MICROSENS

L3 Managed Switch - CLI-based Configuration Guide

Version V1.0

MICROSENS GmbH & Co. KG
Kueferstr. 16
59067 Hamm/Germany

Tel. +49 2381 9452-0
FAX +49 2381 9452-100
E-Mail info@microsens.de
Web www.microsens.de

Table of Contents

1. 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 or contact your dealer.
Web-based Configuration Guide	Including Web network management system configuration instructions.	Please contact your dealer.
CLI-based Configuration Guide	Including CLI-based configuration instructions	Please contact your dealer.

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.

Crossreference-table

Product	**Valid**
MS657308PMX	Yes
MS400980M	Yes
MS400981M	Yes
MS400990M	Yes

Announcement

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

The document is only used as operation guide, except for other promises. 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
Keywords	The keywords of a command line are underlined in light blue, not in boldface.
Parameters	Command arguments are underlined in dark, not in boldface.

Symbol Conventions

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

❗	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.
⚠	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injury.
🔥	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
ℹ	Provides additional information to emphasize or supplement important points in the main text.

2. 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.

2.1. 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

> Users can use the built-in terminal emulation software (such as the HyperTerminal of Windows 2000/XP) on the PC. If no built-in terminal emulation software is available, use the third-party terminal emulation software.

2.2. Configuration Procedure

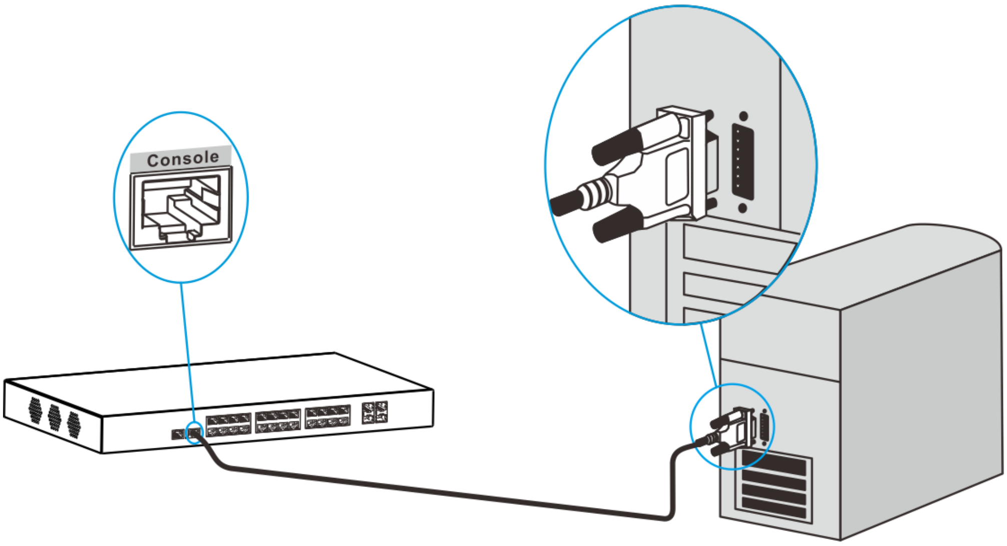
Use the terminal emulation software to log in to the device through the console port, and complete the basic configuration for the device.

Default Configiration

Data	Default Value
Transfer rate	115200 bit/s
Flow control mode	Not Supported
Test mode	Not Supported
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.

> 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

2.3. Configuration 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 calbe 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

3. Cli Overview

3.1. 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.

3.2. 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: **<u>interface interface type interface number</u>** • 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.

4. 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
```

5. 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.

5.1. 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#

5.2. Enable/disable the 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#

5.3. Configure the Port

Command	**description description**
Parameter Descriptions	• **description**: 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**: 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#

5.4. 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#

5.5. 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#

5.6. 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	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	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	storm-control unicast threshold 100 switch_config_g0/24#

5.7. 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	flow-control on switch_config_g0/24# switch_config_g0/24# flow-control off switch_config_g0/24#

5.8. 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#

5.9. Configue 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 1500-13000 bytes.
Procedure	• Enter interface view • Run: **mtu jumbo size** Enter
Example	switch_config_g0/24# mtu jumbo 9000 switch_config_g0/24#

5.10. Configure the IP Address of VLAN Interface

Enter interface view to configure vlanIF logical interface.
Run: **switch_config# interface vlan 1**
The command lines are displayed in this view:

```
switch_config_v1#
switch_config_v1# ?
arp           -- arp timeout configuration commands
bfd           -- BFD protocol configuration commands
end           -- Exit to EXEC mode
exit           -- Exit
gvrp           -- Enable GVRP protocol
help           -- Description of the interactive help system
interface        -- Interface configuration
IP            -- IP configuration commands
ipv6           -- IPv6 configuration commands
name           -- Config the name of current vlan
no            -- Negate configuration
show           -- Show configuration and status
subvlan         -- Config the name of current vlan
supervlan        -- Super vlan
vrrp           -- VRRP Interface configuration commands
```

Change the IP address of the VLAN Interface

Command	**IP address IP address subnet mask**
Parameter Descriptions	• **IP address**: the IP address of the Ethernet interface, no default value. • **Subnet**: the subnet mask of the IP address

Procedure	- Enter config view. - Run: IP **address** IP **address subnet mask** Enter
Example	switch_config_v1# IP address 192.168.1.87 255.255.255.0 switch_config_v1#

5.11. 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#

6. Ethernet Configuration

6.1. 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 group number**
Parameter Descriptions	• **group number**: interface port-aggregator group number, ranges from 0-6
Procedure	• Enter config view • Run: **interface port-aggregator group number** Enter
Example	switch_config# interface port-aggregator 3 switch_config_p3#

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 group number mode mode**
Parameter Descriptions	• **group number**: group number , the aggregator-group number, ranges from 1-6 • **mode:** including: lacp, static
Procedure	• Enter interface view • Run: **aggregator-group group number mode mode** Enter • Checking the configuration • Run: **show aggregator-group summary** Enter
Example	switch_config# interface gigaEthernet 0/7 switch_config_g0/7# aggregator-group 3 mode static switch_config_g0/7#

Checking the configuration

Command	**show aggregator-group summary**
Parameter Descriptions	Null

Procedure	• Enter interface view • Run: **<u>show aggregator-group summary</u>** 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#

6.2. 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	**<u>Interface interface type interface number</u>**
Parameter Descriptions	• **<u>interface type</u>**: interface type, including: GigaEthernet -- GigaEthernet interface TenGigaEthernet -- TenGigaEthernet interface • **<u>interface number:</u>** 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 IDs such as (1,3,5,7) Or (1,3-5,7) Or (1-7)
Procedure	• Enter interface view • Run: **switchport trunk vlan-allowed** 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 IDs such as (1,3,5,7) Or (1,3-5,7) Or (1-7)
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#

6.3. 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:

1. Priority mapping
2. Congestion management
3. Traffic policy

6.3.1. 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--

6.3.2. 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--

6.3.3. 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 the data packet

Command	**exit**
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#

7. IP Service 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.

7.1. 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#

Enter VLAN Interface view

Command	**Interface vlan vlan interface number**
Parameter Descriptions	**vlan interface number:** vlan interface number, the value ranges from 1 to 4094
Procedure	• Enter config view • Run: **Interface vlan vlan interface number** Enter
Example	switch_config# interface s vlan 2 switch_config_v2#

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 s 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> • **subnet mask:** subnet mask of the IP address

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#

Checking the configuration

Command	**show interface vlan**
Example	Switch_config_v6# show interface vlan interface vlan 1 IP address 192.168.1.1 255.255.255.0 interface vlan 2 IP address 192.168.2.1 255.255.255.0 interface vlan 6 IP address 192.168.1.161 255.255.255.255 ipv6 address 2000::1111/64

7.2. 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.

Enable DHCP snooping

Command	**IP dhcp snooping**
Parameter Descriptions	Null
Procedure	• Enter config view • Run: IP **dhcp snooping** Enter
Example	Switch_config# IP dhcp snooping Switch_config#

Disable DHCP snooping

Command	**no IP dhcp snooping**
Parameter Descriptions	Null
Procedure	• Enter config view • Run: **no IP dhcp snooping** Enter
Example	Switch_config# no IP dhcp snooping Switch_config#

Create a DHCP pool (There is no DHCP pool by default)

Command	**IP dhcp pool word**
Parameter Descriptions	**word:** DHCP pool name, the value ranges from 1 to 32.
Procedure	• Enter config view • Run: IP **dhcp pool word** Enter
Example	Switch_config# IP dhcp pool 1 Switch_ip_dhcp#

Specify the range of IP addresses that can be allocated dynamically in the global address pool.

Command	• **network IP address IP subnet mask**
Parameter Descriptions	• **IP address:** IP address • **IP subnet mask:** subnet mask of the IP address
Procedure	• Enter IP DHCP pool view • Run: **network IP address IP subnet mask** Enter
Example	Switch_ip_dhcp# network 192.168.5.16 255.255.255.0 Switch_ip_dhcp#

Note: When configuring the range of dynamically assignable IP addresses in the global address pool, ensure that the range is that same as the network segment on which the DHCP server interface address or the DHCP relay agent interface address resides. This avoids incorrect assignment of IP addresses.

Set the IP address lease

Command	• **lease time**
Parameter Descriptions	• **time:** IP address the IP address lease time, including two ranges: 1. the value ranges from 1 to 365 days 2. infinite: the value is 365 days (31622400 s). the value is 1 day (86400s) by default.
Procedure	• Enter IP DHCP pool view • Run: **lease time** Enter
Example	Switch_ip_dhcp# lease 365 Switch_ip_dhcp#

Set the DNS server

Command	• **Dns-server IP address**
Parameter Descriptions	• **IP address:** IP address of the DNS server

Procedure	- Enter IP DHCP pool view - Run: **Dns-server IP address** Enter
Example	Switch_ip_dhcp# dns-server 3.3.3.3 Switch_ip_dhcp#

Set the default router

Command	- **default-router IP address**
Parameter Descriptions	- **IP address:** IP address
Procedure	- Enter IP DHCP pool view - Run: **default-router IP address** Enter
Example	Switch_ip_dhcp# default-router 192.168.1.100 Switch_ip_dhcp#

Set the IP address range of DHCP

Command	- **range DHCP Start IP address DHCP End IP address**
Parameter Descriptions	- **DHCP Start IP address:** DHCP Start IP address - **DHCP End IP address:** DHCP End IP address
Procedure	- Enter IP DHCP pool view - Run: **range DHCP Start IP address DHCP End IP address** Enter
Example	Switch_ip_dhcp# range 192.168.1.11 192.168.1.210 Switch_ip_dhcp#

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 ! IP dhcp pool 1 network 1,192.168.1.100 255.255.255.255 default-router 192.168.1.100/24192.168.1.11-192.168.1.210 rang 192.168.1.11 192.168.1.210 lease 0 1 0 dns-server 3.3.3.3

7.3. 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.

Create static ARP

Command	• **arp** IP **address MAC address vlan vlanIF number interface interface type interface number/port number**
Parameter Descriptions	• **IP address:** IP address, IP address of the unicast • **MAC address:** MAC address, MAC address of the device • **vlanIF number:** vlanIF number, ranges from 1-4094 • **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. • **port number:** port number, ranges from 1-24

Procedure	• Enter IP DHCP pool view • Run: **arp** IP **address MAC address vlan vlanIF number interface interface type interface number/port number** Enter
Example	switch_config# arp 192.168.1.100 4c-ed-fb-61-4a-e6 vlan 1 interface + gigaEthernet 0/3 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

Configure the aging time

Command	• **arp timeout arp timeout**
Parameter Descriptions	• **arp timeout:** ranges from 1-65535 (seconds)
Procedure	• Exit and enter interface view • Run: **arp timeout** arp timeout Enter
Example	switch_config# switch_config# interface vlan 2 switch_config_v2# arp timeout 10 switch_config_v2#

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 ====================================

7.4. 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 IP address**
Parameter Descriptions	• **IP address:** Domain name server's IP address
Procedure	• Enter config view • Run: **IP dns server IP address** Enter
Example	switch_config# IP dns server 192.168.2.5 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-

8. IP Router Configuration

The device supports to configure RIP, OSPF and static IP router.

8.1. RIP Configuration

RIP is widely used on small-sized networks to discover routes and generate routing information.
No default value.

Creating a RIP process, the protocol type is RIP-V2 by default.

Command	**router RIP**
Parameter Descriptions	Null
Procedure	• Enter config view • Run: **router rip** Enter
Example	switch_config# router rIP switch_router_rip#

Configuring RIP network

Command	**network IP address**
Parameter Descriptions	**IP address** supporting IPv4 address and IPv6 address
Procedure	• Enter router rIP view • Run: **network** IP address Enter
Example	switch_router_rip# network 1.1.1.1 switch_router_rip#

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 ! router rIP network 1.1.1.1 255.255.255.0

8.2. OSPF Configuration

By building OSPF networks, you can enable OSPF to discover and calculate routes in autonomous systems. OSPF is applicable to a large-scale network that consists of hundreds of devices.
No default value.

Creating an OSPF process

Command	**router ospf process-id**
Parameter Descriptions	**process-id** the parameter process-id specifies the ID of an OSPF process. The value ranges from 1 to 65535. The default value is 1
Procedure	• Enter router rIP view • Run: **router ospf process-id** Enter
Example	switch_config# router ospf 1 switch_router_ospf#

Configuring OSPF network

Command	**network** IP **address IP netmask area Area ID**
Parameter Descriptions	• **IP address** supporting IPv4 address and IPv6 address • **IP netmask** subnet mask of the IP address • **area ID** Area ID, including two formats 1. The value ranges from 1 to 65535 2. In IP address format.

Procedure	• Enter router rIP view • Run: **network** IP **address area Area ID**+ Enter
Example	Switch_router_ospf# network 192.168.1.199 255.255.255.255 area 2 Switch_router_ospf#

8.3. Static Routes Configuration

On a simple network, only static routes are required to ensure normal running of the network. On a complex large-scale network, static routes ensure bandwidth for important applications because they remain unchanged even when the topology changes.
No default value.

Default configuration of static routes

Command	**IP route default IP address**
Parameter Descriptions	**Default IP address** Gateway IP address, the gateway IP address
Procedure	• Enter Gateway IP address, the gateway IP address view • Run: IP **route default IP address** Enter
Example	switch_config# IP route default 1.1.1.1 switch_config#

Configuration of static routes

Command	**IP route gateway IP address subnet mask next loop IP address**
Parameter Descriptions	• **gateway IP address** the default IP address • **subnet mask** the netmask of the default IP address • **next loop IP address** next loop IP address
Procedure	• Enter config view • Run: IP **route gateway IP address subnet mask next loop IP address** Enter

Example	switch_config# IP route 1.1.1.1 255.255.255.0 2.2.2.2 switch_config#

Checking the configuration

Command	**show ip route**
Example	Switch_config# show ip route Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area+ * - candidate default S 0.0.0.0/0 [1/0] via 1.1.1.1 inactive S 1.1.1.0/24 [1/0] via 2.2.2.2 inactive C>* 192.168.1.0/24 is directly connected, vlan 1 C>* 192.168.100.0/24 is directly connected, loopback Switch_config#

9. IP Multicast Configuration

9.1. 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#

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#

10. Security Configuration

10.1. 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

10.1.1. 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--

10.1.2. 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	**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

10.1.3. 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 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--
```

11. Reliability

11.1. 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.

11.1.1. 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
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	- 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

11.1.2. 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	- 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 Descriptions	Null
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 enable**
Parameter Descriptions	Null
Procedure	• Run: **spanning-tree bpdufilter enable** Enter
Example	Switch_config_g0/1# spanning-tree bpdufilter enable 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--

11.2. 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#

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--

11.3. VRRP Configuration

VRRP is a fault-tolerant protocol and provides a single default gateway address for hosts. If a VRRP-enabled router fails, another VRRP-enabled router takes over traffic, ensuring continuity and reliability for network communication.

As networks rapidly develop and applications become diversified, various value-added services such as IPTV and video conferencing are widely used. Demands for network infrastructure reliability are increasing, especially in nonstop network transmission for users.

Generally, hosts communicate with external networks through the gateway, as shown in Figure 1. When the gateway is faulty, hosts fail to communicate with external networks. One method to prevent communication interruption is usually to configure multiple egress gateways. However, terminal devices cannot select routes to these gateways because terminal devices often do not support routing protocols.

VRRP virtualizes multiple routing devices into a virtual router and uses the virtual router IP address as the default gateway address. When the gateway device becomes faulty, VRRP uses a new gateway device to transmit service traffic. This ensures reliable communication.

Enter interface VLAN view.

Command	**Interface vlan vlan id**
Parameter Descriptions	Null
Procedure	• Enter config view • Run: **Interface vlan vlan id** Enter
Example	Switch_config# interface vlan 1 Switch_config_v1#

Create a VRRP group.

Command	**vrrp VRID priority priority**
Parameter Descriptions	• **VRID:** VRRP group number • **priority:** VRRP priority, the priority level ranges from 1 to 254. By default the value is 100.
Procedure	• Enter interface VLAN view • Run: **vrrp VRID priority priority** Enter
Example	Switch_config_v1# vrrp 1 priority 1 Switch_config_v1#

Enable preemption of lower priority Master

Command	**vrrp VRID preempt**
Parameter Descriptions	• **VRID:** VRRP group number
Procedure	• Enter interface VLAN view • Run: **vrrp VRID preempt** Enter
Example	Switch_config_v1# vrrp 1 preempt Switch_config_v1#

Enable delay of Virtual Router timer and set the delay time

Command	**vrrp VRID timer time delay**
Parameter Descriptions	• **VRID:** VRRP group number • **time delay:** time delay, the value ranges from 1s to 10s
Procedure	• Enter interface VLAN view • Run: **vrrp VRID timer time delay** Enter
Example	Switch_config_v1# vrrp 1 timer 10 Switch_config_v1#

Enable authentication and set the authentication word

Command	**vrrp VRID authentication authentication word**
Parameter Descriptions	• **VRID:** VRRP group number • **authentication word:** hexadecimal numbers
Procedure	• Enter interface VLAN view • Run: **vrrp VRID authentication authentication word** Enter
Example	Switch_config_v1# vrrp 1 authentication 00111101 Switch_config_v1#

Set the VRRP group IP address

Command	**vrrp VRID authentication virtual IP address**
Parameter Descriptions	• **VRID:** VRRP group number • **virtual IP address:** virtual IP address
Procedure	• Enter interface VLAN view • Run: **vrrp** **VRID authentication** **virtual IP address** Enter
Example	Switch_config_v1# vrrp 1 associate 192.168.1.6 Switch_config_v1#

Checking the configuration.

Command	**show vrrp interface VRRP interface vlan**
Parameter Descriptions	• **VRID interface vlan:** VLAN ID of the VRRP group
Example	Switch_config_v1# show vrrp interface 1 VLAN1 (192.168.1.6 C40880015C23) -- group id: 1 state: Master priority : 99 preempt: on authentication: auth advertisement interval: 1 advertisement timer expiry : 1

12. System Management Configuration

12.1. 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.

12.1.1. 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 methods. 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 methods. 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 tx 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 port number 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#

12.2. 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
Procedure	- Enter config view - Run: **no snmp-server view** Enter
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	• **user name:** supporting 31 strings • **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)
Parameter Descriptions	• **SNMP community string:** Name the SNMP community, supporting strings
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--

12.3. 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#

12.4. 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 Line**
0	System is unstable	emergencies
1	Immediate action needed	alerts
2	Critical conditions	critical
3	Error conditons	errors
4	Warning conditions	warning
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

Procedure	• Enter config view • Run: **no logging on** Enter
Parameter	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#

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#

12.5. System Management

12.5.1. Restore 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.

12.5.2. Reboot the System

The device supports to reboot the system remotely.

Command	**reboot**
Parameter Descriptions	Null
Procedure	• Enter enable view • Run: **delete** 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.

12.5.3. 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.

12.6. 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#

12.7. Configure Loopback Detection

While the Loopback function is enabled, users could check if there is a Loopback for the device under this port. If there is Loopback, the port will be shutdown.

The function is off by default.

Enable/disable the function

Command	**switchport loopback-detected**

Parameter Descriptions	Null
Command	**no switchport loopback-detected**
Parameter Descriptions	Null

The device supports 4 IP addresses. Users can configure the out band IP address of loopback interfaces.

Command	**interface loopback manage number IP address subnet mask**
Parameter Descriptions	- **Manage number:** the number of management interfaces, ranges from 1 to 4. - **Ip address:** the IP address of the management interface. - **Subnet:** the subnet mask of the IP address.
Procedure	- Enter config view - Run: **interface loopback manage number IP address subnet mask** Enter
Example	switch_config# interface loopback 1 192.168.3.101 255.255.255.0 switch_config# interface loopback 2 192.168.3.102 255.255.255.0 switch_config# interface loopback 3 192.168.3.103 255.255.255.0 switch_config# interface loopback 4 192.168.3.104 255.255.255.0 switch_config#

12.8. 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 holdtime interval time** Enter
Example	switch_config# lldp enable switch_config# lldp timer 200 switch_config#

Disclaimer

All information in this document is provided 'as is' and is subject to change without notice.

MICROSENS GmbH & Co. KG disclaims any liability for the correctness, completeness or quality of the information provided, fitness for a particular purpose or ensuing damage.

Any product names mentioned herein may be trademarks and/or registered trademarks of their respective owners.

Document ID: PM-21008_CLI-Manual_MS657308PMX_v1.0