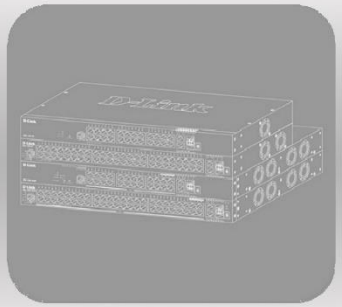
D-Link
Building Networks for People



CLI Reference Guide

Product Model: DGS-F1210 Series
Gigabit Smart Managed PoE+ Switch
Version 1.00

Section 1 Login to the Switch

1.1 System Requirements

Configuration	Minimum Requirements
Processor	Pentium IV/2400MHz or above
RAM	2G or above
Available hard disk space	20G or above
Operation system	Windows 7 or later
Display resolution	1920x1080 (recommended)

1.2 Login method

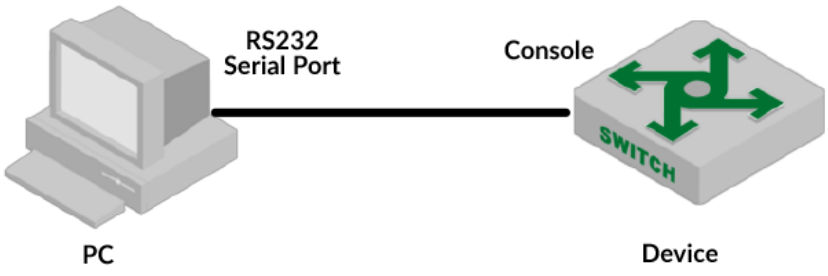
The system supports multiple ways to log in to the management switch: serial port, Telnet, web browser, and network management software.

1.2.1 Login to the switch through the console port

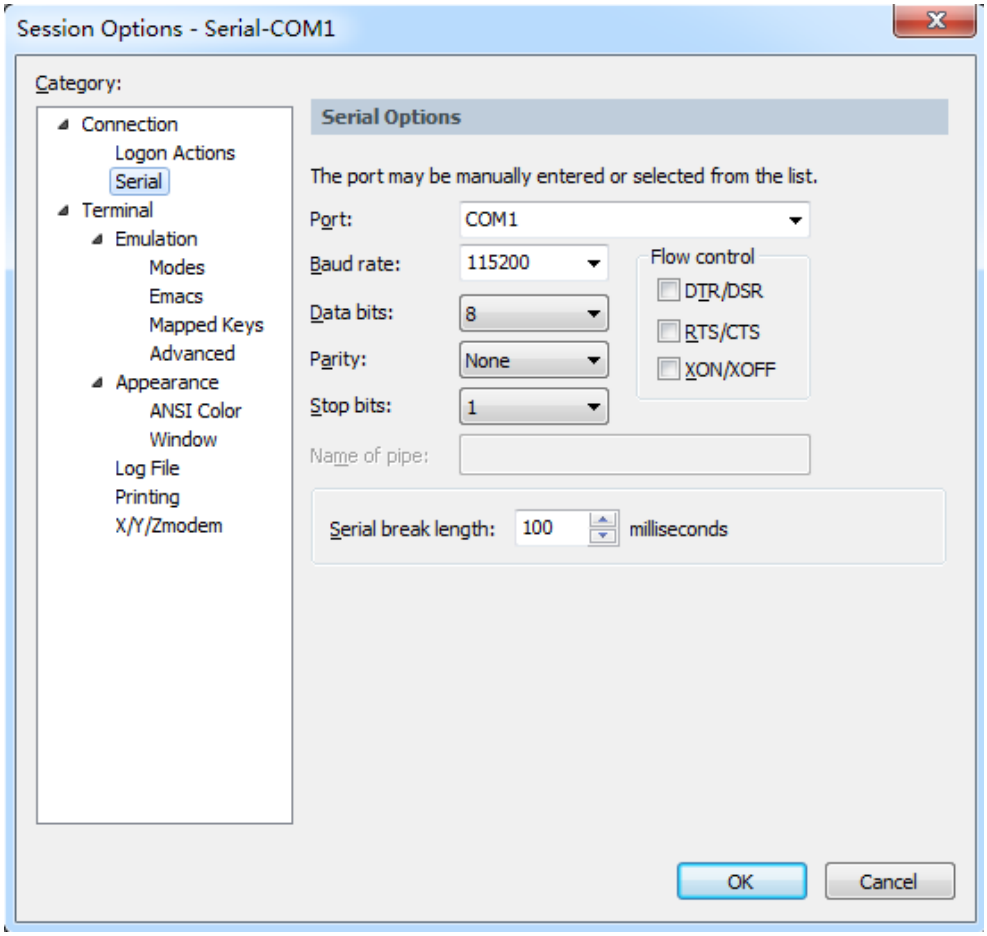
Logging in through the console port is the most basic way to log in to the device. It is also the basis for configuring the device to log in to the device through other methods. By default, you can log in to the device through the serial port. The baud rate of the switch is 115200 bit/s.

Refer to the following steps for specific login:

(1) Use a dedicated serial cable as shown below, first insert the DB-9 (female) plug of the serial cable into the 9-pin (pin) serial port of the PC, and then Insert the RJ-45 plug into the console port of the device.



(2) Run terminal software that supports serial transmission, such as SecureCRT, Windows built-in HyperTerminal, set the required parameters: Baud rate is "115200", Data bit is "8", Parity is "None", The stop bit is "1", the Data Flow control is "None", and the terminal emulation is selected as "Automatic Detection", see the figure below.



(3) Follow the on-screen prompts to enter your username and password and enter the switch. Default username: admin, default password: admin.

1.2.2 Accessing the Switch Through a Web Browser

Enter the IP address of the device in the browser and enter, then prompt for the account password. The default is: admin/admin.

1.2.3 Accessing the Switch Through Network Management Software

The switch supports login management through SNMP network management software. By default the snmp-server feature is turned on and the default community name can be used.

1.2.4 Logging in to the switch through telnet

Specific steps are as follows:
Configure the device as a Telnet server.

Operation	Command	Remarks
Enter enable mode	enable	Required
Enter global configuration	configure terminal	Required
Open Telnet Service	IP telnetd enable	Optional
Close Telnet Service	IP telnetd disable	Optional

After setting up the Telnet service, use a Telnet client to Telnet to the switch.

1.2.5 Logging Into the Switch Through SSH

Specific steps are as follows:
Configure the device as a Telnet server.

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configuring SSH Service	IP ssh-server (enable|disable)	--

After setting up the SSH service, use an SSH client to connect to the switch.

Section 2 Port Configuration

2.1 Basic Port Configuration

For switch devices, only Ethernet ports are supported, so the following configurations are for Ethernet ports. Basic port configuration

2.1.1Configuring the Port Rate

There are different options for different attribute ports: Gigabit interface rate options are: auto-negotiation, 10 half-duplex, 10M full-duplex, 100M half-duplex, 100M full-duplex, 1000M, 10GE interface rate option: 1000M, 10G.

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name eg. G1)	required
Configuration rate	speed(auto|10M-half|10M-full| 100M-half|100M-full|1000M|2500M|10G)	Optional

2.1.2 Configure the maximum frame length

The maximum frame length is used to limit the minimum unit of received messages.

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name eg. G1)	required
Configure the maximum frame length	max-frame <64-16360>	Optional

2.1.3 Configure the flow control switch

Flow control on means that the data transmission rate exceeds the threshold and packet loss occurs.

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name eg. G1)	required
Turn on flow control	flowctrl	required
Turn off flow control	no flowctrl	required

2.1.4 Configuring port enable

Port enable control port UP/DOWN status

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name eg. G1)	required
Configuring port enable	shutdown	required
Turn off flow control	no shutdown	required

2.2 Port isolation

Port isolation means that ports that join the isolation group cannot communicate with each other and are disabled by default.

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name eg. G1)	required
Enable port isolation	Switch port protected	required
Close port isolation	no switch port protected	required

2.3 Port mirroring

The source port specified by port mirroring copies all the communication packets of the specified type (incoming port, egress port, ingress and egress port) of the port to the destination port.

Operation	Command	Remark
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configure the target port	mirror to (port-name eg. G1)	required
Enter port configuration	interface (port-name eg. G1)	required
Configuring the mirror source port	mirror source direction (ingress|egress|both)	required
Back to global configuration	exit	required
View mirror configuration	show mirror	required

2.4 Port speed limit

The port configures the maximum transmission rate of the port. If the maximum burst rate is exceeded, the packet will be lost. The maximum burst rate is twice the configured maximum transmission rate.

Operation	Command	Remark
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name eg. G1)	required
Configure the rate limit on the port	rate-limit <1-10000000> (Direction of entry) <1-1000000> (Direction of export)	required

2.5 Port statistics

The port statistics are used to record the number of packets, the number of bytes, and the number of packets to be filtered. View statistics for all ports.

Operation	Command	Remark
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
View all port statistics	show interface statistics	required

Section 3 POE Configuration

3.1 POE Port configuration

Configure the maximum power of the port. The default is 32W. When the value is exceeded, the port does not supply power. The optical port does not support power supply.

Operation	Command	Remark
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name eg. G1)	required
Configure the port POE power supply.	poe limit (5|10|18|29|32|38)	Optional

3.2 POE display device information

View current POE configuration information

Operation	Command	Remark
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
View current POE configuration	show poe	required

3.3 POE Timing power supply configuration

3.3.1 Configure the timed outage time range

Configure a timed power outage to power off according to the selected time period. The time-range can be added in the ACL. The configuration method is: advanced configuration/ACL configuration/time rang configuration, add a time-range, and then Time-range sets the time.

Operation	Command	Remark
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name eg. G1)	required
Port PoE binding time-range	poe intelligent time-range (name)	Optional

3.3.2 Configure timing power off enable

Configuring intelligent power-off enable is effective for limiting the power-off. If it is configured to disable, the limit power-off effect does not take effect. The default is enable.

Operation	Command	Remark
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name eg. G1)	required
Port POE binding time-range	poe intelligent (enable|disable)	Optional

3.4 POE Intelligent power supply

3.4.1 Configure the maximum total power supply

Operation	Command	Remark
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configure maximum power supply	poe max-total-power <60-250>	-

3.4.2 Configure zero traffic duration

When no traffic passes during the set time, the system automatically disconnects the POE power supply. When the traffic is counted again, the POE power supply automatically turns on.

Operation	Command	Remark
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configure maximum power supply	poe zero-flow-interval <60-600>	-

(This function takes effect when the button AI power supply on the panel is turned on)

Section 4 Layer 2 Configuration

4.1 MAC Address Table Management

4.1.1 Viewing the Current MAC Table

View the MAC learned by the current MAC address table and the static MAC added manually.

Operation	Command	Remark
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
View current mac table	show mac-address	required

4.1.2 Add/delete static MAC

Manually added MAC addresses are not affected by aging time.

Operation	Command	Remark
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Add static MAC	mac-address static (MM-MM-MM-MM-MM-MM) VLAN <1-4094> interface IFNAME	Optional
Delete static MAC	no mac-address static (MM-MM-MM-MM-MM-MM) VLAN <1-4094> interface IFNAME	Optional

4.1.3 Set the dynamic MAC aging time.

Set the MAC address aging time. If the MAC address is not learned again within the specified time, it will be deleted from the MAC address table. The default value is 300s. Unit seconds.

Operation	Command	Remark
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configure the MAC address aging time.	Mac-address aging-time (10-1000000)	Optional
Restore the default MAC address aging time.	No mac-address aging-time	required

4.2 VLAN Configuration

VLAN (Virtual Local Area Network) is a technology that implements a virtual workgroup by logically, rather than physically, dividing devices in a local area network into network segments. The IEEE issued a draft IEEE 802.1Q protocol standard to standardize VLAN implementations in 1999.

VLAN technology allows network managers to logically divide a physical LAN into different broadcast domains (or VLANs). Each VLAN contains a set of computer workstations with the same requirements, and has the same attributes as a physically formed LAN. But because it is logically and not physically divided, each workstation in the same VLAN does not have to be placed in the same physical space. Broadcast and unicast traffic inside a VLAN is not forwarded to other VLANs, which helps control traffic, reduce equIPment investment, simplify network management, and improve network security. The following are the VLAN characteristics:

- VLAN helps control traffic

In a traditional network, a large amount of broadcast data is sent directly to all network devices, whether necessary or not, resulting in a large amount of bandwidth occupied by the network. VLANs can set up which devices in each VLAN must communicate with each other, thereby reducing broadcast and improving network efficiency.

- VLAN provides greater security

Devices in each VLAN can only communicate with devices in the same VLAN. For example, if a device in the R&D department VLAN must communicate with a device in the production department VLAN, it must be routed through the device. In this way, the two departments cannot communicate directly, thereby improving system security.

4.2.1 Configuring basic properties of VLAN

Operation	Command	Remark
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Create/delete VLAN	(no) VLAN RANGE ()	choose list
Configure port descrIPtion	name (NAME)	Configure port descrIPtion
Enter port mode	interface (port-name eg. G1)	Port mode
Add a port to VLAN	Switch port (port-mode)	Configure VLAN port mode

4.2.2 Configure port defaults VLAN

The default VLAN of a port is also called PVID. When a port receives an unmarked message, the system automatically adds a tag to the packet. The VLAN ID in the tag is the default VLAN.

Operation	Command	Remark
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name eg. G1)	Port mode
Configure the port default VLAN	switchport pvid (vid)	Configure the port default VID

4.2.3 Configuring port link attributes

According to the way that tag is processed when the port forwards the packet, the port can be classified into three types.

Access port: A port can belong to only one VLAN and is generally used to connect terminal devices.

Trunk: A port can receive and send multiple VLANs. The default VLAN packets are sent without tags. Other VLANs are sent with tags, which are used to interconnect ports.

Hybrid port: A port can receive and send multiple VLANs, allowing multiple VLANs to be sent with or without tags.

Port type	Processing of received messages		Processing of sent messages
	When receiving untag message	When receiving tag messages	
Access	Add a default VLAN tag	If the VLAN ID of the packet is the VLAN that the port allows, the packet will be accepted. Otherwise, the packet will be discarded.	When the VLAN ID carried in the packet is the VLAN ID allowed by the port, the VLAN tag is strIPped and the packet is sent.
Hybrid			When the VLAN ID carried in the packet is

			the UNTAG VLAN ID that the port allows, the VLAN tag is strIPped and the packet is sent. When the VLAN ID carried in the packet is the TAG VLAN ID that the port allows, the VLAN tag is kept and the packet is sent.
Trunk			If the VLAN ID carried in the packet is the VLAN ID allowed by the port, if the VLAN ID is inconsistent with the port PVID, the VLAN tag is kept and the packet is sent. If the VLAN ID is the same as the PVID of the port, the VLAN tag is strIPped and the packet is sent

Operation	Command	Remark
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port configuration mode	interface (port-name eg. G1)	--
Configure port VLAN mode	Switch port { access | hybrid | trunk }	Optional Default hybrid

4.2.4 Set the VLAN attribute based on the Hybrid port.

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global mode	configure terminal	required
Enter port configuration	interface (port-name eg. G1)	-
Configure port VLAN mode	switchport mode hybrid	Required Default hybrid
Allow the specified VLAN to pass the trunk port	switchport hybrid {tagged | untagged} { VLAN-list | all }	The tagged attribute indicates that the VLAN packet comes out with a tag, and the untagged attribute indicates that the VLAN message comes out without a tag.
The specified VLAN is not allowed to pass through the trunk port.	No switchport hybrid {tagged | untagged} { VLAN-list | all }	Delete the hybrid port member

4.2.4 Set the VLAN attribute based on the trunk port

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global mode	configure terminal	required
Enter port configuration mode	interface (port-name eg. G1)	-

Configure port VLAN mode	switchport modetrunk	Optional Default hybrid
Allow the specified VLAN to pass the trunk port	switchport trunk tag{ VLAN-list | all }	
The specified VLAN is not allowed to pass through the trunk port.	No switchport trunk tag { VLAN-list | all }	

4.2.5 Set the port mode to access

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global mode	configure terminal	required
Enter port configuration mode	interface (port-name eg. G1)	-
Configure port VLAN mode	switchport modeaccess	required default access

4.2.6 Global configuration VLAN learning mode

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global mode	configure terminal	required
Configure VLAN learning mode	VLAN learning {ivl | svl}	required default ivl
View VLAN learning mode	show VLAN learning	

4.2.7 Configuration voice- VLAN

A voice VLAN is a VLAN that is divided into voice data streams for users. By adding a voice VLAN and adding a voice device to a voice VLAN, you can enable voice data to be transmitted in the voice VLAN. This facilitates the QoS (Quality of Service) configuration and improves voice over the voice stream. Priority of traffic transmission to ensure call quality.

Change the VLAN ID of the packet to the specified VLAN ID according to the source MAC address field in the data packet entering the switch port (default is 1); also modify the corresponding COS value (default 5) and DSCP (default 46) Value, improve the priority of packet forwarding, and achieve better forwarding.

Open globally Voice-VLAN

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global mode	configure terminal	required
Open globally voice-VLAN	voice-VLAN enable	required close by default
Close voice-VLAN	voice-VLAN disable	-

Configuration Voice-VLAN VID, COS, DSCP

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global mode	configure terminal	required
Configuration Voice-VLAN VID, COS, DSCP	voice-VLAN vid <1-4094> cos <0-7> dscp <0-63>	-
View the Voice-VLAN configuration information.	Show voice-VLAN	-

Configure the voice-VLAN source MAC address and mask.

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global mode	configure terminal	required
Configuration	voice-VLAN mac MM-MM-MM-MM-MM-MM mask MM-MM-MM-MM-MM-MM	-
Delete Voice-VLAN source MAC	no voice-VLAN mac MM-MM-MM-MM-MM-MM	-
View the Voice-VLAN configuration information.	Show voice-VLAN	-

4.2.8 Configuration MAC Based VLAN

The MAC VLAN is a MAC-based VLAN, which is another way to divide VLANs. It determines the label of a VLAN to be added to the packet based on the source MAC address of the packet.
How does the device classify VLANs based on MAC addresses? After receiving a untagged packet, the port uses the source MAC address of the packet as the matching keyword to obtain the VLAN bound to the terminal.

Configuring MAC Based VLAN Source MAC

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global mode	configure terminal	required
Enter VLAN mode	VLAN (id)	required
Configuring MAC Based	mac VLAN MM-MM-MM-MM-MM-MM	-

VLAN Source MAC		
Delete MAC Based VLAN	no mac VLAN MM-MM-MM-MM-MM-MM	-
Return to global mode	exit	-
View MAC Based VLAN configuration information	show mac VLAN	-

4.2.9 Configuration IP Based VLAN

The IP subnet-based VLAN is divided according to the source IP address and subnet mask of the packet. After receiving the packet from the port, the device determines the VLAN to which the packet belongs based on the source address of the packet, and then automatically divides the packet into the specified VLAN for transmission.

Configure IP Based VLAN, mask：

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global mode	configure terminal	required
Enter VLAN mode	VLAN (id)	required
Configure IP Based VLAN, mas	IP VLAN A.B.C.D/M	-
Remove IP Based VLAN	no IP VLAN A.B.C.D/M	-
Return to global mode	exit	-
View IP Based VLAN configuration information	show IP VLAN	-

4.3.1 Configuration GVRP

GVRP is defined in the IEEE 802.1P standard, allowing control of 802.1Q VLANs. GVRP switches can exchange VLAN configuration information, cut unnecessary broadcasts and unknown unicast traffic, and dynamically create and manage VLANs on switches connected through 802.1Q trunks.

GID and GIP are used in GVRP, which provide a common state mechanism descrIPtion and general information dissemination mechanism for GARP-based applications. GVRP runs only on 802.1Q trunk links. GVRP cuts off the trunk link so that only active VLANs are transmitted over the trunk connection. Before GVRP adds a VLAN to the trunk, it first receives the join information from the switch. GVRP update information and timers can all be changed. GVRP ports have multiple modes of Operation that control how they tailor VLANs. GVRP dynamically adds and manages VLANs for VLAN databases.

In other words, GVRP supports the propagation of VLAN information between devices. In GVRP, you can manually configure the VLAN information of a switch. All other switches in the network can dynamically learn about those VLANs. The endpoint can access any switch and connect to the desired VLAN. To use GVRP, the terminal needs to install a GVRP-compatible network interface card (NIC). A GVRP-compatible NIC can be configured to join the desired VLAN and then access a GVRP-enabled switch. A communication connection is established between the NIC and the switch, and VLAN connectivity is achieved between the two.

Configure GVRP globally

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Turn GVRP on/off globally	(no)gvrp	--
View GVRP configuration information.	Show gvrp configuration	--

Configure GVRP to dynamically create VLANs.

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Globally enable/disable GVRP to dynamically create VLANs.	(no) gvrp dynamic-VLAN-creation	--
View GVRP configuration information.	Show gvrp configuration	--

Configuring GVRP ports:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name eg. G1)	--
Port on/off GVRP	(no) gvrp	--
Return to global mode	exit	--
View GVRP configuration information	show gvrp configuration	--

Configuring port registration mode:

Normal mode: Allows the port to dynamically register, deregister VLANs, propagate dynamic VLANs, and statically VLAN information.

Fixed mode: Disables the port to dynamically register and deregister VLANs, and only propagates static VLAN information.

Propagate dynamic VLAN information. That is to say, the trunk port is set to the fixed mode, even if it is allowed.

If a VLAN is passed, the actual VLAN that passes through can only be manually configured.

Forbidden mode: This port is forbidden to dynamically register and deregister VLANs, and does not propagate except VLAN 1.

Any VLAN information. That is, the trunk port configured as Forbidden mode, even if All VLANs pass, and the actual VLAN that passes is only the default VLAN, that is, VLAN 1.

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name eg. G1)	--
Configuring port registration mode	gvrp registration (normal|fixed|forbidden)	--
Return to global mode	exit	--
View GVRP configuration information.	Show gvrp configuration	--

Configure port application status:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name eg. G1)	--
Configure port application status	gvrp applicant state (normal|active)	--
Return to global mode	exit	--
View GVRP configuration information.	Show gvrp configuration	--

Configuring port timers:

Join timer: In order to ensure that the Join message can be reliably transmitted to other entities, the GARP application entity Join message is sent out twice. The time interval between transmissions is done with the Join timer.

Leave timer: When a GARP application entity wants to log out an attribute information, it will send it out Leave message, the GARP application entity that received the message starts the Leave timer, if the Join message is not received again before the timer expires, the attribute information is logged out.

LeaveAll timer: After each GARP application entity starts, it will start the LeaveAll timer at the same time. After the timer expires, the GARP application entity will send a LeaveAll message to the outside to make the other. GARP application entity re-registers all attribute information on this entity. Then LeaveAll Timer start a new cycle.

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name eg. G1)	--
Configuring port timers	gvrp timer (join|leave|leaveall) VALUE	--
Return to global mode	exit	--
View GVRP timer information.	Show gvrp timer	--

View GVRP statistics

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
View GVRP statistics	show gvrpstatistics	--

4.3 Link aggregation

Port aggregation is to aggregate multiple physical ports to form one aggregation group to implement traffic load balancing and link redundancy backup.

The basic configurations of the ports in the same aggregation group must be the same. The basic configurations include STP, VLAN, and port attributes.

STP configuration includes: STP enable/disable, STP priority, and STP overhead of the port.

VLAN configuration includes: VLANs allowed on the port, port PVID.

The port attribute configuration includes: the rate of the port, the duplex mode (which must be full duplex), and the link type (that is, the trunk, hybrid, and access types).

On the same switch, if the features of a port in an aggregation group are modified, the remaining ports in the same aggregation group are automatically synchronized.
Port aggregation can be classified into static aggregation and dynamic LACP aggregation according to different aggregation modes.

There are three LACP protocol modes for ports.:
Static mode (on): Do not run LACP protocol

Dynamic active mode: The active mode initiates LACP negotiation in active mode.
Dynamic passive mode: In passive mode, the port only responds to LACP negotiation. When it is connected to another device, it can be statically connected to the static interface. Active can be connected to active or passive. Passive can only be connected to active.

4.3.1 Port static aggregation

Different aggregation groups are distinguished based on the id number. The same port cannot be added to multiple aggregation groups at the same time. If a member is not deleted in the aggregation group, you cannot delete the member in the aggregation group.

You can create an aggregation group id directly or globally when you add a port to an aggregation group.

Create a static aggregation group

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter global configuration	interface trunk(id)	-
Delete the aggregation group ID	no interface trunk(id)	-

(ID is the aggregation group ID)
Static aggregation group to add members:

A static aggregation group can have up to 8 port members.

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name e.g. G1)	-
Configuring an aggregation group member	trunk (TID)	-
Delete an aggregate group member	no trunk (TID)	-
Return to global mode	exit	-
View all aggregation groups	show link-aggregation group	-

After the aggregation group takes effect, the service flows are forwarded among the members of the LCP according to certain policies to achieve a balanced load. The default load balancing uses src-mac, which can modify the load basis as needed.

Configure load balancing mode

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configure load balancing mode	trunkload-balance (src-mac|dst-mac|srcdst-mac|src-IP|dst-IP|srcdst-IP)	required
View all aggregation groups	show link-aggregation group	-

4.3.2 Port dynamic aggregation

A dynamic LACP can contain up to 12 members, 8 of which are in the band1 state, and the other four are in the backup state. Only members in the band1 state forward normal traffic. After the member in the band1 state is down, the backup member with the best port priority becomes the band1 state.

Configuring system priority

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configuring system priority	lacp system-priority<1-65535>	required
View all aggregation groups	show link-aggregation group	-

Configure port dynamic aggregation to be enabled.

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name e.g. G1)	required
Open port dynamic aggregation	lacp enable	-
Turn off port dynamic aggregation	lacp disable	-
Return to global configuration	exit	-
View all aggregation group port statuses	show link-aggregation portstate	-

Configuring port activity mode

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name eg. G1)	required
Configuring port activity mode	lacp activity-mode (active|passive)	-
Return to global configuration	exit	-
View all aggregation group port statuses	show link-aggregation portstate	-

Configure port send mode

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name eg. G1)	required
Configuring port activity mode	lacp xmit-mode (slow|fast)	-
Return to global configuration	exit	-
View all aggregation group port statuses	show link-aggregation portstate	-

Configure port priority

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name eg. G1)	required
Configuring port activity mode	lacp port-priority <1-65535>	-
Restore default port priority	no lacp port-priority	-
Return to global configuration	exit	-
View all aggregation group port statuses	show link-aggregation portstate	-

Configuring port key values

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name eg. G1)	required
Configuring port activity mode	lacp port-key <0-65535>	-
Return to global configuration	exit	-
View all aggregation group port statuses	show link-aggregation portstate	-

4.4 MSTP Configuration

Single spanning tree includes spanning tree (STP) and fast spanning tree (RSTP):
STP (Spanning Tree Protocol) is part of the IEEE 802.1D bridge protocol. Its main function is to clear the Layer 2 loop from the topology.

In order to run STP, information needs to be shared between switches. The information they share is the Bridge Protocol Data Unit (BPDU), which is sent in the form of multicast information. Only other Layer 2 devices listen to the bridge data unit. The switch will use BPDUs to learn the network topology: what devices are connected to other devices, and based on this topology, there are some Layer 2 loops in the network.

If some loops are discovered, the switch will disable one or some of the ports in this topology to ensure there are no loops in the network. That is, in a switched network, only one path is available from one device to any other device. If there is any change in the Layer 2 network, such as a link is broken, a new link is added, a new switch is added, or a switch fails, the switch in the network will share this information, which will cause the STP algorithm to re- Execute and generate a new acyclic topology.

Basic concept of STP：

Root Bridge

After the STP algorithm runs, the first step is to elect the root switch. The Root Bridge is located at the top of the entire spanning tree topology. The switch with the lowest switch ID will be selected as the root. The switch ID consists of two parts：

- The priority of the switch. By default, all switches have a priority of 32,768.
- MAC address of the switch.

The administrator can specify a switch as the root by changing the ID of the switch. When the network topology changes, such as the root switch fails or a new switch is added to the network, the election process of the root switch is triggered again.

Root port

After selecting the root switch, you need to select a port closest to the root switch on all non-root switches in the network to communicate with the root switch.

Designated Bridge

In each individual LAN, there is a switch called a designated bridge, which belongs to the bridge that spends the least amount of root path in the LAN. The root switch is the election bridge for all LANs connected to it.

Designated Port

After the root switch and the root port are elected, a port for reaching the root switch is also elected on each link. This port is the designated port. To be a designated port, you must have the following conditions:

Between the two switches on a link, the port on the switch that has the lowest cumulative path cost to the root switch will be selected. If the cumulative path cost of both switches is the same, then select the switch with the lowest switch ID.

If multiple links to the root switch are connected to the same switch, select the switch port with the lowest priority as the designated port. If the priorities of the ports are the same, the port with the lowest physical port number is the designated port.

The basic concept of RSTP:

RSTP (Rapid Spanning Tree Protocol) is an optimized version of the STP protocol. It is “fast in the case that when a port is selected as the root port and the designated port, the delay of entering the forwarding state is greatly shortened under certain conditions, thereby shortening the time required for the network to finally reach the topology stability. In RSTP, The port state of the root port is rapidly migrated. The old root port on the device has stopped forwarding data, and the upstream designated port has started to forward data.

In RSTP, the port state of a specified port can be quickly migrated if the specified port is an edge port or the designated port is connected to a point-to-point link. If the specified port is an edge port, the specified port can directly enter the forwarding state. If the specified port is connected to the point-to-point link, the device can handshake with the downstream device and get the response immediately after entering the forwarding state.

RSTP can converge quickly. However, the STP has the following defects: All the bridges in the LAN share a spanning tree. The redundant links cannot be blocked by VLANs. Packets of all VLANs are forwarded along a spanning tree.

- RSTP port⇓ role is different from the original STP Root Port, Designated Port, Blocking Port adds AlternatePort, Backup Port and Edge Port (included in

Designated Port), canceling the concept of Blocking Port. The stable state of the Root Port and the Designated Port is Forwarding, and the stable state of the Alternate Port and the Backup Port is Discarding.

- ✱ The total port status has also been⇓ reduced from the original five to three types of Learning, Forwarding, Discarding (the original Disable, Blocking, Listening state). Moreover, the BPDUs of the RSTP are no longer sent by the root bridge. Each bridge sends its own BPDU, which is the same as the subsequent TC, which helps to accelerate the convergence of the network.

STP (Spanning Tree Protocol) The port state cannot be quickly migrated. Even on a point-to-point link or an edge port, you must wait for 2 times the delay of Forward Delay before the port can be migrated to the forwarding state.
The Rapid Spanning Tree Protocol (RSTP) can converge quickly. However, the STP has the following defects: all the bridges in the LAN share a spanning tree. The redundant links cannot be blocked by VLANs. Forward along a spanning tree.

MSTP:

MSTP (Multiple Spanning Tree Protocol) The loop network is pruned into a loop-free tree network to avoid the proliferation and infinite loop of packets in the loop network. At the same time, it provides multiple redundant paths for data forwarding, and implements VLAN data in the data forwarding process. Load balancing.

MSTP is compatible with STP and RSTP and can make up for the shortcomings of STP and RSTP. It can quickly converge and distribute traffic of different VLANs along their respective paths, thus providing a better load sharing mechanism for redundant links.

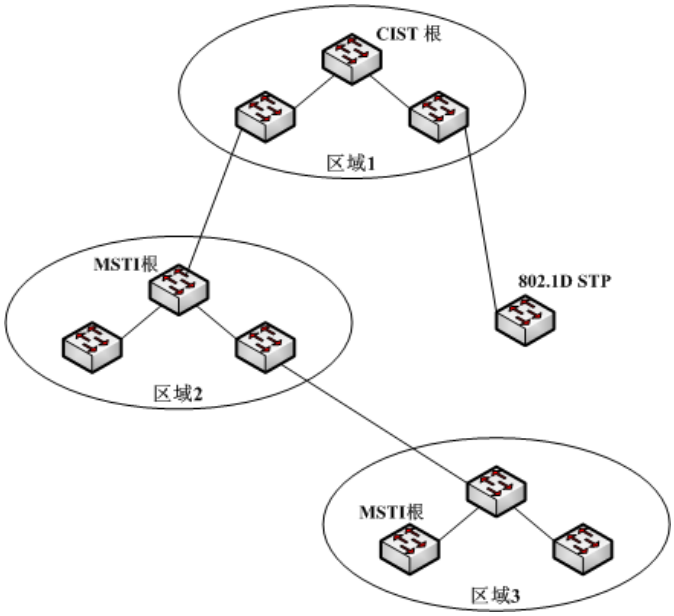


图 1

Figure 1 shows an example MSTP network consisting of three multi-spanning tree areas and a switch running the 802.1D STP protocol.

1. MST domain

As shown in Figure 1, an example MSTP network, Regions 1, 2, and 3 are three MST regions.

Multiple Spanning Tree Regions (MSRs) are composed of multiple switches in a switched network and network segments between them. These switches all start MSTP, have the same domain name, the same VLAN to spanning tree mapping configuration, and the same MSTP revision level configuration, and are physically connected by links.

A switching network can have multiple MST regions. You can use the MSTP configuration command to divide multiple switches into the same MST region.

2. CIST

Common and Internal Spanning Tree, Public and internal spanning trees. A spanning tree consisting of all the individual switches in the network and their connected LANs. These switches may belong to different multiple spanning tree areas, or may be switches running traditional STP or RSTP protocols. Switches running these two protocols are considered to be in an area consisting only of themselves in a multiple spanning tree network.

After the network topology is stable, the entire CIST selects a CIST root bridge. Within each region, the root bridge in the CIST region is also selected as the shortest path from the inside of the region to the CIST root.

3. CST

Common Spanning Tree, Public spanning tree. If each multi-spanning tree area is treated as a single switch, CST is the spanning tree that connects all of these "individual switches." As shown in Figure 1, the zones 1, 2, 3 and the STP switches together form the CST of the network.

4. IST

Internal Spanning Tree, Internal spanning tree. Refers to the part of the CIST that is within a certain spanning tree area. It can also be understood that IST and CST together constitute CIST.

5. MSTI

Multiple Spanning Tree Instance, Multiple spanning tree instances. The MSTP protocol allows different VLANs to be divided into different spanning trees, thus establishing multiple spanning tree instances. In general, the spanning tree instance numbered 0 refers to the CIST, which can be extended to the entire network, and the spanning tree instances pointed to from 1 are all inside a certain area. Multiple VLANs can be assigned to each spanning tree instance. Initially, all VLANs are assigned to the CIST.

All MSTIs in a multiple spanning tree area are independent of each other, and they can select different switches as their respective roots. For example, in the area 3 of FIG. 1, the root bridge of the MSTI01 may be the switch in the lower left corner, and the MSTI00, that is, the inner bridge of the CIST area, may be the switch in the middle position.

6. CIST root

CIST root, is the bridge with the highest priority bridge ID in the entire network.

7. CIST external root path cost

CIST external root path cost, the path between the bridge and the CIST root costs. The change occurs only when the MST region is crossed. The CIST external root path of all bridges in the same MST region costs the same.

8. CIST regional root

CIST regional root, is the bridge that spends the least amount of external root paths to the CIST root in each domain. In fact, it is the root bridge of the IST, which can also be said to be a virtual bridge of the MST domain. If the CIST root is in an MST region, the CIST root is also the CIST region root bridge of the MST region.

9. CIST internal root path cost

CIST internal root path cost, The cost of the bridge in the MST region to the root path of the CIST region root bridge of the domain is valid only in the domain.

10. CIST designated bridge

CIST designated bridge, Same as STP designated bridge.

11. MSTI regional root

MSTI regional root, the root bridge of the MSTI in each MST region may not be the same for the different MSTIs.

12. MSTI internal root path cost

MSTI internal root path cost, the cost of the bridge in the MST region to the root path of the MSTI region root bridge of the domain is valid only in the domain.MSTI designated bridge

13. MSTI designated bridge

MSTI designated bridge，Same as STP designated bridge.

4.4.1 Spanning tree global configuration

Turn spanning tree on/off:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Turn on/off spanning tree	(no) spanning-tree	required

The default is on.

Configure spanning tree mode:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configuring spanning tree mode	spanning-tree mode (stp|rstp|mstp)	optional

Configuring spanning tree Max-age:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configure spanning tree Max-age	(no)spanning-tree max-age <6-40>	required

Configuring spanning tree hello-time:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configure spanning tree hello-time	(no)spanning-tree hello-time <1-10>	required

Configure spanning tree Forward delay:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configure spanning tree Forward delay	(no) spanning-tree forward-delay <4-30>	required

Configure spanning tree Max hop

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configure spanning tree Max hop	(no) spanning-tree max-hop <1-40>	required

Configure spanning tree Revision

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configure spanning tree Revision	(no) spanning-tree mstp revision <0-65535>	required

Configure the spanning tree domain name

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configure the spanning tree domain name	(no) spanning-tree mstp name STRING	required

View the spanning tree information:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
View current spanning tree configuration	show spanning-tree	required

4.4.2 Spanning tree instance configuration

Supports 63 instance configurations, each of which can be configured with a priority range of 0-61400 and must be a multiple of 4096; each instance can be added with VLANs, separated by spaces.

Configure instance priority:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configure instance priority:	spanning-tree instance<1-63> priority <0-61440>	required

Add VLAN to the instance:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Add VLAN to the instance:	spanning-tree instance <1-4096> vid .VID	required

View instance configuration:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
View instance configuration	show spanning-tree instance	required

4.4.2 Spanning tree instance port configuration

Configure the port priority and link cost of the instance:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface [port name]<eg.G1>	optional
Configure an instance port priority	spanning-tree mstp <0-63> port-priority <0-240>	optional

Configuration port bpdu guard:

Operation	Command	Remarks
Enter enable mode	enable	Required
Enter global configuration	configure terminal	Required
Enter port mode	interface [port name]<eg.G1>	Optional
Configuration port bpdu guard	spanning-tree bpduguard {enable|disable}	Optional

Configure the edge port status:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface [port name]<eg.G1>	optional
Configure the edge port status:	spanning-tree mstp edge (force-true|force-false|auto)	optional

Configure point-to-point port status:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface [port name]<eg.G1>	optional
Configuring point-to-point port status	spanning-tree mstp point-to-point (force-true|force-false |auto)	optional

View instance port configuration:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
View instance port configuration	show spanning-tree interface	required
View the detailed port status of the spanning tree	show spanning-tree interface brief	-

4.5 Loop protection configuration

Loop protection prevents bridge loops from occurring on point-to-point links due to unidirectional link failures. When the loop function is enabled globally on the switch, it is applied to all point-to-point ports in the system. Loop protection detects root and blocked ports and ensures that they can receive BPDU packets from designated ports in the network segment. If the root port with loop protection enabled or the blocked port stops receiving BPDU packets from the port specified in the network segment, it assumes that there is a physical link error on the port and turns these ports into a blocking state so that they can be received immediately BPDU package. Loop protection can be enabled on a per-port or global basis. When loop protection is enabled on a port, loop protection is automatically applied to all active instances or VLANs to which the port belongs. When the root protection function is disabled, it is only prohibited on the

specified port. When the loop protection function is disabled, all ports with conflicting loops will be converted to the listening state.

4.5.1 Loop protection global configuration

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Global loop protection on/off	loop-protect (enable | disable)	optional
View loop protection status	show loop-protect status	-

Configure the packet sending period

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configure the packet sending period	loop-protect tx-time <1-10>	optional
View loop protection status	show loop-protect status	-

4.5.2 Loop protection port configuration

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name eg. G1)	--
Configure port to enable/disable loop protection receive mode.	(no) loop-protect portEnabled	default on

Enable loop protection port transmission mode

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name eg. G1)	--
Configure port to enable/disable loop protection port transmission mode.	(no) loop-protect transmit	default on

4.5.3 View loop protection status

Operation	Command	Remarks
Enter enable mode	enable	Required
Enter global configuration	configure terminal	Required
View loop protection status	show loop-protect status	--
View loop protection port status	show loop-protect interface	--

4.6 DHCP-SNOOP Configuaration

For security reasons, the network administrator may need to record the IP address used by the user to access the Internet, and confirm the correspondence between the IP address obtained by the user from the DHCP server and the MAC address of the user. The switch can listen to DHCP broadcast messages and record the IP address information of users through DHCP snooping.

DHCP snooping obtains the IP address and user MAC address information obtained by the user from the DHCP server by listening to the following two types of packets:

- Monitoring DHCP-ACK packets
- Monitoring DHCP-REQUEST packets

In addition, if there is a privately set up DHCP server in the network, the user may get the wrong IP address. To enable users to obtain IP addresses through a legitimate DHCP server, DHCP Snooping security allows ports to be set to trusted and un-trusted ports:

- The trusted port is connected to the port of the DHCP server or other switch, and the port is not trusted to connect to the user or the network.
- The untrusted port discards the received DHCP-ACK and DHCP-Offer packets from the DHCP server. The DHCP packets received by the trusted port are forwarded normally. This ensures that the user obtains the correct IP address.
- Trust VLAN: The untrusted port does not discard the DHCP-ACK and DHCP-Offer that change the VLAN.

4.6.1 DHCP-SNOOP configuration

Turn on/off DHCP-SNOOP

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
On/off DHCP-SNOOP	(no)DHCP-snooping	--

When an interrupt is dynamically obtained through the port, it is recorded. You can manually add a static binding. When the port is enabled with the Untrust, only the specified MAC address, IP address, and port can access the router.

Add a static IP Source Guard binding

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
Add a static binding	IP-source-guard bind mac MM-MM-MM-MM-MM-MM IP A.B.C.D interface (all | IFNAME)	--
Delete static binding	no IP-source-guard bind mac MM-MM-MM-MM-MM-MM	--
View binding table	show DHCP-snooping	

4.6.1 DHCP-SNOOP port configuration

Turn on port Untrust

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
Access port mode	interface (port-name eg. G1)	--
Turn on/off port Untrust	(no) DHCP-snooping untrust	default off

Turn on port IP Source Guard

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
Access port mode	interface (port-name eg. G1)	--
Turn on/off port Untrust	(no) IP-source-guard	default off

4.7 IGMP-SNOOP configuration

IGMP-Snooping is used to listen to IGMP messages between the host and the router. The device can dynamically create, maintain, and delete multicast address tables based on IGMP report messages and IGMP leave messages. The packets are forwarded according to their respective multicast address entries to reduce storms and improve bandwidth utilization.

IGMP-Snooping is a basic function of Layer 2 multicast. It can implement multicast data forwarding and control at the data link layer. When the IGMP messages transmitted between the host and the upstream Layer 3 device pass through the Layer 2 multicast device, IGMP-Snooping analyzes the information carried in the packets and establishes and maintains a Layer 2 multicast forwarding table based on the information. Data is forwarded on demand at the data link layer.

4.7.1 IGMP-SNOOP configuration

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
On/off IGMP-SNOOP	(no) igmp-snooping	--

Configure host aging time

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
Configure IGMP-SNOOP host aging time	igmp-snooping host-age-time <200-1000>	--

Configure IGMP-SNOOP Inquire

You can configure a VLAN-based query source address. The source address will send a Query message to the multicast source address. The maximum waiting time for deleting the group port is deleted. Configured to 10s.

IGMP-Snooping does not remove the port from the multicast group directly after receiving the IGMP Leave message. It waits for a period of time before the port is deleted from the multicast group.

After the fast delete function is enabled, IGMP Snooping directly removes the port from the multicast group when it receives the IGMP Leave message. When there is only one user on the port, the query message will be sent every time the member of the last group is queried. If the last user has left, the user can quickly delete it and save bandwidth.

Configure fast leave:

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
Access VLAN mode	VLAN <1-4094>	--
On/off Leave quickly	(no) igmp-snooping fast-leave	--

Configuring the query interval:

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
Access VLAN mode	VLAN <1-4094>	--
Configuring the query interval	igmp-snooping query-interval <2-300>	--

Configure the query source address:

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
Access VLAN mode	VLAN <1-4094>	--
Configure the query source address	igmp-snooping general-query source-IP A.B.C.D	--

Configure maximum response time:

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
Access VLAN mode	VLAN <1-4094>	--
Configure maximum response time	igmp-snooping max-response-time <1-25>	--

Configure route aging time.:

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
Access VLAN mode	VLAN <1-4094>	--
Configure route aging time	igmp-snooping router-age-time <1-1000>	--

Configure the last member query interval:

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
Access VLAN mode	VLAN <1-4094>	--
Configure the last member query interval	igmp-snooping last-member-query-interval <1-5>	--

4.7.2 IGMP-SNOOP port configuration

When a static multicast is added manually, the terminal connected to the port can obtain the multicast information of the multicast source when the VLAN, the source IP address, the multicast IP address, and the port number are met.

Configuring a static multicast group:

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
Access port mode	interface (port-name eg. G1)	--
Add/delete VLAN allsource adress 址 IGMP-Snooping	(no)igmp-snooping static-group [A.B.C.D] VLAN <1-4094>	--

Add a specific multicast source IP static IGMP-Snooping:

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
Access port mode	interface (port-name eg. G1)	--
Add/delete a specific multicast source IP Static IGMP-Snooping	(no) igmp-snooping static-group [A.B.C.D] source [A.B.C.D] VLAN <1-4094>	--

View all IGMP-SNOOP statistics on VLAN

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
View IGMP-SNOOP VLAN statistics	show igmp-snooping group VLAN <1-4094>	--

4.8 802.1x Configuration

802.1x is an IEEE access management protocol standard based on port access control in June 2001. Since the traditional local area network does not provide access authentication, as long as the user can access the local area network, the devices and resources in the local area network can be accessed, which is a security risk. For applications such as mobile office and resident network operations, the ISP hopes to control and configure user access. There is also a need for billing.

802.1x is a port-based authentication protocol, which is a method and strategy for authenticating users. The ultimate goal of 802.1x authentication is to determine if a port is available. For a port, if the authentication succeeds, the port is "opened" to allow all packets to pass. If the authentication is unsuccessful, the port is kept "off", that is, only 802.1x authentication protocol packets are allowed to pass.

To achieve 802.1X authentication and authorization billing, the system needs to have a certain software and hardware environment. It is summarized into the following three parts.:

- **Client (Supplicant System)**: It is a device that needs to access the LAN and enjoy the services provided by the switch (such as a PC). The client needs to support the EAPOL protocol. The client must run the IEEE 802.1X authentication client software.
- **(Authenticator System)**: In the Ethernet system, the authentication switch is used to upload and send user authentication information, and control whether the port is available according to the authentication result. It's like acting as a proxy between the client and the authentication server.
- **(Authentication Server)**: Usually referred to as a RADIUS server. RADIUS determines whether the user has the right to use the network service provided by the network system by checking the identity (user name and password) sent by the client. After the authentication is completed, the result is sent to the switch.

The certification process is as follows:

The 802.1x-based authentication system uses the EAPOL format to encapsulate the EAP protocol to transmit authentication information between the client and the authentication system. The authentication system and the authentication server transmit authentication information through the RADIUS protocol. Due to the scalability of the EAP protocol, the EAP-based authentication system can use a variety of different

authentication algorithms, such as EAP-MD5, EAP-TLS, EAP-SIM, EAP-TTLS, and EAP-AKA.

The switch supports EAP relay mode and EAP termination mode to interact with the remote RADIUS server to complete authentication.

EAP-Transfer way

This method is defined by the IEEE 802.1X standard. EAP (Extensible Authentication Protocol) is carried in other high-level protocols, such as EAP over RADIUS, so that extended authentication protocol packets traverse complex networks to the authentication server. Generally, the EAP relay mode requires the RADIUS server to support EAP attributes: EAP-Message and Message-Authenticator, which are used to encapsulate EAP packets and protect RADIUS packets carrying EAP-Messages.

The certification process is as follows:

(1) When the user needs to access the network, the user name and password that have been applied for and registered are input through the 802.1X client, and a connection request (EAPOL-Start message) is initiated. At this point, the client program sends a message requesting authentication to the device, and starts an authentication process.

(2) After receiving the data frame requesting authentication, the access device sends a request frame (EAP-Request/Identity message) to request the user's client program to send the input user name.

(3) The client sends the user name information to the device through the data frame (EAP-Response/Identity packet). The device sends the data frame sent by the client to the authentication server for processing after packet processing (RADIUS Access-Request packet).

(4) After receiving the username information forwarded by the device, the RADIUS server compares the information with the username table in the database, finds the password information corresponding to the username, and encrypts it with a randomly generated encryption word. The encrypted word is sent to the device through the RADIUS Access-Challenge packet, and the device forwards it to the client program.

(5) After receiving the encrypted word (EAP-Request/MD5 Challenge message) from the device, the client encrypts the password part with the encrypted word (this encryption algorithm is usually irreversible) and generates EAP- The Response/MD5 Challenge packet is transmitted to the authentication server through the device.

(6) The RADIUS server compares the received encrypted password information (RADIUS Access-Request packet) with the local encrypted password information. If they are the same, the user is considered to be a legitimate user. (RADIUS Access-Accept packet and EAP-Success packet).

(7) After receiving the authentication pass message, the device changes the port to the authorization state, allowing the user to access the network through the port.

4.8.1 802.1X Configuration

Globally open port based 802.1X

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
On/off based port 802.1X	(no)dot1x auth-port system-auth-ctrl	--

Global open based MAC 802.1X

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
On/off based MAC 802.1X	(no) dot1x auth-mac system-auth-ctrl	--

Configure the RADIUS client address and client port number:

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
Configure the RADIUS client address 802.1X and client port number.	Dot1x radius-client source-interface HOSTNAME PORT	--
Delete RADIUS client address	no dot1x radius-client source-interface	--

Configure the RADIUS server shared password.:

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
Configure the RADIUS server shared password.	(no) dot1x radius-server key KEY	--

Configure the number of RADIUS server retransmissions:

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
Configure the number of RADIUS server retransmissions.	(no) dot1x radius-server retransmit RETRIES	--

Configure the RADIUS server timeout time:

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
Configure the RADIUS server timeout period.	(no) dot1x radius-server timeout SEC	--

Configure the RADIUS server dead time:

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
Configure the RADIUS server dead time.	(no) dot1x radius-server deadtime MIN	--

4.8.2 802.1X RADIUS sever configuration

Manually add a RADIUS server

Operation	Command	Remark
Access enable mode	enable	remark
access configuration	configure terminal	must
Configure a RADIUS server	dot1x radius-server host HOSTNAME auth-port PORTNO key STRING retransmit RETRIES timeout SEC	--
Delete RADIUS sever	no dot1x radius-server host HOSTNAME auth-port PORT	

4.8.3 Configure port-based 802.1X authentication

In global mode, you need to select the authentication mode as port authentication.
Configure port authentication and authentication mode.:

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
Access port mode	interface (portname eg.G1 G2 G3)	--
Configure port authentication and authentication mode.	Dot1x port-control force-authorized	--
Return to global mode	exit	--
View port authentication information	show dot1x interface (portname eg.G1 G2 G3)	--

Configure the port authentication control direction:

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
Access port mode	interface (portname eg.G1 G2 G3)	--
Configure the port authentication control direction.	Dot1x port-control dir both	--
Return to global mode	exit	--
View port authentication information	show dot1x interface(portname eg.G1 G2 G3)	--

Configure the port authentication protocol version.:

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
Access port mode	interface (portname eg.G1 G2 G3)	--
Configure the port authentication control direction.	Dot1x protocol-version <1-2>	--
Return to global mode	exit	--
View port authentication information	show dot1x interface(portname eg.G1 G2 G3)	--

Configure port authentication silence time:

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
Access port mode	interface (portname eg.G1 G2 G3)	--
Configure port authentication silent time.	Dot1x quiet-period <1-65535>	--
Configure default silent time	no dot1x quiet-period	
Return to global mode	exit	--
View port authentication information	show dot1x interface(portname eg.G1 G2 G3)	--

Configure port authentication re-authentication times.:

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
Access port mode	interface (portname eg.G1 G2 G3)	--
Configure port authentication re-authentication times.	Dot1x reauthMax <1-10>	--
Configure the default re-authentication times	no dot1x reauthMax	--
Return to global mode	exit	--
View port authentication information	show dot1x interface(portname eg.G1 G2 G3)	--

Configure port authentication EAP sending interval.:

Operation	Command	Remark
Access enable mode	enable	must
Access configuration	configure terminal	must
Access port mode	interface (portname eg.G1 G2 G3)	--
Configure port authentication EAP sending interval.	Dot1x timeout tx-period <1-65535>	--
Configure the default EAP sending interval.	No dot1x timeout tx-period	--
Return to global mode	exit	--
View port authentication information	show dot1x interface(portname eg.G1 G2 G3)	--

Configure port authentication EAP sending interval.

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (portname eg.G1 G2 G3)	--
Configure port authentication EAP sending interval.	Dot1x timeout tx-period <1-65535>	--
Configure the default EAP sending interval.	No dot1x timeout tx-period	--
Return to global mode	exit	--
View port authentication information	show dot1x interface(portname eg.G1 G2 G3)	--

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (portname eg.G1 G2 G3)	--
Configure the port authentication EAP	dot1x timeout tx-period <1-65535>	--

sending interval		
Configure the default EAP sending interval	no dot1x timeout tx-period	--
Return to global mode	exit	--
View port authentication information	show dot1x interface(portname eg.G1 G2 G3)	--

Configure the port authentication re-authentication period.

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (portname eg.G1 G2 G3)	--
Configure port authentication re-authentication	dot1x reauthentication	--
Configure default re-authentication	Operation	command
Return to global mode	exit	--
View port authentication information	show dot1x interface(portname eg.G1 G2 G3)	--

Configure port authentication password transmission

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (portname eg.G1 G2 G3)	--
Configure port authentication password transmission	dot1x keytxenabled (enable|disable)	--
Return to global mode	exit	--
View port authentication information	show dot1x interface(portname eg.G1 G2 G3)	--

4.8.4 Configuring MAC-Based 802.1X Authentication

In global mode, you need to select the authentication mode as MAC authentication.

Configure MAC authentication port security mode.

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (portname eg.G1 G2 G3)	--
Configure MAC authentication port security mode.	Dot1x auth-mac (enable|disable) mode (filter|shutdown)	--
Return to global mode	exit	--
View MAC authentication information	show dot1x all	--

Configure the MAC authentication authentication failure processing action:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (portname eg.G1 G2 G3)	--
Configure MAC authentication authentication failure processing	dot1x auth-mac auth-fail-action (restrict-VLAN <2-4094>|drop-traffic)	--
Return to global mode	exit	--
View MAC authentication information	show dot1x all	--

Configure MAC authentication dynamic VLAN creation:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (portname eg.G1 G2 G3)	--
Configure MAC authentication dynamic VLAN creation.	Dot1x auth-mac dynamic-VLAN-creation (enable|disable)	--
Return to global mode	exit	--
View MAC authentication information	show dot1x all	--

Configure MAC address authentication for MAC address authentication:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (portname eg.G1 G2 G3)	--
Configure MAC address authentication for MAC address authentication.	Dot1x auth-mac mac-aging (enable|disable)	--
Return to global mode	exit	--
View MAC authentication information	show dot1x all	--

Section 5 Three-tier configuration

5.1 Layer 3 Interface Configuration

The IP of the Layer 3 switch can be used as a device management address or gateway. The Layer 3 switch IP needs to be configured on the Layer 3 interface. A Layer 3 IP interface is a VLAN interface. A common VLAN interface is an interface created in a specific VLAN.

Configure a Layer 3 interface:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface VLANIF-NAME eg.VLANif1	optional
Delete an interface	no interface VLANIF-NAME eg.VLANif1	--

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter interface mode	interface VLANIF-NAME eg.VLANif1	optional
Delete an interface	no interface VLANIF-NAME eg.VLANif1	--

Configure interface IPV4:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface VLANIF-NAME eg.VLANif1	optional
Configure IPV4 address	IP address A.B.C.D/M	-
Delete IPV4 address	no IP address A.B.C.D/M	--

Configure interfaceIPV6：

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface VLANIF-NAME eg.VLANif1	optional
Configure IPV6 address	IPv6 address A.B.C.D/M	-
Delete IPV6 address	no IPv6 address A.B.C.D/M	--

VLANif1 is not allowed to be deleted. The eth0 and lo ports cannot be deleted, and the IP address cannot be modified.

5.2 Routing Configuration

View current route:

Operation	Command	Remarks
View current route	show IP route	--

Note: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP, > - selected route, * - FIB route.

Add a static route:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Add a static route	IP route A.B.C.D/M (A.B.C.D|INTERFACE|null0)	--
Delete a static route	no IP route A.B.C.D/M	

5.3 ARP Configuration
View all ARPs:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
View all ARP	show arp (|static|dynamic)	--

Configure static ARP:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configuring static ARP	arp static A.B.C.D MM-MM-MM-MM-MM-MM	--
View all ARP	show arp (|static|dynamic)	--

Configure ARP aging time.

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configure static ARP aging time.	arp timeout <1-2147483>	--
Configure the default aging time.	no timeout	--

Clear all ARPs:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Clear an interface ARP	clear arp interface IFNAME	--
Clear all ARP	clear arp	--

Two computers connected to the Internet must communicate with each other and must have their own IP addresses. Due to limited IP address resources, broadband access operators cannot assign a fixed IP address to each user who subscribes to broadband. (The so-called fixed IP is that even when you are not online, others can not use this IP address, this resource has been monopolized by you), so you must use DHCP to make temporary address allocation for users on the Internet. That is, your computer is connected to the Internet. The DHCP server temporarily assigns an IP address to you from the address pool. The IP address assigned to the Internet may be different each time. This is related to the IP address resource at that time. When offline, the DHCP server may assign this address to other computers that are online later. In this way, the IP address can be effectively saved, which not only ensures network communication, but also increases the usage rate of the IP address.

In a network using the TCP/IP protocol, each computer must have at least one IP address to communicate with other computers. In order to facilitate the unified planning and management of IP addresses in the network, DHCP (Dynamic Host Configure Protocol) has emerged. This network service facilitates efficient management of client IP addresses in the campus network without the need to manually specify an IP address.

DHCP uses one or a group of DHCP servers to manage the allocation of network parameters. This solution is fault tolerant. Even in a network with only a small number of

machines, DHCP is still useful because a machine can be added to the local network with little impact.

Even for servers that rarely change addresses, DHCP is still recommended to set their addresses. If the server needs to be reassigned addresses (RFC2071), it can be done in as few places as possible. For some devices, such as routers and firewalls, you should not use DHCP. It is also useful to place the TFTP or SSH server on the same machine running DHCP for centralized management.

DHCP can also be used to assign addresses directly to servers and desktop computers, and to assign addresses to dial-up and broadband hosts, as well as residential NAT gateways and routers through a PPP proxy. DHCP is generally not available for use on inbound routers and DNS servers.

DHCP is one of the TCP/IP protocol suites and is mainly used to assign dynamic IP addresses to LAN clients. Disadvantages: DHCP has more broadcast overhead. For a metropolitan area network with a large number of users, network Operation efficiency is degraded and configuration is difficult. On the other hand, the problem of users configuring their own IP addresses cannot be solved.

Allocation:

In the working princIPle of DHCP, the DHCP server provides three IP allocation methods: Automatic allocation, manual allocation, and Dynamic Allocation.

- Automatic allocation is the permanent use of this IP address when the DHCP client successfully obtains an IP address from the DHCP server for the first time.

- Manual assignment is an IP address specified by the DHCP server administrator

- Dynamic allocation is that after the client obtains the IP address from the DHCP server for the first time, the address is not used permanently. After each use, the DHCP client needs to release the IP for other clients to use.

The third is the most common form of use.

Lease process:

The process by which a client obtains an IP address from a DHCP server is called a DHCP lease process.

The effective period of use of the IP address is called the lease period. Before the lease expires, the client must request the DHCP server to continue the lease. The server can accept the request after accepting the request, otherwise it will be given up unconditionally.

By default, routers isolate broadcast packets and do not send received broadcast packets from one subnet to another. When the DHCP server and the client are not on the same subnet, the router acting as the default gateway of the client sends the broadcast packet to the subnet where the DHCP server is located. This function is called DHCP Relay.

The types of messages that DHCP refers to during its work and its functions are as follows:

1. DHCP DISCOVER: The first packet that the client starts the DHCP process is a broadcast packet requesting an IP address and other configuration parameters.

2. DHCP OFFER: The response of the server to the DHCP DISCOVER message is a unicast (or broadcast) message containing a valid IP address and configuration.

3. DHCP REQUEST: The client responds to the DHCP OFFER packet, indicating that the configuration is accepted. The packet is also sent when the client renews the IP address lease.

4. DHCP DECLINE: When the client finds that the IP address assigned by the server cannot be used (such as when the IP address conflicts), this message will be sent to notify the server to prohibit the use of the IP address.

5. DHCP ACK: The server acknowledges the response message to the DHCP REQUEST packet of the client. After receiving this message, the client actually obtains the IP address and related configuration information.

6. DHCP NAK: The server rejects the response message from the DHCP REQUEST packet of the client. After the client receives this message, it will restart the new DHCP process.

7. DHCP RELEASE: The client actively releases the IP address assigned by the server. When the server receives the message, it reclaims the IP address and can assign it to other clients.

8. DHCP INFORM: After the client obtains the IP address, it sends this message to request some other network configuration information of the server, such as DNS.

The IP address that the DHCP server leases to the DHCP client generally has a lease term. After the expiration, the DHCP server will reclaim the leased IP address. In order to continue to use the original IP address, the DHCP client sends a request to renew the lease to the DHCP server.

The workflow for renewing the lease is described as follows:

1. At the time of using the past 50% of the lease period, the client sends a unicast DHCP REQUEST message to the server to extend the lease term.

2. If a DHCP ACK packet is received from the server, the lease period is extended forward and the lease renewal is successful. If no DHCP ACK message is received, the client continues to use this IP address. At the time when the lease period is 87.5%, the broadcast DHCP REQUEST message is sent to the server to extend the lease term.

3. If a DHCP ACK packet is received from the server, the lease period is extended forward and the lease renewal is successful. If no DHCP ACK message is received, the client continues to use this IP address. When the lease term expires, the client automatically abandons the use of this IP address and begins a new DHCP process.

5.4.1 DHCP-Server Global Configuration
Enable the global DHCP server:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Turn off DHCP Server	DHCP-server [enable|diasble]	optional

Configure a DHCP Server pool:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter the DHCP pool	DHCP-server pool NAME.	optional

Configure the DHCP Server pool:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter the DHCP pool	DHCP-server pool NAME.	optional
Configure the starting IP and ending IP:	begin-IP [A.B.C.D] end-IP [A.B.C.D]	optional
Configure the default gateway:	default-router [A.B.C.D]	optional
Configuring a DNS server	dns-server [DNSLIST.]	optional
Configuring a domain name service	domain-name NAME.	optional
Configure lease time	lease <0-31536000>	optional
Configuring a NetBIOS server	netbios-name-server [A.B.C.D]	optional

Delete a DHCP Server pool:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Delete DHCP pool	no DHCP-server pool NAME.	optional

View all configured DHCP Server pools:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
View all DHCP Server pools	show DHCP-server	optional

5.4.2 DHCP-Server Client

View all current client information:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
View all DHCP Server pools	show DHCP-server lease	required

5.4.3 DHCP-Server Static Client Configuration

Assigning an IP address to a DHCP pool to a specified MAC address device prevents IP address conflicts. When the request source MAC address is set to the MAC address, the DHCP OFFER packet with the specified IP address is replied.

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter the DHCP pool	DHCP-server pool NAME.	optional
Configuring static client requests	static [A.B.C.D] [MM-MM-MM-MM-MM-MM]	optional

View the static client configuration:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
View all DHCP Server pools	show DHCP-server	required

Configure port binding IP

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter the DHCP pool	DHCP-server pool NAME.	optional
Port binding IP	port-bind [PORT NAME] [A.B.C.D]	

5.5 DHCP-Relay Configuration

DHCPRelay (DHCPR) DHCP Relay (also known as DHCP Relay Agent) is a small program that implements the function of processing and forwarding DHCP information between different subnets and physical network segments.

If the DHCP client is on the same physical network segment as the DHCP server, the client can correctly obtain the dynamically assigned IP address. If you are not on the same physical network segment, you need a DHCP Relay Agent.

1) When the DHCP client starts and performs DHCP initialization, it broadcasts a configuration request message on the local network.

2) If the DHCP server exists on the local network, you can directly configure DHCP without DHCP relay.

3) If the local network does not have a DHCP server, the network device with the DHCPrelay function connected to the local network will process the broadcast packet and forward it to the DHCP server on the specified other network.

4) DHCP server Configure the DHCP client according to the information provided by the DHCP client and send the configuration to the DHCP client through DHCP relay.
In fact, multiple such interactions are required from the beginning to the final completion of the configuration.

5) The DHCP relay device modifies the corresponding field in the DHCP message, changes the broadcast packet of DHCP to a unicast packet, and is responsible for converting between the server and the client.

6) Netcore router (2x05) can be used as a DHCP relay agent.

5.5.1 DHCP-Relay Global Configuration

DHCP Relay is enabled:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enable and disable DHCP Relay	DHCP-relay [enable|disable]	optional

Configure the interface with the DHCP Server pool agent:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter interface mode	interface VLANif<1-4094>	optional
Configure DHCP Relay	DHCP-relay A.B.C.D	optional

Delete the interface and the DHCP Server pool agent:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter interface mode	interface VLANif<1-4094>	optional
Delete DHCP Relay	no DHCP-relay	optional

Check the current configuration of DHCP Relay:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
View DHCP Relay Configuration	show DHCP-relay	optional

Check the current configuration of DHCP Relay:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
View DHCP Relay Configuration	show DHCP-relay	optional

Section 6 Advanced Configuration

6.1 QOS configuration

QOS (Quality of Service) refers to a network that can utilize various basic technologies to provide better service capabilities for specified network communications. It is a security mechanism of the network and a technology is used to solve network delays and congestion ect. Ethernet technology is the most widely used network technology today. At present, Ethernet has not only become the dominant technology in various independent LANs, but many Ethernet LANs have also become an integral part of the Internet. And with the continuous development of Ethernet technology, the Ethernet access method will become one of the main access methods for the majority of ordinary Internet users.

Therefore, to achieve an end-to-end network-wide QoS solution, it is inevitable to consider the problem of QoS service guarantee on Ethernet. This requires Ethernet switching equIPment to apply Ethernet QoS technology to provide different levels of QoS guarantee for different types of service flows, especially to support traffic flows that require high latency and jitter.

QOS part concept:

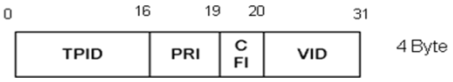
1.Traffic
Traffic, which is a traffic, refers to all packets passing through the switch.

2.Traffic classification
Traffic classification refers to the use of certain rules to identify packets that meet certain characteristics. The classification rule is a filtering rule configured by the configuration administrator according to the management requirements. It can be very simple. For example, the traffic with different priority characteristics can be identified according to the ToS field of the IP packet header. Integrated link layer (Layer 2), network layer (layer 3), transport layer (layer 4) information such as MAC address, IP protocol, source IP address, destination IP address, or application port number, etc. The text is classified, that is the complex flow classification rule. The general classification basis is limited to the header information of the encapsulated message,it is relatively rare to use the content of the message as the classification criterion.

3. Priority

3.1 802.1p Priority

The 802.1p priority is in the Layer 2 packet header. It is applicable to the case where Layer 3 packets are not required to be analyzed, but QoS is required in the Layer 2 environment.
As described in the VLAN Configuration section, each host that supports the 802.1Q protocol adds a 4-byte 802.1Q tag header to the source address in the original Ethernet frame header when sending a packet. As shown in Figure 1-1.

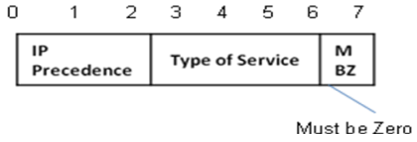


In the above figure, the PRI field is the 802.1p priority. It consists of 3 bits, ranging from 0 to 7. These 3 bits indicate the priority of the frame. There are a total of 8 priority levels, which are mainly used to preferentially send which packets when the switch is blocked.

Cos (Decimal)	Cos (Binary)	Meaning
0	000	spare
1	001	background
2	010	best-effort
3	011	excellent-effort
4	100	controlled-load
5	101	video
6	110	voice
7	111	network-management

3.2 IP priority, ToS and DSCP

In the IP header of an IPv4 packet, the Type of Service (TOS) field has 8 bits.
The Service Type (TOS) field includes a 3-bit IP precedence subfield, 4-bit TOS subfield and a 1-bit unused bit but must be set to 0. The 4-bit TOS represents: minimum delay, maximum throughput, maximum Reliability and minimum cost. Only one bit can be set at the same time in these 4 bits. If all 4bits are 0, then it means a general service.



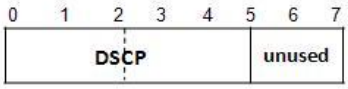
There are 8 priority levels for IP precedence.

IP Precedence (Decimal)	IP Precedence (Binary)	Meaning
0	000	routine
1	001	priority
2	010	immediate
3	011	flash
4	100	flash-override
5	101	critical
6	110	internet
7	111	network

The TOS priority has a total of 5 priority levels.

TOS (Decimal)	TOS (Binary)	Meaning
0	0000	normal
1	0001	min-monetary-cost
2	0010	max-reliability
4	0100	max-throughput
8	1000	min-delay

Soon after, RFC 2474 redefines the TOS field of the IP packet header, which is called the DS domain. The DSCP priority is represented by the first 6 bits (0-5 bits) of the domain, ranging from 0 to 63. The first 3 bits of the DSCP are used as class selectors, 4 to 5 bits are used to indicate the discarding priority, and the 6th bit is set to 0 to indicate that the device is a service class set by the DS model; the last two bits are reserved bits.



Expedited Forwarding (EF) class, which does not consider whether other traffic shares its link, and is suitable for low-latency, low-loss, low-jitter, and bandwidth-preferred services (such as virtual leased lines).

Assured Forwarding (AF) class is divided into 4 sub-categories (AF1/2/3/4). Each AF sub-class is divided into 3 discarding priorities, which can subdivide the level of AF service, AF. The QoS class of the class is lower than the EF class.

The Best Effort (BE) class is a special class in CS. There is no guarantee. After the AF class is overrun, it can be downgraded to BE class. The existing IP network traffic also defaults to this class.

DSCP	COS
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4

40-47	5
48-55	6
56-63	7

6.1.1 Configure QOS scheduling policies and weights

The QOS scheduling policy supports 4 types, SP (Strict-Priority Queueing), RR (Round Robin), WRR (weighted Round Robin), and WFQ (weighted fair queue).

When the network is congested, the problem that multiple packets compete for resources at the same time must be solved. Usually, queue scheduling is used to solve the problem. Commonly used queue scheduling algorithms include FIFS, SP Strict-Priority Queue scheduling, WRR Weighted Round Robin (WRR) scheduling, and SP+WRR scheduling.

FCFS (First Come First Serve) FIFO (First In First Out). The FIFO does not classify the packets. When the rate of the packets entering the interface is greater than the rate that the interface can send, the FCFS forwards the packets to the queue according to the order in which the packets arrive. Dequeue in the order of entering the team, advanced messages will be sent out first, and the incoming messages will be post-departed.

SP (Strict-Priority Queueing) queue scheduling is designed for mission-critical applications. An important feature of critical business is the requirement to prioritize access to services to reduce the latency of response when congestion occurs. The priority queue divides all packets into 8 categories (sequences of 7, 6, 5, 4, 3, 2, 1, 0), and their priorities are reduced in turn.

During queue scheduling, the SP preferentially sends packets in the higher priority queue in the order of priority from high to low. When the higher priority queue is empty, the packets in the lower priority queue are sent. In this way, the packets of the key service are put into the queue of the higher priority, and the packets of the non-critical service are put into the queue of the lower priority, so that the packets of the key service are preferentially transmitted, and the packets of the non-critical service are processed by the key service. The idle gap of data is transmitted.

The disadvantage of SP is that when congestion occurs, if there are packets in the higher priority queue for a long time, the packets in the low priority queue will "starve" due to

lack of service.

WRR queue scheduling divides each port into 8 output queues (sequences of 7, 6, 5, 4, 3, 2, 1, and 0 queues, which are sequentially reduced in priority), and the queues are scheduled in turn to ensure each The queues receive a certain service time. WRR can configure a weight value for each queue (w7, w6, w5, w4, w3, w2, w1, w0 in turn). The weighted value indicates the proportion of resources obtained. For example, if a 100M port is configured, its WRR queue scheduling algorithm has weighted values of 80, 70, 60, 50, 50, 40, 30, and 20 (corresponding to w7, w6, w5, w4, w3, w2, w1, w0, respectively. In this way, the lowest priority queue can obtain at least 5 Mbit/s bandwidth, which avoids the disadvantage that the packets in the low priority queue may not be served for a long time when the SP scheduling is used.

Another advantage of the WRR queue is that although the scheduling of multiple queues is round-robin, the service time slice is not fixedly allocated for each queue - if a queue is empty, then immediately switch to the next queue schedule, This bandwidth resource can be fully utilized.

In the SP+WRR queue scheduling, if the weighted value of the queue is set to 0, the queue performs a strict priority algorithm, otherwise it is the weighted value of the WRR queue.

WFQ has the same princIPle as WRR. The difference is that WRR uses pps to calculate queue weights, and WFQ uses bps to calculate queue weights. For example, a 100M port has a weighted value of 80, 70, 60, 50, 50, 40, 30, 20 for its WFQ queue scheduling algorithm (corresponding to w7, w6, w5, w4, w3, w2, w1, w0 in turn).), this ensures that the lowest priority queue gets at least 20/(80+70+60+50+50+40+30+20) * %100 bandwidth, where bandwidth is calculated using bits/Bytes, as above In the weight of each queue, the ratio of bits/Bytes of each queue export message is or is close to 8:7:6:5:5:4:3:2, that is, the exit bandwidth of the w0 queue is 5M.

SP+WFQ also calculates the queue weight according to bps.

Configure the scheduling policy:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configure scheduling policy	scheduler policy { rr | sp | wfq |wrr}	required

When the policy is configured as WFQ or WRR, you need to configure the weight ratio of each queue:

Configuration weight

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configure scheduling policy	scheduler policy { wfq |wrr} {w1, w2, w3, w4, w5, w6, w7}	optional
View configuration weights	show sched	--

6.1.2 Configuring queue mapping

The system maps between the 802.1p priority of the packet and the hardware queue priority. For each packet entering the switch, the system maps the priority to the specific hardware queue according to the 802.1p protocol priority in the packet.
By default, the mapping between 802.1p and hardware priority is as follows:

802.1p	Hardware priority queue
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

The mapping between the 802.1p priority and the output queue can be changed by changing the mapping between the 802.1p priority and the hardware queue.

Because the random scheduling algorithm is used for the queue scheduling in the chIP, if the two 802.1p priorities are mapped to the same hardware priority queue, the packets of the two 802.1p priorities cannot be forwarded 1:1.

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configuring queue mapping	cos map [cos pri]<0-7> [dscp pri] <0-7>	optional
View queue mapping configuration	show qos-map cos	--

6.1.3 Configure DSCP and COS mapping

The mapping between 802.1p and hardware priority is as follows:

DSCP	Hardware priority queue	DSCP	Hardware priority queue	DSCP	Hardware priority queue	DSCP	Hardware priority queue
0	0	16	2	32	4	48	6
1	0	17	2	33	4	49	6
2	0	18	2	34	4	50	6
3	0	19	2	35	4	51	6
4	0	20	2	36	4	52	6
5	0	21	2	37	4	53	6
6	0	22	2	38	4	54	6
7	0	23	2	39	4	55	6
8	1	24	3	40	5	56	7
9	1	25	3	41	5	57	7
10	1	26	3	42	5	58	7
11	1	27	3	43	5	59	7
12	1	28	3	44	5	60	7
13	1	29	3	45	5	61	7
14	1	30	3	46	5	62	7
15	1	31	3	47	5	63	7

The mapping between the DSCP priority and the output queue can be changed by changing the mapping between the DSCP priority and the 802.1p priority according to the actual network requirements.

The Dscp mapping is disabled by default. After the dscp-map is enabled, if the packets contain 802.1p and dscp, the dscp-map is used first.
Configure DSCP to correspond to the new DSCP, and then configure the queue.

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configure DSCP, new DSCP, COS	dscp map [source dscp] <0-63> [new dscp] <0-63> [cos]<0-7>	optional
View dscp-map	show qos-map dscp	--

6.1.4 Configuring the Port Default COS

The default COS of all ports is 0, and the hardware priority queue is configured.

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	Interface [port name]<eg.G1>	optional
Configure the port default COS	cos default [cos]<0-7>	

6.2 ACL configuration

ACL (Access Control List) is mainly used to implement flow identification. In order to filter packets, network devices need to configure a series of matching rules to identify the objects that need to be filtered. After specific object is identified, the corresponding data packet can be allowed or prohibited according to a preset policy.

The ACL classifies packets based on a series of matching conditions, such as the source address, destination address, and port number of the packet. The switch device detects the data packet according to the conditions specified in the ACL to determine whether to forward or drop the data packet. The packet matching rule defined by the ACL can also be referenced by other occasions that need to distinguish between traffic, such as the

definition of traffic classification rule in QoS.

According to the requirements, we set two types of ACLs, which are based on MAC address and IP address. Based on the MAC address ACL, supports 100 entries, each Entry supports 128 ACL rules, and all exist in parallel. Based on the IP address ACL, each of the 100 Entries is supported. Each Entry supports 128 ACL rules, and all exist in parallel. The action of each rule is divided into deny and permit. The deny indicates that the packet meets the following conditions to be discarded. The permit indicates that the packet that meets the following conditions is forwarded. The source MAC, and MAC mask, specifies that only the address that matches the source MAC and its mask will execute the previous action. The destination MAC, and the MAC mask, specifies that only the address that matches the destination MAC and its mask will execute the previous action. Time-rang is divided into cycle time and absolute time. The cycle time is divided into 7 days a week. The time period is selected. Only during the time period, the relative ACL Entry is executed. The absolute time is a time period. Come out, ACL Entry will be executed during this time period. Support does not add time-rang.

6.2.1 Configuring MAC Address-Based ACLs

Create a MAC ACL Entry:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Create a MAC-based ACL Entry	mac acl <1-100>	required

Add a simultaneous source MAC address under the Entry, destination MAC rule

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Create a MAC-based ACL Entry	mac acl <1-100>	required
Add rules	rule [id]<0-127> {permit | deny} [source MAC/source MAC Mask]{ (any|MM-MM-MM-MM-MM-MM/MM-MM-MM-MM-MM-MM)} [dst MAC/dst MAC Mask]	optional

	{(any|MM-MM-MM-MM-MM-MM/MM-MM-MM-MM-MM-MM)} {Time-Range}[.NAME]	

Delete a rule:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Create a MAC-based ACL Entry	mac acl <1-32>	required
Delete rule	no rule [id]<0-127>	optional

Delete an ACL Entry:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Create a MAC-based ACL Entry	no mac acl [id] <1-100>	required

View the configured ACL

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Create a MAC-based ACL Entry	show mac acl [id] <1-100>	optional

6.2.2 Configuring an IP Address Based ACL

The Entry ID indicates an ACL number. The IP-based ACL supports 899, and each ACL supports 128 rules. The actions include deny and permit. Support for handling some specific protocols like ICMP, IGMP, IP, TCP, UDP, etc., without filling means any. The source IP and mask function are matched with all source IPs set in the mask to execute the above actions. The destination IP and mask functions are matched with all destination IPs set in the mask execute the above action, without filling means any. The port number that supports the transport layer specific protocol. without filling means any. Time-range is used to specify the execution time. The above action is executed during the time-range effective time. without filling means it will take effect at any time.

Create an entry based on the IP address:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Create an IP-based ACL Entry	IP acl [id] <100-999>	optional

Delete an Entry based on IP address:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Create an IP-based ACL Entry	no IP acl [id] <100-999>	optional

Add an IP layer to filter the source IP/mask, destination IP/mask.

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Create an IP-based ACL Entry	IP acl <100-999>	required
Add rules	rule [id]<0-127> {permit | deny} [protocol] {ICMP|IGMP|IP} [sourceIP/sourceIPMask] { (any|MM-MM-MM-MM-MM-MM/MM-MM-MM-MM-MM-MM)} [dst IP/dst IP Mask] {(any|MM-MM-MM-MM-MM-MM/MM-MM-MM-MM-MM-MM)} [Time-Range] {.NAME}	optional

Add an application layer filter source IP/mask, destination IP/mask rule:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Create an IP-based ACL Entry	IP acl <100-999>	required
Add rules	rule [id]<0-127> {permit | deny} [protocol] {TCP|UDP} [sourceIP/sourceIPMask] { (any|MM-MM-MM-MM-MM-MM/MM-MM-MM-MM-MM-MM)} [dst IP/dst IP Mask] {(any|MM-MM-MM-MM-MM-MM/MM-MM-MM-MM-MM-MM)} [Time-Range] {.NAME}	optional

Add an application layer filter source IP/mask, destination IP/mask protocol port number rule:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Create an IP-based ACL Entry	IP acl <100-999>	required
Add rules	rule [id]<0-127> {permit | deny} [protocol] {TCP|UDP} [sourceIP/sourceIPMask] { (any|MM-MM-MM-MM-MM-MM/MM-MM-MM-MM-MM-MM)} [dst IP/dst IP Mask] {(any|MM-MM-MM-MM-MM-MM/MM-MM-MM-MM-MM-MM)} [protocol port]<0-65536> [Time-Range] {.NAME}	optional

View all IP-based ACLs

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
View based IP ACL Entry	show IP acl [id] <1-32>	optional

6.2.3 Configuration time-range

Configuration time-range，It can be divided into absolute time and periodic time. Absolute time is executed in a period of time, and periodic time is executed according to cycle time. First add a time-range name, then configure the time-range relative time or absolute time, or both configure together.

Create a Time-Range:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Create a Time-Range	time-range [name] { (Any character) }	optional

Time-Range Configure absolute time:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Create a Time-Range	time-range [name] { (Any character) }	optional
Configure absolute time	absolute start [time] { HH:MM YYYY-MM-DD} end [time] {HH:MM YYYY-MM-DD}	optional

Time-Range Configure periodic time :

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Create a Time-Range	time-range [name] { (Any character) }	optional
Configure periodic time	periodic [time] {HH:MM} to [time] {HH:MM} [day]{.DAY}	optional

Delete absolute time:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Create a Time-Range	time-range [name] { (Any character) }	optional
Delete absolute time	no absolute start [time] { HH:MM YYYY-MM-DD} end [time] {HH:MM YYYY-MM-DD}	optional

Delete periodic time:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Create a Time-Range	time-range [name] { (Any character) }	optional
Delete periodic time	no periodic [time] {HH:MM} to [time] {HH:MM} [day]{.DAY}	optional

View all Time-Range:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
View all time-range	show time-range	optional

Delete Time-Range:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
View all time-range	no time-range [name]	optional

6.2.1 Configuring ACL group

Bind Let a MAC-based ACL and an IP-based ACL bind to the port. Only bind to the port ACL is activated. The ACLs need to be activated before they take effect, and followed the rules of "first activate first effect" .

Create an ACL group and add the MAC to the ACL group:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name eg. G1)	required
Add MAC Entry to the ACL group	mac access-group [id] <1-100>	optional

Create a ACL group, Add IP to the ACL group:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name eg. G1)	required
Add IP Entry to the ACL group	IP access-group [id] <101-999>	optional

Remove MAC Entry from ACL group:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name eg. G1)	required
Remove MAC Entry from ACL group	no mac access-group [id] <1-100>	optional

Remove IP Entry from ACL group：

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Enter port mode	interface (port-name eg. G1)	required
Remove IP Entry from ACL group	no IP access-group [id] <1-32>	optional

6.3 SNMP Configuration

SNMP (Simple Network Management Protocol) is an important network management protocol on TCP/IP networks. It implements network management by exchanging packets on the network. The SNMP protocol provides the possibility of centralized management of large networks. Its goal is to ensure that management information is transmitted between any two points, making it easy for network administrators to retrieve information, make changes, find faults, and complete troubleshooting, capacity planning, and report generation at any node on the network. Its structure is divided into two parts: NMS and Agent. NMS (Network Management Station) is a workstation running a client program. Agent is a server-side software running on a network device. The NMS can send GetRequest, GetNextRequest, and SetRequest messages to the Agent. After receiving the NMS request message, the Agent performs a Read or Write Operation on the management variable according to the message type, and generates a Response message to return to the NMS. On the other hand, when the device generates an abnormality such as a cold/hot start, the agent will also send a trap message to the NMS to report the event.
The system supports three versions of SNMP v1, v2c, and v3. V1 provides a simple authentication mechanism, does not support administrator-to-administrator communication, and v1 Trap does not have an acknowledgment mechanism. V2c enhanced management model (security enhancement), management information structure, protocol Operation, communication between manager and manager, increased creation and deletion of tables, communication between managers, reduced agents The storage Operation of the party. V3 implements the user authentication mechanism and the message encryption mechanism, which greatly improves the security of the SNMP protocol. This function works with the network management software to log in to the switch and manage the switch.
SNMP (Simple Network Management Protocal)，Its predecessor is the SGMP protocol (Simple Gateway Monitoring Protocol), which is used to monitor and manage devices on the network. It is an application layer protocol.

Network management based on TCP/IP consists of two parts: the network manager (also called management process, manager) and the managed device (agent). The corresponding process of the managed device is called the agent process. The manager control box monitors a set of agents. Typically, the manager is the host and the agent is the router or server. The agent stores the relevant performance information in the database, and the manager can obtain or change the value of the database. The communication between the manager and the managed device mainly includes the following three aspects:

1. The manager requests the agent to obtain certain information.

2. The manager requests certain values in the proxy database from the proxy request to force the proxy to complete a task.

3. The agent sends a warning to the manager for an abnormal condition.
Three important components of network management: SMI, MIB, SNMP.

SMI: Management information structure. The main functions are: (1) defines the rules for object naming; (2) defines the type rules. (3) defines the encoding method.

MIB: Management information base, the main role is: the entity that defines the type object.
SNMP: Defines the packet format in which the manager interacts with the agent.

In order to better understand these three network management components. We compare it to a programming language: SMI is equivalent to syntax. The MIB is equivalent to the declaration and definition of the object, and SNMP is equivalent to the program code.

The following introduction is followed by several components.

SMI management information structure
SMI uses abstract syntax tag 1 (ASN.1 specified by ISO) to define the data type.
Object naming rules: The naming rules are agreed through the object naming tree. SMI uses the object identifier, and all objects managed by SNMP are given an object identifier. This object is for the iso.org.dod.internet.mgmt.mib-2 in the naming tree, and the number is 1.3.6.1.2.1. The object identifier begins with 1.3.6.1.2.1.

Type: Contains a simple data type (equivalent to C built-in types) and structured data types, while structured data types contain a sequence type (equivalent to the type defined by the struct in C) and a sequence of type (equivalent to an array in C)).
Coding method: SMI adopts BER (Basic Encoding Rules), and BER indicates that data can be represented by a trIPle (mark, length, value). Each data type corresponds to a unique tag and length, such as the corresponding flag of the integer INTEGER is 0000 0010. Its length is 4B. Available as 0000 0100.

MIB Management Information Base
The Management Information Base defines a collection of managed objects on the Internet. The following is a brief introduction to MIB2 (version number 2). Each agent has its own MIB2. Includes a collection of all objects that the manager can manage.
MIB2 includes: sys (system, system), if (iterface, interface), at (address translation. address translation), IP, ICMP, TCP, UDP, and SNMP.

How to access MIB variables? Take udp as an example. To analyze the access methods of simple variables and tables. First we must know the difference between variables and instances. We can think of variables as a naming convention, and an instance is an object. If the current node is a leaf node, it can be represented as a variable. If it is a non-leaf node, it corresponds to a table. For access to simple variables (such as udpInDatagrams) whose id is 1.3.6.1.2.1.7.1, the instance of the variable is id.0, which is 1.3.6.1.2.1.7.1.0. For access to the table, as in In our naming tree we have this branch udpTable-->udpEntry--->(udpLocalAddress,udpLocalPort). First say the corresponding number, udp corresponding 7, udpTable corresponding 5, udpEntry corresponding 1. udpLocalAddress corresponds to 1. udpLocalPort corresponds to 2, at any time. To access a particular instance (row) in the table, we should access the id+ index, where the index is the local IP/local port number, such as for socket 181.23.45.14.23. The method for obtaining its IP address is 1.3.6.1.2.1.7.5.1.1.181.23.45.14.23. The method for obtaining its port number is 1.3.6.1.2.1.7.5.1.2.181.23.45.14.23.
The important thing is. The instance identifiers (id+indexes) are arranged in lexicographic order. For the ordering of the tables, used the rules of "first column after row". That is to say, when visiting, first follow the order of the columns.

SNMP
The main role of the SNMP application is to enable the manager and agent to communicate with each other to achieve network management functions. SNMPv3 adds two features to the previous version number: different levels of security and remote management.

PDU: SNMPv3 defines 8 types of PDUs. Each is GetRequest, GetNextRequest, GetBulkRequest, SetRequest, Response, Trap, InformRequest, and Report.
GetRequest: The manager sends to the proxy to read the value of a variable or a set of variables.

GetNextRequest: The manager sends the agent to read the next variable value.

GetBulkRequest: The manager sends the proxy to the block request.

SetRequest: The manager sends the proxy to set the value of the variable.

Response: The agent sends the manager to respond to its request.

Trap: The agent is sent to the manager to report events.
InformRequest: The manager sends a remote manager. Get the value of some variables.

Report: The manager sends a remote manager. Report its errors.

UDPport used by SNMP
The proxy (equivalent to the server) uses 161, and the manager (equivalent to the proxy) uses 162.

Note: These two port numbers are only used to set the destination port number in the message when it is used to send packets to the other party. For passive response messages, the port number uses the temporary port number used by the active requestor.

6.3.1 SNMP System information configuration

Configure SNMP on/off. All users are blocked from access in the closed state:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Turn on/off SNMP	(no) snmp-server	optional

Configure the system name:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
(Restore default) Configure the SNMP system name	(no) snmp-server sysname [name]	optional

Configure location information:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
(Restore default) Configure SNMP location information	(no) snmp-server syslocation [LOCATION]	optional

Configure contact information:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
(Restore default) Configure SNMP contact	(no) snmp-server syscontact [CONTACT]	optional

Configuration alarm turned on:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Turn on/off SNMP trap	snmp-server trap [enable|disable]	optional

The engine number does not support modification.

View SNMP basic configuration information:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Display SNMP configuration information	show snmp-configuration	optional

6.3.2 SNMP Group information configuration

Group information is divided into groups and groups. The corresponding rights are different. Users who log in as a group can only access the device information and cannot modify the content. The writing community can not only access the device information, but also modify the device information and save it to the device.

Configure read group:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Modify read group information	snmp-server community ro [NAME.]	optional
Configure the default read community (default: public)	no snmp-server community ro[NAME.]	--

Configure the write group name:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Modify the write gruop information	snmp-server community rw [NAME.]	optional
Configure the default write group (default: private)	no snmp-server community rw [NAME.]	

The above configuration information is for V1 V2 users.

6.3.3 SNMPV3 User Configuration

V3 users also have two groups by default, read users and write users, and do not support adding new ones. V3 has added authentication function. The authentication methods are divided into: MD5 and SHA. The encrypted information is divided into: DES, AES.

Modify the SNMP V3 username:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configure V3 read/write user name	snmp-server user [ro|rw] [NAME.]	optional
Configure default read/write user name	no snmp-server user [ro|rw] [NAME.]	--

Configure the V3 user authentication mode and password:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configure the V3 user authentication mode and password.	snmp-server user [ro|rw] [NAME.] v3 [MD5|SHA] [authentication protocol] [AUTHENTICATION] [AES|DES] [privacy protocol] [PRIVACY]	optional

6.3.4 SNMP warning

Add a message report address. When an illegal user logs in to the device, a warning message is sent to the report address. The report message is classified as V1 V2C. Both can capture the corresponding report message.

Configure the source address based on the V1 trap report:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configure the source address based on the V1 trap report:	snmp-server trapsink [A.B.C.D]	optional

Configure the source address based on the V2C trap report:

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configure the source address based on the V2c trap report	snmp-server trap2sink [A.B.C.D]	optional

6.4 RMON Configuration

RMON was originally designed to solve the problem of managing local and remote sites from a central point. The RMON specification is an extension of the SNMP MIB. In RMON, network monitoring data contains a set of statistics and performance metrics that are exchanged between different monitors (or probes) and console systems. The resulting data can be used to monitor network utilization for network planning, performance optimization, and assist with network error diagnostics.

There are currently two versions of RMON: RMON v1 and RMONv2. RMON v1 can be found in the widely used network hardware. It defines 9 MIB groups to serve basic network monitoring. RMON v2 is an extension of RMON, focusing on higher traffic layers above the MAC layer. It mainly emphasizes IP. Traffic and application layer traffic. RMON v2 allows network management applications to monitor all network layer packets, unlike RMONv1, which only allows monitoring of MAC and its underlying packets.

The RMON monitoring system consists of two parts: a detector (agent or monitor) and a management station. The RMON agent stores network information in the RMON MIB, which is directly implanted into network devices (such as routers, switches, etc.), and the agent can also be a program running on a PC. The agent can only see the traffic flowing

through them, so the RMON agent is set in each monitored LAN segment or WAN link point, and the network management workstation uses SNMP to obtain RMON data information.

There are currently two versions of RMON: RMON v1 and RMONv2. RMON v1 can be found in the widely used network hardware. It defines 9 MIB groups to serve basic network monitoring. RMON v2 is an extension of RMON, focusing on higher traffic layers above the MAC layer. It mainly emphasizes IP. Traffic and application layer traffic. RMON v2 allows network management applications to monitor all network layer packets, unlike RMONv1, which only allows monitoring of MAC and its underlying packets.

The RMON monitoring system consists of two parts: a detector (agent or monitor) and a management station. The RMON agent stores network information in the RMON MIB, which is directly implanted into network devices (such as routers, switches, etc.), and the agent can also be a program running on a PC. The agent can only see the traffic flowing through them, so the RMON agent is set in each monitored LAN segment or WAN link point, and the network management workstation uses SNMP to obtain RMON data information.

6.4.1 Configuring RMON event groups

Operation	Command	Remarks
Enter enable mode	enable	required
Configuring RMON event groups	configure terminal	required
Configuring RMON event groups	rmon event <0-1024> DESCRPTHION (none|log|trap|logtrap)	optional
Delete the RMON event group	no rmon alarm <0-1024>	--

6.4.2 Configure the RMON statistics group.

Operation	Command	Remarks
Enter enable mode	enable	required
Configure the RMON statistics group.	configure terminal	required
Configure the RMON statistics group.	rmon statistics <0-1024> IFNAME	optional
Delete the RMON statistics group.	no rmon statistics <0-1024>	--

6.4.3 Configuring the RMON history group

Operation	Command	Remarks
Enter enable mode	enable	required
Enter global configuration	configure terminal	required
Configuring the RMON history group	rmon history <0-1024> IFNAME <5-65535> <0-100>	optional
Delete the RMON history group	no rmon history <0-1024>	--

6.4.4 Configuring the RMON warning group

Operation	Command	Remarks
Enter enable mode	Enable	required
Enter global configuration	configure terminal	required
Configuring the RMON warning group	rmon alarm <0-1024> IFNAME <3-19> <5-65535> (absolute|delte) <0-4294967295> <0-4294967295> <0-1024> <0-1024>	optional
Delete RMON warning group	no rmon alarm <0-1024>	--

6.5 LLDP Configuration

LLDP is a proximity discovery protocol. It defines a standard way for Ethernet network devices, such as switches, routers, and Wireless access points, to notice its exit to other nodes in the network and to store discovery information for each proximity devices. such as device configuration and device identification can be noticed using this protocol.

Specifically speaking, LLDP defines a common announcement information set, a protocol for transmitting announcements, and a method for storing received announcement information. A device that notice its own information may transmit multiple pieces of announcement information in a LAN packet, transmission form is Type Length Value (TLV) field.

Working mode:

TxRx: Sends and receives LLDP packets.

Tx: Sends LLDP packets only.
Rx: Receives LLDP packets only.
Disable: neither sends nor receives LLDP packets.

When the LLDP working mode of a port changes, the port initializes the protocol state machine. In order to avoid the port working mode changing frequently and causing the port perform initialization Operations continuously, the port initialization delay time can be configured, after the port working mode is delayed for a period of time, then initialization Operation is performed.

6.5.1 Configuration LLDP global information

LLDP global configuration:

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
Configuration LLDP enable/disable	lldp (enable|disable)	--

Configuration LLDP packet sending interval.:

Operation	Command	Remark
Enter into global configuration	enable	required
Enter into global configuration	configure terminal	required
Configuration LLDP packet sending interval	lldp tx-interval <5-32768>	--
Configuration default LLDP packet sending interval	no lldp tx-interval	

Configuration LLDP packet transmission delay time:

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
Configuring LLDP packet transmission delay time	lldp tx-delay <1-8192>	--
Configuring default LLDP packet transmission delay time	no lldp tx-delay	

Configuration device information to hold multiples:

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
Configure device information to hold multiples interval	lldp tx-hold <2-10>	--
Configure default device information to hold multiples	no lldp tx-hold	--

Configuration interface initialization delay:

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
Configuration interface initialization delay	lldp reinit-delay <2-5>	--
Configuration default interface initialization delay	no lldp reinit-delay	--

Configuration management address:

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
Configuration management address	lldp management-address A.B.C.D	--
Delete management address	no lldp management-address	--

Configure TLV to send optional:

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
Configure TLV to send optional	lldp tlv-select (management-address |port-descrIPtion|system-capabilities| system-descrIPtion|system-name)	--

Configure default TLV to send optional	no lldp tlv-select (management-address| port-descrIPtion|system-capabilities| system-descrIPtion|system-name)	--

View global configuration information:

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
View global configuration information	show lldp global	--

6.5.2 Configure LLDP port information.

Configure port enable/disable transmit:

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
Enter into interface mode	interface (portname eg.G1 G2)	--
Configure port enable/disable transmit	(no)lldp transmit	--

Configure port enable/disable receive:

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
Enter into interface mode	interface (portname eg.G1 G2)	--
Configure port enable/disable receive	(no)lldp receive	--

View LLDP port configuration information:

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
View LLDP port configuration information	show lldp interface	--

6.5.3 View current neighbor information

View current statistics to the neighbor information:

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
View current neighbor information	show lldp neighbors	--

View all port statistics information:

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
View all port statistics information	show lldp traffic	--

6.6 SNTP configuration

The time of the switch system can be implemented in two ways. One is to automatically synchronize the time from the sntp server as the sntp client; the other is the administrator's own configuration.

Simple Network Time Protocol (SNTP) is used for time synchronization between network devices. Usually, there is one SNTP server in the network, and provides reference time for multiple SNTP clients, and finally achieves time synchronization between all network devices.

SNTP can work in four modes: unicast, broadcast, multicast, and anycast.

In unicast mode, the client sends a request to the server. After receiving the request, the server sends a response packet to the client according to the local time.

In broadcast and multicast mode, the server periodically sends broadcast or multicast packets to the client, and the client passively receives the packets from the server.
In anycast mode, the client sends a request by using the local broadcast address or multicast address actively. At this time, the server in the network responds to the client. The client selects the response packet first as the server and discards the other server.

After the server sends the packet, the working mode is the same as the unicast.

In all modes, the client parses the message after receiving the response message to obtain the current standard time, and calculates the network transmission delay and local time compensation through a certain algorithm, and uses the data to calibrate the current time.

6.6.1 SNTP global configuration

Enable / Disable SNTP Client

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
Enable / Disable SNTP Client	sntp {enable | disable}	-
View SNTP client configuration	show sntp	--
View the current time	show clock	--

Configuration automatic synchronization interval:

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
Configuration automatic synchronization interval	sntp auto-sync timer <5-65535>	--
View the current time	show clock	--

Configuration timezone:

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
Configuration timezone	timezone (UCT12|UCT11|UCT10|UCT9|UCT8|UCT7 |UCT6|UCT5|UCT4|UCT3|UCT2|UCT1|UC T|UCT-1 |UCT-2|UCT-3|UCT-4|UCT-5|UCT-5:30|UCT-5:45|	--

	UCT-6|UCT-6:30|UCT-7|UCT-8|UCT-9|UCT-9:30 |UCT-10|UCT-11|UCT-12|UCT-13)	
View the current timezone	show timezone	--

6.6.2 SNTP server configuration

You can test the selected address before configuration the server.:

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
Test the selected server connection status	sntp connect A.B.C.D	--

Configuration an SNTP server

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
Configuration an SNTP server	sntp unicast-server A.B.C.D	--
Delete an SNTP server	no sntp unicast-server A.B.C.D	--
View SNTP configuration	show sntp	--

6.7 Attack Defense Configuration

Distributed Denial of Service (DDoS) attacks refer to the use of client/server technology to combine multiple computers as an attack platform to launch DDoS attacks on one or more targets, thereby multIPlying denial of service attacks. power. Typically, an attacker uses a theft account to install the DDoS host program on a computer. At a set time, the master program communicates with a number of agents that have been installed on many computers on the network. The agent launches an attack when it receives an instruction. With client/server technology, the master can activate hundreds or thousands of agents in seconds.

There are many ways to attack DDoS. The most basic DoS attack is to use a reasonable service request to occupy too many service resources, so that legitimate users can not get the response of the service. A single DoS attack generally adopts a one-to-one approach. When the target CPU speed is low, the memory is small, or the network bandwidth is small, and the performance is not high, the effect is obvious. With the development of computer and network technology, the processing power of computers has increased rapidly, memory has increased greatly, and gigabit-level networks have emerged. This has made the difficulty of DoS attacks more difficult - the target's ability to digest the malicious attack packets. "Strengthened a lot. At this time, distributed denial of service (DDoS) attacks came into being.

Enable anti-DDOS attack:

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
Enable/Disable anti-DDOS attack	(no) system protection ddos	--

Enable ignored ICMP-echo package

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
Enable/Disable ignored ICMP-echo package	(no) system ignore icmp-echo	--

Section 7 System Configuration

7.1 Modify user password

Note that you can modify user password, but modifying the user name and adding users is not supported.

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
Modify user password	username WORD password WORD	--
Return to enable mode	exit	--
View the current user	show user	--

Because of the modification of the username is not supported, the username needs to be entered into the switch for the password to be changed.

7.2 Network Configuration

Support for modifying IPV4, IPV6 addresses, gateways, and DNS servers.

Manually modify the IPV4 address:

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
Enter into interface mode	interface VLANIF-NAME eg.VLANif1	--
Modify the IPV4 address	IP address A.B.C.D/M	--
Delete the IPV4 address	no IP address A.B.C.D/M	--
Return to global mode	exit	--
View current IP address	show zebra interface	--

The above method modifies the IPV4 address, and the previous IP address is not replaced.

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
enter into interface mode	interface VLANIF-NAME eg.VLANif1	--
modify the IPV4 address	IP address old_IP A.B.C.D/M new_IP A.B.C.D/M	--
delete the IPV4 address	no IP address A.B.C.D/M	--
Return to global mode	exit	--
View current IP address	show zebra interface	--

The above method can modify the current IP and delete the old IP.

Configuration IPV4 gateway:

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
enter into interface mode	interface VLANIF-NAME e.g.VLANif1	--
modify the IPV4 gateway	IP default gateway A.B.C.D	--
Return to global mode	exit	--
View current IP address	show zebra interface	--

Configuration IPV4 DNS server:

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
Configuration IPV4 DNS server	dns server A.B.C.D	-
Delete DNS server	no dns server A.B.C.D	
View DNS server	show dns	--

Support two servers, one primary DNS server, one alternate DNS server.

Automatically obtain IPV4 address

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
Enter into interface mode	interface VLANIF-NAME eg.VLANif1	--
Enable automatically obtain IPV4 address	IP address DHCP	--
Disable automatically obtain IPV4 address	no IP address DHCP	--
Return to global mode	exit	--
View current IP address	show zebra interface	--

Manually configure the IPV6 address:

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
Enter into interface mode	interface VLANIF-NAME eg.VLANif1	--
Modify IPV6 address	IPv6 address X:X::X:X/M	--
Delete IPV6 address	no IPv6 address X:X::X:X/M	--
Return to global mode	exit	--
View current IP address	show zebra interface	--

Configuration IPV6 gateway:

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
Enter into interface mode	interface VLANIF-NAME eg.VLANif1	--
Modify IPV6 gateway	IPv6 default gateway A.B.C.D	--
Return to global mode	exit	--
View current IP address	show zebra interface	--

IPV6 dynamic obtain is not yet supported.

7.3 Service configuration

Service configuration can be configured to enable/disable Telnet, SSH enable/disable, HTTP service (i.e. support http or https, or http and https).

Configuration Telnet service:

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
Configuration Telnet service	IP telnetd (enable|disable)	--

Configuration SSH service:

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
Configuration SSH service	IP ssh-server (enable|disable)	--

Configuration HTTP service:

Operation	Command	Remark
Enter into enable mode	enable	required
Enter into global configuration	configure terminal	required
Configuration HTTP service	IP http-server (http|https|both|none)	--

7.4 Configuration management

The configuration management support configuration saves and restores the default configuration. Currently, the load configuration is not supported.

Operation	Command	Remark
Enter into enable mode	enable	required
Save, reset configuration	system config (save|load|restore)	--

7.5 Diagnostic test

For the test support for IPV4, IPV6 address ping, traceroute test. At the same time, it supports network cable detection (used to detect whether the network cable is inserted on the selected port, the error is ±10m). Configuration ping test:

Operation	Command	Remark
Enter into enable mode	enable	required
Ping test	ping WORD (IPV4/IPV6 address)	--

Configuration traceroute test:

Operation	Command	Remark
Enter into enable mode	enable	required
Traceroute test	traceroute WORD (IPV4/IPV6 address)	--

7.6 Restart system

Operation	Command	Remark
Enter into enable mode	enable	required
Reboot device	reboot	-