TP-SW8GBT/AT/PSV-U

L2 Managed 10 Port PoE Switch

CLI-based Configuration Guide

V3.0 20240605

About This Document

This product includes three documents as the table below.

Documents	Description	How to get it
Quick Guide	Including product introductions and installation steps.	In the packing box
Web-based Configuration Guide	Including Web network management system configuration instructions.	tyconsystems.com
CLI-based Configuration Guide	Including CLI-based configuration instructions	tyconsystems.com

This document is **CLI-based Configuration Guide**, including CLI-based configuration instructions. It is intended for engineers or anyone who needs to configure the device by command line parameters.

The configuration instructions here take 24 ports switch as example. If there is inconsistency between the instruction (eg. port number) and the actual product, please refer to the actual product.

Announcement

The information in this document is subject to change without notice.

The document is only used as operation guide. No warranties of any kind, either express or implied are made in relation to the description, information or suggestion or any other contents of the manual.

The images shown here are indicative only. If there is inconsistency between the image and the actual product, the actual product shall govern.

Command line conventions

The command line conventions that may be found in this document are defined as follows.

Convention	Description
Key word	The keywords of a command line are underlined in light blue, not in boldface.
Parameters	Command arguments are underlined in dark, not in boldface.

Change History

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

Version	State	Release Date	Description
V1.0	Released	2020-04-27	Initial commercial release.
V2.0	Released	2020-12-07	Correcting the command lines descriptions and adding “examples” and “checking the configuration” contents.
V3.0	Released	2024-06-05	Add new requirement specifications.

Content

1 Login Through the Console Port

To configure a device that is powered on for the first time, log in to the device through the console port.

A main control board provides a console port. To configure a device, connect the user terminal serial port to the device console port.

After the device is powered on for the first time, you can log in to it from a PC through the console port to configure and manage the device.

1.1 Pre-configuration Tasks

Before logging in to the device through the console port, complete the following tasks:

Preparing the console cable

Installing the terminal emulation software on the PC

> **Note:**
>
> Users can use the built-in terminal emulation software (such as the HyperTerminal of Windows 10/11) on the PC. If no built-in terminal emulation software is available, use the third-party terminal emulation software.

1.2 Configuration Procedure

Use the terminal emulation software to log in to the device through the console port, and complete the basic configuration for the device.

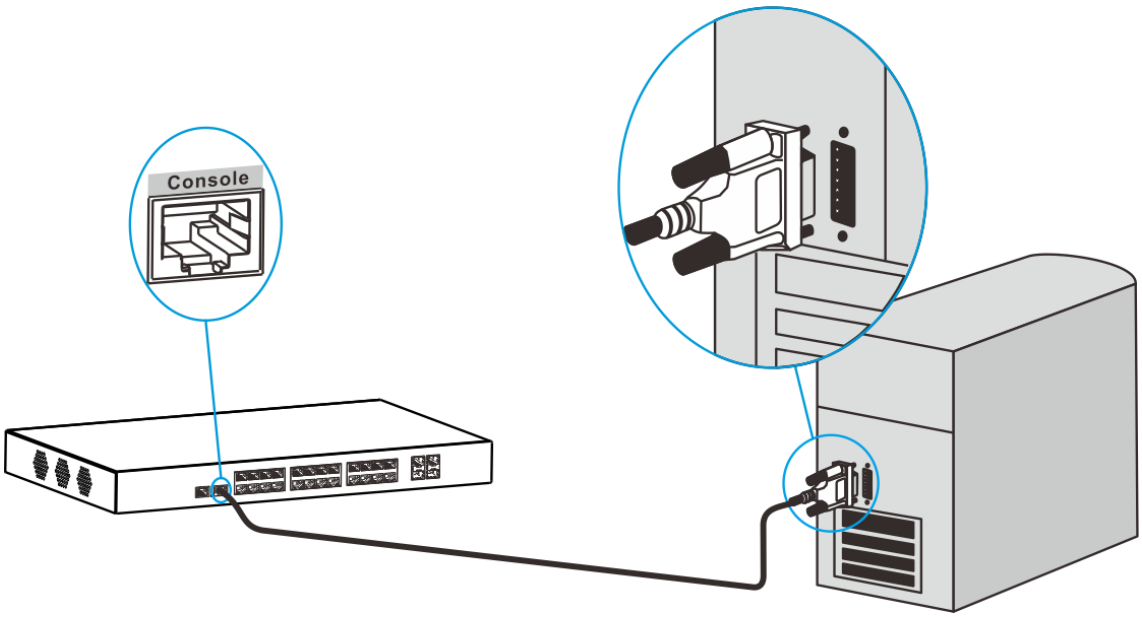
Default configuration

Data	Default value
Transfer rate	115200 bit/s
Flow control mode	Not support
Test mode	Not support
Stop bits	1
Data bits	8

Procedure

Use the terminal emulation software to log in to the device through the console port.

Insert the SUB-D9 connector of the console cable delivered with the product to the 9-pin serial port on the PC, and insert the RJ-45 connector to the console port of the device, as shown in the following figure.



Start the HyperTerminal (Microsoft Windows) or Terminal (Mac OS), and create a connection, set the connection port and communication parameter.

Note:

There are several ports on the PC, the one to be connected here is the port connecting with Console cable. Normally select the port COM1.

If the communication parameter for the serial port of the device is changed, please set the communication parameter in the PC the same value, and reconnect.

Enter until the following information is displayed.

```
User Access Verification!
Username:
```

Enter the default user name and password.

username: admin

password: admin

1.2.1 Configure Cable Connection

The way of cable connection and configuration of DIN rail switch is the same as that of rack type switch. Take DIN rail switch as an example here.

When the switch is configured through the terminal, the connection steps of cable configuration are as follows.

- Connect the SUB-D9 plug of the configured cable to the serial port of the PC to be configured for the switch.
- Connect the RJ-45 end of the configuration cable to the console port of the switch.

2 Cli Overview

2.1 Command Line Interface

The command line interface (CLI) is an interactive interface between a user and a device. A user can enter commands on the CLI to configure and manage a device and view the output of commands to verify the configuration.

Users can configure a device by clicking options in the graphical user interface (GUI), and also can enter more abundant commands in the CLI. The CLI is as follows:

```
User Access Verification!
username: admin
password: admin
```

Input default username and password, login the CLI. Users can enter commands on the command line interface to configure and manage a device.

2.2 Entering Command Views

After successful login, enter “?” or “help” to enter the users view. The command lines under this mode are displayed as followed.

The device provides various configuration commands and query commands to manage and maintain products. To facilitate the use of these commands, they must be classified into groups. Command line interfaces (CLIs) are classified into several command line views. All commands must be executed in command line views. Before a command is executed, the command line view where the command resides is displayed. Command views apply to different configurations.

Following with the main command views list of the device.

Views	How to enter	Description
Users view	When a user logs in to the device, the user enters the user view.	In the user view, users can view the running status and statistics of the device.
Enable view	Enter users view. · Run: enable · Enter	In the enable view, users can look up and set the system parameters of the device, and enter other function views from this view.
Config view	Enter enable view. · Run: config · Enter	In the config view, users can set the global configuration of the device.
Interface view	Enter config view. · Run: interface interface type interface number · Enter	Users can configure interface parameters in the interface view. The interface parameters include physical attributes, link layer protocols, and IP addresses. Run the interface command and specify an interface type and number to enter an interface view.

3 Checking the Configuration

After configuration, users can run the show command to check the configuration and running information on the device.

```
Switch_config# show ?
  access-list          -- Named access-list
  aggregator-group     -- Link Aggregation information
  clock                -- current time
  exec-timeout         -- The EXEC timeout
  flow_interval        -- The flow_interval
  history              -- History command
  interface            -- Interface status and configuration
  IP                   -- IP Configuration information
  lldp                 -- Show the lldp information
  logging              -- Show the contents of logging buffers
  loopback-status      -- show loopback port status
  mac                  -- MAC configuration
  memory               -- Memory information
  mirror               -- Show a mirror session
  mst-config           -- Show the configuration of MST
  ntp                  -- Ntp infomation
  policy-map           -- Show policy-map
  process              -- Processes information
  running-config       -- Current configuration
  spanning-tree        -- Display spanning-tree state
  startup-config       -- Startup configuration
  ssh                  -- The LINES connected in
  telnet               -- Show incoming telnet connection
  version              -- Device version information
```

4 Interface Management Configuration

Interfaces of a device are used to exchange data and interact with other network devices. Interfaces are classified into management interface, physical interface, and logical interfaces as followed.

Interfaces	Description
Management interface	Management interfaces are used to log in to devices. Users can use management interfaces to configure and manage devices. Management interfaces do not transmit service data.
Physical interface	Physical interfaces exist on interface cards and transmit service data.
Logical interfaces	Logical interfaces are manually configured and do not physically exist. They can be used to exchange data and transmit service data.

4.1 Choose Port Range

Before configuring the port, first choose the port range that need to be configured.

Command	Interface interface type interface number
Parameter Descriptions	· interface type : interface type, including GigaEthernet -- GigaEthernet interface TenGigaEthernet -- TenGigaEthernet interface · interface number: interface number, in the format as “0/port number”, the value of port number value is the port number of the switch.
Procedure	· Enter interface view. Run: Interface interface type interface number Enter
Example	Switch> enable Switch# config Switch_config# interface gigaethernet 0/24 switch_config_g0/24#

4.2 Enable/Disable Port

The port is off by default. Using the command line, users can enable the port.

Command	no shutdown
Parameter Descriptions	Null
Procedure	· Enter interface view. Run: Interface gigaEthernet 0/24 Enter · Run: no shutdown Enter
Example	switch_config_g0/24# no shutdown switch_config_g0/24#

· Disable the port

Command	shutdown

Parameter Descriptions	Null
Procedure	· Enter interface view. Run: Interface gigaEthernet 0/24 Enter · Run: shutdown Enter
Example	switch_config_g0/24# shutdown switch_config_g0/24#

4.3 Configure Port

· Change port description

Command	description description
Parameter Descriptions	· dsescription: The description of the port, supporting 31-string. No default value.
Procedure	· Enter interface view. Run: description description Enter
Example	switch_config_g0/24# description switch 1 switch_config_g0/24#

· Configure port speed

Command	speed speed
Parameter Descriptions	· speed: the speed of the port, supporting 10M, 100M, 1000M. The device speed is auto by default.
Procedure	· Enter interface view. Run: speed speed Enter.
Example	switch_config_g0/24# speed 1000 switch_config_g0/24#

· Switch the port speed to auto

Command	speed auto
Parameter Descriptions	Null
Procedure	· Enter interface view. Run: speed auto Enter.
Example	switch_config_g0/24# speed auto switch_config_g0/24#

4.4 Configure Duplex Mode

The device is working in auto-duplex mode by default.

Using the command line, users can switch the mode by Auto, Full and Half.

Command	duplex auto duplex Full duplex Half
Parameter Descriptions	Null
Procedure	· Enter interface view. Run: duplex auto Enter
Example	switch_config_g0/24# duplex auto switch_config_g0/24# switch_config_g0/24# duplex full switch_config_g0/24# switch_config_g0/24# duplex half switch_config_g0/24#

4.5 Configure Rate Limit

Configure the rate-limit of ingress and egress ports.

· Configure port rate-limit ingress

Command	switchport rate limit speed ingress
Parameter Descriptions	· speed: Limit the rate of port(Kbps), the value ranges from 64~1000000.
Procedure	· Enter interface view. · Run: switchport rate-limit speed ingress Enter
Example	Switch_config_g0/24# switchport rate-limit 1000 ingress Switch_config_g0/24#

· Configure port rate-limit egress

Command	Switchport rate-limit speed egress
Parameter Descriptions	· speed: Limit the rate of port(Kbps), the value ranges from 64~1000000.
Procedure	· Enter interface view. · Run: switchport rate limit speed egress Enter
Example	Switch_config_g0/24# switchport rate-limit 1000 egress Switch_config_g0/24#

4.6 Storm Control Configuration

Storm control prevents broadcast storms.

When receiving broadcast packets, multicast packets, and unknown unicast packets, the Switch forwards the packets to other Layer 2 Ethernet interfaces in the same VLAN. This is because the switch cannot determine the outbound interface based on destination MAC addresses of packets. In this case, broadcast storms may occur on the network and forwarding performance of the switch deteriorates.

Storm control can control these packets and prevent broadcast storms.

· Configuring broadcast packets

Command	storm-control broadcast threshold packet storm control
Parameter Descriptions	· packet storm control: ranges from 1 to 1000, the unit is 64kbps.
Procedure	· Enter interface view. Run: storm-control broadcast threshold packet storm control Enter
Example	switch_config_g0/24# storm-control broadcast threshold 100 switch_config_g0/24#

· Configuring multicast packets

Command	storm-control multicast threshold packet storm control
Parameter Descriptions	· packet storm control: ranges from 1 to 1000, the unit is 64kbps.
Procedure	· Enter interface view. · Run: storm-control multicast threshold packet storm control Enter
Example	switch_config_g0/24# storm-control multicast threshold 100 switch_config_g0/24#

· Configuring unicast packets

Command	storm-control unicast threshold packet storm control
Parameter Descriptions	· packet storm control: ranges from 1 to 1000, the unit is 64kbps.
Procedure	· Enter interface view. · Run: storm-control unicast threshold packet storm control Enter
Example	switch_config_g0/24# storm-control unicast threshold 100 switch_config_g0/24#

4.7 Configure Flow Control

The flow control function is off by default.

Using the command, users can turn it off or on.

Command	flow-control on/off
Parameter Descriptions	Null
Procedure	· Enter interface view. Run: flow-control on Enter.
Example	switch_config_g0/24# flow-control on switch_config_g0/24# switch_config_g0/24# flow-control off switch_config_g0/24#

4.8 Configure Port Isolation

The port isolation mode is normal by default.

Using the command line, users can isolate the physical ports.

Command	switchport protected
Parameter Descriptions	Null
Procedure	· Enter interface view. Run: switchport protected Enter
Example	switch_config_g0/24# switchport protected switch_config_g0/24#

4.9 Configure Jumbo Frame Size

The port maximal supports 13000 bytes for Jumbo Frame.

Using the command line, users can change the size.

Command	mtu jumbo size
Parameter Descriptions	· Size: the jumbo frame size, ranges from 1522~13000 bytes.
Procedure	· Enter interface view. Run: mtu jumbo size Enter
Example	switch_config_g0/24# mtu jumbo 9000 switch_config_g0/24#

4.10 Clear Interface Traffic Statistics

To monitor the status of an interface or locate faults on the interface, collect traffic statistics on the interface. Before collecting traffic statistics on an interface within a period, clear the existing traffic statistics on this interface.

Interface statistics cannot be restored after they are cleared. Please confirm your action before you perform the operations.

· Clearing Interface Traffic Statistics

Command	clear counters
Parameter Descriptions	Null
Procedure	· Enter enable view. Run: clear counters Enter.
Example	Switch# clear counters Switch#

4.11 Link Aggregation Configuration

Link aggregation is a technology that bundles a group of physical interfaces into a logical interface to increase link bandwidth.

As the network scale expands increasingly, users propose increasingly higher requirements on the bandwidth and reliability of backbone links. Traditional technologies often use high-speed cards or devices supporting high-speed interface cards to increase the bandwidth. This method, however, is costly and inflexible.

Through the three operations, users could bundles a group of physical interfaces into a logical interface to increase link bandwidth.

Following will describe the command lines and procedures of the three operations.

· Creating link aggregator group

Command	interface port-aggregator INTERFACE
Parameter Descriptions	INTERFACE: <1-6> -- Port-aggregator interface number
Procedure	· Enter interface view. Run: interface truck-name INTERFACE Enter.
Example	switch_config_g0/7# interface port-aggregator 2 switch_config_g0/7 interface port-aggregator 2 switch_config_t2#

· Configuring load pattern mode of link aggregator group

Command	aggregator-group load-balance mode
Parameter Descriptions	· mode: The load balance modes, including 1) src-mac 2) dst-mac 3) both-mac 4) src-ip 5) dst-ip 6) both-ip 7) src-port 8) dst-port

Procedure	· Exit and enter config view. Run: aggregator-group load-balance mode Enter

· Configuring working mode of link aggregator group and members of link aggregator group

Command	aggregator-group GROUPID
Parameter Descriptions	· GROUPID: <1-8> -- Aggregator group number
Procedure	· Enter interface view. Run: aggregator-group GROUP Enter.
Example	switch_config# interface gigaethernet 0/24 switch_config_g0/24# aggregator-group 1 switch_config_g0/24#
Command	port link-aggregation group MODE
Parameter Descriptions	Null
Procedure	· Enter interface view. Run: Enter.
Example	switch_config# interface gigaethernet 0/24 switch_config_g0/24# port link-aggregation group auto switch_config_g0/24#

· Checking the configuration.

Command	show aggregator-group summary
Parameter Descriptions	Null
Procedure	· Enter interface view. Run： show aggregator-group summary Enter
Example	switch_config_g0/7# show aggregator-group summary Flags: D - down A - Use In port-aggregator U - Up I - Not In port-aggregator Group mode Port-aggregator Ports -----+---------+----------------+------------------------------ 1 lacp Po1(D) 2 Po2(D) 3 static Po3(D) G0/7(DI) switch_config_g0/7#

4.12 VLAN Configuration

The VLAN technology enables a physical LAN to be divided into multiple broadcast domains, each

of which is called a VLAN.

The Ethernet technology is used to share communication media and data based on the Carrier Sense Multiple Access/Collision Detection (CSMA/CD). If there are a large number of hosts on an Ethernet network, collision becomes a serious problem and can lead to broadcast storms. Switches can be used to connect LANs, preventing collision. However, broadcast packets cannot be isolated.

The VLAN technology divides a physical LAN into multiple broadcast domains, each of which is called a VLAN. Hosts within a VLAN can communicate with each other, while hosts in different VLANs cannot communicate with each other directly. Therefore, the broadcast packets are limited in each VLAN.

The device supports port-based VLAN assignment function. Users in the same VLAN can communicate with each other.

· Choose the port range.

Command	Interface interface type interface number
Parameter Descriptions	· interface type : interface type, including GigaEthernet -- GigaEthernet interface TenGigaEthernet -- TenGigaEthernet interface · interface number: interface number, in the format as “0/port number”, the value of port number value is the port number of the switch.
Procedure	· Enter interface view. Run: interface gigaEthernet 0/port number Or run: interface ten gigaEthernet 0/port number Enter
Example	Switch_config# interface gigaEthernet 0/24 Switch_config_g0/24#

· Configure the port mode

Command	switchport mode mode
Parameter Descriptions	· mode : Switch port modes, including 1) access, Access mode 2) trunk, Trunk mode
Procedure	· Enter interface view. Run: switchport mode mode Enter
Example	Switch_config_g0/24# switchport mode trunk Switch_config_g0/24#

· Configure PVID

Command	switchport pvid VLAN ID
Parameter Descriptions	· VLAN ID: VLAN ID of the VLAN, ranges from 1~4094
Procedure	· Enter interface view. Run: switchport pvid VLAN ID

	Enter
Example	Switch_config_g0/24# switchport pvid 10 Switch_config_g0/24#

· Configure port vlan-allowed

Command	switchport trunk vlan-allowed VLAN ID
Parameter Descriptions	· VLAN ID: VLAN ID range is 2~100
Procedure	· Enter interface view. Run: switchport trunk vlan-allowed VLAN ID Enter
Example	Switch_config_g0/24# switchport trunk vlan-allowed 12 Switch_config_g0/24#

· Configure port vlan-untagged

Command	switchport trunk vlan-untagged VLAN ID
Parameter Descriptions	· VLAN ID: VLAN ID range is 10~50
Procedure	· Enter interface view. Run: switchport trunk vlan-untagged VLAN ID Enter
Example	Switch_config_g0/24# switchport trunk vlan-untagged 13 Switch_config_g0/24#

· Checking the configuration.

Command	show vlan interface interface type interface number
Example	Switch_config_g0/24# show vlan interface gigaEthernet 0/24 Interface VLAN Name Property PVID Vlan-allowed Vlan-untagged ---------- -------- ---- ---------- ---------- GigaEthernet0/24 trunk 10 12 13 Switch_config_g0/24#

· Configure VLAN Mapping

Command	vlan mapping ID
Parameter Descriptions	Null
Procedure	· Enter interface view. Run: Enter.
Example	config_g0/1# vlan mapping ID translated-vlan ID

· Enable Voice VLAN

Command	voice-vlan enable

Parameter Descriptions	Null
Procedure	· Enter config view. Run: voice-vlan enable Enter.
Example	switch_config# voice-vlan enable switch_config#

· Configure Voice VLAN And MAC Address

Command	voice-vlan mac-address ADDRESS mask MASK mode MODE
Parameter Descriptions	· ADDRESS: HH:HH:HH:HH:HH:HH -- 48 bit mac · MASK: HH:HH:HH:HH:HH:HH -- OUI mask · MODE: auto -- auto mode manual -- manual mode · AGING-TIME: 5-43200 （It is available when mode is auto ） The default is 1440. The units is minutes.
Procedure	· Enter interface view. Run: voice-vlan mac-address ADDRESS mask MASK mode MODE auto aging-time time Enter.
Example	switch_config_g0/7# voice-vlan mac-address 00:00:00:00:22:22 mask ff:ff:ff:ff:ff:ff mode auto aging-time 5 switch_config_g0/7#

4.13 QinQ Setting

QinQ, also known as VLAN stacking or VLAN-in-VLAN, is a feature on switches that allows multiple VLAN tags to be encapsulated within another VLAN tag. This facilitates the creation of hierarchical VLAN structures, enhancing network scalability and isolation.

· Enable QinQ

Command	dot1q-tunnel
Parameter Descriptions	Null
Procedure	· Enter config view. Run: Enter.
Example	switch_config# dot1q-tunnel

· Configure Port QinQ Mode

Command	switchport dot1q-translating-tunnel mode MODE

Parameter Descriptions	· MODE: · serviceprovider -- Select switching mode as ServiceProvider · customer -- Double tag customer mode · flat -- Select switching mode as Vlan Translate
Procedure	· Enter interface view. Run: switchport dot1q-translating-tunnel mode MODE Enter.
Example	switch_config# interface gigaethernet 0/24 switch_config_g0/24# switchport dot1q-translating-tunnel mode flat switch_config_g0/24#

· Enable global TPID

Command	dot1q-tunnel tpid TPID
Parameter Descriptions	TPID : WORD -- TPID tag must be set 4 Hex number, such as '9100' or '8100'
Procedure	· Enter config view. Run: dot1q-tunnel tpid TPID Enter.
Example	switch_config# dot1q-tunnel tpid 9300 switch_config#

4.14 Qos Configuration

Packets carry different priority fields on various networks. For example, packets carry the 802.1p field in a VLAN and the DSCP field on an IP network. The mapping between the priority fields must be configured on the network devices to retain priorities of packets when the packets traverse different networks. When the device functions as the gateway between different networks, the external priority fields (including 802.1p and DSCP) of all packets received by the device are mapped to the internal priorities. When the device sends packets, it maps the internal priorities to external priorities.

While the QoS function is on, the device port trusts DSCP priority, and trust 802.1p secondary by default, which is not supported configuring.

DSCP priority

When receiving a packet, the device searches the mapping table for the DSCP priority of the packet, and then tags the packet with the mapping inner priority.

802.1p priority

When receiving a tagged packet, the device searches the mapping table for the 802.1p priority of the packet, and then tags the packet with the mapping inner priority. When receiving an untagged packet, the device searches the mapping table based on the default 802.1p priority, and then tags the packet with the mapping inner priority.

The device supports to configure the following features:

· Priority mapping

· Congestion management

· Traffic policy

4.14.1 Enable QoS

Command	qos
Parameter Descriptions	Null
Procedure	· Enter config view. Run: qos Enter.
Example	switch_config# qos switch_config#

4.14.2 Configuring QoS Trust Type

Command	qos trust TRUST
Parameter Descriptions	TRUST : · dot1p -- Config Qos trust dot1p · dscp -- Config Qos trust dscp
Procedure	· Enter config view. Run: qos trust TRUST Enter.
Example	switch_config# qos trust dscp switch_config# qos trust dot1p switch_config#

4.14.3 Configuring QoS Scheduler Policy

Command	scheduler policy POLICY
Parameter Descriptions	· POLICY: · sp -- Schedule policy is sp · wrr -- Schedule policy is wrr · drr -- Schedule policy is drr · wfq -- Schedule policy is wfq · wred -- Schedule policy is wred
Procedure	· Enter config view. Run: scheduler policy POLICY Enter.
Example	switch_config# scheduler policy sp switch_config# scheduler policy wrr switch_config#

4.14.4 Configuring Priority Mapping

Priority mapping maps QoS priorities in packets to internal priorities (local priorities assigned by the device to packets) to ensure QoS in the differentiated services (DiffServ) model based on internal priorities.

Packets carry different priority fields on various networks. For example, packets carry the 802.1p field in a VLAN and the DSCP field on an IP network. The mapping between the priority fields must be configured on the network devices to retain priorities of packets when the packets traverse different networks. When the device functions as the gateway between different networks, the external priority fields (including 802.1p and DSCP) of all packets received by the device are mapped to the internal priorities. When the device sends packets, it maps the internal priorities to external priorities.

The device supports mapping between internal priorities and inbound queue indexes: This mapping allows packets to be sent to different queues, implementing differentiated services.

· Configuring mapping of 802.1p COS priority

Command	cos map queue number priority cos value
Parameter Descriptions	· queue number : ranges from 1 to 8 · priority cos value: ranges from 0 to 7
Procedure	· Enter config view. · Run: cos map queue number priority cos value Enter
Example	switch_config# cos map 1 2 switch_config#

· Configuring mapping of DSCP priority

Command	dscp map queue number DSCP value
Parameter Descriptions	· queue number : ranges from 1 to 8 · DSCP value: ranges from 0 to 63, format as “1”/”1-10”.
Procedure	· Enter config view. · Run: network IP address Enter
Example	Example 2 Configuring mapping of DSCP priority switch_config# dscp map 1 2 switch_config#

· Checking the configuration.

Command	show running-config
Example	Switch_config# show running-config Building configuration. Current Configuration: !version 1.1.3c_M28P_B4M_T0 ! Switch_config# show running-config Building configuration. Current Configuration: !

	!version 1.1.3a_M28_B4M_T1 ! username admin password 0 admin ! no spanning-tree ! spanning-tree rstp priority 4096 IP IGMP Snooping IP IGMP Snooping querier ! mac address-table aging-time 1000 dscp enable ! dot1q-tunnel ! qos enable qos dot1p enable cos map 0 8 ! qos dscp enable ! dscp map 0 1 dscp map 1 1 dscp map 2 1 dscp map 3 1 dscp map 4 1 dscp map 5 1 dscp map 6 1 dscp map 7 1 --More--

4.14.5 Congestion Management Configuration

After configuring congestion management, when there is congestion in the network, to process higher priority packet first, the device will decide the packet forwarding queue based on the setting scheduling policy.

The default scheduling policy is SP scheduling.

The device supports the following scheduling policy.

- SP scheduling (Strict Priority)
- WRR scheduling (Weighted Round Robin)
- DRR scheduling (Deficit Round Robin)
- WFQ scheduling (Weighted Fair Queuing)
- WRED scheduling (Weighted Random Early Detection)

Following with the steps.

- Configuring scheduler policy

Command	scheduler policy sp
	scheduler policy wrr
	scheduler policy drr
	scheduler policy wfq
	scheduler policy wred
Parameter Descriptions	Null
Procedure	· Enter config view.

	· Run: scheduler policy sp Or scheduler policy wrr Or scheduler policy drr Or scheduler policy wfq Or scheduler policy wred Enter
Example	switch_config# scheduler policy wfq switch_config#

· Checking the configuration.

Command	show running-config
Example	Switch_config# show running-config Building configuration. Current Configuration: ! !version 1.1.3a_M28_B4M_T1 ! username admin password 0 admin ! no spanning-tree ! scheduler policy wfq --More--

4.14.6 Traffic Policy Configuration

A traffic policy identifies packets of a certain type so that the device can provide differentiated services for these packets.

In the traditional IP network, network devices use the first-in-first-out (FIFO) policy to process all packets and send packets to the destination on a best-effort basis, but cannot guarantee transmission performance such as reliability and latency. Along with emergence of new applications in IP networks, new requirements are raised to QoS of IP networks. For example, delay-sensitive services such as VoIP services and video services demand shorter delay. Email and the File Transfer Protocol (FTP) services are insensitive to the delay.

The traditional IP network cannot provide differentiated services because the BE mode cannot distinguish services. That is, the BE mode cannot meet requirements of applications. A traffic policy solves this problem. The traffic policy classifies traffic based on rules, differentiates different service types, and provides corresponding network services. This function implements differentiated services and improves service provision capabilities.

The configuring processes are as following:

· Creating traffic policy template

· Configuring the traffic classify

· Configuring the traffic behavior

· Apply the traffic policy to interfaces

Following with the steps.

· Creating traffic policy template

Command	policy-map policy map name
Parameter Descriptions	· policy map name: name the policy map

Procedure	· Enter config view. Run: policy-map policy map name Enter
Example	switch_config# policy-map 1 switch_policy_map#

· Configuring the traffic classify

a) Classifies applying to Layer 2

Command	classify mac access-group access-list name
Parameter Descriptions	access-list name: access-list name

Command	classify vlan VLAN ID
Parameter Descriptions	· VLAN ID: ranges from 1 to 4094
Procedure	· Enter config view. Run: policy-map policy map name Enter · Run: classify vlan VLAN ID Enter
Example	switch_config# policy-map 1 Switch_policy_map# classify vlan 1 Switch-classify#

Command	classify cos cos value
Parameter Descriptions	· cos value: cos value， ranges from 0 to 7
Procedure	· Enter config view. Run: policy-map policy map name Enter · Run: classify cos cos value Enter
Example	switch_config# policy-map 1 Switch_policy_map# classify cos 1 Switch-classify#

b) Classifies applying to Layer 3

Command	classify IP access-group IP access-list
Parameter Descriptions	· IP access-list: IP access-list

Command	classify dscp DSCP value
Parameter Descriptions	DSCP value: DSCP value, ranges from 0 to 63
Procedure	· Enter config view. · Run: classify dscp DSCP value Enter
Example	switch_config# policy-map 1 switch_policy_map# classify DSCP 1 switch-classify#

· No classify

Command	classify any
Parameter Descriptions	Null

· Configuring the traffic behavior

a) Configuring bandwidth

Command	bandwidth bandwidth
Parameter Descriptions	· Bandwidth: ranges from 1 to 1600, unit: 64kbps
Procedure	· Enter config view. · Run: bandwidth bandwidth Enter
Example	switch_config# policy-map 1 switch-classify# bandwidth 10 switch-classify#

b) Drop the data packet

Command	drop
Parameter Descriptions	Null

c) Exit to enable mode

Command	end
Parameter Descriptions	Null

· Apply the traffic policy to interfaces

Command	End qos policy policy name ingress
Parameter Descriptions	· policy name: the policy name that already created
Procedure	· Exit and enter interface view Run: Interface gigaethernet 0/port number Enter · Run: qos policy policy name ingress

	Enter
Example	switch_config# interface gigaEthernet 0/4 switch_config_g0/4# qos policy 2 ingress switch_config_g0/4#

4.15 PoE Configuration

PoE configuration functionality on switches allows administrators to manage and customize the power delivery settings for PoE-enabled ports. This feature provides granular control over power allocation to connected devices, ensuring efficient utilization of PoE resources.

4.15.1 Configure PoE Maximum Power

Command	poe max-power POWERLEVEL
Parameter Descriptions	· POWERLEVEL: <1-390> -- Max power
Procedure	· Enter config view. · Run: poe max-power POWERLEVEL Enter
Example	switch_config# poe max-power 100 switch_config#

4.15.2 Enable/Disable PoE

Command	poe enable
Parameter Descriptions	Null
Procedure	· Enter interface view. Run: poe enable Enter.
Example	switch_config# interface gigaethernet 0/24 switch_config_g0/24# poe enable switch_config_g0/24#

4.15.3 Configuring PoE Port Power

Command	poe power portpower
Parameter Descriptions	· Portpower:(0~30) 0-30w
Procedure	· Enter interface view. Run: poe power portpower Enter.
Example	switch_config# interface gigaethernet 0/24 switch_config_g0/24# poe power 20 switch_config_g0/24#

4.15.4 Configuring PoE Port Priority

Command	poe priority PRIORITY
Parameter Descriptions	· PRIORITY: low /middle/high
Procedure	· Enter interface view. Run: poe priority PRIORITY Enter.
Example	switch_config# interface gigaethernet 0/24 switch_config_g0/24# poe priority low switch_config_g0/24#

4.15.5 Configuring PoE Power Reserved

Command	poe power-reserved reserved-rate
Parameter Descriptions	· reserved-rate: 0-100
Procedure	· Enter interface view. Run: poe power-reserved reserved-rate Enter.
Example	switch_config# poe power-reserved reserved-rate

4.15.6 Configuring PoE Power Overload

Command	poe power-verload poe_overload
Parameter Descriptions	· poe_watchdog:1-10
Procedure	· Enter interface view. Run: poe poe-overload poe_overload Enter.
Example	switch_config# poe poe-overload 1

5 IP Services Configuration

Following with the introductions of IP services configuration, including the basic knowledge and configurations of IP addresses (including basic IPv6 functions), DHCP, ARP, and DNS.

5.1 IP Address Configuration

The Internet Protocol (IP) is the core protocol in the TCP/IP protocol suite. Data of TCP, UDP, ICMP and IGMP protocols is transmitted in IP packets. Devices on different network segments communicate with each other using network-layer address, that is, IP addresses.

An IP address is a 32-bit address used on the Internet. Each host on an IP network must have an IP address.

An IP address consists of a network ID and a host ID. The network ID identifies a network and the host ID identifies a specific network device on the network. Network devices with the same network ID are located on the same network, regardless of their physical locations.

The device supports to configure the IP address of vlanIF for the device, including IPv4 and IPv6.

· Query VLAN interface number

Command	show vlan
Parameter Descriptions	Null
Procedure	· Enter config view Run: show vlan Enter
Example	Switch_config# show vlan VLAN Status Name Ports ---- ------- ------------------------------ ------------------------------ 1 Static Default G0/5 , G0/6 , G0/7 , G0/8 G0/9 , G0/10, G0/11, G0/12 G0/13, G0/14, G0/15, G0/16 G0/17, G0/18, G0/19, G0/20 G0/21, G0/22, G0/23, T0/1 T0/2 , T0/3 , T0/4 2 Static Default G0/1 , G0/3 , G0/4 3 Static Default G0/2 12 Static Default G0/24 Switch_config#

· Configuring IPv4

Command	IP address IP address subnet mask
Parameter Descriptions	· IP address : IP address of the unicast · subnet mask: subnet mask of the IP address
Procedure	· Enter config view. · Run: Interface vlan vlan interface number Enter · Run: IP address IP address subnet mask

	Enter
Example	switch_config# interface vlan 2 switch_config_v2# IP address 192.168.2.1 255.255.255.0 switch_config_v2#

· Configuring IPv6

Command	ipv6 address IPv6 global address
Parameter Descriptions	IPv6 global address: ipv6 address, in the form of: X:X:X:X::X/<0-128>
Procedure	· Enter config view. · Run: Interface vlan vlan interface number Enter · Run: Ipv6 address IPv6 address subnet mask Enter
Example	switch_config# interface vlan 6 Switch_config_v6# ipv6 address 2000::1111/64 Switch_config_v6#

5.2 DHCP Configuration

Dynamic Host Configuration Protocol (DHCP) dynamically manages and configures clients in a centralized manner. DHCP uses the client/server model. A client applies to the server for configurations such as the IP address, subnet mask, and default gateway; the server replies with requested configurations based on policies.

As the network expands and becomes complex, the number of hosts often exceeds the number of available IP addresses. As portable computers and wireless networks are widely used, the positions of computers often change, causing IP addresses of the computers to be changed accordingly. As a result, network configurations become increasingly complex. To properly and dynamically assign IP addresses to hosts, DHCP is used.

DHCP rapidly and dynamically allocates IP addresses, which improves IP address usage.

The device supports to enable/disable the DHCP snooping function and configure a DHCP server based on the address pool.

The function is off by default.

5.2.1 Enable/Disable DHCP Server

Command	(no) ip dhcp server
Parameter Descriptions	Null
Procedure	· Enter config view. Run: (no) ip dhcp server Enter.
Example	switch_config# ip dhcp server switch_config# no ip dhcp server switch_config#

5.2.2 IPv4 DHCP Snooping

DHCP (Dynamic Host Configuration Protocol) snooping is a security feature that enhances network integrity by preventing rogue DHCP server attacks and unauthorized IP address assignments. It monitors DHCP messages and ensures only authorized DHCP servers are allowed to assign IP addresses.

· Configuring Trust Mode

Command	ip dhcp snooping trust
Parameter Descriptions	Null
Procedure	· Enter interface view. Run: ip dhcp snooping trust Enter.
Example	switch_config_g0/21# ip dhcp snooping trust switch_config_g0/21#

· Configuring no trust mode

Command	no ip dhcp snooping trust
Parameter Descriptions	Null
Procedure	· Enter interface view. Run: no ip dhcp snooping trust Enter.
Example	switch_config_g0/21#no ip dhcp snooping trust switch_config_g0/21#

5.2.3 IPv6 DHCP Snooping

DHCPv6 (Dynamic Host Configuration Protocol for IPv6) snooping is a security feature that enhances network reliability by preventing unauthorized IPv6 address assignments and mitigating potential rogue DHCPv6 server attacks. It monitors DHCPv6 messages to ensure valid address assignments and protect against malicious activities.

· Turn On/off IPv6 DHCP Snooping

Command	(no) ipv6 dhcp snooping
Parameter Descriptions	Null
Procedure	· Enter config view. Run: (no) ipv6 dhcp snooping Enter.
Example	switch_config# ipv6 dhcp snooping switch_config# no ipv6 dhcp snooping switch_config#

5.3 DHCP Relay

DHCP (Dynamic Host Configuration Protocol) relay is a feature that allows switches to forward DHCP messages between clients and servers across different network segments. It enables DHCP

requests from clients in one subnet to reach DHCP servers in another subnet, facilitating centralized IP address management.

5.3.1 Enable DHCP Relay

Command	ip forward-protocol udp bootps
Parameter Descriptions	Null
Procedure	· Enter config view. Run: ip forward-protocol udp bootps Enter.
Example	switch_config# ip forward-protocol udp bootps

5.4 ARP Configuration

As the basis of Ethernet network communication, ARP maps IP addresses to MAC addresses.

On a local area network (LAN), a host or a network device must learn the IP address of the destination host or device before sending data to it. Additionally, the host or network device must learn the physical address of the destination host or device because IP packets must be encapsulated into frames for transmission over a physical network. Therefore, the mapping from an IP address into a physical address is required. ARP is used to map IP addresses into physical addresses.

The device supports configuring the dynamic ARP aging time, creating and delete static ARP.

Command	arp A.B.C.D HH:HH:HH:HH:HH:HH
Parameter Descriptions	· A.B.C.D -- IP address · HH:HH:HH:HH:HH:HH -- 48 bit hardware address of ARP entry
Procedure	· Enter config view. Run: arp A.B.C.D HH:HH:HH:HH:HH:HH Enter.
Example	switch_config# arp 192.168.0.253 00:00:00:22:22:22 switch_config#

· Checking the configuration.

Command	show arp
Example	switch_config# show arp VLAN ID Port ID IP address MAC Address Type ========== 1(vlan1)ARP 0/3 192.168.1.100 4c-ed-fb-61-4a-e6 ARP Static

· Delete the ARP

Command	no arp IP address
Parameter Descriptions	· IP address : IP address, IP address of the unicast
Procedure	· Enter config view. · Run: no arp IP address

	Enter
Example	switch_config# no arp 192.168.1.100 switch_config#

· Checking the configuration.

Command	show arp
Example	switch_config# show arp VLAN ID Port ID IP address MAC Address Type ==========

5.5 DNS Configuration

DNS is a distributed database used in TCP and IP applications and completes resolution between IP addresses and domain names.

Each host on the network is identified by an IP address. To access a host, a user must obtain the host IP address first. It is difficult for users to remember IP addresses of hosts. Therefore, host names in the format of strings are designed. Each host name maps an IP address. In this way, users can use the simple and meaningful domain names instead of the complicated IP addresses to access hosts.

The switch supports to function as a DNS client and supports static and dynamic domain name resolution.

Command	ip dns server A.B.C.D
Parameter Descriptions	· A.B.C.D -- Domain name server's IP address
Procedure	· Enter config view. Run: ip dns server A.B.C.D Enter.
Example	switch_config# ip dns server 192.168.1.34 switch_config#

· Checking the configuration.

Command	show running-config
Example	Switch_config# show running-config Building configuration. Current Configuration: !version 1.1.3c_M28P_B4M_T0 ! hostname username admin password 0 admin ! no spanning-tree ! IP dns server 192.168.2.5 -More-

5.6 IP ACL

ACL (Access Control List) configuration enables users to define rules that filter and control network traffic based on criteria like source/destination IP addresses, ports, and protocols. ACLs help enforce security policies by permitting or denying specific types of traffic, such as allowing access to certain services

while blocking unauthorized traffic. By configuring ACLs, users can enhance network security, manage bandwidth usage, and control access to resources. It is essential to understand ACL syntax and guidelines to effectively implement and maintain a secure and efficient network environment. IP ACL and IP Extended ACL are parts of ACL feature.

5.6.1 Create Standard IP ACL

Beginning in config view, follow these steps to create an IP standard ACL for IP traffic:

Command	ip access-list standard ACL
Parameter Descriptions	· ACL: WORD -- IP access-list name
Procedure	· Enter config view. Run: ip access-list standard ACL Enter.
Example	switch_config# ip access-list standard acl1 switch_config_std_nacl#

5.6.2 Apply IP ACL to Port

This operation effect in direction by default.

Command	ip access_group ACL
Parameter Descriptions	· ACL: WORD -- IP access-list name
Procedure	· Enter interface view. Run: ip access_group ACL Enter.
Example	switch_config_g0/8# ip access_group acl1 switch_config_g0/8#

5.6.3 Apply IP access-group ACL to Policy

Command	classify ip access-group ACL
Parameter Descriptions	· ACL:WORD -- Access list name
Procedure	· Enter policy_map view. Run: classify ip access-group ACL Enter.
Example	switch_policy_map# classify ip access-group acl1 switch-classify#

5.6.4 Configuring Permit Operation

Command	permit host ADD /any netmask
Parameter Descriptions	· ADD: A.B.C.D -- Address to match · netmask :A.B.C.D -- IP subnet mask

Procedure	· Enter std_nacl view. Run: permit host SOUR /any netmask Enter.
Example	switch_config_std_nacl# permit 192.168.3.123 255.255.25.0 switch_config_std_nacl#

5.6.5 Configuring Deny Operation

Command	permit host ADD /any netmask
Parameter Descriptions	· ADD: A.B.C.D -- Address to match · netmask :A.B.C.D -- IP subnet mask
Procedure	· Enter std_nacl view. Run: deny host SOUR /any netmask Enter.
Example	switch_config_std_nacl# deny 192.168.3.123 255.255.25.0 switch_config_std_nacl#

5.7 Extended IP ACL

Beginning in config view, follow these steps to create an IP extended ACL for IP traffic

5.7.1 Extend ACL

Command	ip access-list extended ACL
Parameter Descriptions	· ACL:WORD -- Extended Access-list name
Procedure	· Enter config view. Run: ip access-list extended ACL Enter.
Example	switch_config# ip access-list extended 7 switch_config_ext_nacl#

5.8 Policy Configuration

A policy map allows for traffic prioritization, QoS implementation, and bandwidth allocation based on specific criteria like IP addresses, protocols, or port numbers. It enables congestion control, traffic shaping, and security enforcement, optimizing network performance. By defining rules and actions, policy maps ensure that critical applications receive necessary resources while preventing non-essential traffic from consuming excessive bandwidth. This leads to efficient resource utilization, reduced latency for time-sensitive applications, and overall network stability. Policy maps also facilitate compliance with network policies and regulatory requirements, contributing to a well-managed and reliable network infrastructure.

5.8.1 Configuring Policy

Command	permit host HH:HH:HH:HH:HH:HH destination
Parameter Descriptions	· HH:HH:HH:HH:HH:HH -- Source mac address

	· Destination: any -- Any destination MAC address · host -- A single destination host
Procedure	· Enter macl view. Run: permit host HH:HH:HH:HH:HH:HH destination Enter.
Example	switch_config# mac access-list acl1 switch_config_macl# permit host 00:00:00:11:11:11 any switch_config_macl# permit host 00:00:00:11:11:11 host switch_config_macl#

5.8.2 Create policy map

Command	policy-map WORD
Parameter Descriptions	· WORD -- Policy-map name
Procedure	· Enter config view. Run: policy-map WORD Enter.
Example	switch_config# policy-map pol1 switch_policy_map#

5.8.3 Create Classify MAC Access Group

Command	classify mac access-group WORD
Parameter Descriptions	· WORD -- Access list name
Procedure	· Enter policy_map view. Run: classify mac access-group WORD Enter.
Example	switch_policy_map# classify mac access-group 2 switch-classify#

5.8.4 Configuring Bandwidth Limit

Command	bandwidth BW
Parameter Descriptions	· BW :1-1600 -- Configure Bandwidth(unit:64kbps)
Procedure	· Enter classify view. Run: bandwidth BW Enter.
Example	switch-classify# bandwidth 1

5.8.5 Configuring COS

Command	· set cos COS
Parameter Descriptions	· COS:<0-7> -- Config cos value
Procedure	· Enter classify view. Run: set cos COS Enter.
Example	switch-classify# set cos 5

5.8.6 Delete Classify

Command	drop
Parameter Descriptions	Null
Procedure	· Enter classify view. Run: drop Enter.
Example	switch-classify# drop switch-classify#

5.8.7 Configuring DSCP

Command	set dscp DSCP
Parameter Descriptions	· DSCP :<0-63> -- Config dscp value
Procedure	· Enter interface view. Run: set dscp DSCP Enter.
Example	switch-classify# set dscp 63 switch-classify#

5.8.8 Configuring VLANID

Command	· set vlanID ID
Parameter Descriptions	· ID:<1-4049> -- Config vlanid value
Procedure	· Enter classify view. Run: set vlanID ID Enter.
Example	switch-classify# set vlanID 10

5.8.9 Configuring Policy Map

Command	qos policy NAME MAP

Parameter Descriptions	· NAME:WORD -- policy-map name · MAP: · ingress -- Config port policy map ingress · egress -- Config port policy map egress
Procedure	· Enter interface view. Run: qos policy NAME MAP Enter.
Example	switch_config_g0/1# qos policy 1 ingress switch_config_g0/1#

6 IP Multicast Configuration

6.1 IGMP Snooping Configuration Based On VLAN

Internet Group Management Protocol Snooping (IGMP Snooping) maintains information about the outgoing interfaces of multicast packets by snooping multicast protocol packets exchanged between the Layer 3 multicast device and user hosts. The IGMP Snooping protocol manages and controls the forwarding of multicast packets at the data link layer.

The device supports to enable/disable the function, and configure IGMP Snooping timer.

· Enable the IGMP Snooping function

Command	IP IGMP Snooping
Parameter Descriptions	Null
Procedure	· Enter config view. Run: IP IGMP Snooping Enter
Example	switch_config# IP IGMP Snooping switch_config#

· Disable the IGMP Snooping function

Command	no IP IGMP Snooping
Parameter Descriptions	Null
Procedure	· Enter config view. Run: no IP IGMP Snooping Enter
Example	switch_config# no IP IGMP Snooping switch_config#

· Enable the IGMP Snooping query function

Command	IP IGMP Snooping querier
Parameter Descriptions	Null
Procedure	· Enter config view. Run: IGMP Snooping querier Enter
Example	switch_config# IP IGMP Snooping querier switch_config#

· Configuring query interval time

Command	IP IGMP Snooping timer querier interval time
Parameter Descriptions	· interval time: Interval time ranges from 60~1000 in seconds
Procedure	· Enter config view.

	Run: IP IGMP Snooping timer querier interval time Enter
Example	switch_config# IP IGMP Snooping timer querier 60 switch_config#

· Configuring group members survival time

Command	IP IGMP Snooping timer survival time
Parameter Descriptions	· survival time: Survival time ranges from 120~5000 in seconds.
Procedure	· Enter config view. Run: IP IGMP Snooping timer survival time Enter
Example	switch_config# IP IGMP Snooping timer survival 120 switch_config#

· **Configuring Global Route Port**

Command	ip igmp-snooping route-port PORTRANGE
Parameter Descriptions	· PORTRANGE: <x-x> -- Config port range
Procedure	· Enter config view. Run: ip igmp-snooping route-port PORTRANGE Enter.
Example	switch_config# ip igmp-snooping route-port 1-3 switch_config#

· Configuring IGMP Snooping Fast Leave

Command	ip igmp-snooping fast-leave
Parameter Descriptions	Null
Procedure	· Enter config view. Run: ip igmp-snooping fast-leave Enter.
Example	switch_config# ip igmp-snooping fast-leave switch_config#

· Checking the configuration

Command	show ip IGMP Snooping
Example	switch_config# show ip IGMP Snooping Global IGMP snooping configuration: ---------- Globally enable : Enabled Querier : Enabled Querier time : 640

	Member age time : 2000 switch_config#

· Static Multicast Table

Command	mac address-table static MAC vlan VLANID interface gigaEthernet PORT
Parameter Descriptions	· MAC: HH:HH:HH:HH:HH:HH -- 48 bit mac address · VLANID: <1-4094> -- VLAN id of mac address table · PORT: <0-0> -- FastEthernet interface number
Procedure	· Enter config view. Run: mac address-table static MAC vlan VLANID interface gigaEthernet PORT Enter.
Example	switch_config# mac address-table static 01:00:5e:c4:c2:f0 vlan 2 interface gigaEthernet 0/5 switch_config#

7 Security Configuration

7.1 MAC Table Configuration

A MAC address table records the MAC address, interface number, and VLAN ID of the device connected to the device.

Each device maintains a MAC address table. A MAC address table records the MAC address, interface number, and VLAN ID of the connected devices. When forwarding a data frame, the device searches the MAC table for the outbound interface according to the destination MAC address in the frame. This helps the device reduce broadcasting.

Categories of MAC Address Entries

The MAC address entry can be classified into the dynamic entry, the static entry and the blackhole entry.

The dynamic entry is created by learning the source MAC address. It has aging time.

The static entry is set by users and is delivered to each SIC. It does not age.

The blackhole entry is used to discard the frame with the specified source MAC address or destination MAC address. Users manually set the blackhole entries and send them to each SIC. Blackhole entries have no aging time.

The dynamic entry will be lost after the system is reset or the interface board is hot swapped or reset. The static entry and the blackhole entry, however, will not be lost.

The device supports configuring:

- Aging time of MAC table
- Static MAC table
- Query MAC table

7.1.1 Configuring Aging Time of MAC Table

Using the command line, users can change the aging time of MAC table.

The default value is 300s.

Command	mac address-table aging-time aging time
Parameter Descriptions	· aging time: Aging time in seconds, ranges from 10-1000000.
Procedure	· Enter config view. Run: mac address-table aging-time aging time Enter
Example	switch_config# mac address-table aging-time 1000 switch_config#

- Checking the configuration.

Command	show running-config
Example	Switch_config# show running-config Building configuration. Current Configuration: !version 1.1.3c_M28P_B4M_T0 ! hostname username admin password 0 admin ! no spanning-tree !

	spanning-tree rstp priority 4096 ! IP IGMP Snooping IP IGMP Snooping querier ! mac address-table aging-time 1000 --More--

7.1.2 Configuring Static MAC Table

Using the command lines, users can add and delete the MAC table.

No default value.

· Add the MAC table

Command	mac address-table static HH:HH:HH:HH:HH:HH vlan vlan id interface interface type interface number
Parameter Descriptions	· HH:HH:HH:HH:HH:HH: 48 bit mac address · Vlan id: VLAN id of mac address table, the value ranges from 1 to 4094. · interface type : interface type, including GigaEthernet -- GigaEthernet interface TenGigaEthernet -- TenGigaEthernet interface · interface number: interface number, in the format as “0/port number”, the value of port number value is the port number of the switch.
Procedure	· Enter config view. Run: mac address-table static HH:HH:HH:HH:HH:HH vlan vlan id interface interface type interface number Enter
Example	switch_config# mac address-table static 00:00:00:00:00:06 vlan 1 interface gigaEthernet 0/24 switch_config#

· Checking the configuration.

Command	show mac address-table static
Example	Switch_config# show mac address-table static Interface VLAN ID Type MAC Address ========== g0/24 1 Static 00:00:00:00:00:06 Switch_config#

· Delete the MAC table

Command	no mac address-table static HH:HH:HH:HH:HH:HH vlan vlan id
Parameter Descriptions	· HH:HH:HH:HH:HH:HH: 48 bit mac address · Vlan id: VLAN id of mac address table, the value ranges from 1 to 4094.
Procedure	· Enter config view. Run: no mac address-table static HH:HH:HH:HH:HH:HH vlan vlan id Enter

Example	Switch_config# no mac address-table static 00:00:00:00:00:01 vlan 1 Switch_config#

· Checking the configuration.

Command	no mac address-table static HH:HH:HH:HH:HH:HH vlan vlan id show mac address-table static
Example	Switch_config# show mac address-table static Interface VLAN ID Type MAC Address ========== g0/3 3 Static 00:00:00:00:00:03 g0/2 2 Static 00:00:00:00:00:02 g0/1 1 Static 00:00:00:00:00:01 Switch_config# no mac address-table static 00:00:00:00:00:01 vlan 1 Switch_config# show mac address-table static Interface VLAN ID Type MAC Address ========== g0/3 3 Static 00:00:00:00:00:03 g0/2 2 Static 00:00:00:00:00:02

7.1.3 Query MAC Table

Using the command line, users can query the MAC table.

No default value.

· Query all the MAC table, including dynamic and static MAC table

Command	show mac address-table
Parameter Descriptions	Null
Example	Switch_config# show mac address-table Interface VLAN ID Type MAC Address ========== g0/23 1 Dynamic 00:0b:82:c4:c3:22 g0/23 1 Dynamic 00:0c:29:f8:63:05 g0/23 1 Dynamic 40:8d:5c:3f:4d:ba g0/23 1 Dynamic c6:08:80:03:5e:b3 g0/23 1 Dynamic 00:e0:66:70:b7:0b g0/23 1 Dynamic 00:0b:82:c0:07:a7 g0/23 1 Dynamic 00:0b:82:c0:07:a9 g0/23 1 Dynamic 00:0b:82:c4:c2:f7 g0/23 1 Dynamic 00:0b:82:c0:07:a5 g0/23 1 Dynamic 00:0b:82:c0:07:ab g0/23 1 Dynamic 00:0b:82:c4:c3:24 g0/23 1 Dynamic 00:0b:82:c0:09:db g0/3 3 Static 00:00:00:00:00:03 g0/23 1 Dynamic 40:b0:34:22:76:6b g0/23 1 Dynamic 10:bf:48:b8:66:c5 g0/23 1 Dynamic 3c:f5:cc:26:c2:39

	g0/23	1	Dynamic	00:0b:82:c0:07:ac
	g0/23	1	Dynamic	10:7b:44:80:8b:86
	g0/23	1	Dynamic	4c:ed:fb:75:12:0d
	g0/23	1	Dynamic	d4:ae:52:cc:d2:d9
	g0/23	1	Dynamic	f8:32:e4:ba:ca:a9
	g0/23	1	Dynamic	00:0b:82:dc:06:5a
	--More--			

· Query a specific MAC address

Command	show mac address-table HH:HH:HH:HH:HH:HH
Parameter Descriptions	· HH:HH:HH:HH:HH:HH: 48 bit mac address
Example	Switch_config# show mac address-table 00:0b:82:c4:c3:22 Interface VLAN ID Type MAC Address ========== g0/23 1 Dynamic 00:0b:82:c4:c3:22

· Query dynamic MAC table

Command	show mac address-table dynamic
Parameter Descriptions	Null
Example	Switch_config# show mac address-table dynamic Interface VLAN ID Type MAC Address ========== g0/23 1 Dynamic 00:0b:82:c4:c3:22 g0/23 1 Dynamic 00:0c:29:f8:63:05 g0/23 1 Dynamic 40:8d:5c:3f:4d:ba g0/23 1 Dynamic c6:08:80:03:5e:b3 g0/23 1 Dynamic 00:e0:66:70:b7:0b g0/23 1 Dynamic 00:0b:82:c0:07:a7 g0/23 1 Dynamic 00:0b:82:c0:07:a9 g0/23 1 Dynamic 00:0b:82:c4:c2:f7 g0/23 1 Dynamic 00:0b:82:c0:07:a5 g0/23 1 Dynamic 00:0b:82:c0:07:ab g0/23 1 Dynamic 00:0b:82:c4:c3:24 g0/23 1 Dynamic 00:0b:82:c0:09:db g0/23 1 Dynamic 40:b0:34:22:76:6b g0/23 1 Dynamic 3c:f5:cc:26:c2:39 g0/23 1 Dynamic 00:0b:82:c0:07:ac g0/23 1 Dynamic 10:7b:44:80:8b:86 g0/23 1 Dynamic 4c:ed:fb:75:12:0d g0/23 1 Dynamic d4:ae:52:cc:d2:d9 g0/23 1 Dynamic f8:32:e4:ba:ca:a9 g0/23 1 Dynamic 00:0b:82:dc:06:5a g0/23 1 Dynamic 40:8d:5c:8e:1d:2d g0/23 1 Dynamic 3c:f5:cc:26:c2:03

· Query static MAC table

Command	show mac address-table static
Parameter Descriptions	Null
Example	Switch_config# show mac address-table static Interface VLAN ID Type MAC Address ========== g0/3 3 Static 00:00:00:00:00:03

· Query MAC table interface

Command	show mac address-table interface interface type interface number
Parameter Descriptions	· interface type : interface type, including GigaEthernet -- GigaEthernet interface TenGigaEthernet -- TenGigaEthernet interface · interface number: interface number, in the format as "0/port number", the value of port number value is the port number of the switch.
Example	Switch_config# show mac address-table interface gigaEthernet 0/3 Interface VLAN ID Type MAC Address ========== g0/3 3 Static 00:00:00:00:00:03 Switch_config#

· Query MAC table in the VLAN

Command	show mac address-table vlan VLAN ID
Parameter Descriptions	· VLAN ID: VLAN ID, ranges from 1~4094
Example	Switch_config# show mac address-table vlan 1 Interface VLAN ID Type MAC Address ========== g0/23 1 Dynamic 00:0b:82:c4:c3:22 g0/23 1 Dynamic 00:0c:29:f8:63:05 g0/23 1 Dynamic 40:8d:5c:3f:4d:ba g0/23 1 Dynamic c6:08:80:03:5e:b3 g0/23 1 Dynamic 00:e0:66:70:b7:0b g0/23 1 Dynamic 00:0b:82:c0:07:a7 g0/23 1 Dynamic 00:0b:82:c0:07:a9 g0/23 1 Dynamic 00:0b:82:c4:c2:f7 g0/23 1 Dynamic 00:0b:82:c0:07:a5 g0/23 1 Dynamic 00:0b:82:c0:07:ab g0/23 1 Dynamic 00:0b:82:c4:c3:24 g0/23 1 Dynamic 00:0b:82:c0:09:db g0/23 1 Dynamic 40:b0:34:22:76:6b g0/23 1 Dynamic 3c:f5:cc:26:c2:39 g0/23 1 Dynamic 00:0b:82:c0:07:ac g0/23 1 Dynamic 10:7b:44:80:8b:86 g0/23 1 Dynamic 4c:ed:fb:75:12:0d

	g0/23	1	Dynamic	d4:ae:52:cc:d2:d9
	g0/23	1	Dynamic	f8:32:e4:ba:ca:a9
	g0/23	1	Dynamic	00:0b:82:dc:06:5a
	g0/23	1	Dynamic	40:8d:5c:8e:1d:2d
	g0/23	1	Dynamic	3c:f5:cc:26:c2:03
	--More--			

7.2 MAC Dynamic Aging

Dynamic addresses are source MAC addresses that the switch learns and then ages when they are not in use. You can change the aging time setting for all VLANs or for a specified VLAN. Setting too short aging time can cause addresses to be prematurely removed from the table. Then when the switch receives a packet for an unknown destination, it floods the packet to all ports in the same VLAN as the receiving port. This unnecessary flooding can impact performance. Setting too long an aging time can cause the address table to be filled with unused addresses, which prevents new addresses from being learned. Flooding results, which can impact switch performance.

7.2.1 Configuring mac aging time

Follow these steps to Configuring the dynamic address table aging time:

Command	mac address-table aging-time
Parameter Descriptions	Null
Procedure	· Enter config view. Run: mac address-table aging-time Enter.
Example	switch_config# mac address-table aging-time switch_config#

7.3 MAC Based ACL

ACL (Access Control List) configuration enables users to define rules that filter and control network traffic based on criteria like source/destination IP addresses, ports, and protocols. ACLs help enforce security policies by permitting or denying specific types of traffic, such as allowing access to certain services while blocking unauthorized traffic. By configuring ACLs, users can enhance network security, manage bandwidth usage, and control access to resources. It is essential to understand ACL syntax and guidelines to effectively implement and maintain a secure and efficient network environment. MAC Based ACL is part of ACL feature.

7.3.1 MAC ACL

You can classify IP traffic by using IP standard or IP extended ACLs. You can classify IP and non-IP traffic by MAC ACLs.

Beginning in config view, follow these steps to create a MAC ACL:

Command	mac access-list ACL
Parameter Descriptions	· ACL:WORD -- IP access-list name
Procedure	· Enter config view. Run: mac access-list ACL

	Enter.
Example	switch_config# mac access-list 1 switch_config_macl#

7.3.2 Configuring Permit Operation

Command	permit host SOUR /any host DEST/any TYPE
Parameter Descriptions	· SOUR :HH:HH:HH:HH:HH:HH -- Source mac address · DEST :HH:HH:HH:HH:HH:HH -- Destination mac address · TYPE:<1536-65535> -- An arbitrary EtherType
Procedure	· Enter macl view. Run: permit host SOUR /any host DEST/any TYPE Enter.
Example	switch_config_macl# permit host 00:60:A7:14:78:52 host 68:A3:C4:CC:7A:F4 switch_config_macl# $ 00:60:A7:14:78:52 host 68:A3:C4:CC:7A:F4 1536 switch_config_macl#

7.3.3 Configuring Deny Operation

Command	deny host SOUR /any host DEST/any TYPE
Parameter Descriptions	· SOUR :HH:HH:HH:HH:HH:HH -- Source mac address · DEST :HH:HH:HH:HH:HH:HH -- Destination mac address · TYPE:<1536-65535> -- An arbitrary EtherType
Procedure	· Enter macl view. Run: deny host SOUR /any host DEST/any TYPE Enter.
Example	switch_config_macl# deny host 00:60:A7:14:78:52 host 68:A3:C4:CC:7A:F4 switch_config_macl# $ 00:60:A7:14:78:52 host 68:A3:C4:CC:7A:F4 1536 switch_config_macl#config_macl# deny host/any host/any type/lenge

7.3.4 Configuring Bandwidth Limit

Command	bandwidth host SOUR /any host DEST/any TYPE BDWIDTH
Parameter Descriptions	· SOUR :HH:HH:HH:HH:HH:HH -- Source mac address · DEST :HH:HH:HH:HH:HH:HH -- Destination mac address · TYPE:<1536-65535> -- An arbitrary EtherType · BDWIDTH :<0-1000> -- Bandwidth(n*64 Kbps)
Procedure	· Enter macl view. Run: bandwidth host SOUR /any host DEST/any TYPE BDWIDTH Enter.
Example	switch_config_macl# bandwidth any host 68:A3:C4:CC:7A:F4 1536 100 switch_config_macl# bandwidth host 00:60:A7:14:78:52 host

	68:A3:C4:CC:7A:F4 1536 100 switch_config_macl#

7.3.5 Apply MAC ACL To Port

This operation effect in direction by default.

Command	mac access-list ACL
Parameter Descriptions	· ACL:WORD -- IP access-list name
Procedure	· Enter interface view. Run: mac access-list ACL Enter.
Example	switch_config# interface gigaethernet 0/24 switch_config_g0/24# mac access-list 1 switch_config_g0/24#

7.3.6 Apply MAC Access-group ACL To Policy Map

Command	classify mac access-group ACL
Parameter Descriptions	· ACL: WORD -- Access list name
Procedure	· Enter policy_map view. Run: classify mac access-group ACL Enter.
Example	switch_policy_map# classify mac access-group 1 switch-classify#

7.4 802.1x Authentication

In the network planning deployment of the access layer, users need to deploy access-side security, only legitimate users can access the network after authentication. 802.1x can be well deployed on the access switch ports to achieve access-side security control.

802.1x authentication is available as a local-based authentication method or as a radius-based remote authentication method. We go through case examples to explain 802.1x local and remote radius authentication in detail.

7.4.1 Enable Authentication Global Setting

Command	dot1x enable
Parameter Descriptions	Null
Procedure	· Enter config view. Run: dot1x enable Enter.
Example	switch_config# dot1x enable switch_config#

7.4.2 Configuring Period re-Authentication

Command	dot1x timeout re-authperiod PERIOD
Parameter Descriptions	· PERIOD
Procedure	· Enter config view. Run: dot1x timeout re-authperiod PERIOD Enter.
Example	switch_config# dot1x timeout re-authperiod 60 switch_config#

7.4.3 Configuring Port Authentication Method

Command	dot1x authentication method Auth-method
Parameter Descriptions	· Auth-method: · MAC-Based -- Select 802.1x chap authenticate type · Port-Based -- Select 802.1x eap authenticate type
Procedure	· Enter interface view. Run: dot1x authentication method Auth-method Enter.
Example	switch_config_g0/1# dot1x authentication method maC-Based switch_config_g0/1#

7.4.4 Configuring Port Control Mode

Command	dot1x port-control MODE
Parameter Descriptions	· MODE provide 3 mode: · Auto -- Authenticate automatically · Authorized-force -- Force port to authorized state · Unauthorized-force -- Force port to unauthorized state
Procedure	· Enter interface view. Run: Enter.
Example	switch_config_g0/2# dot1x port-control auto switch_config_g0/2# dot1x port-control Authorized-force switch_config_g0/2#

7.4.5 Configuring Max User Number

Command	dot1x max-user USERNUM

Parameter Descriptions	· USERNUM : (1-4096)
Procedure	· Enter interface view. Run: dot1x max-user USERNUM Enter.
Example	switch_config_g0/2# dot1x max-user 5 switch_config_g0/2#

7.4.6 Configuring Authentication Way

Command	aaa authentication login default group radius
Parameter Descriptions	Null
Procedure	· Enter config view. Run: aaa authentication login default group radius Enter.
Example	switch_config# aaa authentication login default group radius/local

7.4.7 Enable Dot1x

Command	dot1x enable
Parameter Descriptions	Null
Procedure	· Enter config view. Run: dot1x enable Enter.
Example	switch_config# dot1x enable switch_config#

7.4.8 Enable/Disable AAA

Command	aaa authentication enable default enable/none
Parameter Descriptions	Null
Procedure	· Enter config view. Run: aaa authentication enable default enable/none Enter.
Example	switch_config# aaa authentication enable default enable switch_config# aaa authentication enable default none switch_config#

7.4.9 Configuring Login Authentication Method

Command	aaa authentication enable default group MODE

Parameter Descriptions	· MODE: · radius -- Use list of all Radius hosts · tacacs+ -- Use list of all Tacacs+ hosts
Procedure	· Enter config view. Run: aaa authentication enable default group MODE Enter.
Example	switch_config# aaa authentication enable default group radius switch_config# aaa authentication enable default group tacacs+ switch_config#

7.4.10 Configuring Secret Level and Password

Command	enable secret level LEVEL LINE1/ TYPE LINE2
Parameter Descriptions	· LEVEL :<1-15> -- Level number · LINE1 -- The UNENCRYPIED <cleartext> enable secret · TYPE: · 0 -- Specifies an UNENCRYPTED password will follow · 5 -- Specifies a HIDDEN password will follow · LINE2 -- The ENCRYPTED 'enable' secret string
Procedure	· Enter config view. Run: enable secret level LEVEL LINE1/ TYPE LINE2 Enter.
Example	switch_config# enable secret level 15 0 pswd1 switch_config# enable secret level 15 pswd2 switch_config#

7.4.11 Configuring Host/Back Server

Command	radius-server ip HOST back ip BACK auth-port PORT1 acct-port PORT2
Parameter Descriptions	· HOST: ip -- Specify a RADIUS server · BACK: back -- Specify RADIUS standby server · PORT1:<0-65535> -- Port number for authentication · PORT2: <0-65535> -- Port number for account
Procedure	· Enter config view. Run: radius-server host IP auth-port PORT1 acct-port PORT2 Enter.
Example	switch_config# radius-server host 192.168.3.10 auth-port 1812 acct-port 1813 switch_config#

7.4.12 Configuring Server Key

Command	radius-server key KEY1
Parameter Descriptions	· KEY1:WORD -- Key string
Procedure	· Enter config view. Run: radius-server key KEY1 Enter.
Example	switch_config# radius-server key 123456 switch_config#

7.5 Login Filter

Login filter ACL (Access Control List) functionality allows users to define access rules for login attempts based on criteria like source IP type or protocol type. This feature enhances network security by filtering incoming login requests, allowing only authorized devices or users to access the switch for management purposes. By configuring login filter ACLs, administrators can prevent unauthorized access attempts, protect sensitive network configurations, and ensure a secure management environment. It's crucial to understand ACL syntax and guidelines to effectively implement login filter ACLs and maintain a robust network security posture.

7.5.1 Enable Port Login Security

Command	switchport port-security login-filter IPTYPE PROTOCOL
Parameter Descriptions	· IPTYPE: IPV4/IPV6 · PROTOCOL: SSH/Telnet
Procedure	· Enter interface view. Run: switchport port-security login-filter IPTYPE PROTOCOL Enter.
Example	switch_config# interface gigaethernet 0/24 switch_config_g0/24# switchport port-security login-filter iPV4 ssH switch_config_g0/24#

8 Reliability

8.1 STP/RSTP Configuration

The Spanning Tree Protocol (STP) trims a ring network into a loop-free tree network. It prevents replication and circular propagation of packets. The Rapid Spanning Tree Protocol (RSTP) was developed based on STP to implement faster convergence. RSTP defines edge ports and provides protection functions.

Loops often occur on a complex network. On a complex network, to implement redundancy, network designers tend to deploy multiple physical links between two devices, one of which is the master and the others are the backup.

Loops cause broadcast storms. Consequently, network resources are exhausted and the network breaks down. Loops also damage MAC addresses.

To remove loops, run STP at the data link layer. Devices running STP exchange STP BPDUs to discover loops on the network and block some ports to prune the network into a loop-free tree network. STP prevents infinite looping of packets to ensure packet processing capabilities of switches.

Because STP provides slow convergence, IEEE 802.1w released RSTP in 2001. RSTP enhances STP and speeds up network convergence.

8.1.1 STP/RSTP Global Setting

The device supports STP/RSTP functions, the functions are off by default.

· Switch the Spanning-Tree mode

Command	spanning-tree mode mode
Parameter Descriptions	· Mode: Three modes: stp, setup spanning-tree protocol mode rstp, setup rapid spanning-tree protocol mode mstp, setup multiple spanning-tree protocol mode
Procedure	· Enter config view. Run: spanning-tree mode mode Enter
Example	switch_config# spanning-tree mode stp switch_config# switch_config# spanning-tree mode rstp switch_config#

Following will take STP mode as example to configure STP mode. Including setting priority, hello time, max age time and forward time. The relationship between protocol timer values is enforced as: 2 * (forward time - 1) >= max age time >=2 * (hello time + 1).

The configuration steps of RSTP mode are the same.

· Set STP mode priority

Command	spanning-tree stp priority priority value
Parameter Descriptions	· priority value: Rstp mode priority value, it should be one of the following values: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440

	The default value is 32768.
Procedure	· Run: spanning-tree stp priority priority value Enter
Example	Switch_config# spanning-tree stp priority 40960 Switch_config#

· Set STP mode Hello time

Command	spanning-tree stp hello-time hello time
Parameter Descriptions	· hello -time: STP mode hello time, the value ranges from 1s to 10s. The value is 2s by default.
Procedure	· Run: spanning-tree stp hello-time hello time Enter
Example	Switch_config# spanning-tree stp hello-time 6 Switch_config#

· Set STP mode Max age time

Command	spanning-tree stp max-age max-age time
Parameter Descriptions	· max-age time: STP mode forward time, the value ranges from 4s to 30s. The value is 15s by default.
Procedure	· Run: spanning-tree stp max-age max age time Enter
Example	Switch_config# spanning-tree stp max-age 20 Switch_config#

· Set STP mode forward time

Command	spanning-tree stp forward-time forward time
Parameter Descriptions	· forward-time: STP mode forward time, the value ranges from 4s to 30s. The value is 15s by default.
Procedure	· Run: spanning-tree stp forward-time forward time Enter
Example	Switch_config# spanning-tree stp forward-time 12 Switch_config#

· Checking the configuration.

Command	show spanning-tree
Example	Spanning tree enabled protocol STP STP Root Id: Priority 8193 Address 0025.84d5.c700 Cost 20000000 Port GigaEthernet0/23

	Hello/Max/FwdDly 2/20/15(s) Bridge Id: Priority 40960 Address c408.8001.5c23 Hello/Max/FwdDly 6/20/12(s) Interface Role Sts Cost Prio.Nbr Type ---------- ---- --- --------- -------- -------------------------------- G0/23 Root FWD 20000000 128.23 P2p Switch_config#

· Turning Off Spanning-Tree

Function	After configuring the spanning-tree mode, users can turn it off by using the command line. The spanning-tree function is off by default.
Command	no spanning-tree
Parameter Descriptions	Null
Procedure	· Enter config view. Run: no spanning-tree Enter
Example	switch_config# no spanning-tree switch_config#

· Checking the configuration.

Command	show spanning-tree
Example	Switch_config# show spanning-tree No spanning tree instances exist

8.1.2 STP/RSTP Port Setting

Following will enter the interface view to configure ports mode of Spanning-tree.

· Configuring spanning-tree port-priority

Command	spanning-tree port-priority port priority
Parameter Descriptions	· port priority: The value ranges from 0 to 255. Port Priority in increments of 16 is required
Procedure	· Enter interface view. Run: Interface gigaethernet 0/1 Enter · Run: spanning-tree port-priority port priority Enter
Example	Switch_config# interface gigaEthernet 0/1 Switch_config_g0/1# spanning-tree port-priority 160 Switch_config_g0/1#

· Configuring spanning-tree cost

Command	spanning-tree cost port path cost
Parameter Descriptions	port path cost: port path cost, the value ranges from 0 to 200000000.
Procedure	· Run: spanning-tree cost number Enter
Example	Switch_config_g0/1# spanning-tree cost 100 Switch_config_g0/1#

· Configuring spanning-tree link type

Command	spanning-tree link-type link-type
Parameter Descriptions	· link-type: including two types: 1) point to point 2) shared
Procedure	· Run: spanning-tree link-type link-type Enter
Example	Switch_config_g0/1# spanning-tree link-type point-to-point Switch_config_g0/1#

· Set the port as edge port

Command	spanning-tree portfast
Parameter Descriptions	Null
Procedure	· Run: spanning-tree portfast Enter
Example	Switch_config_g0/1# spanning-tree portfast Switch_config_g0/1#

· Change an interface's spanning tree guard mode

Command	spanning-tree guard mode
Parameter Descriptions	· mode: including two modes: 1) none -- Set guard mode to none 2) root -- Set guard mode to root guard on interface
Procedure	· Run: spanning-tree guard mode Enter
Example	Switch_config_g0/1# spanning-tree guard root Switch_config_g0/1#

· Enable BPDU filtering for this interface

Command	spanning-tree bpdufilter enable
Parameter	Null

Descriptions	
Procedure	· Run: spanning-tree bpdufilter enable Enter
Example	Switch_config_g0/1# spanning-tree bpdufilter enable Switch_config_g0/1#

· Disable BPDU filtering for this interface.

Command	spanning-tree bpdufilter disable
Parameter Descriptions	Null
Procedure	· Run: spanning-tree bpdufilter disable Enter
Example	Switch_config_g0/1# spanning-tree bpdufilter disable Switch_config_g0/1#

· Enable BPDU guard for this interface

Command	spanning-tree bpduguard enable
Parameter Descriptions	Null
Procedure	· Run: spanning-tree bpduguard enable Enter
Example	Switch_config_g0/1# spanning-tree bpduguard enable Switch_config_g0/1#

· Disable BPDU guard for this interface

Command	spanning-tree bpduguard disable
Parameter Descriptions	Null
Procedure	· Run: spanning-tree bpduguard disable Enter
Example	Switch_config_g0/1# spanning-tree bpduguard disable Switch_config_g0/1#

· Checking the configuration.

Command	show running-config
Example	Switch_config# show running-config Building configuration. Current Configuration: !version 1.1.3c_M28P_B4M_T0 ! hostname username admin password 0 admin ! no spanning-tree ! no snmp-server view

	interface GigaEthernet 0/1 spanning-tree cost 100 spanning-tree port-priority 160 spanning-tree link-type point-to-point spanning-tree portfast spanning-tree bpduguard enable spanning-tree bpdufilter enable spanning-tree guard root ! --More--

8.2 Fast Ring

8.2.1 Enable global Fast Ring

Command	ring RINGID mode MODE
Parameter Descriptions	· RINGID : <0-255> -- Config RING id · MODE: single/double/coupling · single -- Config RING single mode · double -- Config RING double mode · coupling -- Config RING coupling mode
Procedure	· Enter config view. Run: ring RINGID mode MODE Enter.
Example	switch_config# ring 20 mode single switch_config#

8.2.2 Add Port into ring

Command	switchport ring RINGID
Parameter Descriptions	· RINGID :<0-65536> -- RING id
Procedure	· Enter interface view. Run: switchport ring RINGID Enter.
Example	switch_config# interface gigaethernet 0/24 switch_config_g0/24# switchport ring 300 switch_config_g0/24#

8.3 ERPS Ring

Ethernet Ring Protection Switching (ERPS) is defined in ITU-T G.8032 Recommendation. It prevents logical loops on a ring network by blocking redundant links.

ERPSv1 supports only the single-ring topology. When there is no faulty link on a ring network, ERPS can eliminate loops on the network. When a link fails on the ring network, ERPS can immediately restore the communication between the nodes on the network. Compared with other ring network protocols, ERPS has the following advantages:

- The network converges fast.
- ERPS is a standard protocol published by the ITU-T; therefore devices from different vendors can communicate with each other when they run ERPS.

ERPS works for ERPS rings. An ERPS ring consists of interconnected Layer 2 switching devices configured with the same control VLAN and data VLAN. Logically, an ERPS ring is a necessity before you configure other related functions.

8.3.1 Enable Global ERPs

Command	erps
Parameter Descriptions	Null
Procedure	· Enter config view. Run: erps Enter.
Example	switch_config# erps Enable ERPS successfully switch_config#

8.3.2 Create ERPs Ring and Interface

Command	erps ring RING-id east-interface east-interface west-interface west-interface
Parameter Descriptions	· RING-id: <1-32> -- Config RING id · east-interface: <1-28> -- Config ERPS RING PORT · west-interface: <1-28> -- Config ERPS RING PORT
Procedure	· Enter config view. Run: erps ring RING-id east-interface east-interface west-interface east-interface Enter.
Example	switch_config# erps ring 1 east-interface 1 west-interface 2 switch_config#

8.3.3 Enter MST View

Command	spanning-tree mst configuration
Parameter Descriptions	Null
Procedure	· Enter config view. Run: spanning-tree mst configuration Enter.
Example	switch_config# spanning-tree mst configuration switch_config_mst#

8.3.4 Configuring MST instance

Command	Instance VLAN vlan vlanIDs
Parameter Descriptions	· VLAN -- Range of vlans to add to the instance mapping · vlanIDs <1-4094> -- VLAN IDs(1-4094), such as(1,3,5,7) or (1,3-5,7) or (1-7)
Procedure	· Enter mst view. Run: instance VLAN vlan vlanIDs Enter.
Example	switch_config# spanning-tree mst configuration switch_config_mst# instance 1 vlan 3

8.4 Loopback Protect Configuration

Loopback detection sends loopback detection packets periodically to detect loops on the network connected to the device.

When a loop occurs on a network, broadcast, multicast, and unknown unicast packets are repeatedly transmitted on the network. This wastes network resources or even causes service interruption on the entire network. To protect the network, certain actions should be taken on the interface where the loop occurs, and the administrator needs to check the network connection and configuration to solve the problem soon. Therefore, a mechanism is required on a Layer 2 network to detect loops and notify the administrator.

Loopback detection is such a mechanism. It sends detection packets from an interface at intervals and checks whether the packets are sent back to the interface. If the packets are sent back, a loopback occurs on the interface.

The Loopback protection function is off by default.

· Enable the Loopback protection function

Command	switchport loppback-detected
Parameter Descriptions	Null
Procedure	· Enter interface view. Run: switchport loppback-detected Enter
Example	Switch_config# interface gigaEthernet 0/1 switch_config_g0/1# switchport loopback-detected switch_config_g0/1#

· Configuring loopback detected Time

Command	error-disable-recovery recovery-time TIME
Parameter Descriptions	· TIME :<300-3600s> -- Timeout in secends
Procedure	· Enter config view. Run: error-disable-recovery recovery-time TIME Enter.
Example	switch_config# error-disable-recovery recovery-time 200 switch_config#

· Enable loopback detected recovery

Command	error-disable-recovery enable
Parameter Descriptions	Null
Procedure	· Enter config view. Run: error-disable-recovery enable Enter.
Example	switch_config# error-disable-recovery enable switch_config#

· Checking the configuration.

Command	show running-config
Example	Switch_config# show running-config Building configuration. Current Configuration: !version 1.1.3c_M28P_B4M_T0 ! hostname username admin password 0 admin ! no spanning-tree ! no snmp-server view interface GigaEthernet 0/1 spanning-tree cost 100 spanning-tree port-priority 160 spanning-tree link-type point-to-point spanning-tree portfast spanning-tree bpduguard enable spanning-tree bpdufilter enable spanning-tree guard root switchport loopback-detected --More--

9 System Management Configuration

9.1 Port Mirroring Configuration

Packet mirroring copies the packets on a mirrored port (source port) to an observing port (destination port).

During network maintenance, maintenance personnel need to capture and analyze packets (for example, when there are suspicious attack packets). However, these operations always affect packet forwarding.

Packet mirroring copies packets on a mirrored port to an observing port so that you can analyze packets copied to the destination port by a monitoring device to monitor the network and rectify faults.

9.1.1 Port-based Mirroring Configuration

The device supports to configure the source interface and target interface of mirror, supporting 1 to 1 and many to 1 modes.

· Configuring source interface of mirror

Command	mirror session SPAN session number source interface interface type interface number mode
Parameter Descriptions	· SPAN session number: SPAN session number, the value is 1 as default, modification is not supported. · interface type : interface type, including GigaEthernet -- GigaEthernet interface TenGigaEthernet -- TenGigaEthernet interface · interface number: interface number, in the format as “0/port number”, the value of port number value is the port number of the switch. And it supports to choose more than one ports by the following mathods. 1) - : port range, format as “ 1-24” 2) , : multiple port numbers, format as “1,8” · mode : including three modes: 1) both: monitor received and transmitted traffic 2) tx: monitor received traffic only 3) rx: monitor transmitted traffic only
Procedure	· Enter config view. Run: mirror session SPAN session number source interface interface type interface number mode Enter
Example	Switch_config# mirror session 1 source interface gigaEthernet 0/1 -24 tx Switch_config#

· Configuring destination interface of mirror

Command	mirror session SPAN session number destination interface interface type interface number mode
Parameter Descriptions	· SPAN session number: SPAN session number, the value is 1 as default, modification is not supported.

	· interface type : interface type, including GigaEthernet -- GigaEthernet interface TenGigaEthernet -- TenGigaEthernet interface · interface number: interface number, in the format as “0/port number”, the value of port number value is the port number of the switch. And it supports to choose more than one ports by the following mathods. 1) - : port range, format as “ 1-24” 2) , : multiple port numbers, format as “1,8” · mode : including three modes: 1) both: monitor received and transmitted traffic 2) tx: monitor received traffic only 3) rx: monitor transmitted traffic only
Procedure	· Enter config view. Run: mirror session SPAN session number destination interface interface type interface number mode Enter
Example	Switch_config# mirror session 1 source interface gigaEthernet 0/1-24 rx Switch_config#

Command	mirror session 1 destination interface gigaEthernet port number
Parameter Descriptions	· port number : Ranges from 1~24
Procedure	· Enter config view. Run: mirror session 1 destination interface gigaEthernet port number Enter
Example	switch_config# mirror session 1 destination interface gigaEthernet 0/9 switch_config#

· Checking the configuration.

Command	show mirror session 1
Example	Switch_config# show mirror session 1 Session 1 --------- Destination Ports:g0/0 Source Ports: RX Only: g0/1-24 TX Only: None Both: None Switch_config#

9.2 SNMP Configuration

As a network management standard protocol used on TCP/IP networks, SNMP uses a central computer (NMS) that runs network management software to manage network elements.

In a large network, it is very difficult for network administrator to detect, locate and rectify the fault as the devices does not report the fault. This affects maintenance efficiency and increases maintenance workload. To solve this problem, equipment vendors have provided network management functions in some products. The NMS then can query the status of remote devices, and devices can send traps to the NMS in the case of particular events.

The device supports the following functions, Enable/disable SNMP function

· Configuring SNMP community permission, including

a) Read only

b) Read and write

· Configuring SNMP V3, The configuration includes the following procedures.

a) User name

b) Identity authentication, including MD 5, SHA

c) Verify password

d) Encryption protocol (optional), including 3des, aes and des

e) Encryption password

f) Read and write Mode, including ro (Read only) and rw (Read and write)

Configuring IP address of SNMP trap host

Following with the steps.

· Enable/disable SNMP function

Command	snmp-server view
Parameter Descriptions	Null
Command	no snmp-server view
Parameter	Null

· Configuring SNMP community permission

a) Read only

Command	snmp-server community SNMP community string ro
Parameter Descriptions	· SNMP community string: Name the SNMP community, supporting strings
Procedure	· Enter config view. Run: snmp-server community SNMP community string ro Enter
Example	switch_config# snmp-server community 123 ro switch_config#

b) Read and write

Command	snmp-server community SNMP community string rw
Parameter Descriptions	· SNMP community string: Name the SNMP community, supporting strings
Procedure	· Enter config view. Run: snmp-server community SNMP community string rw

	Enter
Example	switch_config# snmp-server community 12345 rw switch_config#

· Configuring SNMP V3

Command	snmp-server user user name auth Identity Authentication verify password priv Encryption Protocol Encryption Password Read and Write Mode
Parameter Descriptions	· user name: supporting 31 stings · Identity Authentication: identity authentication, including MD 5, SHA · verify password: authentication password, the range of length is 8-32. · Encryption Protocol: including 3des, aes and des · Encryption Password: encryption password, the range of length is 8-32. · Read and Write Mode: including ro (Read only) and rw (Read and Write)
Procedure	· Enter config view. Run: snmp-server user user name auth Identity Authentication verify password priv Encryption Protocol Encryption Password Read and Write Mode Enter
Example	switch_config# $ user SNMP2 auth md5 s12345678 priv des des12345678 rw switch_config#

· Configuring SNMP V3 host

Command	snmp-server host IP address
Parameter Descriptions	· IP address: IP address of SNMP trap host
Procedure	· Enter config view. Run: snmp-server host IP address Enter
Example	switch_config# snmp-server host 192.168.1.2 switch_config#

· Checking the configuration.

Command	show running-config
Example	Switch_config# show running-config Building configuration. Current Configuration: !version 1.1.3c_M28P_B4M_T0 ! hostname username admin password 0 admin ! no spanning-tree ! no snmp-server view ! snmp-server host 192.168.1.1

	snmp-server community public ro snmp-server community private rw snmp-server user admin123 auth md5 12345678 priv des 12345678 ro mirror session 1 source interface GigaEthernet 0/1-24 rx --More--

· Configuring SNMP Server contact information

Command	snmp-server contact contact
Parameter Descriptions	· contact -- Text for mib object sysContact
Procedure	· Enter config view. Run: snmp-server contact contact Enter.
Example	switch_config# snmp-server contact add-tel-name switch2_config# show running-config Building configuration... snmp-server contact add-tel-name ... switch_config#

· Configuring switch location information

Command	snmp-server location location
Parameter Descriptions	· location:LINE -- Text for mib object sysLocation
Procedure	· Enter config view. Run: snmp-server location location Enter.
Example	switch_config# snmp-server location aaadddd switch2_config# show running-config Building configuration... snmp-server contact add-tel-name snmp-server location aaadddd ... switch_config#

9.3 NTP Management

Network Time Protocol (NTP) is a protocol for synchronizing clocks on the network.

NTP is mainly used to synchronize clocks of all the devices on the network. Users can configure NTP so that all the clocks on the network are synchronized soon with high precision, preventing errors and heavy loads of network administrators.

· Enalbe NTP and set the IP address of NTP server.

Command	ntp server IP address

Parameter Descriptions	· IP address: the IP address of NTP server
Procedure	· Enter config view. Run: ntp server IP address Enter
Example	Switch_config# ntp server 192.168.5.6 Switch_config#

· Set the time interval to query NTP server

Command	ntp query-interval time interval
Parameter Descriptions	· time interval: the time interval to query NTP server, the value ranges from 1 min to 8640 mins (6 days). By default, the value is 1 min.
Procedure	· Enter config view. Run: ntp query-interval time interval Enter
Example	Switch_config# ntp query-interval 10 Switch_config#

· Disable NTP

Command	no ntp server
Parameter Descriptions	Null
Procedure	· Enter config view. Run: no ntp server Enter
Example	Switch_config# no ntp server Switch_config#

· Disable time interval to query NTP server

Command	no ntp query-interval
Parameter Descriptions	Null
Procedure	· Enter config view. Run: no ntp query-interval Enter
Example	Switch_config# no ntp query-interval Switch_config#

9.4 System Log Configuration

Logs of a specific module can be output to the log buffer, console, or log host. By default the log function is on.

The device supports output 8 levels of system log by default.

Levels	Description	Command lines
0	System is unusable	emergencies
1	Immediate action needed[	alerts
2	Critical conditions	critical
3	Error conditions	errors
4	Warning conditions	warnings
5	Normal but significant conditions	notifications
6	Informational messages	informational
7	Debugging messages[	debugging

Using command lines, users can enable/disable the function, configuring the device to output logs to log buffer, log host or to the console, and setting the ouput log levels.

· Enable/ disable the log function

Command	logging on
Parameter Descriptions	Null
Command	no logging on
Parameter Descriptions	Null

· Configuring the device to output logs to the log buffer

a) Configuring buffer size

Command	logging buffered logging buffer size
Parameter Descriptions	· logging buffer size: ranges from 4096 to 1048576
Procedure	· Enter config view. · Run: logging buffered logging buffer size Enter
Example	switch_config# logging buffered 6000 switch_config#

b) Configuring log level. After setting, the device will only record the set level log and levels higher than it.

Command	logging buffered level
Parameter Descriptions	level : level command line, including emergencies -- System is unusable[0] alerts -- Immediate action needed[1] critical -- Critical conditions[2] errors -- Error conditions[3] warnings -- Warning conditions[4] notifications -- Normal but significant conditions[5] informational -- Informational messages[6]

	debugging -- Debugging messages[7]
Procedure	· Enter config view. · Run: logging buffered level Enter
Example	switch_config# logging buffered errors switch_config#

· Configuring the device to output logs to log host

Command	logging host IP address of the logging host
Parameter Descriptions	· IP address of the logging host: IP address of the logging host
Procedure	· Enter config view. · Run: logging host IP address of the logging host Enter
Example	switch_config# logging host 192.168.1.1 switch_config#

· Configuring the device to output logs to the console

After setting, the device will only record the set level log and levels higher than it.

Command	logging console level
Parameter Descriptions	· level : level command line, including emergencies -- System is unusable[0] alerts -- Immediate action needed[1] critical -- Critical conditions[2] errors -- Error conditions[3] warnings -- Warning conditions[4] notifications -- Normal but significant conditions[5] informational -- Informational messages[6] debugging -- Debugging messages[7]

Procedure	· Enter config view. · Run: logging console level Enter
Example	switch_config# logging console informational switch_config#

· Configuring logging trap level

Command	logging trap LEVEL
Parameter Descriptions	· LEVEL support levels as follow: · emergencies -- System is unusable[0]

	· alerts -- Immediate action needed[1] · critical -- Critical conditions[2] · errors -- Error conditions[3] · warnings -- Warning conditions[4] · notifications -- Normal but significant conditions[5] · informational -- Informational messages[6] · debugging -- Debugging messages[7]
Procedure	· Enter config view. Run: logging trap LEVEL Enter.
Example	switch_config# logging trap informational

· Checking the configuration.

Command	show log
Example	Switch_config# show log 2020-08-20 18:00:15 [LINK-3-UPDOWN] Port GE0/23 Link Up! 2020-08-20 18:00:40 [CONFIG-5-WEB] User login successful - IP:192.168.1.191 Name :admin Switch_config#

9.5 System Management

9.5.1 Restore the System

The device supports to restore the system remotely.

Command	delete
Parameter Descriptions	Null
Procedure	· Enter enable view. · Run: delete Enter
Example	Switch# delete Are you sure to reset factory default(y/n)? Switch# delete Are you sure to reset factory default(y/n)? Commit succeed, if you want to enable the configuration, will reboot! Switch# umount: can't remount ramfs read-only umount: devtmpfs busy - remounted read-only swapoff: /etc/fstab: No such file or directory The system is going down NOW! Sent SIGTERM to all processes Sent SIGKILL to all processes Requesting system reboot

	Monitor version 1.06c is Booting. Hit ctrl+c to stop autoboot: 0 ..... Switch con0 is now available Press Return to get started.

9.5.2 Reboot the System

The device supports to reboot the system remotely.

Command	reboot
Parameter Descriptions	Null
Procedure	· Enter enable view. · Run: reboot Enter
Example	Switch# reboot Do you want to reboot the Switch(y/n)? Switch# umount: can't remount ramfs read-only umount: devtmpfs busy - remounted read-only swapoff: /etc/fstab: No such file or directory The system is going down NOW! Sent SIGTERM to all processes Sent SIGKILL to all processes Requesting system reboot Restarting system. Monitor version 1.06c is Booting. Hit ctrl+c to stop autoboot: 0 .... Switch con0 is now available Press Return to get started.

9.5.3 File Management

The device can do as a server or client to manage files.

When the device functions as a server, you can access the device on a terminal to manage files on the device and transfer files between the device and the terminal.

When the device functions as a client, you can use the device to manage files on other devices and transfer files between the device and other devices.

· Copy file from tftp server

Command	copy tftp: file name flash:
Parameter Descriptions	· file name: the name of file that to be copied

Procedure	· Enter enable view. Run: copy tftp: file name flash: Enter
Example	switch# copy tftp:11.img flash: Address or name of remote host []? 192.168.1.1 Source filename [11.img]? Destination filename [11.img]? please wait. 11.img 100% |**********| 11852k 0:00:00 ETA It is very dangerous to update IOS, are you sure(y/n)? switch#

· Copy file from system flash memory

Command	copy flash:file name tftp:
Parameter Descriptions	· file name: the name of file that to be copied
Procedure	· Enter enable view. Run: copy flash:file name tftp: Enter
Example	Example 2 Copy file from system flash memory Switch# copy flash: tftp: Address or name of remote host []? 192.168.1.100 Source filename []? SZ56150M.bin Destination filename [SZ56150M.bin]? please wait. SZ56150M.bin 100% |**********| 13824k 0:00:00 ETA finish. Switch#

The device can do as a server or client to manage files.

When the device functions as a server, users can copy startup configuration file.

Command	copy startup-config tftp:
Parameter Descriptions	Null
Procedure	· Enter enable view. Run: copy startup-config tftp: Enter
Example	Switch# copy startup-config tftp: Address or name of remote host []? 192.168.1.100 Destination filename [startup_config]? 22.cfg 22.cfg 100% |**********| 1252 0:00:00 ETA Building configuration.

9.6 User Setting

The switch manages users at levels. User levels are marked by numbers from 1 to 15, in ascending order. The access privilege of user is determined by the level of this user.

Command	username user name privilege privilege level password password
Parameter Descriptions	· user name: user name, the length should be less than 16. · privilege level: privilege level, the value ranges from 1 to 15. · password: password, the length should be less than 16.
Procedure	· Enter config view. · Run: username user name privilege privilege level password password Enter
Example	Switch_config# username admin123 privilege 15 password 123456789 Switch_config#

9.7 LLDP Configuration

Based on Layer 2 information obtained using LLDP, the NMS can quickly detect configuration conflicts between devices and locate network faults. Users can use the NMS to monitor link status of LLDP-enabled devices and quickly locate faults on the network.

The function is on by default, and the default hold time is 120s.

· Enable/disable LLDP function

Command	lldp enable
Parameter Descriptions	Null
Command	no lldp enable
Parameter Descriptions	Null

· Configuring LLDP timer

a) Hold time

The time that the receiver must keep the packet.

Command	lldp holdtime hold time
Parameter Descriptions	· hold time: ranges from 0 to 65535s.
Procedure	· Enter config view. Run: lldp enable Enter · Run: lldp holdtime hold time Enter
Example	switch_config# lldp enable switch_config# lldp holdtime 160 switch_config#

b) Interval time

When the LLDP status of the device keeps unchanged or the device does not discover new neighbors, the device sends LLDP packets to the neighbors at a certain interval.

Command	lldp timer interval time
Parameter Descriptions	· interval time: ranges from 0 to 65535s.
Procedure	· Enter config view. Run: lldp enable Enter · Run: lldp timer interval time Enter
Example	switch_config# lldp enable switch_config# lldp timer 200 switch_config#

c) Enable/Disable LLDP receive

Command	(no) lldp receive
Parameter Descriptions	Null
Procedure	· Enter interface view. Run: (no) lldp receive Enter.
Example	switch_config# interface gigaethernet 0/24 switch_config_g0/24# lldp receive switch_config_g0/24# no lldp receive switch_config_g0/24#

d) Enable/Disable LLDP transmit

Command	(no) lldp transmit
Parameter Descriptions	Null
Procedure	· Enter interface view. Run: (no)lldp transmit Enter.
Example	switch_config# interface gigaethernet 0/24 switch_config_g0/24# lldp transmit switch_config_g0/24# no lldp transmit

e) Show lldp nighbors list

Display information about neighbors, including device name, interface type and number, holdtime, port ID, and capabilities.

Command	show lldp neighbors
Parameter Descriptions	Null
Procedure	· Enter config view.

	Run: show lldp neighbors Enter.
Example	switch_config# show lldp neighbors Capability Codes: (R)Router,(B)Bridge,(C)DOCSIS Cable Device,(T)Telephone (W)WLAN Access Point, (P)Repeater,(S)Station,(O)Other Device Local_port Holdtime Port-ID Capability MS400980M Ge0/5 109 Ge0/4 B Total entries displayed: 1 switch_config#

9.8 Hostname Configuration

Hostname is the name of the switch. The hostname can be edited by user.

The factory default hostname is switch.

Command	hostname hostname
Parameter Descriptions	· hostname -- Name of switch
Procedure	· Enter config view. Run: hostname hostname Enter.
Example	switch_config# hostname switch2 switch2_config# show running-config Building configuration ... hostname switch2 ... switch2_config#

9.9 System Time Configuration

System time is the time on the switch and it can be edited.

Command	clock set HH:MM:SS DAY MONTH YEAY
Parameter Descriptions	· HH:MM:SS: -- Set time · DAY -- Set day(1-31) · MONTH -- Set month(1-12) · YEAY -- Set year(2000-2035)
Procedure	· Enter enable view.

	Run: clock set HH:MM:SS DAY MONTH YEAY Enter.
Example	switch# clock set 18:27:11 14 11 2023 Tue Nov 14 18:27:11 UTC 2023 switch# show clock 18:27:14 GMT+3 Tue Nov 14 2023 switch#

9.10 Timezone Configuration

Timezone can be edited and it is shown where the switch is installed.

Command	clock timezone NAME TIMEZONE
Parameter Descriptions	· NAME:WORD -- Name of time zone · TIMEZONE:<-12 - +12> -- Hours offset from UTC
Procedure	· Enter config view. Run: clock timezone NAME TIMEZONE Enter.
Example	switch_config# clock timezone dd1 +8 switch_conf#

9.11 Login Method

User authentication enables configuration access via Telnet, SSH, and HTTP. These protocols provide secure remote management, ensuring authorized users can configure and manage network settings efficiently.

· Enable Telnet Server

Command	telnet-server
Parameter Descriptions	Null
Procedure	· Enter config view. Run: telnet-server Enter.
Example	switch_config# telnet-server

· Enable SSH Service

Command	ssh enable
Parameter Descriptions	Null
Procedure	· Enter config view. Run: ssh enable Enter.
Example	switch_config# ssh enable

· Enable Https Service

Command	ip https server
Parameter Descriptions	Null
Procedure	· Enter config view. Run: ip https server Enter.
Example	switch_config# ip https server

10 Network Diagnosis

10.1 Ping Operation with IPv4

User login on a switch allows for the functionality of pinging devices, verifying network connectivity and troubleshooting issues via IPv4 ping in IPv4 network, ensuring seamless communication across the network infrastructure.

Command	ping TARGET
Parameter Descriptions	· TARGET: IP address or domain name
Procedure	· Enter config view. · Run: ping host · Enter.
Example	switch_config# ping 192.168.1.100 switch_config# ping www.google.com

10.2 Ping Operation with IPv6

User login on a switch allows for the functionality of pinging devices, verifying network connectivity and troubleshooting issues via IPv6 ping in IPv6 network, ensuring seamless communication across the network infrastructure.

Command	ping ipv6 TARGET
Parameter Descriptions	· TARGET: x:x:x:x:x:x:x:x -- IPv6 address
Procedure	· Enter config view. Run: ping ipv6 TARGET Enter.
Example	switch_config# ping ipv6 200::12 switch_config#

10.3 Using IP Traceroute

Traceroute is a diagnostic tool that traces the path packets take through a network. It identifies network hops, measures latency, and identifies connectivity issues, helping troubleshoot and optimize network performance. Traceroute aids in understanding network topology and locating bottlenecks for efficient troubleshooting.

You can use IP traceroute to identify the path that packets take through the network on a hop-by-hop basis.

Command	traceroute host
Parameter Descriptions	· host:WORD -- Trace route to destinaton address or hostname
Procedure	· Enter enable view. Run: traceroute host Enter.
Example	switch# traceroute 192.168.3.214

	Flags: ... -----+-----------+---------- traceroute to 192.168.3.214 (192.168.3.214), 30 hops max, 38 byte packets 1 192.168.3.214 (192.168.3.214) 2.190 ms 0.569 ms 0.553 ms switch#