Hardware Fault Handling

The S1700 supports automatic and manual intervention when a hardware fault occurs, for example, a chip on a board fails. The maintenance personnel can locate a hardware fault and handle it quickly to shorten service interruption.

7 System Technical Specifications

About This Chapter

- [7.1 Physical Specifications](#)
- [7.2 Optical Module Attributes](#)
- [7.3 System Configuration](#)
- [7.4 List of Software Features](#)

7.1 Physical Specifications

Table 7-1 Physical specifications

Item		Description
Dimensions (width x depth x height)		<ul style="list-style-type: none"> • S1724G:320.0mm×208.0mm×43.6mm • S1728GWR-4P:442.0mm×220.0mm×43.6mm
Maximum power (full configuration)		<ul style="list-style-type: none"> • S1724G:12.8 • S1728GWR-4P :21.8W
Weight		≤ 3 kg
AC input voltage	Rated voltage	100V AC to 240V AC
	Maximum voltage	90V AC to 264V AC
Temperature	operating temperature	-0 °C to 45 °C
	Storage temperature	-40 °C to 70 °C
Relative humidity		5%RH to 95%RH
Altitude		0 m to 2000 m

7.2 Optical Module Attributes

Table 7-2 Attributes of the ESFP (GE) optical module

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

Attribute	Specification							
	Center wavelength	1571 nm	1591 nm	1551 nm	1511 nm	1611 nm	1491 nm	1531 nm
Transmitting power	0 dBm to 5.0 dBm	0 dBm to 5.0 dBm	0 dBm to 5.0 dBm	0 dBm to 5.0 dBm	0 dBm to 5.0 dBm	0 dBm to 5.0 dBm	0 dBm to 5.0 dBm	0 dBm to 5.0 dBm
Receiver sensitivity	-28.0 dBm	-28.0 dBm	-28.0 dBm	-28.0 dBm	-28.0 dBm	-28.0 dBm	-28.0 dBm	-28.0 dBm
Overload power	-9.0 dBm	-9.0 dBm	-9.0 dBm	-9.0 dBm	-9.0 dBm	-9.0 dBm	-9.0 dBm	-9.0 dBm
Extinction ratio	8.5 dB	8.5 dB	8.5 dB	8.5 dB	8.5 dB	8.5 dB	8.5 dB	8.5 dB
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: 200 MHz
Switching capacity	<ul style="list-style-type: none"> • S1724G:48Gbit/s • S1728GWR-4P:56Gbit/s
Packet forwarding capacity	35.71 Mpps/41.66Mpps
DDR memory	128 MB
Flash Memory	32 MB

7.4 List of Software Features

Table 7-5 List of software features

Software Feature		Description
Ethernet features	LLDP	<p>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.</p> <p>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.</p> <p>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.</p>
	Link aggregation	The S1700 supports link aggregation in manual mode or in static LACP mode.
	Spanning tree	The S1700 supports STP and RSTP. 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. This prevents the increase and infinite circulation of packets on the network with loops and prevents the S1700s from receiving repeated packets. The processing capability of the S1700 is thus ensured.
	VLAN	<ul style="list-style-type: none"> • The S1700 supports the interface-based VLANs. An interface can be an access interface, a trunk, or a hybrid interface. The VLAN IDs range from 1 to 4093. • The S1700 supports the voice VLAN.
Interface and link management	Interface configuration	<ul style="list-style-type: none"> • Logical interfaces: Trunks • Physical interfaces: FE/GE interfaces
	Link protocol	Ethernet
	Management and Maintenance	Support the management of user authentication
	Web management	Support the web browser management
Multicast	IGMP	IGMP snooping
QoS	Queue scheduling	<ul style="list-style-type: none"> • Supports Strict-Priority (SP) + Weighted Round Robin (WRR) scheduling algorithms. • Supports 4 queues per port.

Software Feature		Description
		<ul style="list-style-type: none"> • Supports 802.1p Priority queues inbound. • Supports DSCP Priority queues inbound. • Set port priority support.
	Port rate limiting	Egress support.
Security	Mirroring	<ul style="list-style-type: none"> • Ingress flow Port mirroring. • Egress flow Port mirroring. • Local observation window.
	Port Isolation	In the same broadcast domain for client isolation at the layer 2.
	Authentication	<ul style="list-style-type: none"> • Support local authentication and RADIUS server authentication . • Support port-based 802.1x authentication..
	BroadCast Storm Control	Support broadcast, multicast, unknown unicast storm control.