RAISECOM

www.raisecom.com

Gazelle S1020i (A)
Product Description
(Rel_07)

Raisecom Technology Co., Ltd. provides customers with comprehensive technical support and services. For any assistance, please contact our local office or company headquarters.

Website: http://www.raisecom.com

Tel: 8610-82883305

Fax: 8610-82883056

Email: export@raisecom.com

Address: Raisecom Building, No. 11, East Area, No. 10 Block, East Xibeiwang Road, Haidian District, Beijing, P.R.China

Postal code: 100094

Notice

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.

Preface

Objectives

This document describes overview, hardware structure, technical specifications, networking applications, links features, service features, and management and maintenance of the Gazelle S1020i.

The appendix lists compliant standards and protocols, LEDs, terms, acronyms, and abbreviations involved in this document.

Versions

The following table lists the product versions related to this document.

Product name	Product version	Software version	Hardware version
Gazelle S1020i	P100R001	V2.1.15 or later	A.00 or later

Conventions

Symbol conventions

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

Symbol	Description
⚠ Warning	Indicate a hazard with a medium or low level of risk which, if not avoided, could result in minor or moderate injury.
⚠ Caution	Indicate a potentially hazardous situation that, if not avoided, could cause device damage, data loss, and performance degradation, or unexpected results.
✎ Note	Provide additional information to emphasize or supplement important points of the main text.

Symbol	Description
Tip	Indicate a tip that may help you solve a problem or save time.

General conventions

Convention	Description
Times New Roman	Normal paragraphs are in Times New Roman.
Arial	Paragraphs in Warning, Caution, Notes, and Tip are in Arial.
Boldface	Buttons and navigation path are in **Boldface**.
Italic	Book titles are in *italics*.
`Lucida Console`	Terminal display is in `Lucida Console`.
Book Antiqua	Heading 1, Heading 2, Heading 3, and Block are in Book Antiqua.

Change history

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Issus 07 (2015-06-03)

Seventh commercial release

- Updated safety specifications.
- Updated prints of interfaces on the AC power model.
- Upgraded technical specifications of power supplies.
- Fixed known bugs.

Issus 06 (2015-05-15)

Sixth commercial release

- Updated the UL certification.
- Updated LED prints.
- Updated the input voltage range of the AC power.

Issus 05 (2015-02-17)

Fifth commercial release

- Added the Gazelle S1020i-2GF2GX-16FE.
- Added the Gazelle S1020i-2GF2GX-8FE.

Issus 04 (2014-11-14)

Fourth commercial release

- Fixed known bugs.
- Modified the voltage range.
- Modified EMC specifications.

Issue 03 (2013-12-25)

Third commercial release

- Fixed known bugs.
- Modified the voltage range of the DC power.
- Modified technical specifications of the alarm interface.
- Modified the device structure figure and prints of power interfaces.
- Modified the operating time for the RST button.

Issue 02 (2013-06-24)

Second commercial release

- Fixed known bugs.
- Added the description of the RST button.
- Added the Gazelle S1020i-16FE.

Issue 01 (2012-12-07)

Initial commercial release

Contents

Figures

Tables

1 Overview

This chapter describes basic information about the Gazelle S1020i, including the following sections:

- Introduction
- Characteristics
- Models

1.1 Introduction

The manageable guide-rail Layer 2 industrial Ethernet switch Gazelle S1020i (hereinafter referred to as the Gazelle S1020i unless otherwise stated) adopts a guide-rail chassis with all-metal shell. Featuring fanless design, good heat dissipation, small size, low power consumption, and easy installation, it can meet requirements for the guide-rail switch at the access layer in scenarios, such as industrial control, intelligent transportation, and electric power ring network.

The Gazelle S1020i provides multiple types of interfaces and complete Layer 2 features, thus meetings requirements for high reliability in industrial environments. It includes the following models according to the interface type and quantity:

- Gazelle S1020i-4GF16FE: provide four 1000 Mbit/s SFP optical interfaces and sixteen 100 Mbit/s RJ45 electrical interfaces.
- Gazelle S1020i-16FE: provide sixteen 100 Mbit/s RJ45 electrical interfaces.
- Gazelle S1020i-2GF2GX-16FE: provide two 1000 Mbit/s SFP optical interfaces, two 1000 Mbit/s Combo interfaces, and sixteen 100 Mbit/s RJ45 electrical interfaces.
- Gazelle S1020i-2GF2GX-8FE: provide two 1000 Mbit/s SFP optical interfaces, two 1000 Mbit/s Combo interfaces, and eight 100 Mbit/s RJ45 electrical interfaces.

1.2 Characteristics

1.2.1 High reliability

The Gazelle S1020i is characterized by high reliability:

- Adopt an industrial chip and power supply, thus implementing lower power consumption

- Adopt a guide-rail chassis with all-metal shell, fanless design, good heat-dissipation, and additional cooling fins, thus meeting heat dissipation requirements.
- Support IP40 protection level.
- Support a wide range of operating temperature from -40 to 85 ℃ and storage temperature from -40 to 85 ℃.
- Be dampproof and corrosion-resisting, and support humidity range from 5% to 95% (non-condensing) in the working environment.
- Pass IEC 61000-4 industrial-grade electromagnetic compatibility test with good anti-electromagnetic interference performance.
- Support Mean Time Between Failure (MTBF) of 35 years.

1.2.2 Various interface types

The modular Gazelle S1020i meets special on-site environment requirements with flexible interface configurations, installation, power supply, and networking.

- Provide 1000 Mbit/s SFP optical interfaces and RJ45 electrical interfaces.
- Provide the RJ45 Console interface.
- Provide one alarm output interface.
- Provide one Reset button to restore factory settings or restart the device.

1.2.3 Flexible networking applications

The Gazelle S1020i supports flexible networking as below:

- Support multiple networking applications, such as chain, star, double-star, single ring, intersecting ring, and tangent ring.

1.2.4 Strict QoS guarantee

The Quality of Service (QoS) guarantees the realtime delivery and integrity of important services when the network is overloaded or congested. Meanwhile the whole network can operate efficiently.

The Gazelle S1020i supports the following traffic management features:

- Support QoS based on the IEEE 802.1p standard to provide users with reliable and effective methods for service optimization.
- Support interface trust mode; trust Class of Service (CoS) priority and Differentiated Services Code Point (DSCP) priority.
- Support interface-based priority mapping, mapping from CoS to local priority, and mapping from DSCP to local priority.
- Support scheduling 8 queues and multiple scheduling modes: Strict Priority (SP), Weight Round Robin (WRR), DRR, SP+WRR, and SP+DRR.
- Support traffic policy and traffic classification.
- Support mirroring, rate limiting and redirecting based on flow.
- Support modifying local priority and VLAN based on flow.

1.2.5 Complete security guarantee

The Gazelle S1020i provides complete security guarantee:

- Support user management at different levels and password protection to avoid unauthorized access.
- Support Access Control List (ACL), Remote Authentication Dial In User Service (RADIUS) authentication, Terminal Access Controller Access Control System (TACACS+) authentication, and provide centralized password management. Multiple access control and user authentication technologies can effectively enhance security of the network and devices.
- Support binding MAC addresses with interfaces.
- Support IEEE 802.1x security access control.
- Support storm control (over broadcast, unknown multicast, and unknown unicast packets), which ensures normal operation of the Gazelle S1020i under bad network conditions.
- Support unique loop detection, which ensures long-term stability of network.
- Support Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP), thus improving redundant backup and error tolerance and ensuring stable network operation.
- Support ITU-T G.8032 Ethernet Ring Protection Switching (ERPS) protocol. The network self-healing time is less than 50ms. ERPS solves the multi-ring protection, multi-topology, and multi-protocol problems.
- Support the advanced industrial Raisecom Ring Protection Switching (RRPS), with self-healing time less than 50ms.
- Support IEEE 802.1Q interface-based VLAN partitioning to isolate physical interfaces. Support interface protection to further optimize the protection mechanism of user data.
- Support IGMP Snooping for better providing multicast services.
- Support SNMPv3 encrypted authentication and access security.
- Support DHCP Snooping.
- Support monitoring and protecting the Flash. When the Flash is erased or written too frequently or the times exceed the upper limit, an alarm will be generated and sent to the NMS and written into the system log.

1.2.6 Comprehensive management modes

The Gazelle S1020i supports the following management modes:

- Web mode: it employs the graphic management interface, which reduces the difficulty of Human-Computer Interaction (HCI) and facilitates management and maintenance of the device.
- SNMP/RMON mode: it can be managed through the NView NNM system which can manage one or more devices centralizedly or in terms of alarm management and other features.
- Support cluster management, which can configure devices in batches, automatically discover devices, plan network topology, gather statistics of and analyze online or offline user rate, provide new management modes for customers, and simplify management process.
- Provide the RJ45 Console interface, and support local login through the Console interface to implement local management and maintenance.
- Support TFTP, FTP, Telnet, and SSH login for remote management and maintenance.
- Support software upgrade in RJ45 Console, Web, and NView NNM modes.

1.3 Models

The Gazelle S1020i series can be divided into multiple models by interface type, as listed in Table 1-1.

Table 1-1 Models

Model	Description
Gazelle S1020i-4GF16FE	● Provide four 1000 Mbit/s SFP optical interfaces. ● Provide sixteen 100 Mbit/s RJ45 electrical interfaces.
Gazelle S1020i-16FE	Provide sixteen 100 Mbit/s RJ45 electrical interfaces.
Gazelle S1020i-2GF2GX-16FE	● Provide two 1000 Mbit/s SFP optical interfaces. ● Provide two 1000 Mbit/s Combo interfaces. ● Provide sixteen 100 Mbit/s RJ45 electrical interfaces.
Gazelle S1020i-2GF2GX-8FE	● Provide two 1000 Mbit/s SFP optical interfaces. ● Provide two 1000 Mbit/s Combo interfaces. ● Provide eight 100 Mbit/s RJ45 electrical interfaces.

2 Hardware structure

The hardware structure of the Gazelle S1020i consists of the chassis, switching MCC, and power supply. This chapter describes the hardware structure of the Gazelle S1020i, including the following sections:

- Chassis
- Interfaces and button
- Power supplies
- Cables

2.1 Chassis

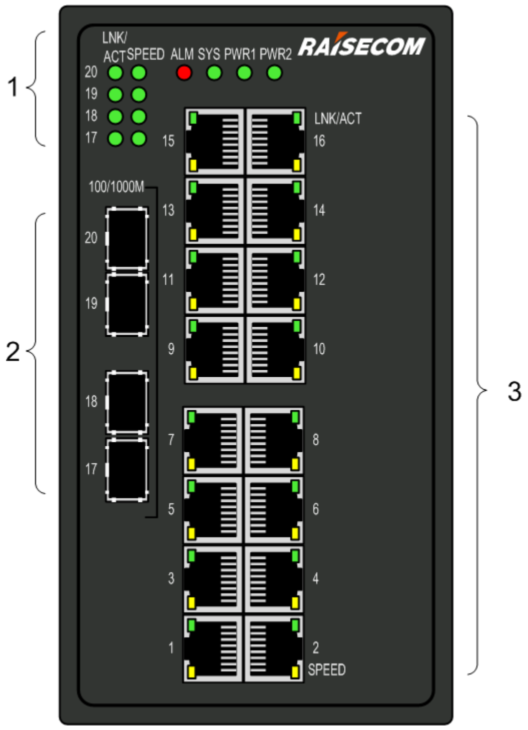
Dimensions of the Gazelle S1020i chassis are 98 mm (Width) × 155 mm (Depth) × 177 mm (Height).

2.1.1 Front appearance

Gazelle S1020i-4GF16FE

Figure 2-1 shows the front appearance of the Gazelle S1020i-4GF16FE.

Figure 2-1 Front appearance of the Gazelle S1020i-4GF16FE

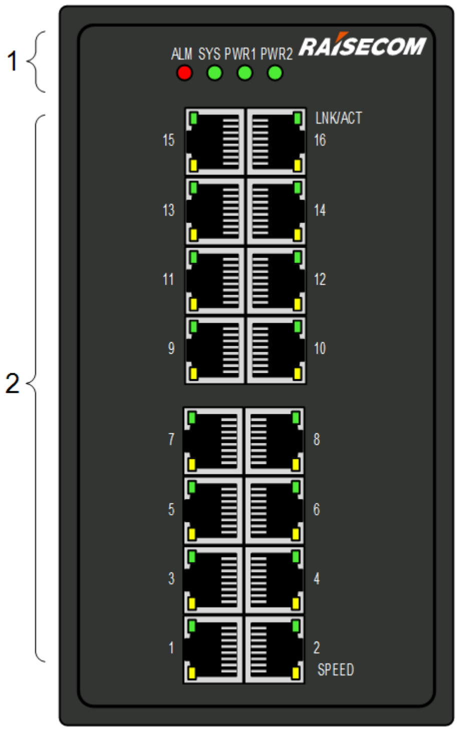


1	LEDs (LNK/ACT, SPEED, ALM, SYS, PWR1, and PWR2)
2	Service uplink interfaces 17–20 (SFP)
3	Service downlink interfaces 1–16 (RJ45) and LEDs (LNK/ACT and SPEED)

Gazelle S1020i-16FE

Figure 2-2 shows the front appearance of the Gazelle S1020i-16FE.

Figure 2-2 Front appearance of the Gazelle S1020i-16FE

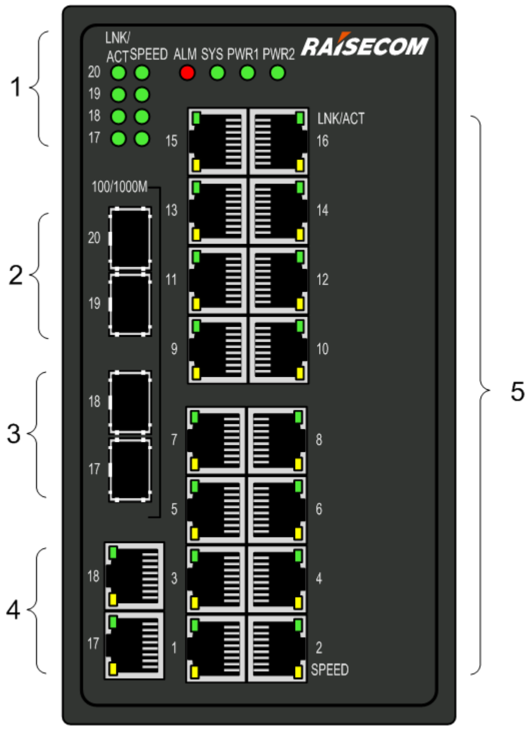


1	LEDs (ALM, SYS, PWR1, and PWR2)
2	Service interfaces 1–16 (RJ45) and LEDs (LNK/ACT and SPEED)

Gazelle S1020i-2GF2GX-16FE

Figure 2-3 shows the front appearance of the Gazelle S1020i-2GF2GX-16FE.

Figure 2-3 Front appearance of the Gazelle S1020i-2GF2GX-16FE

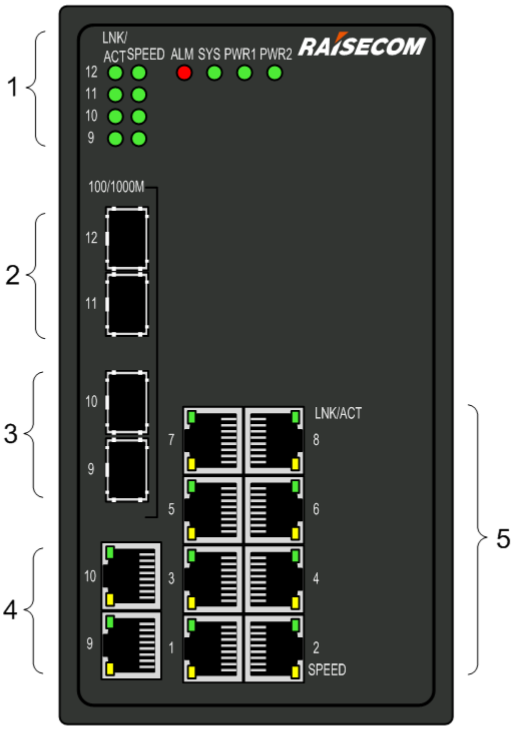


1	LEDs (LNK/ACT, SPEED, ALM, SYS, PWR1, and PWR2)
2	Service uplink interfaces 19–20 (SFP)
3	Service interfaces 17–18 (SFP Combo optical interfaces)
4	Service interfaces 17–18 (SFP Combo electrical interfaces) and LEDs (LNK/ACT and SPEED)
5	Service downlink interfaces 1–16 (RJ45) and LEDs (LNK/ACT and SPEED)

Gazelle S1020i-2GF2GX-8FE

Figure 2-4 shows the front appearance of the Gazelle S1020i-2GF2GX-8FE.

Figure 2-4 Front appearance of the Gazelle S1020i-2GF2GX-8FE



1	LEDs (LNK/ACT, SPEED, ALM, SYS, PWR1, and PWR2)
2	Service uplink interfaces 11–12 (SFP)
3	Service interfaces 9–10 (SFP Combo optical interfaces)
4	Service interfaces 9–10 (SFP Combo electrical interfaces) and LEDs (LNK/ACT and SPEED)
5	Service downlink interfaces 1–8 (RJ45) and LEDs (LNK/ACT and SPEED)

Note

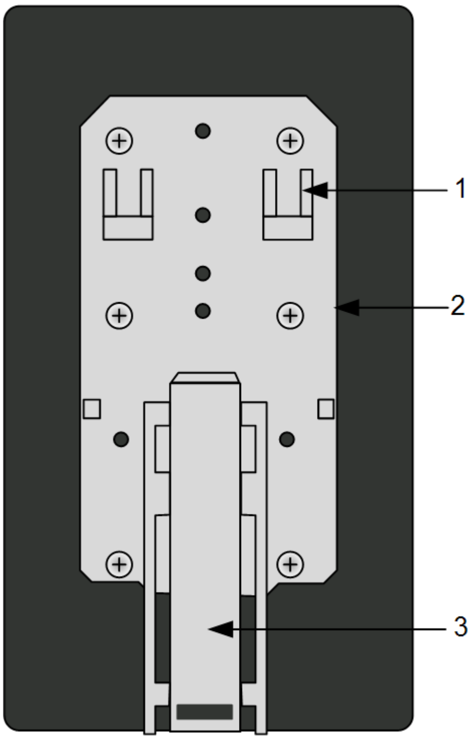
Figure 2-1 to Figure 2-4 show front panels of the Gazelle S1020i DC power model. The DC power supply supports dual inputs, with PWR1 and PWR2 LEDs on the front panel. The Gazelle S1020i AC power model supports single input with only one PWR LED on the front panel.

For details of LEDs, see section 9.2 Lookup table for LEDs.

2.1.2 Rear appearance

Figure 2-5 shows the rear appearance of the Gazelle S1020i.

Figure 2-5 Rear appearance

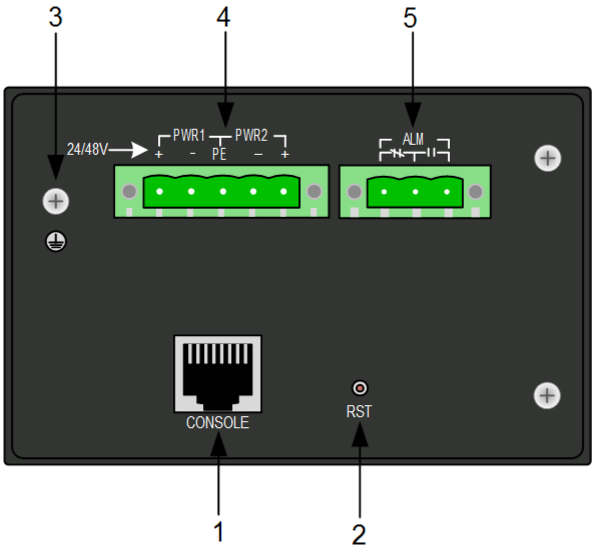


1	Spring clip
2	Rail clip
3	Sliding connector

2.1.3 Front appearance

Figure 2-6 shows the front appearance of the Gazelle S1020i DC power model.

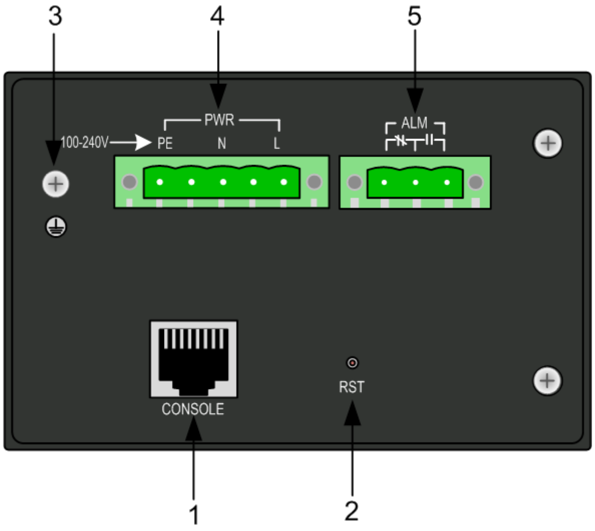
Figure 2-6 Front appearance of the Gazelle S1020i DC power model



1	Console interface (RJ45)	2	RST button
3	Ground terminal	4	Power interfaces (PWR1 and PWR2)
5	Alarm interface (ALM)		

Figure 2-7 shows the front appearance of the Gazelle S1020i AC power model.

Figure 2-7 Front appearance of the Gazelle S1020i AC power model



1	Console interface (RJ45)	2	RST button
3	Ground terminal	4	Power interface (PWR)
5	Alarm interface (ALM)		

2.2 Interfaces and button

Service interfaces

Table 2-1 lists the interfaces types and usage of the Gazelle S1020i.

Table 2-1 Interfaces types and usage

Model	Usage	Type	Description	Quantity
Gazelle S1020i-4GF16FE	Service uplink interface	SFP	Support the following optical module types: • 1000BASE-X • 100BASE-FX	4
	Service downlink interface	RJ45	10/100BASE-TX auto-negotiation electrical interface	16
Gazelle S1020i-16FE	Service interface	RJ45	10/100BASE-TX auto-negotiation electrical interface	16
Gazelle S1020i-2GF2GX-16FE	Service uplink interface	SFP	Support the following optical module types: • 1000BASE-X • 100BASE-FX	2
		Combo optical interface	Support the following optical module types: • 1000BASE-X • 100BASE-FX Note You can forcibly configure the 1000 Mbit/s Combo optical interface to a 100 Mbit/s interface through software. In this case, the 1000 Mbit/s Combo optical interface does not support Combo function; in other words, the Combo electrical interface does not take effect.	2
		Combo electrical interface	10/100/1000BASE-T auto-negotiation electrical interface	2
	Service downlink interface	RJ45	10/100BASE-TX auto-negotiation electrical interface	16

Model	Usage	Type	Description	Quantity
Gazelle S1020i-2GF2GX-8FE	Service uplink interface	SFP	Support the following optical module types: • 1000BASE-X • 100BASE-FX	2
		Combo optical interface	Support the following optical module types: • 1000BASE-X • 100BASE-FX Note You can forcibly configure the 1000 Mbit/s Combo optical interface to a 100 Mbit/s interface through software. In this case, the 1000 Mbit/s Combo optical interface does not support Combo function; in other words, the Combo electrical interface does not take effect.	2
		Combo electrical interface	10/100/1000BASE-T auto-negotiation electrical interface	2
	Service downlink interface	RJ45	10/100BASE-TX auto-negotiation electrical interface	8

Management and auxiliary interfaces

Table 2-2 lists the management and auxiliary interfaces of the Gazelle S1020i.

Table 2-2 Management and auxiliary interfaces

Print	Description	Quantity
CONSOLE (RJ45 Console interface)	Use the DB9 or DB25 Console cable to connect the PC.	1
ALM (Phoenix connector alarm interface)	Output alarms (with spaces of 7.62 mm).	1

Button

Table 2-2 describes the button on the Gazelle S1020i.

Table 2-3 Button

Button	Description
RST (Reset button)	• Short press the RST button for less than 5s to restart the device. • Long press the RST button for over 5s to restore factory settings.

2.3 Power supplies

The power supply supports the following features:

- The DC power supply supports 24/48 VDC power input.
- The AC power supply supports 100–240 VAC power input.
- The DC power supply supports dual power input redundancy. The AC power supply supports single power input.
- Support overvoltage protection and surge protection.
- Support relay alarms and NMS alarms for power faults.

2.4 Cables

Cables include the fiber, power cables, ground cable, service cables, and auxiliary cables. For details, see *Gazelle S1020i (A) Hardware Description*.

3 Technical specifications

This chapter describes technical specifications of the Gazelle S1020i, including the following sections:

- Overall parameters
- Software features
- Laser safety class
- Reliability specifications
- Safety standards
- EMC standards
- Environmental standards

3.1 Overall parameters

Table 3-1 lists overall parameters of the Gazelle S1020i.

Table 3-1 Overall parameters

Parameter			Description
Dimensions			98 mm (Width) × 155 mm (Depth) × 177 mm (Height)
Weight (without the rail clip)			< 2.0 kg
Maximum power consumption			13.2 W
Protection level			IP40
Power supply	DC power supply	Rated voltage	24/48 VDC
		Voltage range	20–72 VDC
	AC power supply	Rated voltage	100–240 VAC
		Frequency	50/60 Hz
Operating temperature			-40 to 85°C

Parameter	Description
Operating humidity	5%–95% (non-condensing)

3.2 Software features

Table 3-2 lists software features of the Gazelle S1020i.

Table 3-2 Software features

Feature	Description
Basic features	● Support RJ45 Console/Telnet/SSH login. ● Support CLI. ● Support Web network management. ● Support file management. ● Support the loading and upgrade (TFTP auto-loading, BootROM, and FTP/SFTP/TFTP). ● Support time management. ● Support interface management. ● Support basic configurations. ● Support task scheduling.
Ethernet	● Support MAC address (16K). ● Support VLAN (4094 VLANs). ● Support basic QinQ. ● Support selective QinQ (1000). ● Support VLAN mapping (680 in the ingress direction). ● Support STP/RSTP/MSTP. ● Support GARP (GVRP and GMRP). ● Support loop detection. ● Support line detection. ● Support interface protection. ● Support port mirroring. ● Support L2 protocol transparent transmission (Dot1x packets, BPDUs, LACP packets, CDP packets, PVST packets, and VTP packets.
Ring protection	● Support ITU-T G.8032 ERPS ● Support RRPS
IP services	● Support ARP. ● Support Layer 3 interfaces. ● Support DHCP Client. ● Support DHCP Server. ● Support DHCP Relay. ● Support DHCP Snooping. ● Support DHCP Option.
IP routing	● Support route management. ● Support the static route. ● Support the default route.

Feature	Description
QoS	• Support ACL rules (1K entries). • Support trusted priority. • Support traffic classification (IP precedence, DSCP priority, and CoS priority) and traffic policy (rate limiting, redirection, and remarking based on traffic policy). • Support local priority mapping and queue scheduling (SP, WRR, and SP+DRR). • Support rate limiting based on interface.
Multicast	• Support multicast entries (1K entries). • Support IGMP Snooping (v1/v2).
Security	• Support port security MAC. • Support dynamic ARP detection. • Support RADIUS authentication. • Support 802.1x. • Support TACACS+. • Support storm control. • Support IP Source Guard. • Support PPPoE+.
Reliability	• Support link aggregation (14 LAGs). • Support interface backup. • Support link-state tracking.
System management	• Support SNMP. • Support KeepAlive. • Support RMON. • Support cluster management. • Support LLDP. • Support optical module DDM. • Support system log. • Support alarm management. • Support hardware environment monitoring. • Support CPU monitoring. • Support CPU protection. • Support Ping and Traceroute.

3.3 Laser safety class

According to the Tx power of Laser, the Gazelle S1020i laser belongs to Class 1 in safety class.

In Class 1, the maximum Tx power on the optical interface is smaller than 10 dBm (10 mW).

Warning

The laser inside fiber may hurt your eyes. Do not stare into the optical interface directly during installation and maintenance.

3.4 Reliability specifications

Table 3-3 lists reliability specifications of the Gazelle S1020i.

Table 3-3 Reliability specifications

Parameter	Description
System availability	99.999%. The annual failure time for the Gazelle S1020i should be no longer than 5 minutes.
Annually system mean repair rate	< 1.5%
MTTR	< 2 hours
MTBF	100000 hours

3.5 Safety standards

The Gazelle S1020i AC power models, Gazelle S1020i-4GF16FE-AC (A.10), Gazelle S1020i-16FE-AC (A.10), Gazelle S1020i-2GF2GX-16FE-AC (A.01), Gazelle S1020i-2GF2GX-8FE-AC (A.01), comply with safety standards listed in Table 3-4.

Table 3-4 Certificates of Gazelle S1020i AC power models

Certificate type	Standard	Issue time
cULus	● UL 60950-1, 2nd Edition,2014-10-14 ● CAN/CSA C22.2 No. 60950-1-07, 2nd Edition, 2014-10	2015-04-30

3.6 EMC standards

The Gazelle S1020i is compliant with the following Electromagnetic Compatibility (EMC) standards:

- Electro Magnetic Interference (EMI) meets CISPR 22 CLASS A requirements.
- Static electricity: IEC 61000-4-2 level 4
- Radiated Immunity Test (RIT): IEC 61000-4-3 level 3
- Electrical fast transient pulse group: IEC 61000-4-4 level 4
- Surge: IEC 61000-4-5 level 4
- RF Conducted Immunity (CI): IEC 61000-4-6 level 3
- Power frequency magnetic field: IEC 61000-4-8 level 5
- Oscillatory wave: IEC 61000-4-12 level 3
- Damped oscillatory wave: IEC 61000-4-18 level 3
- Common mode conduction: IEC 61000-4-16 level 4
- Damped oscillatory magnetic field: IEC 61000-4-10 level 5

- Pulse magnetic field: IEC 61000-4-9 level 5
- DC ripple immunity: IEC61000-4-17 level 3

3.7 Environmental standards

The Gazelle S1020i is applicable to the industrial environment and environmental requirements are as shown in Table 3-5.

Table 3-5 Environmental requirements

Parameter	Description
Air pressure	86–106 kPa
Operating temperature	-40 to 85 ℃
Storage temperature	-40 to 85 ℃
Operating humidity	5%–95% RH (non-condensing)
Protection level	IP40
Environmental authentication	EU RoHS standard-compliant

4 Networking applications

This chapter describes networking applications of the Gazelle S1020i, including the following sections:

- Road monitoring system application
- Tunnel divisional communication system application

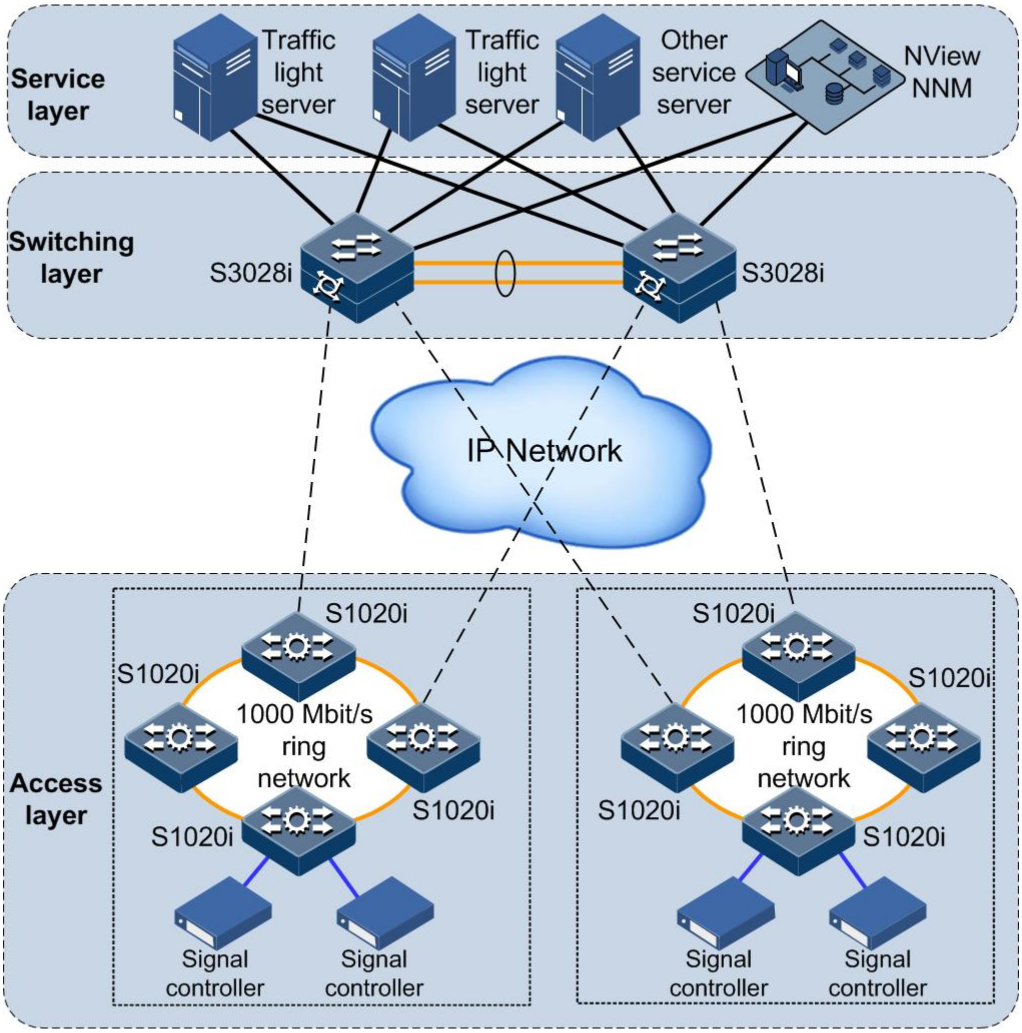
4.1 Road monitoring system application

The road monitoring system is an important part of the command system of public security because it directly reflects on-site situations. The access device at the key spot transmits video signals in various forms (through the fiber or leased line) to the traffic command center, which stores, processes, and distributes information. In this case, the traffic police and stewards can make timely and precise judgment on traffic violations, accidents, and emergent events, and thus adjust control parameters of each system and scheduling policies.

At the access layer, multiple Gazelle S1020i devices form a 1000 Mbit/s redundant ring network, which guarantees stable, reliable, and secure transmission. Two of them on each ring are connected to two Gazelle S3028i devices respectively through a transport network to implement dual-link redundancy protection. Configure Virtual Router Redundancy Protocol (VRRP) on the two Gazelle S3028i devices to guarantee continuity and reliability of communication.

Figure 4-1 shows the road monitoring system application.

Figure 4-1 Road monitoring system application



4.2 Tunnel divisional communication system application

The tunnel divisional communication system adopts hierarchical controls, including the overall monitoring center, sub-monitoring center, tunnel management station, and Programmable Logic Controller (PLC). The substation at the tunnel control, tunnel management station, and sub-monitoring center can respectively monitor and control devices in their jurisdictional limit.

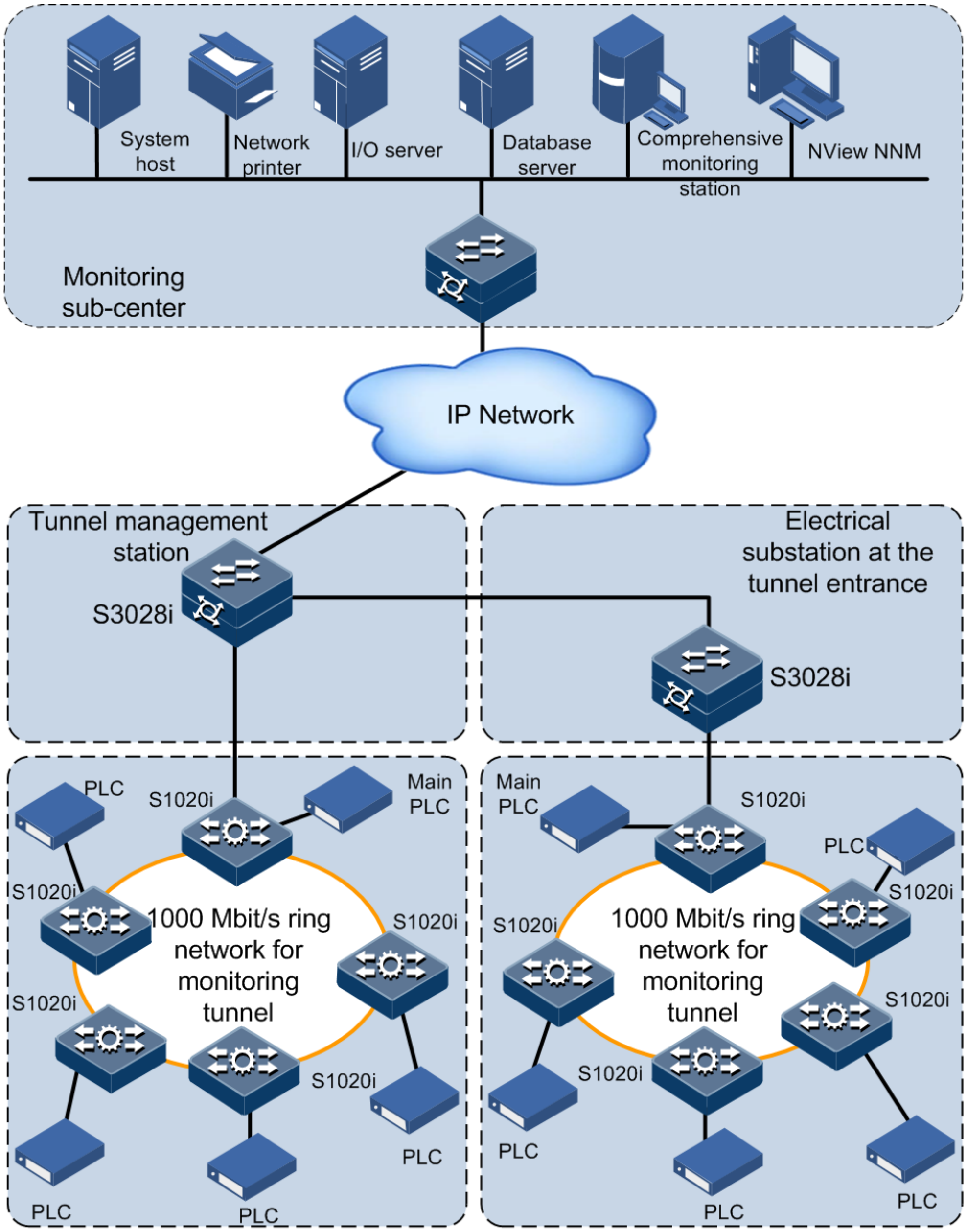
In the tunnel, multiple Gazelle S1020i devices form a 1000 Mbit/s fiber ring network. When the network is faulty, it can resume connection within 50ms and thus guarantee reliable and realtime transmission of data between the tunnel network and superior monitoring network.

The PLC in the tunnel can be connected to the nearby Gazelle S1020i. Tunnel monitoring device data collected by the PLC is transmitted by the fiber ring network to the Gazelle S1020i that is connected with the local main PLC. This Gazelle S1020i transmits data to the Gazelle S3028i at the tunnel management station. Then, the Gazelle S3028i transmits data to the sub-monitoring center.

Data of a neighboring tunnel is transmitted through fibers to the Gazelle S3028i at the electrical substation at the tunnel entrance, and then to the sub-monitoring center through the communication system.

Figure 4-2 shows the tunnel divisional communication system application.

Figure 4-2 Tunnel divisional communication system application



5 Link features

This chapter describes link features of the Gazelle S1020i, including the following sections:

- Ethernet
- Ring network protection
- Reliability

5.1 Ethernet

5.1.1 Ethernet interface

Ethernet is a very important LAN networking technology which is flexible, simple and easy to implement. The Ethernet interface includes the Ethernet electrical interface and Ethernet optical interface.

The Gazelle S1020i supports both Ethernet electrical and optical interfaces.

Auto-negotiation

Auto-negotiation is used to make the devices at both ends of a physical link automatically choose the same working parameters by exchanging information. The auto-negotiation parameters include duplex mode, interface rate, and flow control. Once successful in negotiation, devices at both ends of the link can work in the same duplex mode and interface rate.

Cable connection

Generally, the Ethernet cable can be categorized as the Medium Dependent Interface (MDI) cable and Medium Dependent Interface crossover (MDI-X) cable. MDI provides physical and electrical connection from terminal to network relay device while MDI-X provides connection between devices of the same type (terminal to terminal). Hosts and routers use MDI cables while hubs and switches use MDI-X interfaces. Usually, the connection of different devices should use the MDI cable while devices of the same type should use the MDI-X cable. Auto-negotiation mode devices can be connected by the MDI or MDI-X cable.

The Ethernet cable of the Gazelle S1020i supports auto-MDI/MDIX.

5.1.2 MAC address table

Introduction

The Ethernet device forwards Ethernet packets rapidly by following MAC address forwarding rules. Each Ethernet device has a MAC address table which records mappings among MAC addresses, interfaces, and VLANs. The Ethernet device forwards ingress packets according to the MAC address table, which is the basis for an Ethernet device to implement expedited forwarding of Layer 2 packets. The MAC address is saved in the buffer of the Ethernet device, so the memory of the buffer determines the number of MAC addresses that can be saved.

The MAC address table contains the following information:

- Destination MAC address
- Destination MAC address related interface number
- Interface VLAN ID
- Flag bits

The Gazelle S1020i supports showing MAC addresses by device, interface, or VLAN.

Classification of MAC addresses

The MAC address table contains static address entries and dynamic address entries.

- Static MAC address entry: also called permanent address, added and deleted by the user manually, not aged with time. For a network with small changes of devices, adding static address entry manually can reduce the network broadcast flow, improve the security of the interface, and prevent entries from being lost after the system is restarted or the interface card is hot swapped or restart.
- Dynamic MAC address entry: the Gazelle S1020i can add dynamic MAC address entries through MAC address learning. The entries are aged according to the configured aging time, and will be empty after the system is restarted or the interface card is hot swapped or restart.

The Gazelle S1020i supports the maximum 16K dynamic MAC addresses, and each interface supports 1024 static MAC addresses.

Aging time of MAC addresses

There is limit on the capacity of the MAC address table on the Gazelle S1020i. To maximize the use of the MAC address table, the Gazelle S1020i uses the aging mechanism to update the MAC address table. For example, when the Gazelle S1020i creates a dynamic entry, it starts the aging timer. If it does not receive packets from the MAC address in the entry during the aging time, the Gazelle S1020i will delete the entry.

The aging mechanism takes effect on dynamic MAC addresses only.

MAC address limit

The MAC address limit is used to limit the number of MAC addresses, avoid extending the searching time of forwarding entry caused by over large MAC address table and degrading the forwarding performance of the Ethernet switch, and it is effective to manage the MAC address table.

The MAC address limit can also improve the speed of forwarding packets by the switch chip.

5.1.3 VLAN

Introduction

Virtual Local Area Network (VLAN) is a protocol to solve Ethernet broadcast and security problem. It is a Layer 2 isolation technique that partitions a LAN into different broadcast domains logically rather than physically, and then the different broadcast domains can work as virtual groups without any influence from one another. In terms of functions, VLAN has the same features as LAN, but members in one VLAN can access one another without restriction by physical location.

VLAN partition

The VLAN technique can partition a physical LAN into different broadcast domains logically. Hosts without intercommunication requirements can be isolated by VLAN, so VLAN partitioning improves network security, and reduces broadcast flow and broadcast storm.

The Gazelle S1020i complies with IEEE 802.1Q standard VLAN and supports 4094 concurrent VLANs.

The Gazelle S1020i supports VLAN partition by interface. The Gazelle S1020i has two interface modes: Access mode and Trunk mode.

Layer 3 interface

The Layer 3 interface refers to the IP interface, and it is the virtual interface based on VLAN. Configuring Layer 3 interface is generally used for network management or routing link connection of multiple devices. Associating a Layer 3 interface to VLAN requires configuring IP address; each Layer 3 interface will correspond to an IP address and associate with at least one VLAN.

5.1.4 QinQ

QinQ (also known as Stacked VLAN or Double VLAN) technique is an extension to 802.1Q defined in IEEE 802.1ad standard.

Basic QinQ

Basic QinQ is a simple Layer 2 VPN tunnel technique, which encapsulates outer VLAN Tag for user private network packets at carrier access end, then the packet takes double VLAN Tag to transmit through backbone network (public network) of the carrier. On the public network, packets are transmitted in accordance with outer VLAN Tag (namely the public network VLAN Tag), the user private network VLAN Tag is transmitted as data in packets.

Figure 5-1 Principles of basic QinQ

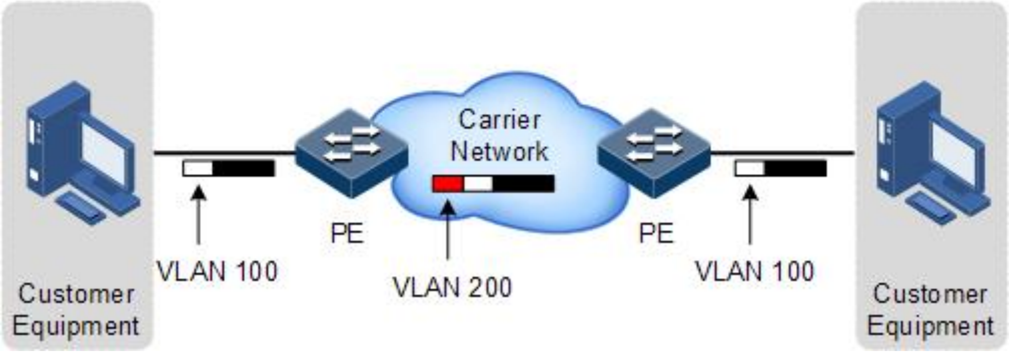


Figure 5-1 shows the basic QinQ networking. The Gazelle S1020i works as the carrier Provider Edge (PE).

The packet is transmitted from the CE to the PE, with the VLAN 100 Tag. The packet will be added with the outer Tag VLAN 200 when passing the user-side interface on the PE and then enter the PE network through the network-side interface on the PE.

The packet with Tag VLAN 200 is transmitted to the PE on the other end through the carrier network, and then the PE at the other end will remove outer Tag VLAN 200 and send the packet to the user device. Now the packet carries only one Tag, namely, Tag VLAN 100.

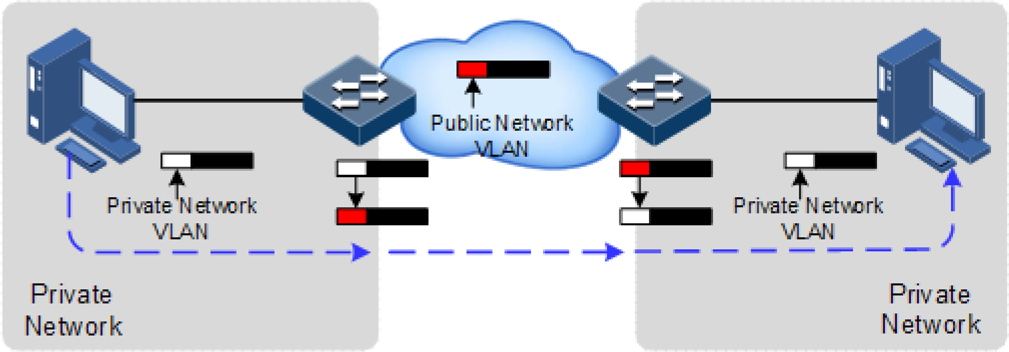
This technique can save public network VLAN ID resources. You can plan private network VLAN ID to avoid conflict with public network VLAN ID.

The Gazelle S1020i supports up to 1000 selective QinQ rules.

5.1.5 VLAN mapping

VLAN mapping is used to replace the private VLAN Tag of Ethernet packets with carrier's VLAN Tag, making packets transmitted according to carrier's VLAN forwarding rules. When packets are sent to the peer private network from the ISP network, the VLAN Tag is restored to the original private VLAN Tag according to the same VLAN forwarding rules. Therefore packets are correctly sent to the destination. Figure 5-2 shows principles of VLAN mapping.

Figure 5-2 Principles of VLAN mapping



After receiving a VLAN Tag contained in a user private network packet, the Gazelle S1020i matches the packet according to configured VLAN mapping rules. If successful, it maps the packet according to configured VLAN mapping rules.

By supporting 1: 1 VLAN mapping, the Gazelle S1020i replaces the VLAN Tag carried by a packet from a specified VLAN to the new VLAN Tag.

Different from QinQ, VLAN mapping does not encapsulate packets with multiple layers of VLAN Tags, but needs to modify VLAN Tag so that packets are transmitted according to the carrier's VLAN forwarding rule.

The Gazelle S1020i supports up to 680 VLAN mapping rules in the ingress direction.

5.1.6 STP/RSTP/MSTP

STP

With the increasing complexity of network structure and growing number of switches on the network, the Ethernet network loops become the most prominent problem. Because of the packet broadcast mechanism, a loop causes the network to generate storms, exhaust network resources, and have serious impact to forwarding normal data.

Spanning Tree Protocol (STP) is compliant to IEEE 802.1d standard and used to remove data physical loop in data link layer in LAN.

The Gazelle S1020i running STP can process Bridge Protocol Data Unit (BPDU) packet with each other for the election of root switch and selection of root port and designated port. It also can block loop interface on the Gazelle S1020i logically according to the selection results, and finally trims the loop network structure to tree network structure without loop which takes a Gazelle S1020i as root. This prevents the continuous proliferation and limitless circulation of packet on the loop network from causing broadcast storms and avoids declining packet processing capacity caused by receiving the same packets repeatedly.

Although STP can eliminate loop network and prevent broadcast storm well, its shortcomings are still gradually exposed with thorough application and development of network technology.

The major disadvantage of STP is the slow convergence speed.

RSTP

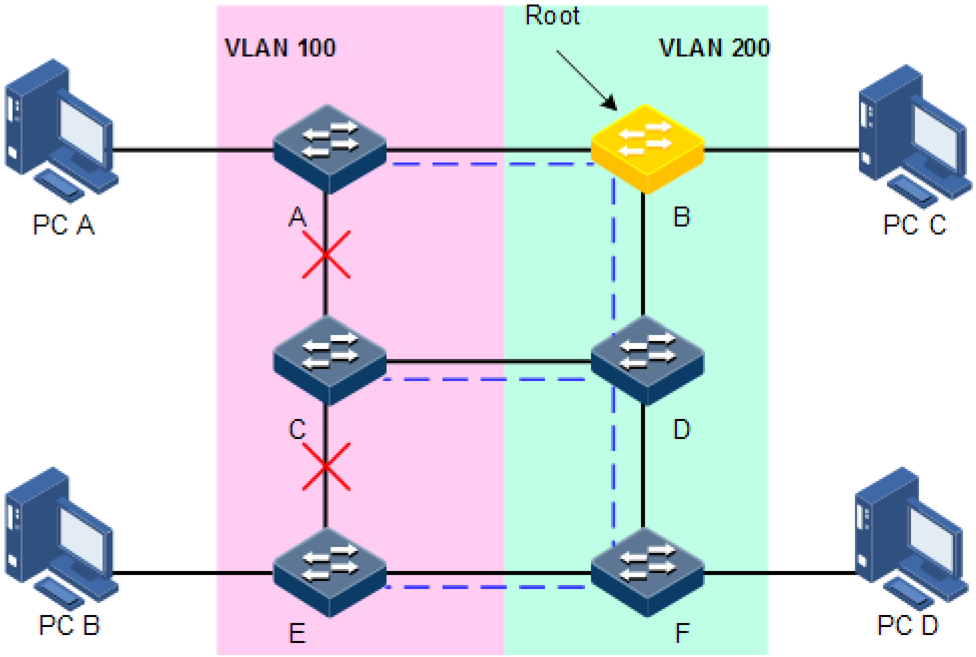
For improving the slow convergent speed of STP, IEEE 802.1w establishes Rapid Spanning Tree Protocol (RSTP).

The purpose of STP/RSTP is to simplify a bridge connection LAN to a unitary spanning tree in logical topology and to avoid broadcast storm.

The disadvantages of STP/RSTP are exposed with the rapid development of VLAN technology. The unitary spanning tree simplified from STP/RSTP leads the below problems:

- The whole switching network has only one spanning tree, which will lead to longer convergence time on a larger network.
- Waste of bandwidth since a link does not carry any flow after it is blocked.
- Packets of partial VLAN cannot be forwarded when network structure is unsymmetrical. As shown in Figure 5-3, Switch B is the root switch; RSTP blocks the link between Switch A and Switch C logically and makes that the VLAN 100 packet cannot be transmitted and Switch A and Switch C cannot communicate.

Figure 5-3 VLAN packet forward failure due to RSTP



MSTP

Multiple Spanning Tree Protocol (MSTP) is defined by IEEE 802.1s. Recovering the disadvantages of STP and RSTP, MSTP implements fast convergence and distributes different VLAN flow following its own path to provide an excellent load sharing mechanism.

MSTP divides a switch network into multiple regions, called MST region. Each MST region contains several spanning trees but the trees are independent from each other. Each spanning tree is called a Multiple Spanning Tree Instance (MSTI).

MSTP protocol introduces Common Spanning Tree (CST) and Internal Spanning Tree (IST) concepts. CST refers to taking MST region as a whole to calculate and generating a spanning tree. IST refers to generating spanning tree in internal MST region.

Compared with STP and RSTP, MSTP also introduces total root (CIST Root) and region root (MST Region Root) concepts. The total root is a global concept; all switches running STP/RSTP/MSTP can have only one total root, which is the CIST Root. The region root is a local concept, which is relative to an instance in a region.

Compared with STP and RSTP mentioned previously, MSTP has obvious advantages, including cognitive ability of VLAN, load balancing, similar RSTP interface status switching, and binding multiple VLAN to one MST instance to reduce resource occupancy rate. In addition, devices running MSTP on the network are also compatible with the devices running STP and RSTP.

5.1.7 GARP

Generic Attribute Registration Protocol (GARP) provides a mechanism to help GARP members in the same LAN to distribute, broadcast, and register information (such as VLAN and multicast information).

GARP is not an entity on a device. Those applications complying with GARP are called GARP applications. GARP VLAN Registration Protocol (GVRP) is a GARP application.

When a GARP application entity is connected to an interface of a device, the interface is mapped into the GARP application entity.

Packets of the GARP application entity use a specific multicast MAC address as its destination MAC address. When receiving packets of the GARP application entity, a device distinguishes them by destination MAC address and transmits them to different GARP applications (such as GAVP) for processing.

GVRP

GARP VLAN Registration Protocol (GVRP) is a GARP application. Based on GARP working mechanism, it maintains VLAN dynamic registration information of the switch, and sends information to other switches.

All GVRP-supportive switches can receive VLAN registration information from other switches, and dynamically update local VLAN registration information. In addition, all GVRP-supportive switches can send local VLAN registration information to other switches so that they have consistent VLAN registration information in the same VLAN. VLAN registration information sent by GVRP includes local manually configured static registration information and dynamic registration information from other switches.

To configure VLAN on multiple devices on a network and allow packets of the specified VLAN to pass are complex. By using GVRP to dynamically register and transmit the specified VLAN, the network administrator can improve working efficiency and accuracy.

GMRP

GARP Multicast Registration Protocol (GMRP) is used to maintain dynamic multicast registration information on the switch. All GMRP-supportive switches can receive multicast registration information from other switches, and dynamically update local multicast registration information. In addition, all GVRP-supportive switches can send local multicast registration information to other switches so that they have consistent multicast registration information in the same VLAN.

When a host needs to join a multicast group, it sends a GMRP Join message. The switch adds the interface that receives the GMRP Join message to the multicast group and sends the GMRP Join message to the multicast VLAN so that multicast sources in the VLAN can sense existence of multicast members. When a multicast source sends multicast packets to the multicast group, the switch forwards these multicast packets to the interface connected to the multicast group members. Multicast registration information sent by GMRP includes local manually configured static multicast registration information and dynamic multicast registration information from other switches.

5.1.8 Loop detection

Loop detection can address the influence on network caused by a loop, providing the self-detection, fault-tolerance, and robustness.

Procedures for the loop detection are as below:

- All interfaces on the Gazelle S1020i send the LoopBack-Detection packet periodically (the interval can be configured. By default, the interval is 4 seconds).
- The Gazelle S1020i checks the source MAC field of the received packet. If the MAC address of the Gazelle S1020i is saved in the source MAC field, it is believed that a loopback is detected on an interface of the Gazelle S1020i. Otherwise, the packet is discarded.

- If the Tx interface number and Rx interface number of a packet are identical, the configured loop detection action will be taken to eliminate the loop.
- If the Tx interface number and Rx interface number of a packet are different, the configured loop detection action will be taken to eliminate the loop on the interface with a bigger interface number.

5.1.9 Interface protection

With interface protection, you can add an interface, which needs to be controlled, to an interface protection group, isolating Layer 2/Layer 3 data in the interface protection group. This can provide physical isolation between interfaces, enhance network security, and provide flexible networking scheme for users.

After being configured with interface protection, interfaces in an interface protection group cannot transmit packets to each other. Interfaces in and out of the interface protection group can communicate with each other.

5.1.10 Layer 2 protocol transparent transmission

Transparent transmission is one of the main Ethernet device functions, and usually the edge network devices of carrier conduct Layer 2 protocol packet transparent transmission. Transparent transmission is enabled on the interface that connects edge network devices of carrier and user network. The interface is in Access mode, connecting to Trunk interface on user device. The layer 2 protocol packet of the user network is sent from transparent transmission interface, encapsulated by the edge network device (ingress end of packets), and then sent to the carrier network. The packet is transmitted through the carrier network to reach the edge device (egress end of packet) at the other end or carrier network. The edged device decapsulates outer layer 2 protocol packet and transparent transmits it to the user network.

The transparent transmission function includes packet encapsulation and decapsulation function, the basic implementing principle as below.

- Packet encapsulation: at the packet ingress end, the Gazelle S1020i modifies the destination MAC address from user network layer 2 protocol packets to special multicast MAC address (it is 010E.5E00.0003 by default). On the carrier network, the modified packet is forwarded as data in user VLAN.
- Packet decapsulation: at the packet egress end, the Gazelle S1020i senses the packet with special multicast MAC address (it is 010E.5E00.0003 by default), reverts the destination MAC address to DMAC of Layer 2 protocol packets, then sends the packet to assigned user network.

Layer 2 protocol transparent transmission can be enabled with QinQ concurrently or independently. In actual networking, after modifying the MAC address of protocol packets, you need to add outer Tag to packets to send them through the carrier network.

The Gazelle S1020i supports transparent transmission of BPDU packet, DOT1X packet, LACP packet, CDP packet, PVST packet, PAGP packet, UDLD packet, and VTP packet.

5.1.11 ARP address table

In the TCP/IP network environment, each host is assigned with a 32-bit IP address that is a logical address used to identify hosts between networks. To transmit packets in physical link, you must know the physical address of the destination host, which requires mapping the IP address to the physical address. In Ethernet environment, the physical address is 48-bit MAC address. The system has to transfer the 32-bit IP address of the destination host to the 48-bit Ethernet address for transmitting packet to the destination host correctly. Then Address

Resolution Protocol (ARP) is applied to resolve IP address to MAC address and set mapping relationship between IP address and MAC address.

The ARP address table includes the following two types of entries:

- Static entry: bind IP address and MAC address to avoid ARP dynamic learning cheating.
  - Static ARP address entry needs to be added/deleted manually.
  - No aging to static ARP address
- Dynamic entry: MAC address automatically learned through ARP.
  - This dynamic entry is automatically generated by switch. You can adjust partial parameters of it manually.
  - The dynamic ARP address entry will be aged after the aging time if not used.

5.2 Ring network protection

5.2.1 G.8032

G.8032 is an APS protocol over ITU-T G.8032 recommendation. It is specially used in Ethernet ring link protocol. Generally, G.8032 can avoid broadcast storm caused by data loopback. When Ethernet has a loop or device malfunction, G.8032 can switch the link to backup link and ensure service restore quickly.

G.8032 takes the control VLAN in ring network to transmit ring network control information and meanwhile, combining with the topology feature of ring network to discover network fault quickly and enable backup link to restore service fast.

G.8032 can block a loop to avoid broadcast storm by defining different roles in the ring under normal situations. G.8032 can switch the service link to the backup link if the ring link or node fails, thus eliminating loops, conducting fault Automatic Protection Switching (APS) and automatic fault restoration. In addition, the APS time is shorter than 50ms. It supports the single ring, intersecting ring, and tangent rings networking modes.

5.2.2 RRPS

With the development of Ethernet to the MAN, voice, video and multicast services have come up with higher requirements to the Ethernet redundancy protection and fault recovery time. The fault recovery convergence time of original STP mechanism is in the second level, which is far from meeting the fault recovery time requirements of MAN.

Raisecom Ring Protection Switching (RRPS) technology is a RAISECOM independent research and development protocol, which can ensure that there is data loop in Ethernet by blocking some interface on the ring. RRPS solves the problems of weak protection to traditional data network and long time to fault recovery, which can theoretically provide 50ms rapid protection features.

5.3 Reliability

Ethernet is widely used because of its simplicity, high efficiency, and low cost. For a long time, the reliability is one major factor that restricts the development of traditional Ethernet in Telecom network. The poor reliability is related to the packet feature of carried services and the mechanism of Ethernet.

Traffics of packet services are transmitted in burst mode, which is difficult for maintaining stable service traffic. As two significant features of Ethernet, the Statistical Time Division Multiplexing (STDM) technology and MAC address learning mechanism improve the utilization rate of channels and devices. However, they also bring uncertainty to service bandwidth and service paths.

To enhance the reliability of Ethernet and to meet the requirements on the Telecom network, you can deploy specified reliability technology in the Ethernet.

5.3.1 Link aggregation

With link aggregation, multiple physical Ethernet interfaces are combined to form a Logical Aggregation Group (LAG). Multiple physical links in one LAG are taken as a logical link to implement load balancing, and they dynamically back up each other. Besides effectively improving reliability on links between devices, link aggregation helps gain higher bandwidth without upgrading hardware.

Generally, link aggregation consists of manual link aggregation, static Link Aggregation Control Protocol (LACP) link aggregation, and dynamic LACP link aggregation.

- Manual link aggregation

Manual link aggregation refers to a process that multiple physical interfaces are aggregated to a logical interface. Links under a logical interface share loads.

- Static LACP link aggregation

Static LACP link aggregation negotiates aggregation parameters and selects the active interface. In this mode, you manually create a LAG and add specified interfaces to the LAG, the LAG sends LACPDUs through LACP to inform the peer of its information, elects the active interface, and implements link aggregation, and so on.

- Dynamic LACP link aggregation

In dynamic LACP link aggregation, the system automatically creates and deletes the LAG and member interfaces through LACP. Interfaces cannot be automatically aggregated into a group unless their basic configurations, speeds, duplex modes, connected devices, and the peer interfaces are identical. In a dynamic LACP aggregation group, the interface in the Active status and with the smallest interface ID is the master interface of the MAG while other interfaces are member interfaces.

The major difference of manual LACP link aggregation from other two modes is that all member interfaces in manual LACP link aggregation mode are in forwarding status and thus balance traffic while there are backup links in other two modes.

The Gazelle S1020i supports manual link aggregation, static LACP link aggregation, and dynamic LACP link aggregation.

5.3.2 Interface backup

In dual uplink networking, Spanning Tree Protocol (STP) is used to block the redundancy link and implements backup. Though STP can meet users' backup requirements, but it fails to meet switching requirements. Though Rapid Spanning Tree Protocol (RSTP) is used, the convergence is second level only. This is not a satisfying performance parameter for high-end Ethernet switch which is applied to the Carrier-grade network core.

Interface backup, targeted for dual uplink networking, implements redundancy backup and quick switching through working and protection links. It ensures performance and simplifies configurations.

Interface backup is implemented by configuring the interface backup group. Each interface backup group contains a primary interface and a backup interface. The link, where the primary interface is, is called a primary link while the link, where the backup interface is, is called the backup interface. Member interfaces in the interface backup group supports physical interfaces and LAGs. However, they do not support Layer 3 interfaces.

In the interface backup group, when an interface is in Up status, the other interface is in Standby statue. At any time, only one interface is in Up status. When the Up interface fails, the Standby interface is switched to the Up status.

By applying interface backup on different VLANs, you can make two interfaces forward packets concurrently in these VLANs.

5.3.3 Link-state tracking

Link-state tracking is used to provide interface linkage scheme for specific application and it can extend range of link backup. By monitoring uplinks and synchronizing downlinks, add uplink and downlink interfaces to a link-state group. Therefore, faults of uplink devices can be informed to the downlink devices to trigger switching. Link-state tracking can be used to prevent traffic loss due to uplink failure.

When all uplink interfaces fail, down link interfaces are in Down status. When at least one uplink interface recovers, the downlink interface recovers to Up status. Therefore, faults of uplink devices can be informed to the downlink devices immediately. Uplink interfaces are not influenced when downlink interfaces fail.

6 Service features

This chapter describes service features of the Gazelle S1020i, including the following sections:

- IPv4
- QoS
- IP routing
- Security
- Multicast
- DHCP

6.1 IPv4

The Gazelle S1020i supports the following IPv4 forwarding features:

- Support basic TCP/IP stack, including ICMP, IGMP, IP, TCP, UDP, and ARP.
- Support FTP Client, TFTP Client, and SSH.
- Support operation and maintenance commands, such as Ping and Traceroute.
- Support DHCP Option, DHCP Client, DHCP Server, DHCP Relay, and DHCP Snooping.

6.2 QoS

When network applications become more and more versatile, users bring forward different Quality of Service (QoS) requirements for them. In this case, the network should distribute and schedule resources for different network applications according to users' requirements. When network is overloaded or congested, QoS can ensure service timeliness, integrity, and efficient operation of the entire network.

6.2.1 ACL

Access Control List (ACL) is a set of ordered rules, which can control the Gazelle S1020i to receive or refuse some data packets.

You need to configure rules on the network to prevent illegal packets from influencing network performance and determine the packets allowed to pass. These rules are defined by ACL.

ACL is a series of rules composed of permit | deny sentences. The rules are described according to source address, destination address, and port ID of data packets. The Gazelle S1020i receives or rejects packets according to rules.

6.2.2 Service model

QoS technical service models:

- Best-effort Service
- Differentiated Services (DiffServ)

Best-effort

Best-effort service is the most basic and simplest service model on the Internet (IPv4 standard) based on storing and forwarding mechanism. In Best-effort service model, the application can send a number of packets at any time without prior approval and notifying the network. For Best-effort service, the network will send packets as possible as it can, but cannot guarantee the delay and reliability.

Best-effort is the default Internet service model now, applying to most network applications, such as FTP and E-mail, which is implemented by First In First Out (FIFO) queue.

DiffServ

DiffServ model is a multi-service model, which can satisfy different QoS requirements. The DiffServ model does not use the RSVP signaling; namely, it does not need the network to reserve resources for it.

DiffServ model does not need to maintain state for each flow. It provides differentiated services according to the QoS classification of each packet. Many different methods can be used for classifying QoS packets, such as IP packet priority (IP precedence), the packet source address or destination address.

Generally, DiffServ is used to provide end-to-end QoS services for a number of important applications, which is implemented through the following techniques:

- Committed Access Rate (CAR): CAR refers to classifying the packets according to the pre-set packets matching rules, such as IP packets priority, the packet source address or destination address. The system continues to send the packets if the flow complies with the rules of token bucket; otherwise, it discards the packets or remarks IP precedence, DSCP, EXP, and so on. CAR can not only control the flows, but also mark and remark the packets.
- Queue technology: the queue technologies of SP, WRR, DRR, SP+WRR, and SP+DRR cache and schedule the congestion packets to implement congestion management.

6.2.3 Priority trust

Priority trust means that the Gazelle S1020i uses priority of packets for classification and performs QoS management.

The Gazelle S1020i supports packet priority trust based on interface, including:

- Differentiated Services Code Point (DSCP) priority
- Class of Service (CoS) priority

6.2.4 Priority mapping

Priority mapping refers when the Gazelle S1020i receives packets, it sends them in queues with different local priorities in accordance with mapping from external priority to local priority, thus scheduling packets in the egress direction of packets.

The Gazelle S1020i supports priority mapping based on DSCP priority or CoS priority.

Table 6-1 lists the default mapping among local priority, DSCP, and CoS.

Table 6-1 Default mapping among local priority, DSCP, and CoS

Local priority	0	1	2	3	4	5	6	7
DSCP	0–7	8–15	16–23	24–31	32–39	40–47	48–55	56–63
CoS	0	1	2	3	4	5	6	7

Local priority refers to a kind of packet priority with internal function assigned by the Gazelle S1020i, namely, the priority corresponding to queue in QoS queue scheduling.

Local priority ranges from 0 to 7. Each interface of the Gazelle S1020i supports 8 queues. Local priority and queue is in one-to-one mapping. The packet can be sent to the assigned queue according to the mapping between local priority and queue, as shown in Table 6-2.

Table 6-2 Mapping between local priority and queue

Local priority	0	1	2	3	4	5	6	7
Queue	1	2	3	4	5	6	7	8

6.2.5 Congestion management

Queue scheduling is necessary when there is intermittent congestion on the network or delay sensitive services require higher QoS service than non-sensitive services.

Queue scheduling adopts different schedule algorithms to transmit packets in queues. The Gazelle S1020i supports Strict Priority (SP), Weight Round Robin (WRR), Deficit Round Robin (DRR), SP+WRR, and SP+DRR algorithm. Each algorithm solves specific network traffic problems, and has different influences on distribution, delay, and jitter of bandwidth resource.

6.2.6 Rate limiting based on interface and VLAN

The Gazelle S1020i supports rate limiting based on traffic policy, based on interface, based on VLAN. Similar to rate limiting based on traffic policy, the Gazelle S1020i discards the exceeding traffic.

6.3 IP routing

The Layer 3 interface refers to the IP interface, the virtual interface based on VLAN. The Layer 3 interface is generally used for network management or routing link connection of multiple devices. Associating a Layer 3 interface to VLAN requires configuring IP address; each Layer 3 interface will correspond to an IP address and associate with at least one VLAN.

Routing is required for communication among different devices in one VLAN, or different VLANs. Routing is to transmit packets through network to destination, which adopts the routing table for packets forwarding.

At present, the Gazelle S1020i supports the default route and static route, rather than dynamic route.

Static route

The static route is a route configured manually. It is available to simple, small and stable network. The disadvantage is that it cannot adapt to network topology changes automatically and needs manual intervention.

Default route

The default route is a special route that is only used when there is no matched item searched from the routing table. It appears as a route to network 0.0.0.0 (with mask 0.0.0.0) in the routing table. You can show default routing configuration through the **show ip route** command. If the destination address of a packet fails to match any item in the routing table, the packet will choose the default route. If the Gazelle S1020i has not configured with the default route and the destination IP address of the packet is not included in the routing table, the Gazelle S1020i will discard the packet and return an ICMP packet to the sender to inform that the destination address or network is unavailable.

6.4 Security

With continuous development of Internet technology, network applications become increasingly widespread. This has become the cornerstone of enterprises' development. How to ensure the data and resource security becomes a key issue. In addition, the device performance is reduced or the device operates improperly in case users access the network in an unconscious but aggressive way.

Security technologies, such as user authentication, can improve network and device security effectively.

6.4.1 Port security MAC

Port security MAC is used for the switching device on the edge of the network user side, which can ensure the security of access data in some interface, control the input packets according to source MAC address.

You can enable port security MAC to limit and distinguish which users can access the network through secure interfaces. Only secure MAC addresses can access the network, unsecure MAC addresses will be dealt with as configured interface access violation mode.

6.4.2 Dynamic ARP inspection

Dynamic ARP inspection is used for ARP protection of unsecure interface and prevents from responding ARP packets which do not meet the requirements, thus preventing ARP spoofing attack on the network.

There are 2 modes for dynamic ARP inspection:

- Static binding mode: configure the binding manually.
- Dynamic binding mode: in cooperation with the DHCP snooping to generate dynamic binding. When DHCP Snooping entry is changed, the dynamic ARP inspection will also update dynamic binding entry synchronously.

The ARP inspection table, which is used for preventing ARP attacks, consists of DHCP snooping entries and statically configured ARP inspection rules, including IP address, MAC address, and VLAN binding information. In addition, the ARP inspection table associates this information with specific interfaces. The dynamic ARP inspection binding table supports the combination of following entries:

- Interface+IP
- Interface+IP+MAC
- Interface+IP+VLAN
- Interface+IP+MAC+VLAN

6.4.3 RADIUS

Remote Authentication Dial In User Service (RADIUS) is a standard communication protocol that authenticates remote access users intensively. RADIUS uses UDP as the transmission protocol (port 1812 and port 1813) which has a good instantaneity; at the same time, RADIUS supports retransmission mechanism and standby server mechanism which has a good reliability.

RADIUS authentication

RADIUS adopts client/server mode, network access device is used as client of RADIUS server. RADIUS server receives user connecting requests and authenticates users, then reply configurations to all clients for providing services. Control user access device and network and improve network security.

Communication between client and RADIUS server is authenticated by sharing key, which will not be transmitted on network. Besides, all user directions need to be encrypted when transmitting between client device and RADIUS server to ensure security.

RADIUS accounting

RADIUS accounting is used to authenticate users through RADIUS. When logging in, a user sends an Accounting-Start packet to the RADIUS accounting server, according to the accounting policy to send an Accounting-Update packet to the RADIUS server. When logging off, the user sends an Accounting-Stop packet to the RADIUS accounting server, and the packet includes user online time. The RADIUS accounting server can record the access time and operations for each user through packets.

6.4.4 TACACS+

Terminal Access Controller Access Control System (TACACS+) is a kind of network access authentication protocol similar to RADIUS. The differences between them are:

- TACACS+ uses TCP port 49, which has higher transmission reliability compared with UPD port used by RADIUS.
- TACACS+ encrypts the holistic of packets except the standard head of TACACS+, and there is a field to show whether the data packets are encrypted in the head of packet. Compared to RADIUS user password encryption, the TACACS+ is much safer.
- TACACS+ authentication function is separated from authorization and accounting functions; it is more flexible in deployment.

In a word, TACACS+ is safer and more reliable than RADIUS. However, as an open protocol, RADIUS is more widely used.

6.4.5 802.1x

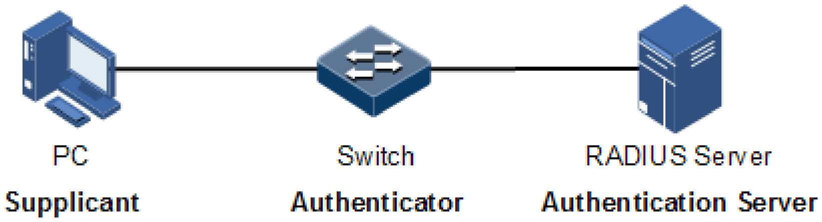
802.1x, based on IEEE 802.1x, is a VLAN-based network access control technology. It is used to solve authentication and security problems for LAN users.

It is used to authenticate and control access devices at the physical later of the network device. It defines a point-to-point connection mode between the device interface and user devices. User devices, connected to the interface, can access resources in the LAN if they are authenticated. Otherwise, they cannot access resources in the LAN through the switch.

802.1x authentication uses C/S mode, including the following three parts:

- Supplicant: a user-side device installed with the 802.1x client software (such as Windows XP 802.1x client), such as a PC
- Authenticator: an access control device supporting 802.1x authentication, such as a switch
- Authentication Server: a device used for authenticating, authorizing, and accounting users. Generally, the RADIUS server is taken as the 802.1x authentication server.

Figure 6-1 802.1x authentication system



6.4.6 Storm control

The Layer 2 network is a broadcast domain. When an interface receives excessive broadcast, unknown multicast, and unknown unicast packets, broadcast storm occurs. If you do not control broadcast packets, broadcast storm occupies much network bandwidth. Broadcast storm can decrease the transmission rate and even cause communication outage, thus affecting normal forwarding of packets.

Restricting broadcast flow generated from network on Layer 2 device can suppress broadcast storm and ensure normal forwarding of normal packets.

Broadcast traffic may exist in following forms:

- Unknown unicast packet: the unicast packet whose MAC destination address is not in the MAC address table, namely, Destination Lookup Failure (DLF) packet. If excessive packets of this type are broadcasted in a period, broadcast storm may occur.
- Unknown multicast packet: the multicast packet whose MAC destination address is not in the MAC address table. If excessive packets of this type are broadcasted in a period, broadcast storm may occur.
- Broadcast packet: the packet whose MAC destination address is a broadcast MAC address. If excessive packets of this type are broadcasted in a period, broadcast storm may occur.

Storm control refers to controlling broadcast packets, unknown multicast packet, and unknown unicast packets that may cause broadcast storm. When the number of broadcast packets received by the Gazelle S1020i reaches the threshold, the Gazelle S1020i will discard received broadcast packets. When storm control is disabled or the number of broadcast packets is smaller than the threshold, the Gazelle S1020i will normally broadcast packets to other interfaces.

6.4.7 IP Source Guard

IP Source Guard uses a binding table to defend against IP Source spoofing and solve IP address embezzlement without identity authentication. IP Source Guard can cooperate with DHCP Snooping to generate dynamic binding. In addition, you can configure static binding manually. DHCP Snooping filters untrusted DHCP packets by establishing and maintaining the DHCP binding database.

IP Source Guard is used to match the packets characteristics, including source IP address, source MAC address, and VLAN tags, and can support the interface to combine with the following characteristics (hereinafter referred to as binding entries):

- Interface+IP
- Interface+IP+MAC
- Interface+IP+VLAN
- Interface+IP+MAC+VLAN

According to the generation mode of binding entry, IP Source Guard can be divided into static binding and dynamic binding:

- Static binding: configure binding information manually and generate binding entry to complete the interface control, which fits for the case where the number of hosts is small or where you need to perform separate binding on a single host.
- Dynamic binding: obtain binding information automatically from DHCP Snooping to complete the interface control, which fits for the case where there are many hosts and you need to adopt DHCP to perform dynamic host configurations. Dynamic binding can effectively prevent IP address conflict and embezzlement.

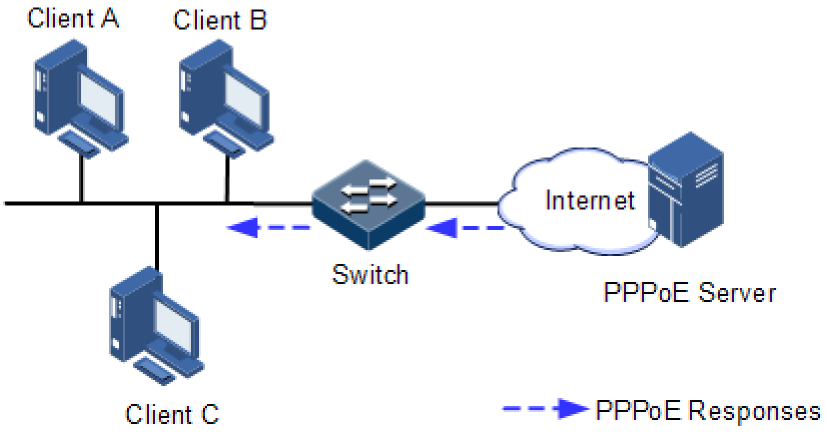
6.4.8 PPPoE+

PPPoE Intermediate Agent (PPPoE+) is used to process authentication packets. PPPoE+ adds user information into the authentication packet to bind account and access device so that the account is not shared and stolen, and the carrier's and users' interests are protected. This provides the server with enough information to identify users, avoiding account sharing and theft and ensuring the network security.

With PPPoE dial-up mode, you can access the network through various interfaces of the device only when one authentication is successfully. However, the server cannot accurately differentiate users just by the authentication information, which contains the user name and password. With PPPoE+, besides the user name and the password, other information, such as the interface ID, is included in the authentication packet for authentication. If the interface ID identified by the authentication server cannot match with the configured one, authentication will fail. This helps prevent illegal users from stealing accounts of other legal users for accessing the network.

PPPoE adopts the Client/Server mode, as shown in Figure 6-2. The Switch is an agent. Clients are connected to the network after PPPoE authentication. To locate the client, the PPPoE server needs more client information.

Figure 6-2 Network connection through PPPoE authentication



6.5 Multicast

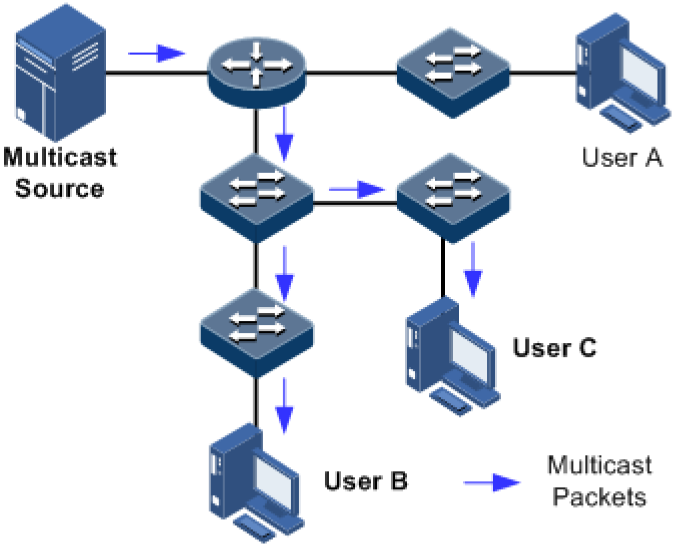
6.5.1 Introduction

With the continuous development of Internet, more and more various interactive data, voice, and video emerge on the network. On the other hand, the emerging e-commerce, online meetings, online auctions, video on demand, remote learning, and other services also rise gradually. These services come up with higher requirements for network bandwidth, information security, and paid feature. Traditional unicast and broadcast cannot meet these requirements well, while multicast has met them timely.

Multicast is a point-to-multipoint data transmission method. The method can effectively solve the single point sending and multipoint receiving problems. During transmission of packets on the network, multicast can save network resources and improve information security.

As shown in Figure 6-3, assume that User B and User C need information, and you can use multicast transmission to combine User B and User C as a receiver set. Then the information source just needs to send one copy of information. Each switch on the network will establish their multicast forwarding tables according to IGMP packets, and finally transmit the information to the actual receiver User B and User C.

Figure 6-3 Multicast transmission networking



In summary, unicast is for sparse network users and broadcast is for dense network users. When the number of users in the network is uncertain, unicast and broadcast will present low efficiency. When the number of users are doubled and redoubled, the multicast mode does not need to increase backbone bandwidth, but sends information to the user in need. These advantages of multicast make multicast a hotspot in study of the current network technology.

Advantages and application of multicast

Compared with unicast and broadcast, multicast has the following advantages:

- Improve efficiency: reduce network traffic, relieve server and CPU load.
- Optimize performance: reduce redundant traffic and guarantee information security.
- Support distributed applications: solve the problem of point-point data transmission.

The multicast technology is used in the following aspects:

- Multimedia and streaming media, such as network television, network radio, and realtime video/audio conferencing
- Training, cooperative operations communications, such as distance education, telemedicine
- Data warehousing and financial applications (stock)
- Any other point-to-multipoint applications

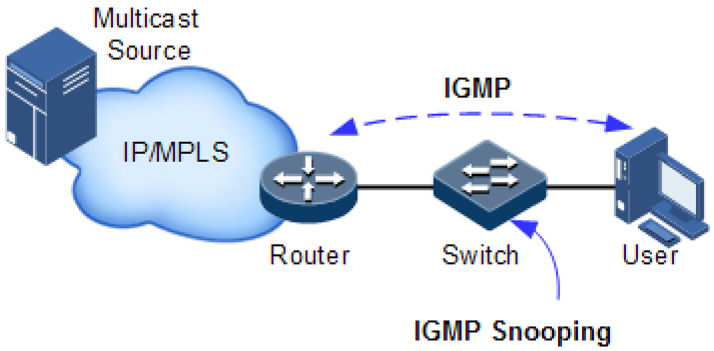
Basis of multicast protocol

To implement complete set of multicast services, you need to deploy a variety of multicast protocols in various positions of network and make them cooperate with each other.

Typically, IP multicast working at network layer is called Layer 3 multicast, so the corresponding multicast protocol is called Layer 3 multicast protocol, including Internet Group Management Protocol (IGMP). IP multicast working at data link layer is called Layer 2 multicast, so the corresponding multicast protocol is called Layer 2 multicast protocol, including Internet Group Management Protocol (IGMP) Snooping.

Figure 6-4 shows the operating of IGMP and Layer 2 multicast features

Figure 6-4 Operating of IGMP and Layer 2 multicast features



IGMP, a protocol in TCP/IP protocol suite, is responsible for managing IPv4 multicast members. IGMP runs between the multicast router and host, defines the establishment and maintenance mechanism of multicast group membership between hosts and the multicast router. IGMP is not involved in transmission and maintenance of group membership between multicast routers, which is completed by the multicast routing protocol.

IGMP manages group members through interaction of IGMP packets between the host and multicast router. IGMP packets are encapsulated in IP packets, including Query packets, Report packets, and Leave packets. Basic functions of IGMP are as below:

- The host sends Report packets to join the multicast group, sends Leave packets to leave the multicast group, and automatically decides which multicast group packets to receive.
- The multicast router sends Query packets periodically, and receives Report packets and Leave packets from hosts to understand the multicast group members in connected network segment. The multicast data will be forwarded to the network segment if there are multicast group members, and not forward if there are no multicast group members.

Up to now, IGMP has three versions: IGMPv1, IGMPv2, and IGMPv3. The newer version is fully compatible with the elder version. Currently the most widely used version is IGMPv2, while the Leave packet does not IGMPv1.

Layer 2 multicast runs on Layer 2 devices between the host and multicast router.

Layer 2 multicast manages and controls multicast groups by monitoring and analyzing IGMP packets exchanged between hosts and multicast routers to implement forwarding multicast data at Layer 2 and suppress multicast data diffusion at Layer 2.

Supported multicast features

The Gazelle S1020i supports the following multicast features:

- Basic functions of IGMP
- IGMP Snooping

Note

The Gazelle S1020i supports both IGMPv1 and IGMPv2.

6.5.2 Basic functions of IGMP

Basic functions of IGMP are as below:

- Assign the multicast router interface.

- Enable immediate leaving.
- Configure multicast forwarding entries and the aging time of router interfaces.
- Enable IGMP ring network forwarding.

Basic functions of IGMP provide Layer 2 multicast common features, which must be used on the Gazelle S1020i enabled with IGMP Snooping.

After IGMP ring network forwarding is enabled, multicast services can be backed up and protected on the ring network to enhance stability and avoid faults of multicast services caused by faults of some links.

The types of ring networks suitable for IGMP ring network forwarding are RRPS, STP/RSTP/MSTP, and G.8032.

6.5.3 IGMP Snooping

IGMP Snooping is a multicast constraining mechanism running on Layer 2 devices, used for managing and controlling multicast groups, and implementing Layer 2 multicast.

IGMP Snooping allows the Gazelle S1020i to monitor IGMP session between the host and multicast router. When monitoring a group of IGMP Report from host, the Gazelle S1020i will add host-related interface to the forwarding entry of this group. Similarly, when a forwarding entry reaches the aging time, the Gazelle S1020i will delete host-related interface from forwarding entry.

IGMP Snooping forwards multicast data through Layer 2 multicast forwarding entry. When receiving multicast data, the Gazelle S1020i will forward them directly according to the corresponding receiving interface of the multicast forwarding entry, instead of flooding them to all interfaces, to save bandwidth of the Gazelle S1020i effectively.

IGMP Snooping establishes a Layer 2 multicast forwarding table, of which entries can be learnt dynamically or configured manually.

Note

Currently, the Gazelle S1020i supports up to 1024 Layer 2 multicast entries.

6.6 DHCP

Dynamic Host Configuration Protocol (DHCP) refers to assigning IP address configurations dynamically for users in TCP/IP network. It is based on Bootstrap Protocol (BOOTP), and automatically adds the specified available network address, network address re-use, and other extended configuration options over BOOTP protocol.

With enlargement of network scale and development of network complexity, the number of PCs on a network usually exceeds the maximum number of distributable IP addresses. Meanwhile, the widely use of notebooks and wireless networks lead to frequent change of PC positions and also related IP addresses must be updated frequently. As a result, network configurations become more and more complex. DHCP is developed to solve these problems.

DHCP adopts client/server communication mode. A client applies configuration to the server (including IP address, Subnet mask, and default gateway), and the server replies with IP address for the client and other related configurations to implement dynamic configurations of IP address, and so on.

DHCP technology ensures rational allocation, avoid waste and improve the utilization rate of IP addresses in the entire network.

6.6.1 DHCP Option

DHCP transmits control information and network configuration parameters through Option field in packet to implement address dynamical distribution to provide abundant network configurations for client. DHCP protocol has 255 kinds of options, the final option is 255. Table 6-3 lists frequently used DHCP options.

Table 6-3 Common DHCP options

Options	Description
3	Router option, to assign gateway for DHCP client
6	DNS server option, to assign DNS server address distributed by the DHCP client
18	IPv6-based DHCP client flag option, to assign interface information for DHCP client
51	IP address lease option
53	DHCP packet type, to mark type for DHCP packets
55	Request parameter list option. Client uses this optical to indicate network configuration parameters need to obtain from server. The content of this option is values corresponding to client requested parameters.
61	DHCP client flag option, to assign device information for DHCP clients.
66	TFTP server name, to assign domain name for TFTP server distributed by DHCP clients.
67	Startup file name, to assign startup file name distributed by DHCP clients.
82	DHCP client flag option, user-defined, mainly used to mark position of DHCP client, including Circuit ID and remote ID.
150	TFTP server address, to assign TFTP server address distributed by DHCP clients.
184	DHCP reserved option, at present Option184 is used to carry information required by voice calling. Through Option184 it can distribute IP address for DHCP client with voice function and meanwhile provide voice calling related information.
255	Complete option

Options 18, 61, and 82 in DHCP Option are relay information options in DHCP packets. When request packets from DHCP clients arrive the DHCP server, DHCP Relay or DHCP Snooping added Option field into request packets if request packets pass the DHCP relay device or DHCP snooping device is required.

Options 18, 61, and 82 implement record DHCP client information on the DHCP server. By cooperating with other software, it can implement functions such as limit on IP address distribution and accounting. For example, by cooperating with IP Source Guard, Options 18, 61, 82 can defend deceiving through IP address+MAC address.

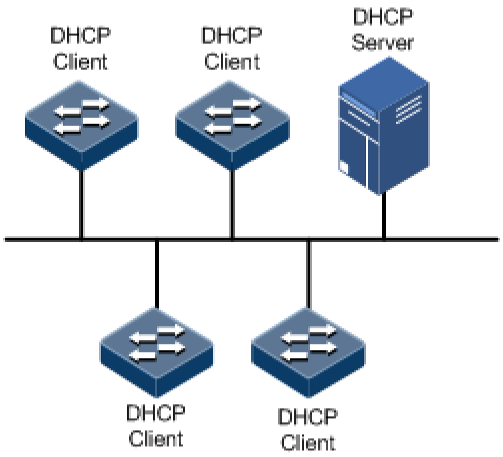
Option 82 can include at most 255 sub-options. If defined field Option 82, at least one sub-option must be defined. The Gazelle S1020i supports the following two sub-options:

- Sub-Option 1 (Circuit ID): it contains interface number, interface VLAN, and the additional information about DHCP client request packet.
- Sub-Option 2 (Remote ID): it contains interface MAC address (DHCP Relay), or bridge MAC address (DHCP snooping device) of the Gazelle S1020i, or user-defined string of DHCP client request packets.

6.6.2 DHCP Client

The Gazelle S1020i can be used as a DHCP client to obtain IP address from the DHCP server for future management, as shown in Figure 6-5.

Figure 6-5 DHCP Client networking



6.6.3 DHCP Server

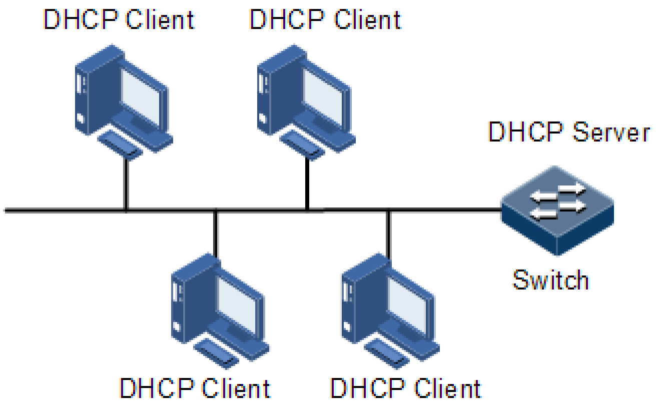
DHCP works in client/server mode, so a specified server assigns network addresses and transmits configured parameters to hosts on the network. The specified server is called the DHCP server.

Under normal circumstances, use the DHCP server to assign IP addresses in following situations:

- The network scale is large. It requires much workload for manual configurations, and is difficult to manage the entire network intensively.
- The number of hosts on the network is greater than the number of IP addresses, which make it unable to assign a fixed IP address for each host, and restrict the number of users connected to network simultaneously.
- A large number of users must obtain their own IP address dynamically through DHCP service.
- Only the minority of hosts on the network need fixed IP addresses, most of hosts have no requirement for fixed IP address.

The Gazelle S1020i can work as the DHCP server to assign dynamic IP addresses for clients, as shown in Figure 6-6.

Figure 6-6 DHCP Server networking



After a DHCP client obtains the IP address from the DHCP server, it cannot use the IP address permanently but in a fixed period, which is called the leased period. You can specify the duration of the leased period.

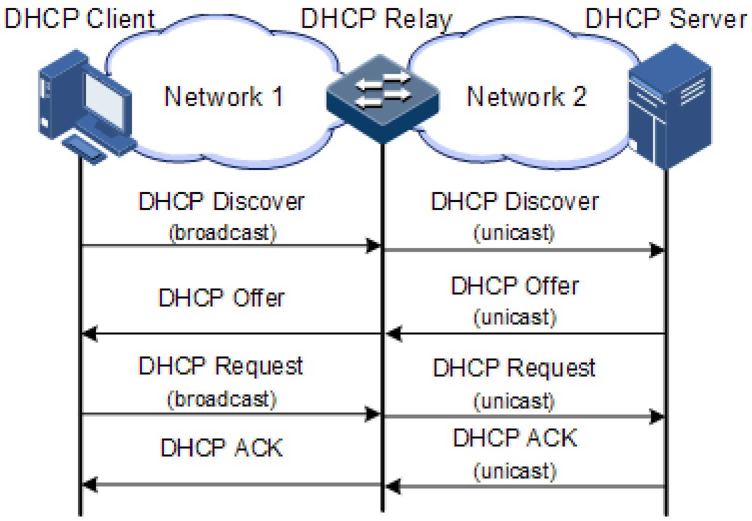
6.6.4 DHCP Relay

At the beginning, DHCP requires the DHCP server and clients to be in the same network segment, instead of different network segments. As a result, a DHCP server is configured for all network segments for dynamic host configuration, which is not economic.

DHCP Relay is introduced to solve this problem. It can provide relay service between DHCP clients and DHCP server that are in different network segments. It relays packets across network segments to the DHCP server or clients.

Figure 6-7 shows principles of DHCP Relay.

Figure 6-7 Principles of DHCP Relay



Step 1 The DHCP client sends a request packet to the DHCP server.

Step 2 After receiving the packet, the DHCP relay device process the packet in a certain way, and then sends it to the DHCP server on the specified network segment.

Step 3 The DHCP server sends acknowledgement packet to the DHCP client through the DHCP relay device according to the information contained in the request packet. In this way, the configuration of the DHCP client is dynamically configured.

6.6.5 DHCP Snooping

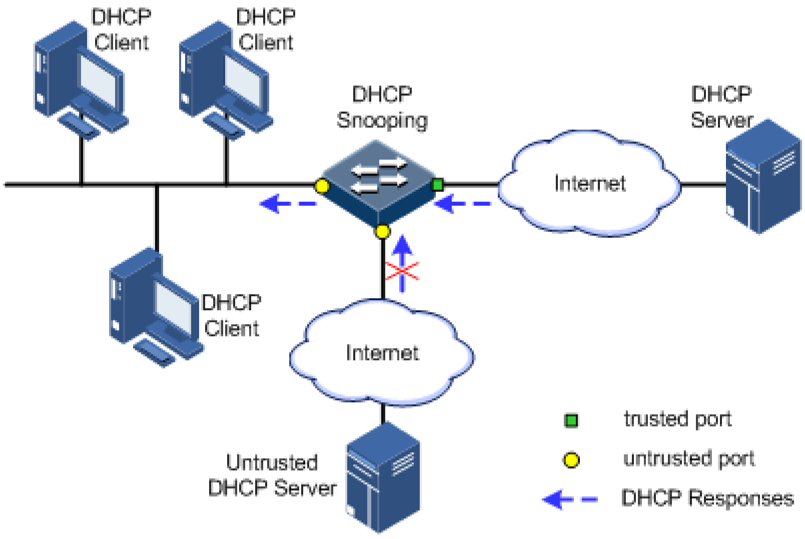
Introduction

DHCP Snooping is a security feature of DHCP with the following functions:

- Configure the DHCP client to obtain the IP address from a legal DHCP server.

If a false DHCP server exists on the network, the DHCP client may obtain incorrect IP address and network configuration parameters, but cannot communicate normally. As shown in Figure 6-8, to make DHCP client obtain the IP address from a legal DHCP server, the DHCP Snooping security system permits to configure an interface as the trusted interface or untrusted interface: the trusted interface forwards DHCP packets normally; the untrusted interface discards the reply packets from the DHCP server.

Figure 6-8 DHCP Snooping networking



- Record mapping between DHCP client IP address and MAC address.

DHCP Snooping records entries through monitor request and reply packets received by the trusted interface, including the client MAC address, obtained IP address, DHCP client connected interface, VLAN of the interface, and so on. Then implement following by the record information:

  - ARP detection: judge legality of a user that sends ARP packet and avoid ARP attack from illegal users.
  - IP Source Guard: filter packets forwarded by interfaces by dynamically getting DHCP Snooping entries to avoid illegal packets to pass the interface.
  - VLAN mapping: modify mapped VLAN of packets sent to users to original VLAN by searching IP address, MAC address, and original VLAN information in DHCP Snooping entry corresponding to the mapped VLAN.

DHCP Snooping to support Option

The Option field in DHCP packet records position information of DHCP clients. The Administrator can use this Option filed to locate DHCP clients and control client security and accounting.

If the Gazelle S1020i configures DHCP Snooping to support Option function:

- When the Gazelle S1020i receives a DHCP request packet, it processes packets according to Option field included or not, filling mode, and processing policy configured by user, then forwards the processed packet to the DHCP server.
- When the Gazelle S1020i receives a DHCP reply packet, it deletes the field and forward to DHCP client if the packet does not contain Option field; it then forwards packets directly if the packet does not contain Option field.

7 Management and maintenance

This chapter describes how to manage and maintain the Gazelle S1020i, including the following sections:

- Management and operation modes
- Maintenance and test modes
- NView NNM

7.1 Management and operation modes

You can access the Gazelle S1020i through the Console interface, Telnet, or SSH, and then manage and maintain the Gazelle S1020i in the following modes:

- Command Line Interface (CLI)
- NView NNM system
- Web

7.1.1 Console interface management

Console interface management refers to configuring and managing the Gazelle S1020i through its RS45 control interface a terminal or a PC that runs the terminal emulation program. This is the local management mode and does not rely on the service network. Though the service network is operating improperly, you can configure and manage the Gazelle S1020i through the Console interface.

7.1.2 Telnet management

The Telnet protocol, one of the TCP/IP protocol stack, is a standard protocol for remote login via the Internet. By adopting the Telnet protocol, a local PC can be a terminal for the remote host system. You can log in to the Gazelle S1020i through the PC which runs the Telnet program. You can type commands through Telnet, and these commands will be executed on the Gazelle S1020i as you directly execute commands on the Gazelle S1020i.

7.1.3 Web management

The Gazelle S1020i can be managed through Web. You can access, manage, and maintain it through a Web browser. By adopting a Graphic User Interface (GUI), the Web management mode is easier than the CLI.

For details, see *Gazelle S1020i (A) Configuration Guide (Web)*.

7.1.4 SSH management

SSH is a protocol that provides secure remote login and other secure network services on unsecure networks. When you remotely log in to the Gazelle S1020i on an unsecure network, SSH automatically encrypts data every time the device sends data. When data reaches the destination, SSH automatically decrypts data. In this way, SSH prevents the Gazelle S1020i from attacks, such as plain text interception.

SSH works between TCP/IP and other protocols in the application layer. It ensures secure data communication and provides the following services:

- Authenticate users and servers to ensure that data can be sent to the correct clients and server.
- Encrypt data to prevent it from being stolen.
- Maintain the data integrity to prevent data being altered during transmission.

SSH can replace the Telnet for managing remote devices or provide secure paths for protocols such as FTP.

7.1.5 SNMP mode

Simple Network Management Protocol (SNMP) is designed by the Internet Engineering Task Force (IETF) to solve problems in managing network devices connected to the Internet. Through SNMP, a network management system that can manage all network devices that support SNMP, including monitoring network status, modifying configurations of a network device, and receiving network alarms. SNMP is the most widely used network management protocol in TCP/IP networks.

Till now, SNMP has three versions: v1, v2c, and v3, described as below.

- SNMPv1 uses community name authentication mechanism. The community name, a string defined by an agent, acts like a secret. The network management system can access the agent only by specifying its community name correctly. If the community name carried in a SNMP packet is not accepted by the Gazelle S1020i, the packet will be dropped.
- Compatible with SNMPv1, SNMPv2c also uses community name authentication mechanism. SNMPv2c supports more operation types, data types, and errored codes, and thus better identifying errors.
- SNMPv3 uses User-based Security Model (USM) authentication mechanism. You can configure whether USM authentication is enabled and whether encryption is enabled to provide higher security. USM authentication mechanism allows authenticated senders and prevents unauthenticated senders. Encryption is to encrypt packets transmitted between the network management system and agents, thus preventing interception.

The Gazelle S1020i supports v1, v2c, and v3 of SNMP.

7.2 Maintenance and test modes

The Gazelle S1020i caters to users' requirements on operation and maintenance in aspects of hardware design and function configuration, thus providing users with powerful maintenance performance.

The Gazelle S1020i supports diagnosing and debugging its software and hardware through the following modes.

7.2.1 Ping

Packet Internet Grope (Ping) is the most widely used command for fault diagnosis and removal. It is usually used to detect whether two hosts are connected or not. Ping is achieved with ICMP echo packets. If an Echo Reply packet is sent back to the source address during a valid period after the Echo Request packet is sent to the destination address, it indicates the route between source and destination address is reachable.

7.2.2 Traceroute

Traceroute is used to discover the real route taking by the packet to be transmitted to the destination. Although the Ping feature can test the connectivity, it cannot record all network devices on the route limited by the IP header. Traceroute can be used to test routing information from the source host to the destination host.

7.2.3 Environment monitoring

Environmental monitoring is to monitor key parameters of the device, including, temperature and voltage, and so on. When those parameters are abnormal, environmental monitoring can record the hardware environment monitoring alarm table, generate syslog, or send Traps. Then, you can take corresponding measurements to prevent failures.

7.2.4 RMON management

Remote Network Monitoring (RMON) is a standard developed by the Internet Engineering Task Force (IETF). RMON is used to monitor network data through different agents and NMS. RMON is an extension of SNMP, but ROMN is more active and efficient for monitoring remote devices. The administrator can quickly trace faults generated on the network, network segments or devices.

At present, RMON implements four function groups: statistic group, historical group, alarm group, and event group.

- Statistic group: gather statistics on one interface, including the number of received packets, the number of sent packets, and the size and distribution of packets.
- Historical group: similar to statistic group, gather statistics during a specified detection period.
- Alarm group: monitor a specified MIB object within a specified interval, configure the upper and lower threshold, and trigger an event if the monitored object reaches the threshold.
- Event group: work together with the alarm group, record event information when an alarm triggers an event, such as sending Trap information, and recording the information to the log.

The differences between RMON and SNMP are as below:

- RMON is derived from SNMP. It sends Trap messages to the device to inform the device of the abnormal alarm variable. However, all monitored objects, trigger conditions, and contents reported to the NMS are different from those of RMON.
- RMON stipulates that the managed device should initiatively send Trap messages to the NMS when it reaches the alarm threshold. The NMS does not need to query statistics constantly, thus saving traffic.

You can configure the RMON statistics group, historical group, alarm group, and event group in this feature.

7.2.5 Optical module DDM

The Small Form-factor Pluggable (SFP) optical module and 10 Gigabit Small Form Factor Pluggable (SFP+) are optical transceivers. Optical module DDM provides a performance monitoring method for the Gazelle S1020i. By analyzing data provided by the SFP, the network administrator can predict the life of the SFP module, isolate system fault, and verify module compatibility during on-site installation.

Each SFP provides five performance parameters:

- Transceiver temperature
- Internal voltage
- Tx bias current
- Tx optical power
- Rx optical power

With this function, you can globally configure optical modules on the Gazelle S1020i, view and export the following tables:

- Optical module information table
- Optical module detection table
- Optical module current period detection table
- Optical module period detection table.

7.2.6 Watchdog

By configuring Watchdog, you can prevent the system program from endless loops due to uncertain fault and thus improve system stability.

7.2.7 Port mirroring

Port mirroring refers to mirroring all packets of the source port to the monitor port without affecting packet forwarding. You can use this function to monitor the receiving and sending status of one or more ports and analyze the network situation.

The Gazelle S1020i supports port mirroring based on ingress port, egress port, or both. When port mirroring is enabled, packets on the ingress/egress mirroring port will be mirrored to the monitor port which analyzes and monitors packets. The monitor port and mirroring port cannot be the same one.

7.3 NView NNM

7.3.1 Intruction

"Comprehensive Access, Overall Network Management" is a vision that Raisecom has been in pursuit of. The NView NNM system is developed to meet overall and efficient OAM requirements. It is of complete functions, friendly User Interface (UI), and easy operations, and can meet requirements by service activation and daily maintenance.

The NView NNM system, based on SNMP, can perform centralized configurations and fault detection over all manageable devices of Raisecom. It has the following functions:

- Topology management: display network topology graphically, organize and manages nodes of various types and links between these nodes, and support automatic or manual planning of network functions.
- Alarm management: collect, classify, display, and manage all alarms reported by managed devices. It supports query, sorting, filtering, statistics, forwarding, and voice prompt.
- Performance management: enable you to view realtime or historical performance metrics, such as cards, interfaces, traffic, and bandwidth utilization.
- Inventory management: manage physical inventory, such as devices, chassis, cards, and interfaces.
- Customer management: manage information about all connected users, and allow the mapping between customer information and device/card/interface. This function helps quickly locate affected customers.
- Security management: support user account and password rules according to security management features in network management; control authorized access from a client according to the *Client Access Control List*; provide the Invalid Login Verification function, which will lock a user if the times of typing incorrect user name and password exceeds the configured number; provide security control policies based on level, authority, and domain; provide detailed system/device operation logs to facilitate you to control operation authorities.
- Service management: manages predefined system services through the application service management framework, such as Trap receiving service, alarm storm prevention service, and alarm forwarding service.
- Data center: enable you to manage devices and cards, such as backing up, restoring, rolling back, and activating; enable you to manage upgradable files, backup files, operations, and logs for backup. The backup operation is easy, simple and with high security.
- Data downloading: download logs, historical alarms, and performance data from database as viewable files and then delete these data from database. This ensures efficient operation of database in the NView NNM system.

7.3.2 Features

The NView NNM system has the following features:

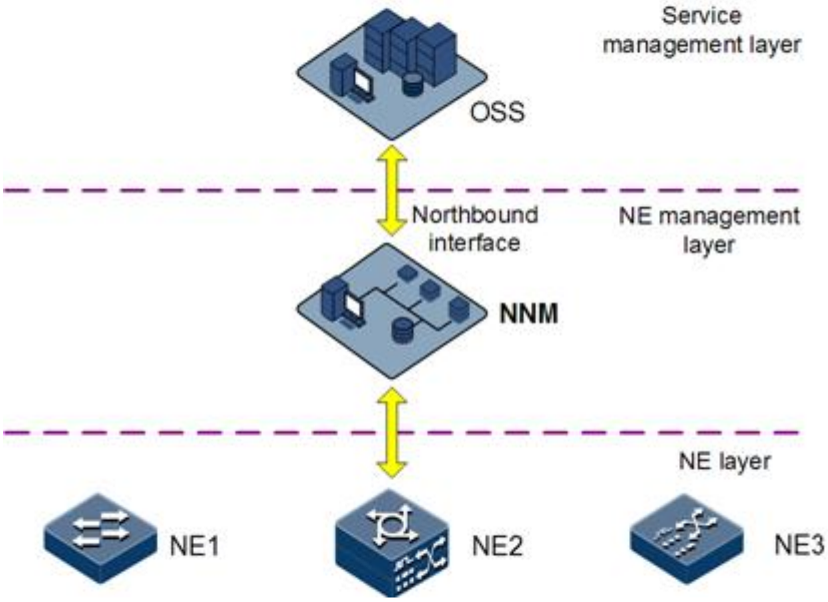
- Work as the uniform platform for all Raisecom manageable devices.
- Uniformly manage data network and transport network.
- Provide strong NE-level management and subnet-level management.

- Provide northbound interfaces for integration with the OAM system, such as COBRA, SNMP, JDBC, and SOCKET interfaces.
- Communicate with NE-level devices through SNMP in southbound. With a modular design, it supports flexible deployment according to actual situation.

The NView NNM system can be interconnected to the Operation Support System (OOS). It implements OAM functions between the OSS and NEs through the northbound interface, such as service activation, alarm reporting, alarm synchronization, fault diagnosis, and periodical inspection.

Figure 7-1 shows the orientation of the NView NNM system.

Figure 7-1 Orientation of the NView NNM system



8 Hardware installation

The Gazelle S1020i is installed with all necessary software before delivery so that it can be powered on immediately for use after hardware installation is complete. You can install and upgrade its system software through CLI or the NView NNM system.

This chapter describes easy installation of software and hardware of the Gazelle S1020i, which shortens the installation time and makes network establishment faster for providing services, including the following sections:

- Hardware installation
- Software installation

8.1 Hardware installation

The Gazelle S1020i supports the following three installation modes:

- Guide-rail installation
- Wall-mount installation
- 19-inch rack-shelf installation

Note

The guide-rail installation is the standard installation mode. When the Gazelle S1020i is taken out of the packing box, it is installed with a 35-mm DIN guide rail.

The installation of the Gazelle S1020i in a guide rail, on a wall, or on the shelf of a rack is simple. Then, connect the power cable, fiber, and Ethernet cable to it.

For detailed installation process, see *Gazelle S1020i (A) Quick Installation Guide*.

8.2 Software installation

8.2.1 Installing and upgrading BootROM

The BOOTROM file is a Bootstrap program for initializing the device. It is installed before delivery. After powering on the Gazelle S1020i, run the BootROM file first, press **Ctrl+B** to enter BootROM menu when the prompt "Press CTRL+B to stop auto-boot…" appears. Then follow the instructions.

8.2.2 Installing and upgrading system software

The files (system software and configuration file) needed in the operation of the Gazelle S1020i are saved in the memory. By default, the Gazelle S1020i prompts you to confirm the operations which may result in data loss, such as deleting files and overriding files.

You can upload system software and configuration files of the Gazelle S1020i to the server through TFTP or FTP by executing the **upload** command, or download them to the Gazelle S1020i by executing the **download** command.

For installation and upgrade of the system software, see *Gazelle S1020i (A) Configuration Guide (CLI)*.

8.2.3 Installing and upgrading NView NNM software

The installation of NView NNM software follows the guidance mode. The installation program guides you to install NView NNM software step by step easily.

For installation and detailed operation of the NView NNM system, see related NView NNM manuals.

9 Appendix

This chapter lists compliant standards and protocols, LEDs, terms, acronyms, and abbreviations involved in this document, including and following sections:

- Compliant standards and protocols
- Lookup table for LEDs
- Terms
- Acronym and abbreviations

9.1 Compliant standards and protocols

- IEEE 802.1Q VLAN
- IEEE 802.3ad Link Aggregation
- IEEE 802.1ad QinQ
- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1w RSTP
- IEEE 802.1s MSTP
- IEEE 802.1x Security
- IEEE 802.1p CoS Prioritization
- IEEE 802.3x Flow Control
- IEEE 802.1ab LLDP
- IEC 62351 Power systems management and associated information exchange - Data and communications security
- IEC 61588 Precision clock synchronization protocol for networked measurement and control systems
- IEEE 802.3 Information Technology
- IEEE1613 Environmental and Testing Requirements for Communications Networking Devices Installed in Electric Power Substations

9.2 Lookup table for LEDs

There are 2 power LEDs on the panel of the Gazelle S1020i DC power model. The Gazelle S1020i AC power model supports single power input and there is one power LED on the panel. Each RJ45 electrical interface or SFP optical interface has a LNK/ACT LED and a SPEED LED, as listed in Table 9-1.

Table 9-1 LEDs

Print	LEDs	Color	Description
SYS	System LED	Green	• Green: the system is working improperly. • Blinking green: the system is working properly. • Off: the system is working improperly or powered off.
ALM	Alarm LED	Red	• Red: alarms are generated. • Off: no alarms are generated.
PWR1	Power supply 1 status LED on the DC power model	Green	• Green: power supply 1 is normal. • Off: power supply 1 is abnormal or off.
PWR2	Power supply 2 status LED on the DC power model	Green	• Green: power supply 2 is normal. • Off: power supply 2 is abnormal or off.
PWR	Power supply status LED on the AC power model	Green	• Green: the power supply is normal. • Off: the power supply is abnormal or off.
LNK/ACT	Optical interface status LED	Green	• Green: the optical interface is in Link Up status. • Blinking green: the optical interface is receiving or sending data. • Off: the optical interface is in Link Up status.
SPEED	Optical interface rate LED	Green	• Green: the optical interface is working at 1000 Mbit/s. • Off: the optical interface is working at 100 Mbit/s or faulty.
LNK/ACT	Electrical interface status LED	Green	• Green: the electrical interface is in Link Up status. • Blinking green: the electrical l interface is receiving or sending data. • Off: the electrical interface is in Link Up status.

9.3 Terms

A

Access Control List (ACL)

A series of ordered rules composed of permit | deny sentences. These rules are based on the source MAC address, destination MAC address, source IP address, destination IP address, interface ID, and so on. The device decides to receive or refuse the packets based on these rules.

Automatic Laser Shutdown (ALS)

The technology that is used for automatically shutting down the laser to avoid the maintenance and operation risks when the fiber is pulled out or the output power is over great.

Auto-negotiation

The interface automatically chooses the rate and duplex mode according to the result of negotiation. The auto-negotiation process is: the interface adapts its rate and duplex mode to the highest performance according to the peer interface; namely, both ends of the link adopt the highest rate and duplex mode they both support after auto-negotiation.

Automatic Protection Switching (APS)

APS is used to monitor transport lines in real time and automatically analyze alarms to discover faults. When a critical fault occurs, through APS, services on the working line can be automatically switched to the protection line, thus the communication is recovered in a short period.

B

Bracket

A component installed on both sides of the chassis, used for install the chassis to the rack.

C

Challenge Handshake Authentication Protocol (CHAP)

CHAP is a widely supported authentication method in which a representation of the user's password, rather than the password itself, is sent during the authentication process. With CHAP, the remote access server sends a challenge to the remote access client. The remote access client uses a hash algorithm (also known as a hash function) to compute a Message Digest-5 (MD5) hash result based on the challenge and a hash result computed from the user's password. The remote access client sends the MD5 hash result to the remote access server. The remote access server, which also has access to the hash result of the user's password, performs the same calculation using the hash algorithm and compares the result to the one sent by the client. If the results match, the credentials of the remote access client are considered authentic. A hash algorithm provides one-way encryption, which means that calculating the hash result for a data block is easy, but determining the original data block from the hash result is mathematically infeasible.

D

Dynamic ARP Inspection (DAI)

A security feature that can be used to verify the ARP data packets in the network. With DAI, the administrator can intercept, record, and discard ARP packets with invalid MAC address/IP address to prevent common ARP attacks.

Dynamic Host Configuration Protocol (DHCP)

A technology used for assigning IP address dynamically. It can automatically assign IP addresses for all clients in the network to reduce workload of the administrator. In addition, it can implement centralized management of IP addresses.

E

Ethernet in the First Mile (EFM)

Complying with IEEE 802.3ah protocol, EFM is a link-level Ethernet OAM technology. It provides link connectivity detection, link fault monitoring, remote fault notification, and other features for a link between two directly-connected devices. EFM is mainly used for the Ethernet link on edges of the network accessed by users.

Ethernet Ring Protection Switching (ERPS)

It is an APS protocol based on ITU-T G.8032 standard, which is a link-layer protocol specially used for the Ethernet ring. In normal conditions, it can avoid broadcast storm caused by the data loop on the Ethernet ring. When the link or device on the Ethernet ring fails, services can be quickly switched to the backup line to enable services to be recovered in time.

F

Full duplex

In a communication link, both parties can receive and send data concurrently.

G

GFP encapsulation

Generic Framing Procedure (GFP) is a generic mapping technology. It can group variable-length or fixed-length data for unified adaption, making data services transmitted through multiple high-speed physical transmission channels.

Ground cable

The cable to connect the device to ground, usually a yellow/green coaxial cable. Connecting the grounding cable properly is an important guarantee to lightning protection, anti-electric shock, and anti-interference.

H

Half duplex

In a communication link, both parties can receive or send data at a time.

I

Institute of Electrical and Electronics Engineers (IEEE)

A professional society serving electrical engineers through its publications, conferences, and standards development activities. The body responsible for the Ethernet 802.3 and wireless LAN 802.11 specifications.

Internet Assigned Numbers Authority (IANA)

The organization operated under the IAB. IANA delegates authority for IP address-space allocation and domain-name assignment to the NIC and other organizations. IANA also maintains a database of assigned protocol identifiers used in the TCP/IP suite, including autonomous system numbers.

Internet Engineering Task Force (IETF)

A worldwide organization of individuals interested in networking and the Internet. Managed by the Internet Engineering Steering Group (IESG), the IETF is charged with studying technical problems facing the Internet and proposing solutions to the Internet Architecture Board (IAB). The work of the IETF is carried out by various working groups that concentrate on specific topics, such as routing and security. The IETF is the publisher of the specifications that led to the TCP/IP protocol standard.

L

Label

Symbols for cable, chassis, and warnings

Link Aggregation

With link aggregation, multiple physical Ethernet interfaces are combined to form a logical aggregation group. Multiple physical links in one aggregation group are taken as a logical link. Link aggregation helps share traffic among member interfaces in an aggregation group. In addition to effectively improving the reliability on links between devices, link aggregation can help gain greater bandwidth without upgrading hardware.

Link Aggregation Control Protocol (LACP)

A protocol used for realizing link dynamic aggregation. The LACPDU is used to exchange information with the peer device.

Link-state tracking

Link-state tracking is used to provide interface linkage scheme for specific application and it can extend range of link backup. By monitoring uplinks and synchronizing downlinks, add uplink and downlink interfaces to a link-state group. Therefore, the fault of the upstream device can be informed to the downstream device to trigger switching. Link-state tracking can be used to prevent traffic loss due to failure in sensing the uplink fault by the downstream device.

M

Multi-mode Fiber (MMF)

In this fiber, multi-mode optical signals are transmitted.

N

Network Time Protocol (NTP)

A time synchronization protocol defined by RFC1305. It is used to synchronize time between distributed time server and clients. NTP is used to perform clock synchronization on all devices that have clocks in the network. Therefore, the devices can provide different applications based on a unified time. In addition, NTP can ensure a very high accuracy with an error of 10ms or so.

O

Open Shortest Path First (OSPF)

An internal gateway dynamic routing protocol, which is used to decide the route in an Autonomous System (AS)

Optical Distribution Frame (ODF)

A distribution connection device between the fiber and a communication device. It is an important part of the optical transmission system. It is mainly used for fiber splicing, optical connector installation, fiber adjustment, additional pigtail storage, and fiber protection.

P

Password Authentication Protocol (PAP)

PAP is an authentication protocol that uses a password in Point-to-Point Protocol (PPP). It is a twice handshake protocol and transmits unencrypted user names and passwords over the network. Therefore, it is considered unsecure.

Point-to-point Protocol over Ethernet (PPPoE)

PPPoE is a network protocol for encapsulating PPP frames in Ethernet frames. With PPPoE, the remote access device can control and account each access user.

Private VLAN (PVLAN)

PVLAN adopts Layer 2 isolation technology. Only the upper VLAN is visible globally. The lower VLANs are isolated from each other. If you partition each interface of the switch or IP DSLAM device into a lower VLAN, all interfaces are isolated from each other.

Q

QinQ

802.1Q in 802.1Q (QinQ), also called Stacked VLAN or Double VLAN, is extended from 802.1Q and defined by IEEE 802.1ad recommendation. This VLAN feature allows the equipment to add a VLAN tag to a tagged packet. The implementation of QinQ is to add a public VLAN tag to a packet with a private VLAN tag, making the packet encapsulated with two layers of VLAN tags. The packet is forwarded over the ISP's backbone network based on the public VLAN tag and the private VLAN tag is transmitted as the data part of the packet. In this way, the QinQ feature enables the transmission of the private VLANs to the peer end transparently. There are two QinQ types: basic QinQ and selective QinQ.

Quality of Service (QoS)

A network security mechanism, used to solve problems of network delay and congestion. When the network is overloaded or congested, QoS can ensure that packets of important services are not delayed or discarded and the network runs high efficiently. Depending on the specific system and service, it may relate to jitter, delay, packet loss ratio, bit error ratio, and signal-to-noise ratio.

R

Rapid Spanning Tree Protocol (RSTP)

Evolution of the Spanning Tree Protocol (STP), which provides improvements in the speed of convergence for bridged networks

Remote Authentication Dial In User Service (RADIUS)

RADIUS refers to a protocol used to authenticate and account users in the network. RADIUS works in client/server mode. The RADIUS server is responsible for receiving users' connection requests, authenticating users, and replying configurations required by all clients to provide services for users.

S

Simple Network Management Protocol (SNMP)

A network management protocol defined by Internet Engineering Task Force (IETF) used to manage devices in the Internet. SNMP can make the network management system to remotely manage all network devices that support SNMP, including monitoring network status, modifying network device configurations, and receiving network event alarms. At present, SNMP is the most widely-used network management protocol in the TCP/IP network.

Simple Network Time Protocol (SNTP)

SNTP is mainly used for synchronizing time of devices in the network.

Single-Mode Fiber (SMF)

In this fiber, single-mode optical signals are transmitted.

Spanning Tree Protocol (STP)

STP can be used to eliminate network loops and back up link data. It blocks loops in logic to prevent broadcast storms. When the unblocked link fails, the blocked link is re-activated to act as the backup link.

V

Virtual Local Area Network (VLAN)

VLAN is a protocol proposed to solve broadcast and security issues for Ethernet. It divides devices in a LAN into different segments logically rather than physically, thus implementing multiple virtual work groups which are based on Layer 2 isolation and do not affect each other.

VLAN mapping	VLAN mapping is mainly used to replace the private VLAN Tag of the Ethernet service packet with the ISP's VLAN Tag, making the packet transmitted according to ISP's VLAN forwarding rules. When the packet is sent to the peer private network from the ISP network, the VLAN Tag is restored to the original private VLAN Tag according to the same VLAN forwarding rules. Thus, the packet is sent to the destination correctly.

9.4 Acronym and abbreviations

A

AAA	Authentication, Authorization and Accounting
ABR	Area Border Router
ACL	Access Control List
APS	Automatic Protection Switching
ARP	Address Resolution Protocol
AS	Autonomous System
ASE	Autonomous System External
ATM	Asynchronous Transfer Mode
AWG	American Wire Gauge

B

BC	Boundary Clock
BDR	Backup Designated Router
BITS	Building Integrated Timing Supply System
BOOTP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
BTS	Base Transceiver Station

C

CAR	Committed Access Rate
CAS	Channel Associated Signaling
CBS	Committed Burst Size
CE	Customer Edge

CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common Internal Spanning Tree
CLI	Command Line Interface
CoS	Class of Service
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CST	Common Spanning Tree

D

DAI	Dynamic ARP Inspection
DBA	Dynamic Bandwidth Allocation
DiffServ	Differentiated Service
DNS	Domain Name System
DRR	Deficit Round Robin
DS	Differentiated Services
DSL	Digital Subscriber Line

E

EAP	Extensible Authentication Protocol
EAPoL	EAP over LAN
EFM	Ethernet in the First Mile
EMC	Electro Magnetic Compatibility
EMI	Electro Magnetic Interference
EMS	Electro Magnetic Susceptibility
ERPS	Ethernet Ring Protection Switching
ESD	Electro Static Discharge
EVC	Ethernet Virtual Connection

F

FCS	Frame Check Sequence

G

GARP	Generic Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
GVRP	Generic VLAN Registration Protocol

H

HDLC	High-level Data Link Control
HTTP	Hyper Text Transfer Protocol

I

ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IS-IS	Intermediate System to Intermediate System Routing Protocol
ISP	Internet Service Provider

L

LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol Data Unit
LCAS	Link Capacity Adjustment Scheme
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit

M

MAC	Medium Access Control
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface cross-over
MIB	Management Information Base
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTBF	Mean Time Between Failure
MTU	Maximum Transmission Unit
MVR	Multicast VLAN Registration

N

NMS	Network Management System
NNM	Network Node Management
NTP	Network Time Protocol
NView NNM	NView Network Node Management

O

OAM	Operation, Administration, and Management
OC	Ordinary Clock
ODF	Optical Distribution Frame
OID	Object Identifiers
Option 82	DHCP Relay Agent Information Option
OSPF	Open Shortest Path First

P

P2MP	Point to Multipoint
P2P	Point-to-Point
PADI	PPPoE Active Discovery Initiation
PADO	PPPoE Active Discovery Offer
PADS	PPPoE Active Discovery Session-confirmation
PAP	Password Authentication Protocol
PDU	Protocol Data Unit
PE	Provider Edge
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PPP	Point to Point Protocol
PPPoE	PPP over Ethernet
PTP	Precision Time Protocol

R

RADIUS	Remote Authentication Dial In User Service
RCMP	Raisecom Cluster Management Protocol
RED	Random Early Detection

RH	Relative Humidity
RIP	Routing Information Protocol
RMON	Remote Network Monitoring
RNDP	Raisecom Neighbor Discover Protocol
ROS	Raisecom Operating System
RPL	Ring Protection Link
RRPS	Raisecom Ring Protection Switching
RSTP	Rapid Spanning Tree Protocol
RSVP	Resource Reservation Protocol
RTDP	Raisecom Topology Discover Protocol

S

SCADA	Supervisory Control And Data Acquisition
SF	Signal Fail
SFP	Small Form-factor Pluggable
SFTP	Secure File Transfer Protocol
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SP	Strict-Priority
SPF	Shortest Path First
SSH	Secure Shell
STP	Spanning Tree Protocol

T

TACACS+	Terminal Access Controller Access Control System
TC	Transparent Clock
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLV	Type Length Value
ToS	Type of Service
TPID	Tag Protocol Identifier

U

UDP	User Datagram Protocol
UNI	User Network Interface
USM	User-Based Security Model

V

VRRP	Virtual Router Redundancy Protocol

W

WRR	Weight Round Robin

瑞斯康达科技发展股份有限公司
RAISECOM TECHNOLOGY CO.,LTD.

Address: Raisecom Building, No. 11, East Area, No. 10 Block, East Xibeiwang Road, Haidian District, Beijing, P.R.China Postal code: 100094 Tel: +86-10-82883305
Fax: 8610-82883056 http://www.raisecom.com Email: export@raisecom.com