GTWave L2 Switch CLI User Guide

V1.0

GT-Wave

Contents

Preface 7

Ⅰ Introduction 9

1. Product Overview 9

2. Product Features 10

Ⅱ. CLI Management Service Access 13

1. Accessible Management Services 13

2. Default Device Settings 13

3. Console Connection 14

4. SSH 16

5. Telnet 18

Ⅲ. Basic CLI Commands 19

1. CLI Basic Symbols 19

2. Basic CLI Keys 19

3. Classification of CLI modes 20

4. CLI Basic Command 22

Ⅳ. Switch Configuration 24

1. System Configuration 24

1.1 System Information 24

1.2 Serial Information ····28
1.3 User Management ····29
1.4 Safe Management ····32
1.5 SNTP Configuration ····39
1.6 Jumbo Frame Configuration ····42
1.7 Save Current Configuration ····43
1.8 Configuration File ····44
1.9 File Upload ····45
1.10 Ping Diagnosis ····46
1.11 System Reboot ····47

2 Port ····48
2.1 Basic Configuration ····48
2.2 Port Statistics ····51
2.3 Flow Control ····53
2.4 Broadcast Storm ····54
2.5 Port Ratelimit ····57
2.6 Protected Port ····58
2.7 Learn Limit ····60
2.8 Port Trunking ····61
2.9 Mirror ····64
2.10 DDM Information ····66
2.11 Cable Diagnosis ····68

3 MAC Configuration ····69
3.1 MAC Table ····69
3.2 MAC Binding ····69

3.3 MAC Auto Binding ····71
3.4 MAC Filter ····72
3.5 MAC Auto Filter ····73

4. VLAN Configuration ····75
4.1 VLAN Information ····75
4.2 VLAN Configuration ····76
4.3 VLAN Port Configuration ····78

5. SNMP Configuration ····83
5.1 Community Name ····84
5.2 TRAP Target ····86
5.3 SNMP User ····88

6. ACL Configuration ····90
6.1 Standard IP ····90
6.2 Extended IP ····92
6.3 MAC IP ····95
6.4 MAC ARP ····97
6.5 ACL Information ····100
6.6 ACL Reference ····101

7. QOS Configuration ····103
7.1 QoS Apply ····103
7.2 QoS Schedule ····106

8. IP Basic Configuration ·····109

8.1 IP Address Configuration ·····110

8.2 ARP Configuration and Display ·····111

8.3 Host Static Route Configuration ·····113

9. AAA Configuration ·····115

9.1 AAA Authentication ·····115

9.2 Tacacs+ Configuration ·····116

9.3 Radius Configuration ·····118

9.4 802.1x Configuration ·····121

9.5 802.1x Port Configuration ·····123

9.6 802.1x User Auth-Information ·····125

10. MSTP Configuration ·····126

10.1 MSTP Global Configuration ·····126

10.2 MSTP Port Configuration ·····130

10.3 Port Information ·····132

11. IGMP SNOOPING Configuration ·····133

11.1 IGMP SNOOPING Configuration ·····133

11.2 Multicast Group Information ·····136

12. GMRP Configuration ·····138

12.1 GMRP Global Configuration ·····138

12.2 GMRP Ports Configuration ·····139

12.3 GMRP State Machine ·····142

13. GVRP Configuration ·····143
13.1 GVRP Global Configuration ·····143
13.2 GVRP Ports Configuration ·····144
13.3 GVRP State Machine ·····146

14. EAPS Configuration ·····148
14.1 EAPS Configuration ·····148
14.2 EAPS Information ·····153

15. RMON Configuration ·····154
15.1 Statistics Configuration ·····154
15.2 History Configuration ·····157
15.3 Alarm Configuration ·····160
15.4 Event Configuration ·····162

16. Cluster Management ·····164
16.1 NDP Configuration ·····164
16.2 NTDP Configuration ·····166
16.3 Cluster Configuration ·····168

17. ERPS Configuration ·····172
17.1 ERPS Configuration ·····172
17.2 ERPS Information ·····178

18. LLDP Configuration ·····180

18.1 LLDP Global Configuration ····180
18.2 LLDP Ports Configuration ····182
18.3 LLDP Neighbor ····186

19. Log Management ····188
19.1 Log Configuration ····188
19.2 Log Information ····189

20. PoE ····190
20.1 PoE Port Configuration ····190
20.2 PoE Policy Configuration ····193
20.3 PD Query Configuration ····195

21. Industrial Switch Monitoring ····197

Ⅴ Troubleshooting ····202

Preface

GTWave Co.,Ltd. is committed to continuously improving product specifications and performance through continuous research and development. The contents of this manual are subject to change without prior notice due to product function changes, error corrections, and other reasons. The companies, names, and materials used as examples in this Administrator's User Manual are arbitrary and are otherwise indicated separately. Furthermore , this manual may contain technical errors or typos, and the product screens used in the User Manual may differ from the actual product.

Contact Us

Web site : http://www.gtwave.co.kr

e-Mail : master@gtwave.co.kr

Address : 804-2, Technopark-B,
723, Pangyo-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Republic of Korea

Phone : 031-707-4670

About This Manual

Purpose and Intended Audience

This product manual has been created to explain how to access, configure, and monitor the GTWave Switch Series using Console, SSH, Telnet, and Web interfaces.

The intended audience includes network administrators and engineers in organizations using the GTWave Switch Series. This manual is written under the assumption that readers have a solid understanding of TCP/IP, network protocols, and general networking concepts.

Copyright

The copyright and intellectual property rights of this product manual belong to GTWave Co., Ltd.

No part of this manual may be reproduced or distributed in whole or in part without the prior written consent of the company. When quoting a portion of this manual, the source must be clearly indicated as: Source: GTWave_Switch_Series."

Notes

This product manual has been written for the entire GTWave_Switch_Series. Although the GTWave Switch Series shares core hardware components such as CPU, memory, and flash across models, additional hardware specifications may vary by model.

In particular, some switch models include features such as system monitoring, while basic network switch models do not.

The fundamental switching and security functions are the same, but configuration items may differ depending on additional hardware specifications, such as the presence of cooling fans.

I Introduction

1. Product Overview

1.1. Product Description

The GTWave_Switch_Series is a security-certified managed network switch equipped with 1Gbps TP ports and SFP slots supporting 1/10Gbps. This secure and standards-compliant 1/10Gbps Ethernet switch can automatically detect the correct transmission speed and determine the port's full-duplex or half-duplex mode. In backbone or server-connected secure topologies, it is capable of handling high-volume data traffic.

To ensure low latency and high data integrity, the switch supports the store-and-forward transmission method, which removes unnecessary traffic and alleviates congestion in critical network paths. Through an intelligent address learning algorithm, the managed 10G Ethernet switch can recognize up to 8K different MAC addresses, providing complete wire-speed filtering and forwarding performance.

Designed for high performance, reliability, and secure access, GIOTI switch products offer a wide range of options for enterprise networks, extending from stable indoor environments to outdoor and industrial applications.

The GIOTI Switch Series, built on a next-generation high-performance platform and an independently developed switching system, supports flexible network management features such as IEEE 802.1Q VLAN, IGMP, port monitoring, port aggregation, bandwidth control, and ring applications.

Engineered to meet the needs of high-performance and complex network infrastructures, the GIOTI_Security_Switch_Series provides a comprehensive security protection system, robust QoS policies, rich VLAN capabilities, and simplified management and maintenance, making it ideal for deployment at the core layer of SMEs, communities, and educational institutions.

The GIOTI_Security_Switch_Series industrial network switches are a modern, rugged Ethernet switch family designed for harsh environments, making them ideal for connecting IoT devices, access points, and user terminals.

The PoE-supported GIOTI Switch Series is a high-power managed AUTO PoE switch. It features ports supporting 24V + 48V PoE power supply and 90W output compliant with IEEE 802.3af/at/PoE++/BT standards. As a highly compatible PoE power supply device, it provides flexible and cost-effective Gigabit ports that automatically detect and identify standard-compliant powered devices, delivering power through network cables.

With plug-and-play operation, easy configuration, and simple management, the GIOTI PoE switches are ideal for outdoor high-power APs, Skynet cameras, and other applications, forming a cost-effective PoE network solution.

2. Product Features

■ Layer 2 Features

- High-performance Store-and-Forward architecture that removes erroneous packets to ensure frame integrity.
- Storm Control support
  - Controls Broadcast, Multicast, and Unknown Unicast storms.
- VLAN Support
  - IEEE 802.1Q tagged VLAN
  - Supports up to 255 VLAN groups, selectable from 4,094 VLAN IDs
    - MAC-based VLAN
  - GVRP (GARP VLAN Registration Protocol)
- Spanning Tree Protocol Support
  - IEEE 802.1D Spanning Tree Protocol (STP)
  - IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
  - IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), spanning tree by VLAN
  - BPDU Guard
- Link Aggregation Support
  - 802.3ad Link Aggregation Control Protocol (LACP)
  - Supports up to 8 trunk groups, with up to 8 ports per trunk group
- Port Mirroring (1 : 1 / N : 1)
  - Allows monitoring of ingress or egress traffic from specific ports.

■ Power over Ethernet (PoE Switch Models)

- Complies with IEEE 802.3af/at/bt Power over Ethernet PSE standards
- Selectable PoE modes: IEEE 802.3af / 802.3at / 802.3bt
- Automatic PD (Powered Device) detection
- Protection circuitry prevents power interference between ports

■ QoS (Quality of Service)

- Bandwidth control via Ingress Shaper and Egress Rate Limiting per port
- Four priority queues supported on all switch ports
- Traffic Classification

- IEEE 802.1p Class of Service (CoS)
- TOS / DSCP / IP Precedence for IPv4/IPv6 packets

- Strict Priority and Weighted Round Robin (WRR) CoS policies
- QoS and In/Out bandwidth control per port

- Traffic Policing supported on switch ports
- DSCP remarking support

■ Multicast

- Support IPv4 IGMP Snooping v1, v2 and v3
- Support IPv6 MLD Snooping v1 and v2
- Querier Mode Support
- IPv4 IGMP Snooping Port filtering
- Multicast VLAN Registration(MVR) support

■ Security

- Authentication
  - Built-in RADIUS client for integration with RADIUS servers
  - TACACS+ login user authentication
  - RADIUS / TACACS+ user access authentication
  - Guest VLAN assigns clients to a VLAN with limited service access
- Access Control Lists (ACLs)
  - IP-based ACLs
- Source MAC / IP address binding
- DHCP Snooping for filtering untrusted DHCP messages
- Dynamic ARP Inspection (DAI) removes ARP packets with invalid MAC-IP bindings
- IP Source Guard prevents IP spoofing attacks

■ Management

- Switch Management Interfaces
  - Console service via Command Line Interface (CLI)
  - Web-based management via HTTP/HTTPS
  - HTTPS (SSL/TLS v1.2/v1.3) secure access
  - SSH v2.0 secure access
  - Telnet Command Line Interface
  - SNMP v1, v2c, and v3 switch management
- IPv6 support, IP Addressing, and NTP synchronization
- BOOTP / DHCP for IP address assignment
- System Maintenance
  - Firmware upload/download via CLI or Web interface
  - Reset button for system reboot or factory reset
- DHCP Relay
- DHCP Option 82 support

- Built-in DHCP Server
- User privilege level control
- NTP (Network Time Protocol) support
- Link Layer Discovery Protocol (LLDP) and LLDP-MED support
- Network Diagnostics
  - ICMPv4 / ICMPv6 remote ping
  - Cable diagnostics to detect and report potential cable issues
- Remote alerting via Syslog
- System Log support

Ⅱ. CLI Management Service Access

This section provides a brief overview of how to access the switch.

1. Accessible Management Services

The switch can be accessed using the following management services: Local (Console) access, SSH, Telnet.

Telnet is disabled when shipped from the factory or after a reset. If you need access to the Telnet management access service, you must connect to the Console or SSH access management service and activate the management service.

2. Default Device Settings

The switch's default configuration values are as follows:

Item	Default Value	Remarks
Administrator Account	admin	
Administrator Password	admin	
Password for Changing Operation Mode		
Console	Enable	Baud rate : 38400 Data bits : 8 Parity : None Stop bits : 1
SNMP	Disable	
Telnet	Disable	
SSH	Enable	
HTTP	Disable	
HTTPS	Enable	
Basic IP Address	192.168.192.168	Subnet Mask : 255.255.255.0
Port Status	Enable	

3 Console Connection

The console connection is used for simple initial setup, and the device should always be connected in a 1-to-1 configuration.

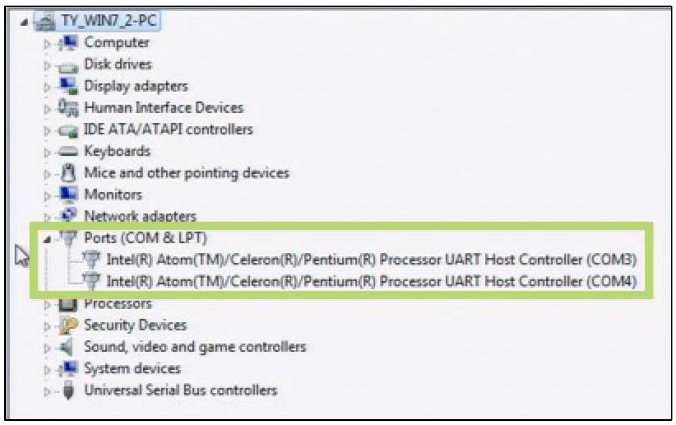
Connect the console cable to the switch's console port and to the PC's RS-232 port.

If your PC does not have an RS-232 port, use a USB-to-Serial converter to connect.

The following setup example uses PuTTY, a free console communication program.

Note: Before connecting to the device, confirm the active serial port.

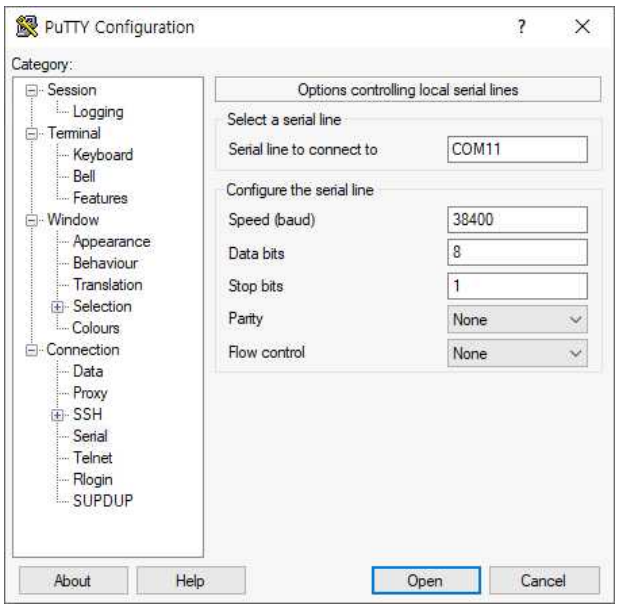
Check this in: Control Panel → System → Device Manager → Ports (COM & LPT)



Steps:

① Run the PuTTY program.

② Select Serial under Connection Type.



③ Configure the serial port as follows:

-Serial line to connect to: Enter the port number confirmed in Device Manager

→ Ports (COM & LPT)

- Speed (baud rate): 38400
- Data bits: 8 bits
- Stop bits: 1 bit
- Parity: None
- Flow control: None

④ Click the "Open" button.

⑤ Enter the User ID and Password to log in.

Default credentials: ID – admin / Password – admin

⑥ When connecting for the first time or after a factory reset, you will be prompted to set a new administrator password.

Enter a new password (9–23 characters) containing lowercase letters, numbers, and special characters.

Note : Password requirements for the admin account:

Must be at least 9 characters long.

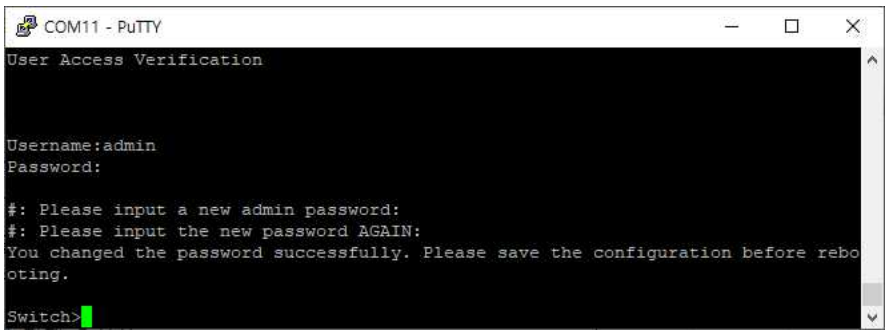
Must include uppercase letters, lowercase letters, numbers, and special characters.

Must not contain the same string as the user account name (e.g., "admin").

Must not include consecutive keyboard sequences (e.g., "qwer").

Must not contain the same character repeated 4 or more times (e.g., "aaaa").

Must not reuse the previous password.



⑦ Once connected to the console, enter the password, then type enable to enter the switch configuration (privileged) mode.

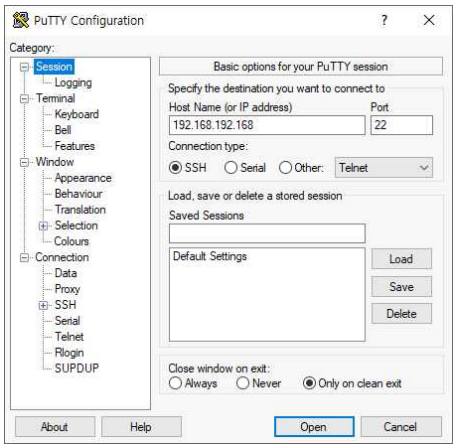
⑧ Enter *write* or *copy running-config startup-config* to save the new password..



4 SSH

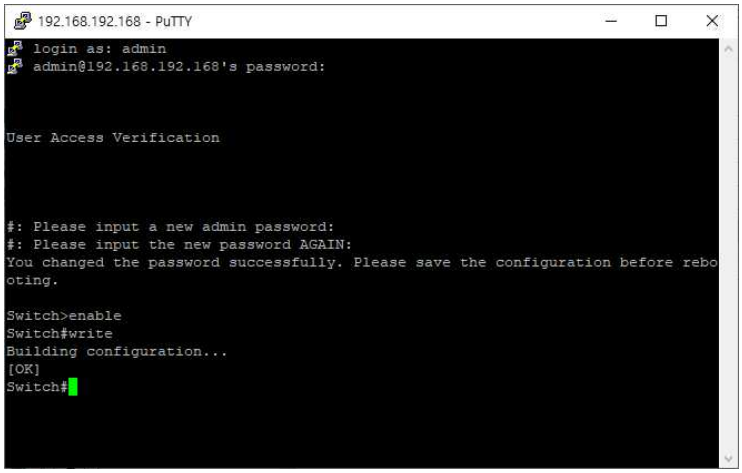
This page explains how to connect via SSH (using the PuTTY program).

① Run PuTTY.



② Select SSH as the Connection Type.
③ Enter the device's IP address in the Host Name field.
④ Enter 22 in the Port field.
⑤ Click the "Open" button.

Default credentials: ID - admin / Password - admin



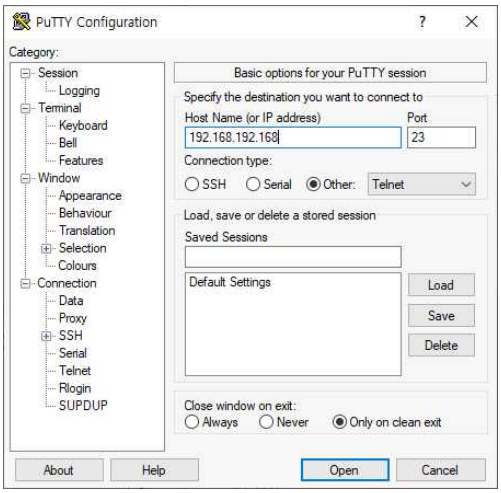
- If this is the first login or after a factory reset (for security-enabled models), you will be prompted to set a new password (9–23 characters, including uppercase/lowercase letters, numbers, and special characters).
- After entering the password, type enable to enter switch operation mode.
- Type *write* or *copy running-config startup-config* save the new password.

5 Telnet

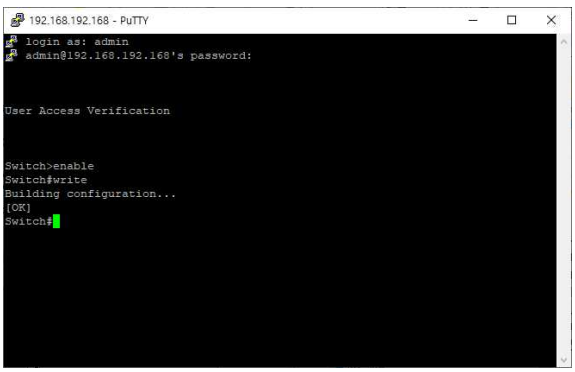
This page explains how to connect via Telnet.

Note:
After the initial setup or a factory reset, Telnet access is disabled.
You must log in through Console, SSH, or HTTPS, and then enable Telnet manually.
The system does not enforce an administrator password change when using Telnet.

Steps:
① In PuTTY, select Telnet under Connection Type.
② Enter the device IP address in the Host Name (or IP address) field.
③ Enter 23 in the Port field.
④ Click the “Open” button.



After connecting, enter the password and then type enable to enter switch operation mode.



Type write to save the new password.

Ⅲ. Basic CLI Commands

This chapter provides a description of basic commands used in the Command-Line Interface (CLI).

1. CLI Basic Symbols

This page provides explanations of symbols commonly used in CLI (Command Line Interface) commands.

Sign	Description
< >	Indicates a value that must be entered directly. Enter letters, numbers, or special characters.
{ }	Indicates optional items; you must choose one from the listed options.
[ ]	Indicates optional items; you may choose none or some of the listed options.
( )	Indicates required items; you must enter one of the items.
¦	Used as a separator to represent multiple items.

2. Basic CLI Keys

● TAB Key

When entering a command, pressing the TAB key displays the next command or completes the current command. When “<cr>“ is displayed, the command can be entered in the CLI.

● ‘?’ Key

Pressing the ‘?’ key at any time will bring up help on the commands you can enter.

```
Switch#?
Exec commands:
  backup          Backup
  clear           Reset functions
  cluster         Cluster
  configure       Enter configuration mode
  copy            Copy from one file to another
  debug           Debugging functions
  delete          Delete
  disable         Turn off privileged mode command
```

3. Classification of CLI modes

CLI modes are divided into four categories: normal mode, privileged mode, global configuration mode and configuration submode. The configuration submode is composed of many CLI modes.

Normal users have access only to normal mode, and privileged users have access to all CLI modes.

Command Mode	Describe	Prompt	Command to enter mode	Command to exit mode
Normal Mode	Provides the display command to view status information for the switch.	Switch>	The mode that the terminal enters first.	There is no exit mode command on the Console terminal. Use the exit or quit command on the Telnet terminal to exit the Telnet terminal.
Privileged Mode	In addition to providing display commands to view the status information of the switch, it also provides commands such as debugging, version upgrade, and configuration maintenance.	Switch#	Enter the enable command in normal mode.	Use the disable command to return to normal mode. Use the exit or quit command on the Console terminal to exit to normal mode and the exit or quit command on the Telnet terminal to exit the Telnet terminal.
Global Config Mode	Provides generic commands that cannot be implemented within the configuration submode, such as the configure static route command.	Switch(Config)#	Enter configure in privileged mode The terminal command.	Use the exit, quit, or end command to exit to privileged mode.
Terminal Configuration Mode	Commands are provided to configure Console and Telnet terminals, such as a timeout for the terminal.	Switch(config-line)#	Enter the line vty command in global configuration mode.	Use the exit or quit command to exit to global configuration mode and use the end command to exit to privileged mode.

Interface Config Mode	Provides commands for configuring ports and VLAN interfaces.	Interface: Switch(config-if)# VLAN: Switch(config-if-vlan)#	Enter the interface < if-name > command in global configuration mode.	Use the exit or quit command to exit to global configuration mode and use the end command to exit to privileged mode.
VLAN Configuration Mode	Commands to configure VLANs are provided. Uch as commands to create and delete VLANs.	Switch(config-vlan)#	Enter the VLAN database command in global configuration mode.	Use the exit or quit command to exit to global configuration mode and use the end command to exit to privileged mode.
MSTP Configuration Mode	Commands to configure MSTP are provided. Uch as the commands to create and delete an MSTP instance.	Switch(config-mst)#	Enter the spanning-treemst configuration command in global configuration mode.	Use the exit or quit command to exit to global configuration mode and use the end command to exit to privileged mode.
Terminal Configuration Mode	Commands are provided to configure Console and Telnet terminals, such as a timeout for the terminal.	Switch(config-line)#	Enter the line vty command in global configuration mode.	Use the exit or quit command to exit to global configuration mode and use the end command to exit to privileged mode.

4. CLI Basic Command

● Login

When logging in for the first time, the user must enter a username and password.

```
Username:admin
Password:
Switch>
```

● exit

To log out the current user or log in as a different user

```
Switch#exit
This vty is closed.
```

● Enable

To use administrator-level commands, enter the enable command.

```
Switch>enable
Switch#
```

● No

To cancel a command or restore a setting to its default value, use the no command.

```
Switch(config)#no ?
  access-list       Add an access list entry
  arp               Address Resolution Protocol (ARP)
```

● Show

To check the current system status or information, use the show command.

```
Switch#show ?
  aaa               AAA
  access-group      Access Group
  access-list       List IP access lists
  arp               Internet Protocol (IP)
```

● Configure

To enter configuration mode, use the configure command.

```
Switch#configure ?
  terminal  Configure from the terminal

Switch#configure  terminal
Switch(Config)#
```

● Copy running-config startup-config / write

To save the current Running-Config to Startup-Config, use the write command.
This command can only be executed in Privileged mode.

```
Switch#copy running-config startup-config
Building configuration...
[OK]
------------------------------------------------------------
--
Switch#write
Building configuration...
[OK]
```

Ⅳ. Switch Configuration

1. System Configuration

You can check and modify the System Information, User management, SNTP configuration,

1.1 System Information

On the System Information page, you can view the basic information of the system.
If the NTP server is not available, the system time can be manually set by the administrator.

System Information

Item	Description
System Description	Description of the system-related parameters
System Object ID	Used as the System ID to identify the device in network management. When SNMP is enabled, this value is used as the System ID.
System Version	Displays the software version of the system.
Num Network Interfaces	The number of network interfaces displays the current number of network interfaces in the switch.
Serial Number	Displays the serial number of the system
MAC Address	Displays the default MAC address of the system.
IP Address	Displays the management IP address of the system.
System Start Time	Displays the system uptime.
System Date Time	Displays the system time. - When the device is connected to the internet and SNTP is enabled, the system time is periodically synchronized and displayed. - If the NTP server is not reachable, the administrator can manually set and modify the system time. - The time must be entered in the format: YYYY/MM/DD HH:MM:SS.

System Name	The system name displays the system name of the switch in the network. The user can modify the system name.
System Location	The system location displays the physical location of the switch in the network, and the user can modify the system location.
System Contact	System contact display management of the current node contacts and contact information, the user can modify the system contact
Web Login Attempt Number	Enter the number of login attempts allowed.
Web Login Waiting Time	Enter the number of login attempts allowed. The connection time is restricted after the number of failed login attempts equals the number of Web Login Attempts.
Web Auto Logout Time	The automatic logout time is set for inactive tasks.

■ Displaying System Information in the CLI

Item	Description
System Description	show snmp system information --System Description
System Object ID	show snmp system information --System Object ID
System Version	show version --Firmware
Base MAC Address	show switch --MAC address:
Serial Number	show switch --Serial number
CPU Utilization	show process cpu
Memory Utilization	show memory

System Uptime	show snmp system information --System Up Time
System Clock	show date-time
System Name	show snmp system information -- System Name
System Location	show snmp system information -- System Lcation
System Contact	show snmp system information -- System Contact
Web Login Attempt Number	show running-config -- ip web auth-retry times *Number*
Web Login Waiting Time	show running-config -- ip web auth-retry silence-period *Number*
Web Auto Logout Time	show running-config --ip web logout time *Number*

■ Configuration System Information in CLI

● Configuration System Date Time

◎ Configuration Date Time
Switch#set date-time *<Year> <Month> <Day> <Hour> <Minute> <Second>*
Switch#set date-time 2022 10 15 11 18 0

◎ Displaying Configuration
Switch#show date-time
System Date Time : 2022/06/02 10:54:28

● Configuration System Name, Location and Contact

◎ Configuration System Name
Switch(config)#snmp system information name *<System Name>*
Switch(config)#snmp system information name Center_Switch

◎ Configuration System Location
Switch(config)#snmp system information location *<System Location>*
Switch(config)#snmp system information name Headquarter_1F

◎ Configuration System Contact
Switch(config)#snmp system information contact *<System contact>*
Switch(config)#snmp system information contact <1234-5678>

◎ Displaying System System Name, System Location, System Contact

```
Switch#show snmp system information
 System Description : DG8P-2SMB 7.6.8
 System Object ID   : 1.3.6.1.4.1.12284.1
 System Up Time     : 0-Days 0-Hours 44-Minutes 15-Seconds
 System Name        : Center_Switch
 System Location    : Headquarter_1F
 System Contact     : 1234-5678
 System services    : 3 (physical,datalink/subnetwork)
```

1.2 Serial Information

Displays information about the serial port transmission speed and COM port settings.

When the host connects to the switch through the console, the serial port configuration must match the information shown on this page.

This serial port information cannot be modified and is provided for reference only..

◎ GTWave Switch Series_Serial Information

- Baud Rate : 38400
- Character(Data bits) Size: 8bit
- Parity Code : None
- Stop bits : 1
- Flow Control: None

1.3 User Management

You can change the admin password on the User Management page. You can also add, edit, and delete users. Users use their username and password to access the device via the web or SSH.

Both user IDs and passwords are case-sensitive.

User Management

Item	Description
User Name	This is the user's identification name.
Privilege	This is the user's permission level. There are two levels: Administrator (Privilege) and Normal (Normal). - The Administrator (Privilege) level has full access to configuration and monitoring. - Normal (Normal) users only have monitoring permissions. -The Web Management Service is only in Privilege mode, so normal users cannot access it.
Password	This is the user's password. If security features are enabled, you must enter the password in accordance with the security rules.
Confirm Password	Confirm new password

◆ Password security standards

Item		Content detail
1	Compliance	Password length: 9 or more characters.
2		Enter a combination of at least three of the following: numbers, uppercase letters (English), lowercase letters (English), and special characters
3	Prohibited items	Do not use the same password as your user account (ID)
4		Do not repeatedly enter the same letters or numbers.
5		Do not enter consecutive letters or numbers on the keyboard.
6		Do not reuse a previously used password.
7	Supported Special Characters	~ , ! , @ , # , $, % , ^ , & , * , (,) , - , + , _ , = , ¦ , { , } , [,] , : , ; , < , > , /

■ Configuration User Management on the CLI

● User Add

```
Switch(config)#username <User_ID> <level> password
#: Please input the new password:
#: Please input the new password AGAIN:

Example 1) 1. Adding a user with administrator Level, changing the password
Switch(config)#username root privilege password
#: Please input the new password:
#: Please input the new password AGAIN:

Example 2) Adding a Normal user, change password.
Switch(config)#username normaluser normal password
#: Please input the new password:
#: Please input the new password AGAIN:
```

Note) You can add an administrator account by entering a command in the format "username <UserID> password <PASSWORD> <Level>", but when you enter the password, it will be displayed on the screen and may be exposed to others. Please add an administrator account or change the password using the method above.

● Delete User

```
Switch(config)#no username <username>
ex)
Switch(config)#no username user1
```

● Displaying the User

```
Switch#show running-config
!
username admin algorithm-type sha256 enc-password 59e873f36d6d126dc51636f0
d21dee41514fe11e03c06e75176b11fe2700bb67dae60b05c810ac11 privilege
username root algorithm-type sha256 enc-password  b9074fcb739d47cbfaa1b1e4e
9df0077b332e27a1b1dde1e1336b79c120b0af79224a500a3d034f8 privilege
!
```

■ Operation Mode Change Password Input

The WEB management service provides only the Privilege mode, and only users with Privilege-level authority can access it. Therefore, operation mode changes are available only through the CLI mode.

You can configure the system to require a password when switching operation modes. When a password is set for mode switching, the system will prompt for it when changing from Normal mode to Privilege mode.

● Configuration

- In Privilege mode, enter configure terminal to switch to Global Configuration mode.
- Enter enable password.
- Enter the password to be used for switching operation modes, and then re-enter it for confirmation.
- Save the configuration.

```
Switch#
Switch#configure terminal
Switch(config)#enable password
#: Please input the new password:
#: Please input the new password AGAIN:
Switch(config)#
```

(Note) Both the administrator authentication password and the operation mode change password are stored in the configuration file after being hashed using a random salt and SHA-256, and then Hex-encoded.

(Caution): You can also enter the command in the format enable password <password>. However, if you use this format, the password will be displayed on the screen and may be exposed to others. Please enter the operation mode change password using the method described above.

1.4 Safe Management

System access management can control HTTP, Telnet, SSH, and SNMP services. Depending on your security or usage environment, you can enable or disable these services. Additionally, you can control which hosts can access the switch by linking with a Standard IP ACL.

By default, HTTPS and SSH services are enabled, and ACL filtering is disabled, allowing all hosts to access the switch for management and configuration. It is recommended to disable unnecessary services after switch installation and configuration. To use ACL filtering, you must first configure the ACL.

Note)

HTTP and HTTPS services cannot be supported simultaneously.

HTTP services displayed on webpages are integrated into HTTPS and HTTP web services, expressed as HTTP. HTTPS access services are enabled by default.

To use the HTTP management access service, access the CLI management access service and disable the HTTPS service. This will then enable the HTTP service.

Safe Management

Item	Description
Service Type	Access Service Type
Management State	Enabled or Disabled status of the service.
ACL Group	ACL Group: The ACL group applied to the service. (means no ACL.) ACL groups can only be applied to the Standard IP group.

■ Configuring Safe Management in the CLI

● WEB(HTTP/HTTPS) Management Access Service

```
Enable Web Access service
Switch(config)#security-manage http enable

Disable  Web Access service
Switch(config)#security-manage http disable

Apply ACL
Switch(config)#security-manage http access-group <ACL_Group>
Switch(config)#security-manage http access-group 10

Disable ACL
Switch(config)#no security-manage http access-group
```

● HTTPS or HTTP Management Access Service

```
Use HTTPS management access service
Switch(config)#https enable

Use HTTP management access service
Switch(config)#no https enable
```

● Telnet Service

```
Enable service
Switch(config)#security-manage telnet enable

Disable Service
Switch(config)#security-manage telnet  disable

Apply ACL
Switch(config)#security-manage telnet  access-group <ACL_Group>
Switch(config)#security-manage telnet  access-group 10

Disable ACL
Switch(config)#no security-manage telnet access-group
```

● SSH Service

```
Enable service
Switch(config)#security-manage ssh enable

Disable Service
Switch(config)#security-manage ssh disable

Apply ACL
Switch(config)#security-manage ssh access-group <ACL_Group>
Switch(config)#security-manage ssh access-group 10

Disable ACL
Switch(config)#no security-manage ssh  access-group
```

● SNMP Service

```
Enable service
Switch(config)#security-manage snmp enable

Disable Service
Switch(config)#security-manage snmp disable

Apply ACL
Switch(config)#security-manage snmp access-group <ACL_Group>
Switch(config)#security-manage snmp access-group 10

Disable ACL
Switch(config)#no security-manage snmp access-group
```

● Displaying the System Management configuration

```
Switch#show security-manage
 Service type      Admin state      Access-list name
 ------------      -----------      ----------------
 HTTP              enable           0
 SNMP              enable           0
 TELNET            enable           0
 SSH               enable           0
```

● Configuring Safe Management Timeout

```
Switch(config)#line vty
Switch(config-line)#exec-timeout <Minute> <Second>

Switch(config)#line vty
Switch(config-line)#exec-timeout 10 0
```

● WEB(HTTP/HTTPS) Service

- Enable web management access service
  Switch(config)#security-manage http enable

- Disable Web Management Access Service
  Switch(config)#security-manage http disable

- Apply ACL
  Switch(config)#security-manage http access-group <ACL_Group>
  Switch(config)#security-manage http access-group 10

- Remove ACL
  Switch(config)#no security-manage http access-group

● SSH management access service

- Enables SSH management access service
  Switch(config)#security-manage ssh enable

- Disable SSH management access service
  Switch(config)#security-manage ssh disable

- Apply ACL
  Switch(config)#security-manage ssh access-group <ACL_Group>
  Switch(config)#security-manage ssh access-group 10

- Remove ACL
  Switch(config)#no security-manage ssh access-group

● Telnet 관리접속 서비스

■ Enable Telnet service
Switch(config)#security-manage telnet enable

■ Disable Telnet service
Switch(config)#security-manage telnet disable

■ Apply ACL
Switch(config)#security-manage telnet access-group <ACL_Group>
Switch(config)#security-manage telnet access-group 10

■ Remove ACL
Switch(config)#no security-manage telnet access-group

● SNMP Servie

■ Enable Telnet service
Switch(config)#security-manage snmp enable

■ Disable Telnet service
Switch(config)#security-manage snmp disable

■ Apply ACL
Switch(config)#security-manage snmp access-group *<ACL_Group>*
Switch(config)#security-manage snmp access-group 10

■ Remove ACL
Switch(config)#no security-manage snmp access-group

● Check management access service settings

```
Switch#show security-manage
 Service type      Admin state      Access-list name
 ------------      -----------      ----------------
 HTTP              enable           0
 SNMP              enable           0
 TELNET            enable           0
 SSH               enable           0
```

● Configuring Safe Management Timeout

```
Switch(config)#line vty
Switch(config-line)#exec-timeout <Minute> <Second>

Switch(config)#line vty
Switch(config-line)#exec-timeout 10 0
```

1.5 SNTP Configuration

The system time can be set either by the administrator directly entering the time on the system basic information page or by synchronizing with a standard NTP server. You can synchronize the time with a standard NTP server.

Note: To synchronize time using the SNTP feature, you must be connected to an SNTP time server via the network. If using an Internet SNTP server, you must first configure an IP address with Internet access, then configure SNTP. Once the time is synchronized with the SNTP server, the last update time will be displayed, and the system date/time will change to the current standard time.

SNTP Configuration

Item	Description
Server IP Address 1,2,3	Enter the NTP server 1, 2, and 3 IP addresses.
Time Interval	Period of synchronization with the NTP server (input is greater than 60)
Time zone	Enter the time zone (Republic of Korea: +9)
DST	Select Enable/Disable DST
DST Start Time	DST start date and time
DST End Time	DST ending date and time
DST Bias	Time offset when DST is applied
Enable Status	Select whether to enable synchronization with the NTP server.
Last Update Time	Displays the last synchronization time.
System Date Time	Displays the time of the system.

■ Configuration SNTP on the CLI

● Enable SNTP

```
Switch(config)#sntp enable
```

● Disable SNTP

```
Switch(config)#sntp disable
```

● SNTP Server Configuration

```
Switch(config)#sntp server <A.B.C.D >

ex)
Switch(config)#sntp server 216.239.35.12
```

● Time Interval Configuration

```
Switch(config)#sntp interval <60-65535>

ex)
Switch(config)#sntp interval 300
```

● Time Zone configuration

```
Switch(config)#sntp time-zone <word>

Ex)
Switch(config)#sntp sntp time-zone +9.00
```

note : Republic of Korea Time-zone: +9.00

● DST configuration

```
Switch(config)#sntp dst start-time <start-time> end-time <end-time>
               <DST bias minutes>

Ex) From June 1st to September 30th, DST 60 minutes will be applied.
Switch(config)#sntp dst 6/1 start-time  9/30 60
```

● Displaying Time Synchronization

```
Switch#show sntp
 SNTP Server IP:          216.239.35.4   216.239.35.8   216.239.35.12
 SNTP Interval:           60s
 SNTP Time Zone:          GMT+9.00
 SNTP DST:                Enabled
 SNTP DST Start Time:     6/1 (Month/Day)
 SNTP DST End Time:       9/30 (Month/Day)
 SNTP DST Bias:           60 (Minutes)
 SNTP Status:             Enabled
 SNTP Last Update time:   2025/11/18 16:05:09
 System Date Time:        2025/11/18 16:05:13
```

1.6 Jumbo Frame Configuration

In computer networking, jumbo frames are Ethernet frames with more than 1500 bytes of payload, the limit set by the IEEE 802.3 standard.

Jumbo Frame Configuration

Item	Description
Jumbo Frame Bytes	Enter the jumbo frame size.

note> If you apply jumbo frame, it will be applied to all ports.

■ **Configuration Jumbo Frame on the CLI**

```
Switch(config)#jumbo frame <Frame Size>

Switch(config)#jumbo frame 4096
```

1.7 Save Current Configuration

After changing configuration values on each feature page and clicking the Apply button, the system will operate with the changed values without saving them to the configuration file. If the system operates normally with the changed configuration values, you should save them to the system configuration file. If you restart the system without saving them, the system will operate with the values before the changes.

■ Save configuration in CLI

```
Switch#copy running-config startup-config
or
Switch#write
```

1.8 Configuration File

The Configuration File Management page displays the configuration values stored in the system flash. If the configuration items do not display any configuration values, as shown in the image (Configuration File 1_Configuration Not Saved), the system is in a factory reset state or has not saved the configuration values, meaning there is no configuration file. You can download the configuration file to the host computer and save the configuration values. You can then restore the configuration values using the saved file.

■ Backup & Delete Configuration file in CLI

● Backup configuration files

```
Switch#upload configure <TFTP Server IP Address> <Backup File Name>

ex)
Switch#upload configure 192.168.10.30 running-config.cfg
```

Note: The TFTP server must be running before performing a backup.

● Delete startup-config file

```
Switch#delete startup-config
```

Note) After running this command and restarting the system, the result will be the same as a reset.

1.9 File Upload

Users can upload configuration files and image files to the switch.

■ File Upload in CLI

Note: The TFTP server must be running before performing a restore or firmware upgrade.

● Restore Configuration

```
Switch#download configure <TFTP Server IP Address> <File Name>

Switch#download configure 192.168.10.30 running-config.cfg
```

● Firmware Upgrade

```
Switch#download image<TFTP Server IP Address> <Image File Name>

Switch#download image 192.168.10.30 switch.img
```

1.10 Ping Diagnosis

Ping is a network diagnostic tool that tests connectivity by sending packets of data to a destination and measuring the time it takes to receive a response

Ping Diagnosis

Item	Description
Target IP Address	Enter the Ping Test destination IP address.
Data Length	Enter the ping data length.(32~4000)
Count	Enter the ping test number.

■ Ping Diagnosis in CLI

```
Switch#ping <Target IP Address> -n <Count> -l <Data Length>
```

- Success

```
Switch#ping 192.168.10.1 -n 5 -l 1024
PING 192.168.10.1: 1024 data bytes
1024 bytes from 192.168.10.1 : icmp_seq=0. time=0. ms
1024 bytes from 192.168.10.1 : icmp_seq=1. time=0. ms
1024 bytes from 192.168.10.1 : icmp_seq=2. time=0. ms
1024 bytes from 192.168.10.1 : icmp_seq=3. time=0. ms
1024 bytes from 192.168.10.1 : icmp_seq=4. time=0. ms
----192.168.10.1 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 0/0/0
```

- Fail

```
Switch#ping 192.168.10.100 -n 5 -l 1024
PING 192.168.10.100: 1024 data bytes
no answer from 192.168.10.100
```

1.11 System Reboot

If a system restart is required, administrators can initiate one via the System Reboot page. After restarting, users will need to log in to the webpage again.

Ping Diagnosis

Item	Description
Reboot	Restart the system.
Reboot Factory	Restarts the system by initializing its configuration.

■ System Reboot in CLI

● Reboot

```
Switch#reboot
Do you wish to reboot the switch? [Y/N]: y
```

● Reboot Factory

```
Switch#reboot factory
Do you wish to restore the factory settings and reboot the switch? [Y/N]: y
```

2 Port

2.1 Basic Configuration

This webpage allows you to enable or disable ports and configure port speeds. You can also view basic information about all ports.

Port Basic Configuration

Item	Description
Selected Port(s)	Select the checkbox next to the port you wish to change in the table below. You can select one port, multiple ports, or all ports. To select all ports, select the Select All checkbox.
Admin Status	Ports can be enabled or disabled by the administrator. The default setting is Enable.
Config Speed	You can configure the port's duplex and bandwidth. You can choose from Auto-NeGTWaveiate, Full-1000Mbps, Full-100Mbps, Half-100Mbps, Full-10Mbps, or Half-10Mbps. Selecting Auto-NeGTWaveiate will determine the maximum speed of the connected device. The default setting is Auto-NeGTWaveiate.
Description	Enter a port description.

■ Common configuration of ports in CLI

● Enter interface configuration mode for the interface you want to change.

```
Switch(config)#interface <Interface name>
Switch(config)#interface ge1/1
Switch(config-ge1/1)#
```

● Enable selected interface

```
■ Enable
Switch(config)#interface ge1/1
Switch(config-ge1/1)#no shutdown
```

● Check the selected interface enable

```
Switch#show running-config
!
interface ge1/1
!
```

Note: If there is no shutdown in the interface ge1/1 entry, the interface is in the enabled state.

● Disable selected interface

```
Switch(config)#interface ge1/1
Switch(config-ge1/1)#shutdown
```

● Check the selected interface disable

```
Switch#show running-config
!
interface ge1/1
 shutdown
```

Note) If there is shutdown in the interface ge1/1 entry, the interface has been disabled by the administrator.

● Speed/Duplex configuration

```
Switch(config)#interface ge1/1
Switch(config-ge1/1)#speed <Speed/duplex>
Switch(config-ge1/1)#speed full-1000
```

Speed

Item	Speed	Duplex	Item	Speed	Duplex
Auto/Auto	Auto Negotiate	Auto Negotiate	1G/Full	1000Mbps	Full_Duplex
100M/Full	100Mbps	Full_Duplex	100M/Half	100Mbps	Half_Duplex
10M/Full	10Mbps	Full_Duplex	10M/Half	10Mbps	Half_Duplex

● View Speed/Duplex configuration

```
Switch#show running-config
!
interface ge1/1
  speed full-1000
```

● Enter the selected interface description

```
Switch(config)#interface ge1/1
Switch(config-ge1/1)#description <description>
Switch(config-ge1/1)#description Connection_Server
```

● View selected interface description

```
Switch#show running-config
!
interface ge1/1
 description Connection_Server
!
```

2.2 Port Statistics

You can check the status of data transmission and reception packets of the port.

Port Statistic

Item	Description
Received Total Bytes	Total data received through the port (bytes)
Received Unicast Packets Num (ifInUcastPkts)	Number of unicast data received through the port
Received Non-Unicast Packets Num (ifInNUcastPkts)	Number of Non-unicast data received through the port
Received Discard Packets Num (ifInDiscards)	Number of discarded data received through the port.
Received Error Packets Num (ifInErrors)	Number of error data received through the port
Received Unknown Protocol Packets Num (ifInUnknownProtos)	Number of Unknown protocol Packet data received through the port
Send Total Bytes (ifOutOctets)	Total data transmitted through the port(bytes)
Send Unicast Packets Num (ifOutUcastPkts)	Number of unicast data transmitted through the port
Send Non-Unicast Packets Num (ifOutNUcastPkts)	Number of Non-unicast data transmitted through the port
Send Discard Packets Num (ifOutDiscards)	Number of discarded data transmitted through the port.
Send Error Packets Num (ifOutErrors)	Number of error data transmitted through the port

■ Port Statistics in CLI

● Check the data transmission and reception status of the selected port

```
Switch#show interface statistics ge1/1
    Last 300 seconds input:  2 packets/sec  485 bytes/sec
    Last 300 seconds output:  5 packets/sec  1155 bytes/sec
    input bytes 02978408
    input unicast packets 012618
    input broadcast packets 045
    input multicast packets 09
    receive error packets 00
    output bytes 010124676
    output unicast packets 015121
    output multicast packets 02765
    output broadcast packets 05877
    send error packets 00
    64 bytes packets 05154
    65-127 bytes packets 04620
    128-255 bytes packets 0496
    256-511 bytes packets 0556
    512-1023 bytes packets 0861
    1024-1518 bytes packets 0985
    drop packets 00
    undersize 64 packets 00
    oversize 1518 packets 00
    CRC error packets 00
    collisions packets 00
    bad packets 00
```

2.3 Flow Control

The user can use this page to open or close the flow control for each port.

Flow Control

Item	Description
Port	Ports selected from the list / Port
Flow Enable/Disable	Enable/disable the Port Flow feature (Default: enable)

2) Flow Control in CLI

- Port selection

Switch(config)#interface *<IF_Name>*
Switch(config)#interface ge1/1

- Enable Port Flow feature

Switch(config-ge1/1)#flowcontrol

- Disable Port Flow feature

Switch(config-ge1/1)#no flowcontrol

- Port Flow Interval configuration

Switch(config-ge1/1)#flow interval *<Flow Interval>*
Switch(config-ge1/1)#flow interval 10

● Port Flow configuration verification and monitoring

```
Switch#show flow
Port      Flow control
-----     ------------
ge1/1     on
ge1/2     on
ge1/3     on
```

2.4 Broadcast Storm

Network interface cards (NICs) transmit high-speed unicast, multicast, and broadcast packets, which can cause network disruption. Therefore, suppression capabilities are crucial. All ports on the switch support suppression of broadcast, multicast, and DLFpackets, which prevents data packets from flooding the network and causing network congestion. You can set rate limits for broadcast, multicast, and DLFpackets, and simultaneously check the broadcast, multicast, and DLFpacket storm control settings for all ports.

Port Storm Control

Item	Description
Selected Port(s)	Select the port for which you want to configure Storm Control.
Broadcast Suppression	Enable Broadcast throttling.
Multicast Suppression	Enable Multicast throttling.
DLFSuppression	Enable DLFthrottling.
Ratelimit	Enter the Broadcast and Multicast DLFthrottling rates. The range is 1 to 1024,000 kbps.

■ Flow Control in CLI

● Enables Broadcast Suppression feature.

```
Switch(config)#interface <interface Name>
Switch(config)#interface ge1/1
Switch(config-ge1/1#storm-control broadcast
```

● Disables the Broadcast Suppression feature.

```
Switch(config)#interface <interface Name>
Switch(config)#interface ge1/1
Switch(config-ge1/1#no storm-control broadcast
```

● Enables Multicast Suppression feature.

```
Switch(config)#interface <interface Name>
Switch(config)#interface ge1/1
Switch(config-ge1/1#storm-control multicast
```

● Disables Multicast Suppression feature

```
Switch(config)#interface <interface Name>
Switch(config)#interface ge1/1
Switch(config-ge1/1#no storm-control multicast
```

● Enables DLFSuppression feature

```
Switch(config)#interface <interface Name>
Switch(config)#interface ge1/1
Switch(config-ge1/1#storm-control dlf
```

● Disables DLFSuppression feature

```
Switch(config)#interface <interface Name>
Switch(config)#interface ge1/1
Switch(config-ge1/1#no storm-control dlf
```

● Storm Control Ratelimit Configuration

```
Switch(config)#interface <interface Name>
Switch(config-ge1/1)#storm-control ratelimit <broadcast ¦ multicast : dlf> <ratelimit>

Switch(config)#interface ge1/1
Switch(config-ge1/1#storm-control ratelimit brocast 128
Switch(config-ge1/1#storm-control ratelimit multicast 128
Switch(config-ge1/1#storm-control ratelimit DLF128
```

● Displaying Storm control interface configuration in CLI

- Display all interface Storm control configurations

```
Switch#show storm-control
Port        Bcast/limit(kbits)    Mcast/limit(kbits)      Dlf/limit(kbits)
ge1/1          set/128                 set/128                 set/128
ge1/2        unset/64                unset/64                unset/64
…
```

- Displaying Storm control configuration for a specific interface

```
Switch#show storm-control <Interface Name>
Switch#show storm-control ge1/1
Port        Bcast/limit(kbits)    Mcast/limit(kbits)      Dlf/limit(kbits)
ge1/1          set/128                 set/128                 set/128
```

2.5 Port Ratelimit

It is used to configure the rate at which ports transmit and receive. If the port is not configured with bandwidth control, it is displayed as off. If the port is configured with bandwidth control, it will be displayed in the list.

Port Ratelimit

Item	Description
Port	Select the port for which you want to set the Port Rate.
Send Packets Rate Control	Enter the bandwidth in the Outgoing Speed Control field. The input range is 1-1024000 kbps.
Receive Packets Rate Control	Enter the bandwidth in the Incoming Speed Control field. The input range is 1-1024000 kbps.
Cancel	Cancel Send/Receive Packets Rate Control

■ Port Ratelimit in CLI

● Configure a specific interface port rate

```
Switch(config)#interface <interface Name>
Switch(config)#interface ge1/1

Switch(config-ge1/1#portrate {egress/ingress}, <1-1024000>
Switch(config-ge1/1)#portrate egress 409600
Switch(config-ge1/1)#portrate ingress 409600
```

● Displays the interface Port Rate configuration.

```
Switch#show portrate
Port     Egress Rate kbps     Ingress Rate kbps
-----    ----------------     ----------------
ge1/1            409600            409600
```

● Deletes a specific interface Port Rate configuration.

```
Switch(config)#interface <interface Name>
Switch(config)#interface ge1/1
Switch(config-ge1/1#portrate {egress/ingress}
Switch(config-ge1/1)#no portrate egress
Switch(config-ge1/1)#no portrate ingress
```

● 인터페이스에서 Port Ratelimit 삭제

```
Switch(config)#interface <interface Name>
Switch(config)#interface ge1/1
Switch(config-ge1/1#portrate {egress/ingress}
Switch(config-ge1/1)#no portrate egress
Switch(config-ge1/1)#no portrate ingress
```

2.6 Protected Port

For security or other reasons, data transmission and reception can be blocked on specific ports.

Ports can be divided into multiple VLANs to achieve Layer 2 packet blocking, but this wastes VLAN resources. This functionality can be implemented through Protected Ports, providing users with a more secure and flexible networking system.

Each port can be configured as a Protected Port. Protected Ports cannot communicate with each other

Protected Port

Item	Description
Selected Port(s)	Select the port for which you want to configure a Protected Port.
Is Protected Port	Indicates whether the Protected Port is enabled.
Protected Port	Enables the Protected Port feature for the selected port.
Unprotected Port	Disables the Protected Port feature for the selected port.

■ Protected Port in CLI

● Configuring a Protected Port on an Interface

```
Switch(config)#interface <interface Name>

Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport port-security protect
```

● Display interface Protected Port configuration

```
Switch#show port-security protect
Port      Port protected
-----     --------------
ge1/1     ON
ge1/2     ON
```

● Disable interface Protected Port configuration

```
Switch(config)#interface <interface Name>
Switch(config)#interface ge1/1
Switch(config-ge1/1)#no switchport port-security protect
```

2.7 Learn Limit

Learn Limit is used to limit the number of MAC addresses a port can learn. The range is 0 to 8191. The default is 8191, which is also the maximum. This indicates that no learning limit has been configured for the port. The list displays the learning limits for all ports.

MAC Bind

Item	Description
Port	Ports to restrict MAC address learning
MAC Address Num able to Learn	Number of MAC addresses that can be learned (Range 0~8191)
Cancel Limit	No learning restrictions

■ Learn Limit in CLI

● Learn Limit configuration

```
Switch(config)#interface <IF_NAME>
Switch(config-ge1/1)# switchport port-security learn-limit  <Limit>

Switch(config)#interface ge1/1
Switch(config-ge1/1)# switchport port-security learn-limit 8191
```

● View Learn Limit Configuration

```
Switch#show port-security learn-limit <IF_NAME>

Switch#show port-security learn-limit ge1/1
 interface ge1/1 dynamic learn limit is 2048.
```

2.8 Port Trunking

Port trunking is a method of combining multiple physical ports into a single logical port to increase bandwidth. TRUNK can be used to configure multiple ports as a single logical port, increasing bandwidth, providing redundant connections, and distributing load. When a trunk group is used as an output logical port, the switch selects a port within the port group to send packets based on a user-configured policy. Port and policy configuration in a trunk group is performed in software, but data stream forwarding is performed in hardware. All ports in a trunk group must be configured for the same speed and Full-Duplex mode. A switch can support up to 32 trunk groups, with up to eight trunk members per group. Each port can belong to only one trunk group. Port trunking configuration consists of four steps: selecting a trunk group ID, selecting a trunking method, displaying trunking ports, and adding trunking member ports.

Trunk Group

Item	Description
Trunk Group ID	Select the trunk group to use as the trunk group.
Trunk Method	There are six configurable trunk methods. To configure a trunking method, you must select it when activating the trunk group.
Create Status	The trunk group's creation status is indicated: - Created: Trunk group is enabled - Uncreated: Trunk group is disabled
Able Config Port	Port to be added as a member port to the Trunk Group
Member port	Displays member ports included in the selected Trunk Group.

● Trunk Method

- dst-mac : Trunking method based on the destination MAC address.
- src-mac : Trunking method based on the source MAC address.
- src-dst-mac : Trunking method based on the source and destination MAC addresses.
- src-ip : Trunking method based on the source IP address.
- dst-ip : Trunking method based on the destination IP address.
- src-dst-ip : Trunking method based on the source and destination IP addresses.

Note: There must have at least one trunk group when you configure trunk method. All the trunks use the same trunk method. You can only delete or add a member port when a trunk already exists. Delete trunk groups when they have no member.

■ Port Trunking in CLI

● Creating a Port Trunk Group

```
Switch(config)#trunk <trunk group ID> <Trunk type> :
Switch(config)#trunk load-balance <Trunk Method>

Switch(config)#trunk 1 dynamic
Switch(config)#trunk load-balance src-ip
```

Note: Trunk type: If not entered, it will be configured as Static (Static/Dynamic)

◉ Turnk Load-Balance Type

- dst-ip Destination IP address based load balancing
- dst-mac Destination Mac address based load balancing
- src-dst-ip Source and Destination IP address based load balancing
- src-dst-mac Source and Destination Mac address based load balancing
- src-ip Source IP address based load balancing
- src-mac Source Mac address based load balancing

● Displays the configuration for creating a port trunk group.

```
Switch#show trunk
 Trunk name: trunk1 dynamic
 Load-balance: Source IP address
```

● Deleting a Port Trunk Group

```
Switch(config)#no trunk <trunk group ID>
Switch(config)#no trunk 1
```

note: Before deleting a trunk group, you must first remove its member ports.
If member ports are configured, the message "% The port trunk1 is not empty" will appear.

● Add member ports to a trunk group

```
Switch(config)#interface <Trunk_Group_Name>
Switch(config-trunk1)#interface <IF_NAME> <IF_NAME>

Switch(config)#interface trunk1
Switch(config-trunk1)#interface ge1/9 ge1/10 ge1/11 ge1/12
```

● Delete a member from a trunk group

```
Switch(config)#interface <Trunk_Group_Name>
Switch(config-trunk1)#no interface <IFNAME>

Switch(config)#interface trunk1
Switch(config-trunk1)#no interface ge1/1
```

● Display trunk group configuration

```
Switch#show trunk <Trunk_Group_ID>
Switch#show trunk 1
 Trunk name: trunk1 static
 Load-balance: Source Mac address
 Member:
    xe1/9
    xe1/10

Switch#show running-config
!
trunk 1
trunk load-balance src-ip
!
interface trunk1
 trunk interface xe1/9
 trunk interface xe1/10
!
```

2.9 Mirror

Port mirroring allows you to monitor network traffic by forwarding copies of packets sent and received from one port on a network switch to another port where they can be inspected. This allows you to closely monitor switch performance and make adjustments as needed. While only one port mirroring destination port can be selected, the mirroring target port can mirror information from multiple mirrored ports simultaneously.

Port Mirror

Item	Description
Mirror Port	This port receives packets from the mirroring target port. Only one port can be configured.
Able Config Mirrrored Ports	This is the mirroring target port.
Mirror Direction	Select the data traffic direction to mirror. ■ RECEIVE - Only incoming data is transmitted to the mirroring target port. ■ TRANSMIT - Only outgoing data is transmitted to the mirroring target port. ■ Both – incoming and Outgoing data is transmitted to the mirroring target port. ■ NOT_RECEIVE - Excludes incoming data from the port mirroring configuration of the selected port. ■ NOT_TRANSMIT - Excludes outgoing data from the port mirroring configuration of the selected port. ■ NEITHER - Excludes port mirroring configuration for the selected port.

■ Mirror in CLI

```
Switch(config)#interface <interface Name>
      Interface Name : Port Mirroring Destination Port
Switch(config)#interface ge1/1

Switch(config-ge1/1)#mirror interface <interface Name> direction <traffic direction>
      <interface Name> : Mirroring target port
      <traffic direction> : Traffic direction

Switch(config-ge1/1)#mirror interface ge1/2 direction both
```

Traffic direction

- *both : Mirror traffic in both directions*
- *receive : Mirror received traffic*
- *transmit : Mirror transmit traffic*

● Configuring Port Mirroring in the CLI

```
Switch#show mirror
Mirror Test Port Name: ge1/1
Mirror option: Enabled
Mirror direction: both
Monitored Port Name: ge1/2
```

● Disable Port Mirroring in CLI

```
Switch(config)#interface <interface Name>
   <interface Name> : Mirroring destination port
Switch(config-ge1/1)#no mirror interface <interface Name>
  <interface Name> : Mirroring target port

Switch(config)#interface ge1/1
Switch(config-ge1/1)#no mirror interface ge1/2
```

2.10 DDM Information

You can display SFP information for an SFP port.

This only applies to systems with SFP ports.

You can display the optical module's device name, connector name, encoding code, transmit distance, laser wave length, and more.

DDM Information

Item	Description
Connector Name	Connector type of the optical module
Encoding Code	Optical module encoding line code
Bit Rate	Maximum transmission speed of the installed optical module
Transmit Distance	Maximum transmission distance of the installed optical module
Laser WaveLength	Transmission optical wavelength
Tx Bias	Required current of the SFP (mA)
TX Power	Signal strength emitted from the optical transceiver
RX Power	Signal strength received by the optical transceiver

2) DDM Information **in CLI**

● **DDM Information_Optical Module Installation**

Note) Ports included in trunk members cannot be displayed.

```
Switch#show optical xe1/9
 Device Name              :SFP
 Connector Name           :LC
 Encoding Code            :8B/10B
 Bit Rate                 :1.3GBd
 Transmit Distance        :20km
 Vendor Name              :OEM
 Vendor OUI               :00-00-00
 Part Number              :GWSFP-LX20-SM131
 Revision Number          :A0
 Serial Number            :CO2304270481
 Production Date          :23/04/27
 Laser WaveLength         :1310
 Vendor Specific          :
 Monitor Parameters       :0x58

Type              Value      Alarm-High  Alarm-Low   Warning-High  Warning-Low
Temperature(C)    59.9805    100.0000    -40.0000    95.0000       -35.0000
Voltage(V)        3.3890     3.5999      2.9000      3.5000        3.0000
Tx Bias(mA)       18.9000    80.0000     1.0000      70.0000       2.0000
Tx Power(dBm)     -6.0818    2.9999      -15.0031    0.0000        -12.0135
Rx Power(dBm)     -Infinity  0.0000      -30.0000    -3.0008       -27.2125
```

● DDM Information_no optical module

```
Switch#show optical xe1/10
%  The interface hasn't optical module.
```

2.11 Cable Diagnosis

You can display the connection status of cables and devices connected to the Ethernet port.

- A switch and Ethernet device must be connected.

Cable Diagnosis

용 어	설 명
Port	케이블을 점검할 포트

■ Cable Diagnosis**in CLI**

● If connected normally: Displayed as Normal

```
Switch#show cable-diag interface <IFNAME>

Switch#show cable interface ge1/5
port   channel-a length-a channel-b length-b channel-c length-c channel-d length-d
ge1/5          normal              normal              normal              normal
!
```

● If no device is connected: Open is displayed.

```
Switch#show cable-diag interface <IFNAME>

no Device equipment connection
Switch#show cable interface ge1/1
port   channel-a length-a channel-b length-b channel-c length-c channel-d length-d
ge1/1 open       4.00(m)   open       4.00(m)   open       2.40(m)   open       3.20(m)
!
```

3 MAC Configuration

3.1 MAC Table

Displays dynamically learned MAC addresses

MAC Table

Item	Description
Port	The port for which you want to check the learned MAC address.
VLAN ID	The VLAN for which you want to check the learned MAC address. (0 means All VLAN
MAC Number	Number of learned MAC addresses.

3.2 MAC Binding

Port-based VLANs are commonly used for VLANs. While a common approach, Port-based VLANs are not suitable for networks with frequent network changes or with a large number of mobile users. For example, a user who previously accessed the switch via Port 1 (VLAN 10) may be moved to Port 2 (VLAN 20). In this case, the switch must be reconfigured to ensure the user belongs to their original VLAN. MAC VLANs can avoid this problem. This method ensures that the user always belongs to the MAC VLAN, even if the access port changes.

MAC Bind

Item	Description
Port	Port to apply MAC VLAN binding to
MAC Address	Enter the MAC address to which you want to apply MAC VLAN binding. (Input format: AAAA.BBBB.CCCC)
VLAN ID	VLAN to which the MAC address belongs

■ MAC Binding in CLI

● MAC VLAN Binding configuration

```
Switch(config)#interface <IF_NAME>
Switch(config-ge1/1)# switchport port-security mac-bind <MAC_Address> vlan <VLAN_ID>

Switch(config)#interface ge1/1
Switch(config-ge1/1)# switchport port-security mac-bind 8836.6caf.1056 vlan 10
```

● View MAC VLAN Binding Configuration

```
Switch#show port-security mac-bind <IF_NAME>

Switch#show port-security mac-bind ge1/1
Total Number 1
    VLAN ID   MAC ADDRESS    IFNAME
    10        8836.6caf.1056   ge1/1
```

3.3 MAC Auto Binding

You can bind the MAC address learned from the port to a VLAN without directly entering the MAC address.

MAC Bind

Item	Description
Port	Port to which the MAC address will be applied
MAC Address	MAC address to which the MAC Bind will be applied
VLAN ID	VLAN to which the MAC address will belong

■ MAC Auto Binding in CLI

```
Switch(config-ge1/1)#switchport port-security mac-bind auto-conversion number <number>

Switch(config-ge1/1)#switchport port-security mac-bind auto-conversion number 100
```

```
Switch#show port-security mac-bind <IF_NAME>

Switch#show port-security mac-bind ge1/1
Total Number 1
    VLAN ID  MAC ADDRESS    IFNAME
    10       8836.6caf.1056    ge1/1
```

3.4 MAC Filter

A MAC address is a unique physical address assigned to a device's network interface. You can use the MAC address to control device access. You can deny access from specified MAC addresses.

MAC Filter

Item	Description
Port	Port to which the MAC address will be applied
MAC Address	MAC address to which the MAC Bind will be applied
VLAN ID	VLAN to which the MAC address will belong

2) MAC Filter in CLI

● MAC Filter configuration

```
Switch(config)#int <IF_Name>
Switch(config-IF_Name)#switchport port-security mac-filter <MAC Address> vlan <VLAN_ID>

Switch(config)#int ge1/1
Switch(config-ge1/1)#switchport port-security mac-filter 0028.7901.0132 vlan 1
```

● Delete MAC Filter configuration

```
Switch(config)#int <IF_Name>
Switch(config-IF_Name)#no switchport port-security mac-filter <MAC Address> vlan <VLAN_ID>

Switch(config)#int ge1/1
Switch(config-ge1/1)#no switchport port-security mac-filter 0028.7901.0132 vlan 1
```

3.5 MAC Auto Filter

You can filter MAC addresses learned on a port without manually entering the MAC address.

This feature displays dynamically learned MAC addresses and VLAN IDs and allows automatic filtering of MAC addresses on specific ports. The list displays the MAC addresses and VLAN IDs dynamically learned by the port. Select one or more items from the list and click Apply to filter those MAC addresses on that port.

MAC Auto Filter

Item	Description
Port	Port to which the MAC address will be applied
MAC Address	MAC address to which the MAC Bind will be applied
VLAN ID	VLAN to which the MAC address will belong
Number	MAC address number to filter

■ MAC Auto Filter in CLI

● MAC Filter configuration

```
Switch(config)#int <IF_Name>
Switch(config-IF_Name)#switchport port-security mac-filter auto-conversion number <Number>
Switch(config-ge1/1)#witchport port-security mac-filter auto-conversion number 8191

Switch(config-IF_Name)#switchport port-security mac-filter auto-conversion vlan <VLAN_ID>
Switch(config-ge1/1#switchport port-security mac-filter auto-conversion vlan 1
```

● Delete MAC Auto Filter configuration

```
Switch(config)#int <IF_Name>
Switch(config-IF_Name)#no switchport port-security mac-filter
```

● View MAC Auto Filter results

```
Switch#show port-security mac-filter
Switch#show port-security mac-filter <IF-Name>

Switch#show port-security mac-filter
    VLAN ID   MAC ADDRESS     IFNAME
    1         001d.9a01.a9b8   ge1/3
    1         0028.79f1.00ce   ge1/3
    1         04f0.2139.5f2f   ge1/3
    1         04f0.213c.7e45   ge1/3


Switch#show port-security mac-filter ge1/3
Total Number 15
    VLAN ID   MAC ADDRESS     IFNAME
    1         001d.9a01.a9b8   ge1/3
    1         0028.79f1.00ce   ge1/3
    1         04f0.2139.5f2f   ge1/3
    1         04f0.213c.7e45   ge1/3
```

4. VLAN Configuration

A Virtual Local Area Network (VLAN) logically divides a LAN into multiple subgroups, each forming its own broadcast area network. VLAN is a communications technology that logically divides a physical LAN into multiple broadcast area networks (multiple VLANs). Hosts within the same VLAN can communicate directly. However, hosts within different VLAN groups cannot communicate directly with each other. Therefore, broadcast packets are restricted within VLANs. Network security is enhanced because direct access between VLAN groups is prevented.

4.1 VLAN Information

Shows the current VLAN information page. The page is a read-only page that shows the current VLAN, VLAN status, and VLAN port members. Drop-down box will show all the current vlan, the list shows up to 30 vlan VID, state and port members. Select a vlan from the drop-down box, and the list will display information with a VID greater than 30 vlan for that vlan. But if all the vlan no more than 30, regardless of the drop-down box to choose which vlan, the list will show all the vlan information.

VLAN Information

Item	Description
VLAN ID	VLAN identification number
VLAN Type	S: Static D: Dynamic
Member	VLAN의 Member T(tagged)) : The port is a tagged member of this VLAN U((untagged)): The port is a untagged member of this VLAN

■ VLAN Information in CLI

● Display VLAN status

```
Switch#show vlan / show vlan all / show vlan static
VLAN  Name       State          Member ports ([u]-Untagged, [t]-Tagged)
----  -------- -------------- ------------------------------------
1     vlan1      active   [S]     [u]ge1/1  [u]ge1/2  [u]ge1/3  [u]ge1/4
                                  [u]ge1/5  [u]ge1/6  [u]ge1/7  [u]ge1/8
                                  [u]xe1/9  [u]xe1/10 [u]xe1/11 [u]xe1/12
10    vlan10     active   [S]
20    vlan20     active   [S]
```

4.2 VLAN Configuration

You can create and delete VLANs. To create a new VLAN, enter a VID between 2 and 4094 in the active row. The system generates a VLAN name based on the VLAN ID and cannot be modified. Clicking “Apply“ displays the VID and VLAN name of the VLAN you created in the list box. The switch creates VLAN 1 by default, and VLAN 1 cannot be deleted.

To delete a VLAN, click the VLAN in the list box. The VLAN will appear in the active row, and clicking the “Delete“ button will remove the VLAN information from the list box.

If you delete a VLAN ID that contains port members, the member ports in the deleted VLAN will become members of VLAN 1.

VLAN Configuration

Item	Description
VLAN ID	VLAN identification number
VLAN Name	VLAN Interface Name

■ **VLAN Configuration in CLI**

● Add VLAN and enable VLAN

```
- Add VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan <VLAN_ID>

- Enable VLAN
Switch(config)# ip interface vlan <VLAN_ID>
```

```
Ex)
Switch(config)#vlan database
Switch(config-vlan)#vlan 10
Switch(config-vlan)#vlan 20
Switch(config)# ip interface vlan 10
Switch(config)# ip interface vlan 20
```

● Display VLAN configuration

```
Switch(config)#show running-config
!
vlan database
 vlan 10
 vlan 20
!
ip interface vlan 10
ip interface vlan 20
```

● Display VLAN status

```
Switch#show vlan / show vlan all / show vlan static
VLAN  Name          State          Member ports ([u]-Untagged, [t]-Tagged)
----  ----------- -------------- ------------------------------------
1     vlan1         active   [S]     [u]ge1/1  [u]ge1/2  [u]ge1/3  [u]ge1/4
                                     [u]ge1/5  [u]ge1/6  [u]ge1/7  [u]ge1/8
                                     [u]xe1/9  [u]xe1/10 [u]xe1/11 [u]xe1/12
10    vlan10        active   [S]
20    vlan20        active   [S]
```

4.3 VLAN Port Configuration

Access Port

Item	Description
Port	The physical port to which the VLAN will be applied.
Mode	VLAN operation mode(Access, Trunk, Hybrid)
Current VLAN	All the current VLAN are VLAN that can be created by the port
Port Members	The port belongs to a VLAN, resulting in VLAN port configuration.

VLAN Mode

1) Access Port

Access ports are typically used to connect to end stations. Access ports have the following characteristics:

- They are members of exactly one VLAN, the port VLAN (aka Access VLAN), which defaults to 1.
- All frames not classified to the Access VLAN are discarded.
- All frames classified to the Access VLAN at transmission are transmitted untagged. Others (dynamically added VLANs) are transmitted with tags.

2) Trunk Port

Trunk ports can simultaneously forward traffic from multiple VLANs and are typically used to connect to other switches. Trunk ports have the following characteristics:

By default, a trunk port is a member of all VLANs (1-4094). The VLANs to which a trunk port belongs can be restricted by allowing the use of permitted VLANs.

Frames classified to a VLAN to which the port is not a member are discarded. By default, all frames except those classified to the port VLAN (the native VLAN) are tagged at egress.

Frames classified to the port VLAN are untagged at egress. You can change the egress tagging to tag all frames. In this case, only tagged frames are accepted for ingress.

2) Hybrid Port

Hybrid ports are similar to trunk ports in many ways, but add additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have the following features:

- Can be configured as VLAN tag-unaware, C-tag-aware, S-tag-aware, or Scustom-tag-aware
- Control over ingress filtering
- Ingress acknowledgement and egress tagging of frames can be independently configured.

■ VLAN Port Configuration in CLI

◆ Configured as Access Port

● Access Port configuration

```
Switch(config)#interface <IF_NAME>
Switch(config-ge1/1)#switchport access vlan <VLAN_ID>

ex)
Switch(config)#interface <IF_NAME>
Switch(config-ge1/1)#switchport access vlan 10
```

● Display Access Port configuration

```
Switch#show running-config
!
interface ge1/1
 switchport access vlan 10
```

● Display VLAN configuration status of all interfaces

```
Switch#show vlan
VLAN  Name          State          Member ports ([u]-Untagged, [t]-Tagged)
---- ------------ -------------  ------------------------------------
1     vlan1         active   [S]    [u]ge1/2  [u]ge1/3  [u]ge1/4  [u]ge1/5
                                    [u]ge1/6  [u]ge1/7  [u]ge1/8  [u]ge1/9
                                    [u]ge1/10 [u]ge1/11 [u]ge1/12 [u]ge1/13
                                    [u]ge1/14 [u]ge1/15 [u]ge1/16 [u]ge1/17
                                    [u]ge1/18 [u]ge1/19 [u]ge1/20 [u]ge1/21
                                    [u]ge1/22 [u]ge1/23 [u]ge1/24 [u]xe1/25
                                    [u]xe1/26 [u]xe1/27 [u]xe1/28
10    vlan10        active   [S]    [u]ge1/1
20    vlan20        active   [S]
```

● Display VLAN configuration status of a specific interface

```
show interface [IF_Name]

Switch#show interface ge1/1
Interface ge1/1
  Hardware Type:      Ethernet
  MAC Address:        0082.442f.3b84
  Description:
  Flags:              <UP,BROADCAST,MULTICAST>
  Admin Status:       UP
  Operate Status:     DOWN
  Index:              2001
  Metric:             1
  MTU:                1500
  Duplex:             ---
  Config Duplex:      AutoNego
  Bandwidth:          ---
  Config Bandwidth:   AutoNego
  Switchport Mode:    access
  Default Vlan:       10
```

● Delete VLAN Access port configuration

```
Switch(config)#interface <IF_NAME>
Switch(config-ge1/1)#no switchport access vlan

If you enter the command, the port will be included in VLAN1.
```

◆ **Configured as Trunk Port**

● Trunk Port Configuration

```
Switch(config)#interface <IF_Name>
Switch(config-ge1/1)#switchport trunk allowed vlan add <VLAN_ID>

Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport trunk allowed vlan add 10
Switch(config-ge1/1)#switchport trunk allowed vlan add 20
```

● Displaying Trunk Port Configuration in CLI

```
Switch#show running-config
interface ge1/1
 switchport mode trunk
 switchport trunk allowed vlan add 10
 switchport trunk allowed vlan add 20

Switch#sh vlan all
VLAN  Name          State          Member ports ([u]-Untagged, [t]-Tagged)
----  ----------  -------------  ------------------------------------
1     vlan1       active   [S]   [u]ge1/1  [u]ge1/2  [u]ge1/3  [u]ge1/4
                                 [u]ge1/5  [u]ge1/6  [u]ge1/7  [u]ge1/8
                                 [u]xe1/9  [u]xe1/10 [u]xe1/11 [u]xe1/12
10    vlan10      active   [S]   [t]ge1/3  [t]ge1/4
20    vlan20      active   [S]   [t]ge1/3  [t]ge1/4
30    vlan30      active   [S]   [t]ge1/3  [t]ge1/4
```

◆ Configured as Hybrid Port

```
Switch(config)#interface <IF_Name>
Add Default VLAN
Switch(config-ge1/3)#switchport trunk native vlan <VLAN_ID>
  /*If not configured, VLAN 1 will be added as the Native VLAN.

Add Tagged VLAN
Switch(config-ge1/1)#switchport hybrid allowed vlan add <VLAN_ID> egress-tagged enable

Add Untagged VLAN
Switch(config-ge1/1)#switchport hybrid allowed vlan add <VLAN_ID> egress-tagged disable

ex)
Switch(config)#interface ge1/3
Switch(config-ge1/3)#switchport trunk native vlan 10
Switch(config-ge1/3)#switchport hybrid allowed vlan add 20 egress-tagged enable
Switch(config-ge1/3)#switchport hybrid allowed vlan add 30 egress-tagged disable
```

● Displaying Trunk Port Configuration in CLI

```
Switch#show running-config
interface ge1/3
 switchport mode hybrid
 switchport hybrid native vlan 10   /* Native VLAN
 switchport hybrid allowed vlan add 20 egress-tagged enable /* Tagged VLAN
 switchport hybrid allowed vlan add 30 egress-tagged disable /* Untagged VLAN

Switch#show vlan all
VLAN  Name          State            Member ports ([u]-Untagged, [t]-Tagged)
----  ----------- -------------- -------------------------------------
1     vlan1       active   [S]     [u]ge1/1  [u]ge1/2  [u]ge1/5  [u]ge1/6
                                   [u]ge1/7  [u]ge1/8  [u]xe1/9  [u]xe1/10
                                   [u]xe1/11 [u]xe1/12
10    vlan10      active   [S]     [u]ge1/3  [u]ge1/4
20    vlan20      active   [S]     [t]ge1/3  [t]ge1/4
30    vlan30      active   [S]     [u]ge1/3  [u]ge1/4
```

5. SNMP Configuration

SNMP is a simple network management protocol, which is the most widely used network management protocol. It has five functions: fault management, accounting management, configuration management, performance management, security management. It provides the information format for the communication between the network management application software and the network management agent.

SNMP network management protocol has four elements: management station, management agent, management information base, network management protocol. On the switch, the management agent is the server for the management workstation to access the switch. The information of the management workstation accessing the network management agent is organized in the for m of MIB to form a management information base.

SNMP has three operations: GET, SET, and TRAP. The GET operation enables the management station to get the value of an object in the agent. The SET action enables the management station to set the value of an object in the agent. The TRAP action enables the agent to advertise events to the management station.

TRAP messages are actively sent to the management workstation when an event occurs on the switch. These messages include cold start, warm start, link up and link down of the port, authentication failure of the common entity name, status switching of STP, etc.

At present, there are three versions of SNMP: SNMPV1, SNMPV2 and S NMPV3. The latter version is the upgraded version of the former, with enhanced functions and improved security. The switch supports all three versions of SNMP and can parse all three versions of SNMP protocol packets. When a TRAP message is sent, it may be sent using any one of SNMPV1, SNMPV2, and SNMPV3.

The switch supports RFC, BRIDGE, and proprietary MIB objects, and can be fully managed via SNMP. Some of the MIBs supported by the switch are listed below: RFC 1213, RFC 1493, RFC 1724, RFC 1850, RFC 1907, RFC 2233, RFC 2571, RFC 2572, RFC 2573, RFC 2574, MIBs common to RFC 2575, RFC 2674, etc.

The management station can access the switch management agent by sending SNMP messages for Get Request, GetNext Request, GetBulk Request, and Set Request to obtain or set the values of the MIB objects of the switch. The switch management agent sends back an SNMP message of Get Response to the management workstation. W hen some events occur on the switch, the management agent of the switch ac tively sends SNMP TRAP messages to the management station.

5.1 Community Name

SNMP (Simple Network Management Protocol) is an Internet standard protocol that uses UDP/IP (User Datagram Protocol/Internet Protocol) to collect and manage information from devices on an IP network, and to modify the information to alter device operation. Eight SNMP communities can be configured.

The default SNMP community is Public, which has read access.

SNMP communities are configured for SNMP V1/V2.

SNMP Community

Item	Description
Community Name	Indicates the community string to allow access to the SNMP agent. (English or numeric characters, 0 to 255 characters)
Read / Write	Select read or read/write permissions to allow access to the SNMP agent.
Operation	Indicates the SNMP operation status

■ Community Name in CLI

● Add Community

```
Switch(config)#snmp community <Community Name> {ro/rw}

ex)  Switch(config)#snmp community privilege rw
```

● Delete Community

```
Switch(config)#no snmp community <Community Name>

ex) Switch(config)#no snmp community privilege
```

● View Community

```
Switch#show snmp community
 Community-Access      Community-String
 ----------------      ----------------
 read-only             public (public is the Read-only community string)
 read-write            private (private is the Read-write community string)


Switch#show running-config
!
username admin enc-password ********************  privilege
!
snmp community public ro
snmp community private rw
!
```

5.2 TRAP Target

Typically, SNMP operates by periodically requesting information and responding to requests using a polling method. However, with SNMP traps, the agent sends an SNMP message to the manager when a specific event occurs, rather than requesting and responding to system information. After receiving an event, the manager can choose to take action based on the event.

SNMP Trap

Item	Description
Name	Indicates the Trap name of the trap configuration (target).
Transmit IP Address	Indicates the SNMP trap destination IP address. (Server IP Address)
SNMP Version	Indicates the SNMP trap support version. SNMPv1: Set the SNMP trap support version to 1. SNMPv2c: Set the SNMP trap support version to 2c. SNMPv3: Set the SNMP trap support version to 3.

■ TRAP Target in CLI

● Add SNMP Trap

```
Switch(config)#snmp trap <trap name> host <server IP address> version {snmp version}

ex) Switch(config)#snmp trap snmp-trap host 192.168.192.30 version 3
```

● Display SNMP Trap configuration

```
Switch#sh snmp trap
Trap Name:snmp_trap
IP Address:192.168.192.30
Version:3
```

● Delete SNMP Trap

```
Switch(config)#no snmp trap <trap name>

ex) Switch(config)#no snmp trap snmp-trap
```

● SNMP Keep Alive configuration

```
■ Configuring SNMP Keep Alive Activation
Switch(config)#snmp keep-alive enable

■ Configuring Keep-Alive Transmission Periods
Switch(config)#snmp keep-alive period <times>
 times unit : Second

ex)
Switch(config)#snmp keep-alive enable
Switch(config)#snmp keep-alive period <10>
```

5.3 SNMP User

An SNMP user is an account used in the SNMPv3 protocol to control secure access to network devices. Unlike the simple “community string“ used in SNMPv1 and v2c, an SNMPv3 user provides robust security features.

Enhanced Security: SNMPv3 provides enhanced security by providing message integrity, sender authentication, and message encryption.

Credentials: An SNMP user is defined by login credentials, such as a user name, authentication password, and encryption password.

Authorization: Network administrators can associate SNMP users with specific “groups“ to restrict access rights and visibility to the Management Information Base (MIB).

Engine ID: Each SNMP user is associated with a unique “Engine ID“ associated with the network device.

Configuration: Users can be created and configured through network management software, the device’s command-line interface (CLI), or the web interface.

SNMP users are securely used for network management tasks, such as collecting performance data, detecting errors, and remotely configuring network devices.

SNMP User Configuration

Item	Description
User Name	Unique user name used for SNMP communications.
Auth Algo	Algorithm used for message authentication (MD5, SHA).
Auth password	Password used for authentication.
Priv Algo	Algorithm used for data encryption (DES, AES).
Prive Password	Password used for encryption.

■ Add SNMPv3 user in CLI

● Add SNMPv3 user

```
Switch(config)#snmp user <snmpuser> {rw : ro} v3
                auth {sha:md5} <auth_password> priv {des } <priv_password>

    - SNMP_USER : SNMP v3 User
    - ro, rw : ro(Read-Only) , rw(Read Write)
    - sha/md5 : Authentication algorithm
    - Auth_Password: Authentication password
    - Priv_Password: Encryption password
    - des : Encryption Algorithm

Switch(config)#snmp user snmpuser rw v3 auth sha Password priv des Password
```

● Delete SNMPv3 user

```
Switch(config)#no snmp user <snmpuser>

Switch(config)#snmp user snmpuser
```

Note) MD5 and DES algorithms can be used. However, MD5 and DES are vulnerable to security vulnerabilities, so SHA and AES are recommended.

● SNMP v3 User 확인

```
show running-config
!
snmp user snmpuser ro auth sha ********** priv aes **********
!
```

*Note) The password is converted to a local key and stored in a location that is inaccessible to all administrators. *** only displays the password input location and notifies that it has been successfully created.*

6 ACL Configuration

Network access control is achieved by analyzing packets sent and received through an interface and allowing or denying them based on established rules.

This feature is applicable to network segments. It controls incoming and outgoing packets by creating a list that allows or denies specific ports or segments based on IP addresses, port numbers, and protocols. This list is then applied to the interface.

A key characteristic of ACLs is that they are applied in the order in which they appear in the ACL list. The last clause of each access list, [deny any] or [deny ip any any], indicates that all traffic is blocked. Therefore, if an allow list is created, anything except the allow list will be denied. If there is only a deny list and no allow list, everything will be denied.

There are two methods:

1. Whitelist: By default, all addresses are denied and only those allowed are specified.
2. Blacklist: By default, all addresses are allowed and only those denied are specified.

6.1 Standard IP

In an Access Control List (ACL), a “Standard IP :Source IP-based ACL“ is an access control method that allows or blocks access based on the source IP address of a packet when filtering traffic. It is often used by network administrators to allow or restrict traffic coming from a specific IP address or IP address range. It offers the following advantages:

- Simple access control based on a specific source IP address makes configuration easy.
- Network resources can be protected by restricting access to only trusted IP addresses or internal networks.
- Network Control: Network access can be controlled by specific users or devices, facilitating access control to internal resources.

Standard IP controls packets based solely on the source IP address. You can create one or more rules by selecting an ACL group number from 1 to 99 or 1300 to 1999. When you create and add an ACL list to a Standard ACL group, the system applies the ACL list in the order in which it was added. If you delete an ACL list from a group, other ACL lists remain unchanged and are automatically sorted and applied.

ACL Based Source IP

Item	Description
ACL Standard Group Num ACL Group:	Standard ACL Group Number Numbers can be 1-99 or 1300-1999.
Source IP Address:	Source Host or Source Network IP Address
Source Wildcard	A filter value used to extract specific IP addresses or networks. The bits to be filtered are distinguished by “0“ and “1.“ “0“ indicates a required match, while “1“ indicates a non-required match.
Filter [Deny : Permit]	Whether matching data packets are denied or allowed.

■ Standard IP in CLI

● Configuring an ACL Based on Source IP

```
Switch(config)#access-list 1 {permit/deny} <Source IP address> <Source Wildcard>

Switch(config)#access-list 1 permit 192.168.192.0 0.0.0.255
```

● View ACL Based Source IP configuration

```
Switch#show access-list

Standard IP access list 1,
    permit 192.168.192.0, wildcard bits 0.0.0.255
    deny   any
```

● Delete ACL List

```
Delete ACL Group
Switch(config)#no access-list <ACL ID>
Switch(config)#no access-list 1

Delete ACL List
Switch(config)#no access-list 1 {permit/deny} <Source IP address>
Switch(config)#no access-list 1 permit <Source IP address>
```

6.2 Extended IP

Extended IP ACLs control packets by referencing the source IP address, destination IP address, TCP/UDP port number, and port number. You can create one or more rules for a group by selecting an ACL group number between 100 and 199 or 2000 and 2699. When you create and add an ACL list to an Extended IP ACL group, the system applies the ACL list in the order in which it was added. If you delete an ACL list from a group, other ACL lists remain unchanged and are automatically sorted and applied. Extended IP-based ACLs are primarily used in routers and firewalls to allow/block specific application traffic, control access between network segments, prevent data leaks, or enforce security rule compliance.

You can specify various conditions to control traffic based on specific protocols and ports, enhancing network security. ACL conditions can be configured in various ways to allow or block only specific application traffic.

Extended ACLs can be controlled based on the following detailed elements:

- Source and Destination IP Addresses: You can specify the source and destination IP addresses of the traffic to be filtered.
- Protocol Type: You can filter specific protocols, such as TCP, UDP, or ICMP.
- Port Number: You can filter only specific application traffic by specifying a specific TCP or UDP port number (e.g., port 80 for HTTP or port 443 for HTTPS).
- Other Fields: You can configure conditions such as packet flags and protocol-specific options.

ACL Based Extended IP

Item	Description
ACL Extended IP Group Num / ACL Group ID:	Extended ACL group number. Numbers can be 100 to 199 or 2000 to 2699. You can select from the drop-down menu.
Source IP	Source Host or Destination Network IP Address
Source Wildcard	A filter value used to extract a source IP address or network. The filter bits are separated by “0“ and “1,“ where “0“ indicates a match and “1“ indicates an optional match.
Destination IP	Destination Host or Destination Network IP Address
Destination Wildcard	A filter value used to extract the destination IP address or network. The bits to be filtered are distinguished as “0“ or “1,“ with “0“ indicating a required match and “1“ indicating an optional match.
Protocol Type	Protocols to Apply to the ACL Group
Source Port	Source Port Number Only valid for TCP/UDP protocols.
Destination Port	Destination Port Number Only valid for TCP/UDP protocols.
TCP Flag	A 1-bit field in the TCP packet header that contains various control information regarding the TCP connection status or data transfer.
Filter	Select whether to reject or allow matching data packets.

■ Extended IP in CLI

● Configuring Extended IP ACLs

```
Switch(config)#access-list 100 {permit ¦ deny}  {protocol} <Source IP address>
   <Source Wildcard> <Port Number><destination IP address> <Destination Wildcard>
   <Port Number> <tcp flag>

Switch(config)#access-list 100 permit tcp 192.168.192.0 0.0.0.255 80
   192.168.10.0 0.0.0.255 80
Switch(config)#access-list 100 deny any any
```

● View Extended IP ACL

```
Switch#show access-list <ACL Number>
Switch#show access-list 100
Extended IP access list 100,
     permit tcp 192.168.192.0 0.0.0.255 www 192.168.10.0 0.0.0.255 www
     deny   ip any any
```

● Delete Extended IP ACL

```
Delete ACL Group
Switch(config)#no access-list <ACL ID>
Switch(config)#no access-list 100

Delete ACL List
Switch(config)#no access-list <ACL ID> {permit ¦ deny}  {protocol} <Source IP address>
 <Source Wildcard> <Port Number> <destination IP address> <Destination Wildcard>
 <Port Number>

Switch(config)#no access-list 1 permit <Source IP address>
Switch(config)#no  access-list  100  permit  tcp  192.168.192.0  0.0.0.255  80  192.168.10.0
0.0.0.255 80
```

6.3 MAC IP

A MAC-IP-based ACL is a method of access control that combines MAC addresses and IP addresses. MAC-IP-based ACLs provide a higher level of security and play a crucial role in protecting network resources by simultaneously verifying both MAC and IP addresses on the network.

This ACL restricts network access to specific devices using only specific IP addresses. MAC-IP-based ACLs are primarily used when network devices are difficult to identify based on IP addresses alone or when a higher level of security is required.

The advantages of a MAC-IP-based ACL include:

- By displaying both MAC and IP addresses, unauthorized access attempts are difficult. This helps defend against attacks such as IP spoofing and MAC address spoofing.
- Protects network resources by restricting network access to only specific devices.
- Restricts access to network devices or services to specific devices, enabling more granular access control.

MAC-IP-based ACLs strengthen security by restricting external network access to only devices with registered MAC addresses and IP addresses within the corporate network. This allows access only to authorized devices within the company, or restricts network access to specific devices with predefined IP addresses. This protects network resources and security. In security-critical environments, this feature can be used to prevent unauthorized network access by granularly controlling access based on MAC and IP addresses.

You can create one or more rules for a group by selecting an ACL group number between 700 and 799.

ACL Based MAC IP

Item	Description
ACL Group ID:	MAC ACL group number. Numbers can be selected from 700 to 799.
Filter	Whether to reject or allow matching data packets.
Source MAC	Source Host or Network MAC Address
Source MAC Wildcard	This is a filter value used to extract MAC addresses or networks. The filter bits are separated by “0“ and “1“, with “0“ indicating a match and “1“ indicating a non-match.

Destination MAC	Destination Host or Network MAC Address
Destination MAC Wildcard	This is a filter value used to extract MAC addresses or networks. The bits to be filtered are separated by “0“ and “1“, with “0“ indicating a match and “1“ indicating an optional bit.
Source IP	Source Host or Network IP Address
Source IP Wildcard	This is a filter value used to extract the source IP address or network. The filter bits are separated by “0“ and “1“, with “0“ indicating a required match and “1“ indicating an optional match.
Destination IP:	Destination Host or Destination Network IP Address
Destination IP Wildcard	This is a filter value used to extract the destination IP address or network. The filter bits are separated by “0“ and “1“, with “0“ indicating a required match and “1“ indicating an optional match.

■ MAC IP in CLI

● Configuring ACL Based MAC IP

```
Switch(config)#access-list <ACL_Number> {permit¦deny} <Source MAC address>
    <Source MAC Wildcard> <Destination MAC address> <Destination MAC Wildcard>
    <Source IP address> <Source IP  Wildcard> <Destination IP address>
    <Destination IP Wildcard>

Switch(config)#access-list 700 permit 001d.9a01.0000 0000.0000.ffff 001d.9a01.0000
0000.0000.ffff ip 192.168.192.0 0.0.0.255 192.168.10.0 0.0.0.255

Switch(config)#access-list 700 permit 001d.9a01.0000 0000.0000.ffff 001d.9a01.0000
0000.0000.ffff ip 192.168.192.0 0.0.0.255 192.168.10.0 0.0.0.255
```

● Displaying MAC IP-based ACL configuration

```
Switch#show access-list <ACL_Number>

Switch#show access-list 700

Extended MAC IP access list 700,
 deny   001d.9a01.0000 0000.0000.ffff 0028.7901.0000 0000.0000.ffff ip 192.168.192.0
0.0.0.255 192.168.10.0 0.0.0.255
 deny   001d.9a01.0000 0000.0000.ffff 0028.7901.0000 0000.0000.ffff ip 192.168.100.0
0.0.0.255 192.168.10.0 0.0.0.255
```

● Delete MAC IP-based ACL lists

```
Switch(config)#no access-list <ACL_Number> {permit ¦ deny} <Source MAC address>
  <Source MAC Wildcard> <Destination MAC address> <Destination MAC Wildcard>
  <Source IP address> <Source IP  Wildcard> <Destination IP address>
  <Destination IP Wildcard>

Switch(config)#no access-list 700 permit 001d.9a01.0000 0000.0000.ffff 001d.9a01.0000
  0000.0000.ffff ip 192.168.192.0 0.0.0.255 192.168.10.0 0.0.0.255
```

6.4 MAC ARP

This refers to an ACL that filters network traffic based on MAC addresses and ARP (Address Resolution Protocol). It applies filtering based on MAC addresses and IP addresses to ARP request and ARP response packets. This allows you to allow or block ARP communications between specific IP addresses and MAC addresses.

ARP is a protocol that translates IP addresses into MAC addresses on a network and operates primarily at Layer 2. ACL-Based MAC ARP filters ARP packets and controls traffic based on MAC addresses and ARP requests/responses.

MAC ARP can apply ACLs to ARP packets. MAC ARP group numbers range from 1100 to 1199. MAC ARP groups are only valid for ARP packets.

ACL Based MAC ARP

Item	Description
ACL Group ID	MAC ARP ACL Group Number The group number can be selected from 1100 to 1199. Select from the drop-down menu.
Filter	Controls whether matching data packets are rejected or allowed.
Sender MAC	Source Host or Network MAC Address
Sender MAC Wildcard	Filter values used to extract source MAC addresses or networks are “0“ and “1“ to distinguish the bits to filter. “0“ indicates a bit that must match, while “1“ indicates a bit that does not need to match.
Sender IP	Source Host or Network IP Address
Sender IP Wildcard	Filter values used to extract source IP addresses or networks. “0“ and “1“ to distinguish the bits to filter. “0“ indicates a bit that must match, while “1“ indicates a bit that does not need to match.

■ MAC ARP in CLI

● Configuring MAC ARP-based ACLs

```
Switch(config)#access-list <ACL_Number> {permit /deny} arp
                <Sender Mac Address> <Sender Mac Wildcard>
                <Sender IP Address> <Sender IP Wildcard>


Switch(config)#access-list 1100  permit arp  001d.9a01.0000 0000.0000.ffff
              192.168.192.0 0.0.0.255
```

● Display MAC ARP-based ACL configuration

```
Switch#show access-list <ACL_number>

Switch#show access-list 1100
Extended MAC ARP access list 1100,
    permit arp 001d.9a01.0000 0000.0000.ffff 192.168.192.0 0.0.0.255
```

● Delete MAC ARP-based ACLs

```
Switch(config)#no access-list <ACL_Number> {permit /deny} arp
                <Sender Mac Address> <Sender Mac Wildcard>
                <Sender IP Address> <Sender IP Wildcard>

Switch(config)#no access-list 1100  permit arp
    001d.9a01.0000 0000.0000.ffff  192.168.192.0 0.0.0.255
```

6.5 ACL Information

This section displays information about the configured ACL. An ACL Resource refers to the resource or target used to configure or apply an ACL. Generally, an ACL defines a set of rules used to control and filter network traffic. The resource or target to which an ACL is applied is called an ACL Resource. This resource can take various forms and includes the concept of multiple targets to which an ACL can be applied on a network device.

■ ACL Information in CLI

```
Switch#show access-list

Standard IP access list 1,
    permit 192.168.192.0, wildcard bits 0.0.0.255

Extended IP access list 100,
    permit ip 192.168.10.0 0.0.0.255 any

Extended IP access list 700,
    permit 001d.9a01.0000 0000.0000.ffff vid 1 ip 192.168.192.0 0.0.0.255
 192.168.192.0 0.0.0.255

Extended IP access list 1100,
    permit arp 001d.9a01.0000 0000.0000.ffff 192.168.192.0 0.0.0.255
Switch#
```

6.6 ACL Reference

Applying an ACL Group is a method of grouping multiple Access Control List (ACL) rules and applying them to network devices. This allows multiple ACLs to be grouped and configured and applied simultaneously, resulting in more efficient and consistent management.

An ACL Group is a method of grouping multiple Access Control Lists (ACLs) and managing or applying them as a single unit. While each ACL can typically be managed separately when filtering traffic on network devices, managing and applying multiple ACLs simultaneously is often more efficient. This is where ACL Groups come into play. ACL Groups allow you to group multiple individual ACLs and manage them as a single group. Using these groups allows for more efficient management than managing and applying multiple ACLs individually.

Configuring an ACL involves classifying traffic using Access Lists, defining allow/deny rules, and then creating an ACL group. This group is then applied to a specific interface. Before applying an ACL to an interface, an ACL group containing the rules must already be created.

ACL Group

Item	Description
Port	Ports to which the ACL will be applied
All ACL Groups	All configured ACL groups
Referenced ACL Groups	ACL groups applied to the port

■ CLI에서 ACL 그룹(ACL Group) 설정

● ACL Reference in CLI

● Configure ACL group port application

```
Switch(config)#interface <IF_Name>
Switch(config-ge1/1)#access-group <ACL_Number>

Switch(config)#interface ge1/1
Switch(config-ge1/1)#access-group 100
```

● View ACL group applied to ports

```
Switch#show access-group
    Interface ge1/1
      access-list 100 is set (in hardware)
```

● Delete the ACL group applied to the port

```
Switch(config)#interface <IF_Name>
Switch(config-ge1/1)#no access-group <ACL_Number>

Switch(config)#interface ge1/1
Switch(config-ge1/1)#no access-group 100
```

7 QOS Configuration

Quality of Service (QoS) is a technology that manages and optimizes data flow on a network. It ensures the quality of data transmission and prioritizes applications, users, and data flows to ensure critical traffic is delivered without delay or loss. It is a quality-of-service improvement measure that ensures a certain level of performance for data transmission.

QoS allows you to assign different levels of network service to various types of traffic, such as multimedia, video, specific protocols, time-critical real-time traffic (e.g., VoIP, video conferencing, streaming services), and file backup traffic. This feature not only reserves bandwidth but also limits other non-critical traffic.

QoS prioritizes network traffic and prioritizes critical traffic, ensuring the quality of real-time services. It minimizes delays that may occur in real-time applications, preventing degradation in call quality or video streaming. It efficiently utilizes network bandwidth to ensure sufficient bandwidth for critical traffic. It ensures stable data transmission by preventing the loss of critical data during network congestion.

7.1 QoS Apply

QoS Apply

Item	Description
Port	Select the port to which QoS will be applied.
QOS Type	QoS service type.
User Priority	QOS policy priority.

COS-Based: This method groups traffic by class to indicate communication quality. This is a class-based traffic control method. When a priority-assigned packet arrives at a port, the priority is mapped to a differentiated service class that can be processed. Packets with higher service classes are processed first. The mapping between priorities and service classes is primarily port-based. Each service class is associated with a differentiated queue on the output port.

DSCP-Based: The DSCP (DS Code Point) defines the action that a Diffserv-aware system should take on a packet marked in the packet header. The IPv4 header defines the Type of Service (TOS) field, which applications use to indicate low latency, high throughput, and low loss rates. However, existing systems ignore these application requirements and treat all packets equally.

The Diffserv architecture defines a set of DS Code Points for QoS-enabled systems and Diffserv routers to use. DiffServ redefines the TOS field by renaming it the DS field and defines a set of existing packet forwarding methods called Per-Hop-Behavior (PHB). DiffServ is essentially a relative priority technique that creates differentiated classes of service by marking packets' DS fields differently and processing packets according to these markings. The DiffServ architecture also defines a set of actions called forwarding behaviors that correspond to DSCPs. A QoS-enabled system marks the priority bits in the DS field in the packet header as DSCPs. When a system receives a packet with a DSCP value, the router applies the forwarding behavior associated with that DSCP. The packet is then sent onto the network.

■ Applying QoS in CLI

● QoS DSCP-Base configuration

```
Switch(config)#interface <IF_Name>
Switch(config)#interface ge1/1
Switch(config-ge1/1)#qos dscp-based
```

● QoS Class configuration

```
Switch(config)#qos class <Class ID> remark {acl¦cos¦dscp}
                {ACL_ID¦COS Value¦DSCP Value}
Switch(config)#qos class 1 match cos 7
```

● QoS Policy configuration

```
Switch(config)#interface <IF_Name>
Switch(config)#interface ge1/1

Switch(config-ge1/1)#qos apply-policy <Policy_ID>
Switch(config-ge1/1)#qos apply-policy 10
```

● Displaying QoS configuration

```
Switch#show running-config
!
interface ge1/1
 qos apply-policy 10
 qos dscp-based

------------------------------------------------------------------------
Switch#show qos policy
 policy   10:
  class    1: remark cos 7,

------------------------------------------------------------------------
Switch#show qos interface <IF_Name>

Switch#show qos interface ge1/1
interface                    : ge1/1
trust mode                   : dscp based
default priority             : 1/qp1

------------------------------------------------------------------------
Switch#sh qos interface
 ifname   trust mode   default priority/queue
 ge1/1    policy 10    3/qp3
 ge1/2    cos based    0/qp0
 …
```

7.2 QoS Schedule

Configure QoS scheduling mode and queue priority and weight values.
Display the port scheduling mode and weight values for each queue.

QoS Schedule

Item	Description
Selected Port(s)	Ports to which QoS is applied
QoS Schedule Mode	How to define processing priorities for traffic queues when applying QoS policies
Weight of queue	Values used when defining priorities for multiple traffic queues

- WRR: A scheduling algorithm used to schedule data flows in a network. WRR provides a fixed number of opportunities for each queue or task, as determined by configured weights that influence the portion of capacity received by each queue or task.

- SP: Configure a Behavior Aggregate (BA) or Multifield (MF) classifier to identify delay-sensitive traffic. All delay-sensitive packets are assigned to a strict priority queue to minimize delay. Configure a policer to inspect the data stream entering the strict priority queue to prevent starvation in other queues. The policer defines a lower bound, marks packets exceeding the bound as out-of-profile, and drops out-of-profile packets if the physical interface is congested. If there is no congestion, the software forwards all packets, including out-of-profile packets. Optionally, configure another policer to define an upper bound and drop packets exceeding the bound, regardless of physical interface congestion.

- WFQ: WFQ (Weighted Fair Queue) has 4096 classes, and each class is weighted by IP Precedence to reduce the actual packet size and increase priority for processing.

■ Configuring QoS Schedule in CLI

● QoS Schedule Mode SP configuration

```
Switch(config)#interface <IF_Name>
Switch(config)#interface ge1/1
Switch(config-ge1/1)#qos sched sp
```

● QoS Schedule Mode WFQ configuration

```
Switch(config)#interface <IF_Name>
Switch(config)#interface ge1/1
Switch(config-ge1/1)#qos sched wfq
```

● QoS Schedule Mode WRR configuration

```
Switch(config)#interface <IF_Name>
Switch(config)#interface ge1/1
Switch(config-ge1/1)#qos sched wrr
```

● Weight of Queue configuration

```
Switch(config)#interface <IF_Name>
Switch(config)#interface ge1/1
Switch(config-ge1/1)#qos qosprofile <qp1:qp1:qp2¦qp3:qp4:qp5¦qp6¦qp7}
                    weight <Value of Weight>
Switch(config-ge1/1)#qos qosprofile qp7 weight 120
```

● Displaying QoS Schedule Configuration

```
Switch#sh qos interface ge1/1
interface                    : ge1/1
trust mode                   : apply policy 10
 class    1: remark cos 7,
default priority             : 3/qp3
priority queues              : 8
```

```
schedule algorithm          : wrr(weighted round robin)
weight of queues            :
 qp0[0],qp1[2],qp2[4],qp3[8],qp4[16],qp5[32],qp6[64],qp7[100]
cos map qosprofile          :
cos0[qp0],cos1[qp1],cos2[qp2],cos3[qp3],cos4[qp4],cos5[qp5],cos6[qp6],cos7[qp7]
dscp map qosprofile         :
dscp0-dscp7[qp0],dscp8-dscp15[qp1],dscp16-dscp23[qp2],dscp24-dscp31[qp3],dscp32
-dscp39[qp4],dscp40-dscp47[qp5],dscp48-dscp55[qp6],dscp56-dscp63[qp7]
qosprofile configuration :
    QP0 Priority[0] Queue[0]
    QP1 Priority[1] Queue[1]
    QP2 Priority[2] Queue[2]
    QP3 Priority[3] Queue[3]
    QP4 Priority[4] Queue[4]
    QP5 Priority[5] Queue[5]
    QP6 Priority[6] Queue[6]
    QP7 Priority[7] Queue[7]
```

8 IP Basic Configuration

You can configure the VLAN interface, remove the VLAN interface, configure the IP address of the interface, delete the IP address of the interface, and view the interface information. Only when the VLAN already exists can it be set as an interface. Only the interface address can be configured on the configured interface.

IP Address

Item	Description
VLAN ID	Displays the VLAN.
IP Address/Subnet Prefix	You can edit the IP address by entering the IP address/ Subnet Prefix of the system's VLAN.
DHCP Client	The IP address of the VLAN Interface is assigned by the DHCP Server.
MAC Address	MAC Address of the corresponding VLAN Interface
Create VLAN Interface	After entering the VLAN ID and clicking, the entered VLAN ID will be displayed
Delete VLAN Interface	After selecting and clicking the VLAN ID, the entered VLAN ID will be deleted.
Set IP Address /DHCP client	IAfter entering the IP Address and clicking, it will be changed to the IP Address.
Delete IP Address	After selecting the item for which you want to delete the IP address from Line Item, click to delete the IP address.

Note)1. VLAN1 Interface cannot be deleted.

2. If you change the VLAN IP address you're connected to, your web connection will be lost. You'll need to reconnect using the changed IP address.

3. If only VLAN1 exists and DHCP Client is enabled and an IP address is not allocated from the DHCP Server, web/SSH/Telnet access is not possible.

8.1 IP Address Configuration

■ IP Address Configuration in CLI

● Change VLAN1 IP Address

```
Switch(config)#interface vlan1
Switch(config-vlan1)#ip addr <IP Address/Subnet Prifix>

Switch(config-vlan1)#ip addr 192.168.10.39/24
```

● Delete IP Address

```
Switch(config)#interface <IF_Name>

Switch(config-vlan1)#no ip address
```

● Create VLAN Interface

```
Switch(config)#ip interface vlan <VLAN ID>

Switch(config)#ip interface vlan 100
```

```
Switch(config)#show ip interface brief
Interface              IP-Address       Status          Protocol
vlan1                   192.168.10.39   up               up
vlan100                 unassigned      up               down
ge1/1                    unassigned      up               up
```

● Delete VLAN Interface

```
Switch(config)#no ip interface vlan <VLAN ID>

Switch(config)#no ip interface vlan 100
```

```
Switch(config)#show ip interface brief
Interface              IP-Address       Status              Protocol
vlan1                   192.168.10.39   up                   up
ge1/1                   unassigned      up                   up
-------
```

8.2 ARP Configuration and Display

This page displays all the information of the ARP table of the switch. You can use this page to configure static ARP entries, delete ARP entries, and modify dynamic ARP entries to static ARP entries.

When you configure a static ARP entry, you need to enter the IP address and MAC address. The MAC address must be a unique MAC address, and then click the Add key.

When a user deletes an ARP entry, you can choose to delete an ARP entry from one IP address, delete an ARP entry from one network segment, delete all ARP entries, delete all dynamic ARP entries, and delete all static ARP entries. The To delete an IP ARP entry or delete an ARP entry from a network segment, enter the specified IP address or IP segment in the input box. And then click the Delete key.

When a dynamic ARP entry is modified to a static ARP entry, you can choose to change the dynamic ARP entry in a network segment to a static ARP entry. For a network segment, enter the specified network segment in the input box. And then click the Apply button.

ARP Configuration

Item	Description
IP Address	IP Address Learned by the System
MAC Address	MAC Address Learned by the System
Type	How the System Learned

■ ARP Configuration and Display in CLI

● Add manual ARP

```
Switch(config)#arp <IP_Address> <MAC_Address>

Switch(config)#arp 192.168.10.100 1111.2222.3333
```

Enter the MAC address in the format HHHH.HHHH.HHHH.

● Delete manual ARP

```
Switch(config)#no arp <IP_Address>

Switch(config)#no arp 192.168.10.100
```

● View ARP list

```
Switch#show arp
Address                 HWaddress           Interface    Type
192.168.192.100         11:11:22:22:33:33   vlan1        Static
192.168.10.101          aa:aa:bb:bb:cc:cc   vlan1        Dynamic
```

Note) Type: Static: ARP list entered directly by the administrator
Dynamic: ARP list learned dynamically by the system

8.3 Host Static Route Configuration

Static routing is a user-defined route that enables packets to reach the destination address through a specified path from the source address. You can configure a static route as the default route to send packets that cannot be routed to the default gateway.

Static Routes

Item	Description
Target Address /Subnet Prefix	Destination Network Address and Subnet Prefix To configure the default gateway, enter 0.0.0.0/0.
Next Hop:	Enter the IP address of the next hop. The next hop must be on the same network as the interface's IP address.

■ Host Static Route Configuration in CLI

● Add Static Routing

```
Switch(config)#ip route  <A.B.C.D/M> <E.F.G.H>

Switch(config)#ip route 192.168.30.0/24 192.168.10.254
```

<A.B.C.D/M> : Destination Network and IP Subnet Prefix
<E.F.G.H>: Next hop IP Address

● IP Routing Table

```
Switch#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
```

```
C        127.0.0.0/8 is directly connected, lo
C        192.168.10.0/24 is directly connected, vlan1
S        192.168.30.0/24 [1/0] via 192.168.10.1, vlan1
```

C: Route directly connected to the system

S: Route added directly by the administrator

Routing Table

Item	Description
Route State	Select all routing routes or active routing routes. All: All active and inactive routing routes. Active: Active routing routes.
Route Type	Select the routing path acquisition method. - Connected: Routing paths configured on interfaces directly connected to the system. - Static: Manually entered routing paths. - RIP: Routing paths learned using the RIP protocol. - OSPF: Routing paths learned using the OSPF protocol.

● Delete Static Routing

```
Switch(config)#no ip route  <A.B.C.D/M>

Switch(config)#no ip route 192.168.30.0/24
```

9 AAA Configuration

AAA stands for Authentication, Authorization, and AAA provide a consistent framework for configuring security functions. Configuring AAA is essentially a form of network security management, where network security primarily refers to access control.

9.1 AAA Authentication

AAA Authentication Configuration

Item	Description
AAA Authentication Type	Authentication Type

■ AAA Authentication in CLI

Local Authentication
Switch(config)#aaa authentication local

TACACS Authentication
Switch(config)#aaa authentication tacacsplus

Radius Authentication
Switch(config)#aaa authentication radius

9.2 Tacacs+ Configuration

TACACS+ authentication and authorization provides stricter user privilege management, not only verifying user legitimacy but also authorizing commands. After TACACS+ authentication is enabled, users must provide their username and password to the TACACS+ server when accessing the switch. Authentication is only successful if the username and password are accurate and consistent. After authentication, users can access the switch. TACACS+ also divides user privileges into two levels: normal users and privileged users. Normal users can only access the CLI command-line interface in normal mode, while privileged users can access all modes of the CLI command-line interface. Command execution permissions are also configured based on the privilege level. When a user enters a command (except enable, end, and exit), the TACACS+ server must provide authorization. Failure to do so will result in the command not being executed.

TACACS+ authentication and authorization only applies to Telnet and SSH terminals and does not control console terminals. Username and password verification is required when accessing the switch via Telnet or SSH. Access to the CLI is only possible after the username and password have been verified. During SSH access, only authorized users can pass through.

TACACS+ authentication also applies to web logins, but only password permissions and authorizations are verified, without command privileges.

By default, the switch does not enable TACACS+. Telnet, SSH, or web logins all use the multi-user management feature. After enabling TACACS+, you can still configure the multi-user management feature, but it is not actually used.

TACACS+ Config

Item	Description
Server IP	Primary TACACS server address
Option Server IP	Secondary TACACS server address
Authentication Type	TACACS+ basic authentication method. Supports PAP and CHAP - PAP sends passwords unencrypted - CHAP sends MD5-encrypted passwords
Shared Secret	Shared key used to encrypt transmitted data
Authorization	Ability to set controls on specific actions or resources a user can access after authenticating a user
Accounting	Ability to log user sessions and activities

■ Tacacs+ Configuration in CLI

● Server Configuration

```
Switch(config)# tacacsplus enable
Switch(config)# tacacsplus host <server-ip>
Switch(config)# tacacsplus option-host <server-ip>
Switch(config)# tacacsplus key WORD
Switch(config)# tacacsplus auth-type (PAP¦CHAP)

Switch(config)# tacacsplus enable
Switch(config)# tacacsplus host 192.168.10.254
Switch(config)# tacacsplus option-host 192.168.10.253
Switch(config)# tacacsplus key password
Switch(config)# tacacsplus auth-type chap
```

● Display TACACS configuration

```
Switch#show tacacsplus

Tacacs+ Authentication Type  : CHAP
Tacacs+ Host                 : 192.168.10.254
Tacacs+ Option-host          : 192.168.10.253
Tacacs+ Shared Secret        : password
Tacacs+ Authorization        : Disable
Tacacs+ Accounting           : Disable
Tacacs+ Privilege            : Local
Tacacs+ Current Server       : Primary
```

● Delete TACACS configuration

```
Switch(config)# tacacsplus disable
Switch(config)# no tacacsplus host
Switch(config)# no tacacsplus option-host
Switch(config)# no tacacsplus key
```

9.3 Radius Configuration

Once a user is authenticated, the RADIUS protocol, which supports the EAP extension, is used for interaction between the switch and the authentication server. The RADIUS protocol uses a client/server model, where the switch must implement a RADIUS client, and the authentication server must implement a RADIUS server. To ensure the security of the interaction between the switch and the authentication server and prevent unauthorized interactions between the switch and the authentication server, the switch and the authentication server must authenticate each other. The switch and the authentication server require the same key. When the switch or authentication server sends a RADIUS protocol packet, all protocol packets generate a message digest using the HMAC algorithm based on the key. When the switch and authentication server receive the RADIUS protocol packet, the message digest of each protocol packet is verified using the key. If the verification passes, the RADIUS protocol packet is considered legitimate; otherwise, it is considered illegitimate and is discarded. The 802.1X protocol is a port-based access control and authentication protocol, where a port refers to a logical port, which can be a physical port, a MAC address, or a VLAN ID. Switches on a network implement the 802.1X protocol based on MAC addresses. 802.1X is a Layer 2 protocol. The authenticated switch and the user's PC must be on the same subnet, and protocol packets cannot cross network segments. 802.1X authentication uses a client-server model and requires a server to authenticate all users. Before a user is authenticated, only authentication flows can pass through the switch's ports. After successful authentication, data flows can pass through the switch's ports. In other words, a user must be authenticated before accessing the network. When a user authenticates, the PC communicates with the switch using the 802.1X protocol. 802.1X information can be configured.

Radius Configuration

Item	Description
Primary Server	Radius server IP address, in the authentication and billing must be set when this field.
Optional server	Optional Radius server IP address, which can be set if there is an alternate Radius server
UDP Port	Authentication UDP port, the default value is 1812, the user generally do not need to modify this field.

Accounting	Whether to start billing, the default is to start, when doing the authentication and billing to start billing.
Accounting UDP Port	Billing UDP port, the default value is 1813.
Shared Key:	used to set the switch and the Radius server encryption between the shared password, in the authentication and billing must be set this field, and to the same settings on the Radius server.
Accounting Status	Vendor-specific information, users generally do not need to modify this field.
NAS Port NAS Port Type NAS Service Type	NAS port, NAS port type, NAS service type, these three values users generally do not need to modify.
Roaming	Whether to start or turn off the roaming function of Radius.

■ Radius Configuration in CLI

● 802.1x/Radius General Configuration

```
Switch(config)#dot1x
Switch(config)#radius-server host <Radius-Server IP address>
Switch(config)#radius-server option-host <Option-Server IP address>
Switch(config)#radius-server key <share Key>

Switch(config)#dot1x
Switch(config)#radius-server host 192.168.1.254
Switch(config)#radius-server option-host 192.168.1.253
Switch(config)#radius-server key password123
```

● Displaying 802.1x/Radius General Configuration

```
Switch#show radius-server
 PrimaryServerIp    : 192.168.1.254
 OptionServerIp     : 192.168.1.253
 UdpPort            : 1812
 accountingPort     : 1813
 ShareKey           : password123
```

9.4 802.1x Configuration

When a user authenticates, the PC communicates with the switch using the 802.1x protocol. You can configure 802.1x information.

802.1x Configuration

Item	Description
802.1x	Whether to start the 802.1x protocol, be sure to start the 802.1x protocol when doing authentication and accounting. Whether the switch is a common authentication method or an extended authentication method
Reauthentication	Whether to open the re-authentication function, the default is not open, when doing the authentication and billing according to the actual situation to decide. Turning on the authentication function will make the user more reliable when using authentication and billing, but will slightly increase the traffic to the network
Reauthentication Period	Set the re-authentication interval, only in the case of re-authentication function is enabled, the default is 3600 seconds, when doing authentication and billing according to the actual situation to set the value, but the value should not be too small.
Quiet Period	Quiet Period timer, the user generally does not need to modify this field.
Tx-Period	Tx-Period timer, the user generally does not need to modify this field.
Server Timeout	Server timeout timer, users generally do not need to modify this field.
Supplicant Timeout	supplicant timeout timer, the user generally do not need to modify this field.
Max Request	The number of requests, users generally do not need to modify this field.
Reauth Max	Show Reauth Max size.

■ 802.1x Configuration in CLI

● 802.1x Configuration

```
Switch(config)#dot1
Switch(config)#dot1x reauthenticate
Switch(config)#dot1x timeout re-authperiod <time>

Switch(config)#dot1x timeout re-authperiod 1800
```

● Displaying 802.1x Configuration

```
Switch#sh dot1x
  Global 802.1X Parameters
  Dot1x Status            :            Enable
  ReAuth-enabled          :             yes
  Accounting-enabled      :            yes
  ReAuth-period           :             1800
  Quiet-period            :            60
  Tx-period               :             30
  Supp-timeout            :             30
  Server-timeout          :            10
  Max-req                 :              3
  reAuthMax               :              3
  transmit ports          :

  802.1X Interface Summary
  IfName     Status          Mode          Method       Guest Vlan    HostNum
  ge1/1      Link Up         n/a           macbased     n/a           256
```

9.5 802.1x Port Configuration

Before applying 802.1x ports, enable the 802.1x protocol in the 802.1x configuration. This page allows you to configure enforcement on 802.1x ports.

802.1x Port Config

Item	Description
Port Num	The port to which you want to apply the 802.1X protocol.
Port Mode	Determines how 802.1X authentication will operate on the network port. - Auto Mode - Force-Authorized Mode - Force-Unauthorized Mode - N/A
Support Host Num	The number of devices that can be authenticated simultaneously during the 802.1X authentication process.

◆ Port Mode

■ Auto Mode

When a device is connected to a port, 802.1X authentication is automatically performed. If authentication succeeds, the port switches to the “Authorized“ state, allowing network access. If authentication fails, the port switches to the “Unauthorized“ state, blocking network access.

■ Force-Authorized Mode

The port always remains in the “Authorized“ state, allowing network access without authentication. This mode is useful when you need to bypass 802.1X authentication to allow network access. For example, this mode is useful when a device that doesn’t support 802.1X authentication is connected.

■ Force-Unauthorized Mode

The port always remains in the “Unauthorized“ state, blocking network access even after authentication.

■ 802.1x Port Configuration in CLI

● 802.1x port configuration

```
Switch(config)#interface <IF_Name>
Switch(config-ge1/1)#dot1x control auto
Switch(config-ge1/1)#dot1x support-host <Host_Number>

Switch(config)#interface ge1/1
Switch(config-ge1/1)#dot1x control auto
Switch(config-ge1/1)#dot1x support-host 128
```

● Delete 802.1x port configuration

```
Switch(config)#interface <IF_Name>
Switch(config-ge1/1)#no dot1x control auto
Switch(config-ge1/1)#no dot1x support-host <Host_Number>

Switch(config)#interface ge1/1
Switch(config-ge1/1)#no dot1x control auto
Switch(config-ge1/1)#no dot1x support-host 128
```

● Display 802.1x port configuration

```
Switch(config)#show dot1x
Switch#sh dot1x
 Global 802.1X Parameters
 Dot1x Status            :          Enable
 ReAuth-enabled          :           no
 Accounting-enabled      :          yes
 ReAuth-period           :          3600
 Quiet-period            :          60
 Tx-period               :          30
 Supp-timeout            :          30
 Server-timeout          :          10
 Max-req                 :           3
 reAuthMax               :           3
 transmit ports          :
```

```
802.1X Interface Summary
IfName          Status          Mode          HostNum
ge1/1           Link Down       auto          128
ge1/2           Link Down       n/a           256


Switch#show dot1x interface <IF_Name>

Switch#sh dot1x interface ge1/1
 interface ge1/1
 Port-control                : auto
 Maximum hosts               : 128
 Current Connecting hosts    : 0
```

9.6 802.1x User Auth-Information

View 802.1x user authentication information

802.1x Port Config

Item	Description
Username	A user attempting to access a network in the 802.1X authentication protocol.
MAC Address	The user's network interface MAC address.
Authentication state	The authentication status of a port or device during the 802.1X authentication process.
Authenticator state	The status of the authenticator during the 802.1X authentication process.
Back-End state	The status of the authentication process handled by the 802.1X authentication server.
Reauthentication state	The status that occurs during the re-authentication procedure when a network device renews an authentication session after a certain period of time

10 MSTP Configuration

Implementing redundancy between devices is effective for network stability. However, if the connection between switches exceeds the redundancy, looping can occur due to the nature of the switch. This can be caused by broadcast storms, unicast frame duplication, and unstable MAC address tables. Spanning Tree Protocol (STP) is the algorithm that prevents this bridge looping.

MSTP uses RSTP to quickly converge multiple VLANs into Spanning Tree instances, each with its own Spanning Tree topology independent of other Spanning Tree instances. This architecture provides multiple forwarding paths for traffic, enables load balancing, and reduces the number of Spanning Tree instances required to support a large number of VLANs.

MSTP groups multiple VLANs on the network, allowing each VLAN group to have its own independent Spanning Tree. This ensures that specific VLAN traffic is routed through its own unique path, resulting in more efficient use of network resources. Similar to STP, MSTP also prevents network loops. However, unlike STP, which creates a single spanning tree, MSTP creates multiple spanning trees per VLAN group, providing a more flexible structure.

MSTP distributes VLAN-based traffic across each tree, reducing traffic bottlenecks. This allows for more efficient utilization of network links, resulting in better performance than STP or RSTP.

MSTP is also compatible with existing STP and RSTP, allowing it to be used as a gradual upgrade to existing networks.

MSTP is particularly common in large-scale networks and extends the capabilities of existing Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) to provide enhanced flexibility and performance.

10.1 MSTP Global Configuration

Configure MSTP basic parameters.

MSTP Global Configuration

Item	Description
MSTP	Enables or disables the MSTP
Priority	Bridge Priority value. Enter a multiple of 4096.
Portfast Bpdu-Filter	A feature that filters BPDUs from being sent or received on a PortFast port (either completely blocking BPDUs or restricting their processing).

Portfast Bpdu-Guard	A protection feature that immediately blocks a PortFast port from receiving a Bridge Protocol Data Unit (BPDU) and places the port in an err-disable state.
Forward-Time:	The amount of time the Spanning Tree Protocol waits when changing a port's state to ensure stability and prevent loops. The default is 15 seconds. Adjust the time between 4 and 30 seconds.
Hello-Time:	The interval at which the root bridge in the Spanning Tree Protocol periodically transmits Hello messages (Hello BPDUs) to other switches. The default is 2 seconds. Adjust the time between 1 and 10 seconds.
Errdisable-Timeout	A global feature that enables the switch to automatically recover ports that have entered the err-disabled state.
Errdisable-Timeout Interval	A timer that sets the interval between re-enabling the port (the retry cycle) to automatically recover an err-disabled port. The default is 300 seconds (5 minutes).
Max-Age:	The time period that determines how long Bridge Protocol Data Unit (BPDU) information transmitted from the root bridge in the Spanning Tree Protocol will remain valid for other switches in the network. The default is 20 seconds. Adjust the time between 6 and 40 seconds.
Max-Hops	The maximum number of hops a BPDU can traverse within an MSTP network.

■ MSTP Global Configuration in CLI

● Enable MSTP

```
Switch(config)#spanning-tree mst enable
```

● Disable MSTP

```
Switch(config)#no spanning-tree mst
```

● MSTP Priority Configuration

```
Switch(config)#spanning-tree mst priority <Priority_value>
Switch(config)#spanning-tree mst priority 4096
```

● MSTP Forward time Configuration

```
Switch(config)#spanning-tree mst forward-time <Forward time>
Switch(config)#spanning-tree mst forward-time 15
```

● MSTP Hello time Configuration

```
Switch(config)#spanning-tree mst hello-time <Hello time>
Switch(config)#spanning-tree mst hello-time 2
```

● MSTP Max age Configuration

```
Switch(config)#spanning-tree mst max-age <Max age>
Switch(config)#spanning-tree mst max-age 20
```

● MSTP Max Hop Configuration

```
Switch(config)#spanning-tree mst max-hops <Max Hop>
Switch(config)#spanning-tree mst max-hops 20
```

● Displaying the MSTP global configuration

```
Switch#show spanning-tree mst
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 -  CIST Bridge Priority 4096
% 1: Forward Delay 15 - Hello Time 1 - Max Age 6 - Max-hops 10

Switch#show running-config
!
spanning-tree mst configuration
!
spanning-tree mst priority 4096
spanning-tree mst hello-time 1
spanning-tree mst max-age 6
spanning-tree mst max-hops 10
spanning-tree mst enable
```

● Check MSTP global settings

```
Switch#show spanning-tree mst
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 -  CIST Bridge Priority 4096
% 1: Forward Delay 15 - Hello Time 1 - Max Age 6 - Max-hops 10

Switch#show running-config
!
spanning-tree mst configuration
!
spanning-tree mst priority 4096
spanning-tree mst hello-time 1
spanning-tree mst max-age 6
spanning-tree mst max-hops 10
spanning-tree mst enable
```

10.2 MSTP Port Configuration

Select an MSTP port and configure MSTP port parameters for the selected port.
Displays the STP configuration status for all ports.

MSTP Port Configuration

Item	Description
Selected Port	Ports to which MSTP is applied
Portfast	A feature that allows a switch port to immediately transition to the Forwarding state without going through the Listening/Learning transition process of the Spanning Tree.
Portfast Bpdu-Filter	A feature that filters BPDUs from being sent or received on a PortFast port (either completely blocking BPDUs or restricting their processing).
Portfast Bpdu-Guard	A protection feature that immediately blocks a PortFast port from receiving a Bridge Protocol Data Unit (BPDU) and places the port in an err-disable state.
Root Guard	Root Guard is a feature that prevents a specific port from becoming a Root Port (RP).
Link-Type	Type of connection medium(Shared, Point-to-Point)
Port Priority	Configures the priority of a switch port, adjusting the likelihood that the port will be selected as a path in spanning tree calculations to prevent loops. Bridge Priority
Path-Cost	Path Cost value for each link when the Spanning Tree Protocol determines a network path.
STP Version	STP Protocol version

■ MSTP Port Configuration in CLI

● Select a port

```
Switch(config)#interface <IF_Name>
Switch(config)#interface ge1/1
```

● Port Priority Configuration

```
Switch(config-ge1/1)#spanning-tree mst priority <Priority>
Switch(config-ge1/1)#spanning-tree mst priority 0
```

● Path-Cost Configuration

```
Switch(config-ge1/1)#spanning-tree mst path-cost <Path Cost>
Switch(config-ge1/1)#spanning-tree mst path-cost 20000000
```

● STP Version Configuration

```
Switch(config-ge1/1)# spanning-tree mst force-version <STP Version>
Switch(config-ge1/1)# spanning-tree mst force-version 2
```

● Port Priority Configuration

```
Switch(config-ge1/1)# spanning-tree mst portfast
```

10.3 Port Information

You can view the port MSTP status

■ MSTP Port Information in CLI

● Displaying port configuration in CLI

```
Switch#show running-config
interface ge1/1
 spanning-tree mst priority 128
 spanning-tree mst path-cost 20000000
 spanning-tree mst force-version 2
 spanning-tree mst portfast

Switch#show spanning-tree mst interface ge1/1
%    ge1/1: Port 2001 - Id 87d1 - Role Designated - State Forwarding
%    ge1/1: Configured Path Cost 20000000  - Add type Explicit ref count 1
%    ge1/1: Designated Port Id 87d1 - CST Priority 128  -
%    ge1/1: Message Age 0 - Max Age 20
%    ge1/1: CIST Hello Time 2 - Forward Delay 15
%    ge1/1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
%    ge1/1: Version Multiple Spanning Tree Protocol - Received None - Send MSTP
%    ge1/1: Portfast configured - Current portfast on
...
```

11 IGMP SNOOPING Configuration

IGMP (Internet Group Management Protocol) is a protocol for managing the destinations of multicast packets across subnets. A multicast router periodically requests all subnets it connects to for hosts participating in a multicast group (IGMP Query Message).

If a host on a subnet participates in a multicast group, the host reports to the multicast router which multicast group it is participating in (IGMP Report Message).

A multicast router remembers which subnet a received report originated from and determines which multicast group to forward the packet to.

If no query reports are received or an IGMP Leave message is received from a host in a specific multicast group, the multicast router will not forward the packet to all or the specified multicast groups on that subnet. This method prevents multicast packets from being forwarded to subnets without any hosts participating in the multicast group, thereby reducing unnecessary traffic.

While IGMP can reduce unnecessary traffic on a subnet-by-subnet basis, unnecessary traffic can still occur within the subnet. Because the destination MAC address of a multicast packet is a special value, it is not learned in the MAC address table of the L2 switch and is always broadcast. Therefore, even if a host participating in a multicast group is connected to only one port, the L2 switch will forward the received multicast packet to all ports. IGMP snooping detects IGMP reports sent from multicast group-participating hosts to the multicast router. This method learns the destination port of a multicast packet by snooping messages on the L2 switch. This method can reduce unnecessary traffic because multicast packets are not transmitted to ports where there are no multicast group participating hosts within the subnet. With IGMP snooping, the L2 switch only sends one IGMP Report Message with a query even if it receives an IGMP Report Message indicating that multiple hosts are participating in the same multicast group. In addition, if an IGMP Leave Message is received from a host and there are other hosts participating in the same multicast group, the L2 switch does not send an IGMP Leave Message with a query. This makes it appear as if the query is exchanging IGMP messages with a single host, and also suppresses the transmission of unnecessary IGMP messages.

11.1 IGMP SNOOPING Configuration

Enables IGMP Snooping functionality.

IGMP SNOOPING

Item	Description
Global IGMP SNOOPING	Enables/disables IGMP Snooping globally.
VLAN ID	VLAN to which the IGMP SNOOPING feature is applied
VLAN IGMP SNOOPING	Whether the IGMP SNOOPING feature is enabled for the selected VLAN
Fast Leave	Whether the Fast Leave feature is enabled
Fast Leave Timeout:	GMP SNOOPING Fast Leave feature application time
Query Membership Timeout	The interval at which the software responds to an IGMP query after receiving a host shutdown message from the last known active host on the subnet. The value can be between 1 and 25 seconds. The default is 1 second.
Group Membership Timeout	Interval before the switch determines that there are no members of a multicast group or source on the network. The input value is 3 to 65,535 seconds. The default is 260 seconds.

Note)

- *Query Membership Timeout: If no reports are received within this interval, the group status is deleted. This value allows you to adjust the speed at which the software stops transmitting on the subnet. The software can detect the loss of the last member of a group or source more quickly when the value is lower.*
- *Fast Leave: In some scenarios, a query interface is connected to only one receiver host. If a host frequently switches between multiple multicast groups, you can configure the Fast Leave feature on the interface to allow the interface to respond quickly to leave messages sent by the host. After Fast Leave is configured, the query writer does not send group-specific query messages after receiving a leave message from the host. Instead, the query writer directly notifies the upstream multicast device that the host has left the multicast group. Fast Leave reduces the delay in leaving message responses and saves network bandwidth. IGMP Fast Leave applies only to IGMPv2 and IGMPv3.*
- *Group Membership Timeout: The interval before the switch determines that there are no members of a multicast group or source on the network. The value can be between 3 and 65,535 seconds. The default is 260 seconds.*

■ IGMP SNOOPING Configuration in CLI

● IGMP SNOOPING Global Configuration

▪ IGMP SNOOPING Global Configuration

Switch(config)#ip igmp snooping

▪ Disable Global IGMP SNOOPING

Switch(config)#no ip igmp snooping

▪ Configure VLAN IGMP Snooping

Switch(config)#ip igmp snooping vlan *<VLAN_ID>*

Switch(config)#ip igmp snooping vlan 10

▪ Configure Fast Leave

Switch(config)#ip igmp snooping fast-leave vlan *<VLAN_ID>*

Switch(config)#ip igmp snooping fast-leave vlan 10

▪ Configure Fast Leave Timeout

Switch(config)#ip igmp snooping fast-leave-timeout *<fast-leave-timeout>* vlan *<VLAN_ID>*

Switch(config)#ip igmp snooping fast-leave-timeout 10 vlan 10

▪ Configure Query Membership Timeout

Switch(config)#ip igmp snooping query-membership-timeout *<query-membership-timeout>* vlan *<VLAN_ID>*

Switch(config)#ip igmp snooping query-membership-timeout 100000 vlan 10

▪ Configure Group Membership Timeout

Switch(config)#ip igmp snooping group-membership-timeout <group-membership-timeout> vlan *<VLAN_ID>*

Switch(config)#ip igmp snooping group-membership-timeout 100000 vlan 10

Note: Before configuring an IGMP snooping VLAN, you must enable the VLAN interface on which you want to configure it.

11.2 Multicast Group Information

Multicast group information can be displayed.

Multicast group information is data used to efficiently forward multicast traffic. This allows you to track multicast addresses and devices subscribed to the group, ensuring traffic is forwarded only to the required network ports. IGMP snooping and multicast routing manage multicast group information and optimize multicast traffic delivery.

You can view the igmp snooping multicast program information

Group Information

Item	Description
VLAN ID	VLAN ID with Multicast Snooping enabled
Address	Multicast address learned using Multicast Snooping
Port	Port to forward multicast packets

■ Multicast Group Information in CLI

```
Switch#show ip igmp snooping
IGMP Snooping is globally enabled
IGMP Snooping send-query source-address is 192.168.10.1
IGMP Snooping send-query version is v2
Bridge 1: VLAN 1
        IGMP Snooping is enabled
        IGMP Snooping fast-leave is enabled
        IGMP Snooping fast-leave-timeout is 300000 ms
        IGMP snooping query interval is 60000 ms
        IGMP snooping query membership timeout is 300000 ms
        IGMP snooping group membership timeout is 400000 ms
```

```
Muticast Group Aging Information
Switch#show ip igmp snooping age-table group-membership
VLAN   Address              Port      Seconds
1      239.255.255.250     ge1/7     90000 ms

Query Aging Information
Switch#show ip igmp snooping age-table query-membership
VLAN   Address              Port      Seconds
```

```
Multicast Group Forwarding Information
Switch#show ip igmp snooping forwarding-table
VLAN Multicast Address Member-Ports
1      224.0.1.55           ge1/2(v2)
       239.192.152.143      ge1/2(v3)
       239.255.102.18       ge1/2(v3), ge1/5(v3)
       239.255.255.250      ge1/2(v3), ge1/5(v3)

Multicast IGMP Snooping Mroute Information
Switch#sh ip igmp snooping mrouter
Bridge 1:
 VLAN: 1   Igmp Snooping Enabled
 VLAN: 10   Igmp Snooping Enabled
     Mrouter -> ge1/3 (Configured)
 VLAN: 20   Igmp Snooping Enabled
```

12 GMRP Configuration

Currently, GMRP (GARP Multicast Registration Protocol, GARP Multicast Registration Protocol) is a multicast registration protocol based on GARP and is used to maintain multicast registration information on switches. Any switch supporting GMRP can receive multicast registration information from other switches, dynamically update local multicast registration information, and propagate local multicast registration information to other switches. This information exchange mechanism ensures the consistency of multicast information maintained by all GMRP-supporting devices in the same switching network.

To join a multicast group, a host sends a GMRP join message. The switch adds the port receiving the GMRP join message to the multicast group and broadcasts the GMRP join message on the VLAN where the receiving port resides, allowing multicast sources in the VLAN to be notified of the presence of multicast members. When a multicast source sends a multicast packet to a multicast group, the switch forwards the multicast packet only to ports associated with members of the multicast group, thereby achieving Layer 2 multicast within the VLAN.

12.1 GMRP Global Configuration

GMRP Global Configuration

Item	Description
Global GMRP	Select enable/disable GMRP function

■ GMRP Global Configuration in CLI

● GMRP Global Configuration

```
Enable GMRP globally
Switch(config)#set gmrp enable

Disable GMRP globally
Switch(config)#set gmrp disable

Apply GMRP to a specific VLAN
Switch(config)#set gmrp enable vlan <VLAN_ID>
Switch(config)#set gmrp enable vlan 10
```

Note: If you want to use GMRP functionality only on specific VLANs, the GMRP global configuration must be disabled.

● **Displaying GMRP Global Configuration**

```
Switch#show gmrp configuration
Global GMRP Configuration for bridge :1
GMRP Feature: Enabled

Port based GMRP Configuration:      Timers(centiseconds)
Port      GMRP Status    Registration    Forward All    Join    Leave    LeaveAll
------------------------------------------------------------------------------
ge1/1     Enabled        Normal          Disabled       10      30       500
```

12.2 GMRP Ports Configuration

GMRP is a protocol that dynamically manages multicast group membership and membership information. Using GMRP on a switch, a switch can forward multicast traffic only to the ports it needs. To use GMRP, a switch must configure GMRP on a port-by-port basis, which manages multicast group membership and membership on each port.

GMRP port configuration allows you to specify which ports will join or leave a multicast group. Typically, GMRP port configuration is performed on a VLAN basis, and the switch manages multicast group information.

GMRP Global Configuration

Item	Description
Selected Port	Select the port to which GMRP will be applied
GMRP Status	Select Enable/Disable GMRP on the port

■ GMRP Ports Configuration in CLI

● GMRP port configuration

```
Switch(config)#set port gmrp enable <IF_Name>

Switch(config)#set port gmrp enable ge1/1
```

● Display GMRP port configuration

```
Switch#show gmrp configuration
Global GMRP Configuration for bridge :1
GMRP Feature: Enabled

Port based GMRP Configuration:              Timers(centiseconds)
Port     GMRP Status    Registration    Forward All    Join    Leave    LeaveAll
------------------------------------------------------------------------------
ge1/1    Enabled        Normal          Disabled       20      60       1000
ge1/2    Enabled        Normal          Disabled       20      60       1000
...
```

```
Switch#show gmrp statistics vlanid <VLAN_ID>
Switch#show gmrp statistics vlanid 1
GMRP Statistics for bridge 1 vlan 1
-------------------------------------------------
Total GMRP packets Received:       556
Leave alls:                        276
Join Empties:                      0
Join Ins:                          0
Leave Empties:                     0
Leave Ins:                         0
Empties:                           280
```

```
Total GMRP packets Transmitted:    3356
Leave alls:                        3096
Join Empties:                       0
Join Ins:                          0
Leave Empties:                      0
Leave Ins:                          0
Empties:                            260
```

```
Switch#show gmrp statistics <IF_Name>
Switch# show gmrp timer ge1/1
Timer              Timer Value (centiseconds)
----------------------------------------
Join                    10
Leave                   30
Leave All               500
```

● GMRP Timer Configuration

```
set gmrp timer {join| leave |leaveall}<time-value> <IF_Name>

Joing Timer
Switch(config)#set gmrp timer join 10 ge1/1

Leave Timer
Switch(config)#set gmrp timer leave 30 ge1/1

Leaveall Timer
Switch(config)#set gmrp timer leaveall 500 ge1/1
```

12.3 GMRP State Machine

The GMRP State Machine defines the behavior of GMRP, representing the states that occur during GMRP's process of managing multicast group membership and membership. The GMRP State Machine tracks the state changes that occur when a port joins or leaves a multicast group, ensuring that network devices correctly forward multicast traffic.

■ GMRP State Machine in CLI

```
show gmrp statistics vlanid <VLAN_ID>

Switch#show gmrp statistics vlanid 1
GMRP Statistics for bridge 1 vlan 1
-------------------------------------------------
Total GMRP packets Received:       688
Leave alls:                        338
Join Empties:                      0
Join Ins:                          0
Leave Empties:                     0
Leave Ins:                         0
Empties:                           350

Total GMRP packets Transmitted:    4184
Leave alls:                        3864
Join Empties:                      0
Join Ins:                          0
Leave Empties:                     0
Leave Ins:                         0
Empties:                           320
```

13 GVRP Configuration

GVRP(GARP VLAN Registration Protocol) is an application of GARP(Generic Attribute Registration Protocol).

Allows the switch to dynamically create 802.1Q-compliant VLANs on links with other devices running GVRP and automatically create VLAN links between GVRP-aware devices. (GVRP links may include non-GVRP-aware intermediate devices.)

This action automatically provides VLAN ID (VID) consistency across the network, reducing the likelihood of VLAN configuration errors. After a switch creates a dynamic VLAN, you can convert it to a static VLAN using the CLI static <vlan-id> command. GVRP can also be used to dynamically activate port membership in a static VLAN configured on the switch.

GVRP advertises static VLANs using GVRP BPDUs(GVRP Bridge Protocol Data Units). These GVRP BPDUs are called advertisements. On a switch, advertisements are sent outbound from a port to devices directly connected to that port.

GVRP automatically creates and deletes VLANs, reducing management complexity and network configuration errors. However, because not all switches support GVRP, it can cause problems in mixed environments. It also propagates unnecessary VLAN information, requiring caution in security-sensitive environments.

13.1 GVRP Global Configuration

GVRP Global Configuration

Item	Description
Global GVRP	You can enable or disable the GVRP feature.

■ GVRP Global Configuration in CLI

● Enable GVRP

```
Switch(config)#set gvrp enable
```

● Display GVRP configuration

```
Switch#show running-config
!
set gvrp enable
!
```

13.2 GVRP Ports Configuration

Port Configuration

Item	Description
Selected Port	Selected port to enable/disable GVRP functionality
GVRP Status	GVRP feature enabled status
Port	Physical port
Join Timer	In GVRP, VLAN Join Request Transmission Cycle
Leave Timer	When a device leaves a specific VLAN, the delay is set to allow other devices to recognize the information and clear the VLAN configuration.
Leave All Timer	A timer configured to periodically display all VLAN information and automatically remove unnecessary VLAN information.

■ **GVRP Ports Configuration in CLI**

● **GVRP port configuration**

```
Enable GVRP
Switch(config)#set port gvrp enable <IF_Name>

Switch(config)#set port gvrp enable ge1/1

Disable GVRP
Switch(config)#set port gvrp disable <IF_Name>

Switch(config)#set port gvrp disable ge1/1
```

● **Display GVRP port configuration**

```
Switch#show running-config
!
set gvrp enable
set port gvrp enable ge1/1
set port gvrp enable ge1/2
set port gvrp enable ge1/3
set port gvrp enable ge1/4
…
!
Switch#show gvrp configuration
Global GVRP Configuration: Enabled
Dynamic Vlan Creation: Enabled
Port based GVRP Configuration:                    Timers(centiseconds)
Port      GVRP Status   Registration    Applicant    Join    Leave    LeaveAll
-----------------------------------------------------------------
ge1/1     Enabled       Normal          Normal       20      60       1000
ge1/2     Enabled       Normal          Normal       20      60       1000
ge1/3     Enabled       Normal          Normal       20      60       1000
ge1/4     Enabled       Normal          Normal       20      60       1000
```

● GVRP Timer Configuration

```
Join Timer configuration
Switch(config)#set gvrp timer join 40 <IF_Name>
Switch(config)#set gvrp timer join 40 ge1/1

Leave Timer configuration
Switch(config)#set gvrp timer leave 120  <IF_Name>
Switch(config)#set gvrp timer leave 120 ge1/1

Leave all Timer configuration
Switch(config)#set gvrp timer leaveall 2000  <IF_Name>
Switch(config)#set gvrp timer leaveall 2000 ge1/1
```

```
Display GVRP Timer Configuration
Switch#sh gvrp timer <IF_Name>

Switch#sh gvrp timer ge1/1
Timer              Timer Value (centiseconds)
----------------------------------------
Join                    40
Leave                   120
Leave All               2000
```

13.3 GVRP State Machine

GVRP (GARP VLAN Registration Protocol) allows ports or devices to display their status while managing VLAN information.

GVRP State Machine

Item	Description
Port Name	Ports with GVRP enabled
VLAN ID	VLAN ID of the port
Applicant State	This state indicates the state of a specific port while GVRP registers and manages VLAN information. ■ LO (Listening Only): The port only receives VLAN information and does not request VLAN membership. ■ VO (Very Anxious): The port immediately requests new VLAN membership and propagates VLAN information with high priority. ■ QA (Quiet): The port quietly maintains existing VLAN information and does not propagate new information
Registrar State	When GVRP manages VLAN information, this indicates the status of receiving and maintaining VLAN information within the network for a specific port. ■ MT (Mature): VLAN information has been successfully registered and is in a stable state, making the VLAN available for use within the network. ■ INR (In Registration): VLAN information is in the registration process but has not yet been completed.

■ GVRP State Machine in CLI

```
Switch#show gvrp machine
 Port     VLAN   Applicant State   Registrar State
 ------   ----   ---------------   ---------------
 ge1/1    1      LO                INR
 ge1/1    10     LO                MTF
 ge1/1    20     LO                MTF
 ge1/1    30     LO                MTF
 ge1/1    11     LO                MTF
 ge1/2    1      VO                INR
 ge1/3    1      VO                INR
 ge1/4    11     VO                INR
```

14 EAPS Configuration

Ethernet Automatic Protection Switching (EAPS) is a protocol that provides high availability and fast fault recovery in Ethernet ring-structured networks. EAPS is primarily used to prevent traffic looping in Ethernet rings and to provide a quick bypass path when the ring is broken. It creates a fault-tolerant topology by configuring primary and secondary paths for each VLAN. EAPS rings can operate on up to 16 rings.

Under normal conditions, the protection link is blocked to prevent loops, allowing traffic to flow normally through the ring. If a failure occurs in a specific section of the ring, the controller node detects the failure and activates the protection link to divert traffic in the opposite direction. Once the failure is resolved, the protection link is re-blocked, and traffic is restored to the original, normal path. While EAPS offers a rapid fault recovery time of less than 50ms, increasing network availability is advantageous. However, the configuration of controller nodes and protection links can be complex to manage, and performance can degrade as the number of devices increases. Therefore, it may not be suitable for larger networks.

14.1 EAPS Configuration

Create and configure EAPS information, delete EAPS information, and display configuration information.

Note: Before configuring an EAPS ring, you must first configure the VLAN configuration appropriate for your network environment. MSTP must be disabled.

EAPS Ring

Item	Description
EAPS Ring ID	A unique identifier (ID) used to identify the EAPS Ring. Select a Ring ID from 1-16 from the drop-down menu.
Create Status	Displays whether the EAPS Ring ID is enabled.
Primary Port	This port serves as the primary port for the master node to forward traffic in the EAPS Ring.
Secondary Port	A secondary port used by the Master Node in an EAPS Ring, serving as a bypass path in the event of a failure.

Mode	Defines the role of the device in the EAPS Ring network and determines how traffic within the ring is managed. ◆ Transit Mode: Manages the status of the entire EAPS Ring and initiates failover operations. It periodically monitors the status of the ring and, if a failure occurs, activates Protect Link to reroute traffic through a bypass path. Typically, a single master is required for an EAPS ring, which manages the entire ring. ◆ Transit Mode: This mode is configured by devices that act as general devices within the ring, rather than as masters. It follows the control of the transit device and supports the role of bypassing traffic during failover. The transit node can report the status of the ring to the transit node and, when a ring failure occurs, adjusts traffic flow according to the transit node's instructions.
Control VLAN	A VLAN used by switches within an EAPS domain to forward ERPS protocol messages, detect failures, and coordinate recovery operations.
Protected VLANs	A VLAN to which data traffic is transferred and protected by EAPS when a failure occurs on an EAPS ring network.
Hello Time Interval	The time it takes for each switch on an EAPS ring network to periodically exchange status messages (Hello Packets).
Fail Time:	The time it takes to detect and recover from a network failure on an EAPS ring network.
Data Span	The time interval at which data traffic can be transmitted and received through the Primary Port. This function is required to forward data to other rings when multiple rings are present.
Extreme Interoperability	Compatibility with Network Devices This function allows devices from various vendors to seamlessly perform automatic protection and failover within a single EAPS network
EAPS Status	Enable/Disable the EAPS Function ("Enable"/"Disable"): Enables or disables the creation of the selected EAPS Ring ID. If enabled, the Create Status will be "Created"; if disabled, it will be "Not Created."

■ EAPS Configuration in CLI

● EAPS Ring ID Configuration

```
Switch(config)#eaps create <EAPS Ring_ID>
Switch(config)#eaps create 1
```

● EAPS Ring Mode Configuration

```
Configuration as Master
Switch(config)#eaps mode <EAPS Ring_ID> master
Switch(config)#eaps mode 1 master

Configuration as Transit
Switch(config)#eaps mode <EAPS Ring_ID> transit
Switch(config)#eaps mode 1 transit
```

● EAPS Ring Primary Port configuration

```
Switch(config)#eaps primary-port <EAPS Ring_ID> <IF_Name>
Switch(config)#eaps primary-port 1 xe1/11
```

● EAPS Ring Secondary Port configuration

```
Switch(config)#eaps secondary-port <EAPS Ring_ID> <IF_Name>
Switch(config)#eaps secondary-port 1 xe1/12
```

● EAPS Ring Control VLAN configuration

```
Switch(config)#eaps control-vlan <EAPS Ring_ID><VLAN_ID>
Switch(config)#eaps control-vlan 1 30
```

● EAPS Ring Protected VLANs configuration

```
Switch(config)#eaps protected-vlan <EAPS Ring_ID><VLAN_ID>
Switch(config)#eaps protected-vlan 1 10
```

● EAPS Ring Hello Time Interval configuration

```
Switch(config)#eaps hello-time <EAPS Ring_ID><Hello-Time Interval>
Switch(config)#eaps hello-time 1 1
```

● EAPS Ring Fail Time configuration

```
Switch(config)#eaps fail-time <EAPS Ring_ID><Fail Time>
Switch(config)#eaps fail-time 1 3
```

● EAPS Ring Data Span configuration

```
Switch(config)#eaps data-span <EAPS Ring_ID>
Switch(config)#eaps data-span 1
```

● EAPS Ring Extreme Interoperability configuration

```
Switch(config)#eaps extreme-interoperability <EAPS Ring_ID>{enable ¦ disable}
Switch(config)#eaps extreme-interoperability 1 enable
Switch(config)#eaps extreme-interoperability 1 disable
```

● EAPS Ring EAPS Status configuration

```
Switch(config)#eaps {enable ¦ disable} <EAPS Ring_ID>
Switch(config)#eaps disable 1
Switch(config)#eaps disable 1
```

● Displaying EAPS rings in the CLI

```
Switch#show eaps <EAPS Ring_ID>
Switch#show eaps 1
%  EAPS Ring 1 - enable, Version 1, Mode - Master,  State - Complete.
%  Hello Time Interval              - 1 secs, Current - on.
%  Fail Time Age                    - 2 secs, Current - on.
%  Pre-forwarding Time Age          - 0 secs, Current - off.
%  Primary Port                     - ge1/9, State - Forwarding.
%  Secondary Port                   - ge1/10, State - Blocking.
%  Extreme interoperability admin - on, oper - on.
%  Data spanning with rings         - off.
%  Bridge Id                        - 24:72:60:F0:A3:58.
%  Control Vlan ID                  - 2.
%  Protected Vlan list              - 1.
%  Last LinkDown Bridge             - 00:28:24:13:5D:17.  2020/01/01 02:36:17
```

```
// EAPS Mode Master configuration
Switch#show running-config
EAPS
eaps create 1
eaps mode 1 Master
eaps primary-port 1 xe1/11
eaps secondary-port 1 xe1/12
eaps control-vlan 1 2
eaps protected-vlan 1 1
eaps hello-time 1 2
eaps fail-time 1 2
eaps enable 1

// EAPS Mode Transit configuration
Switch#show running-config
eaps create 1
eaps mode 1 Transit
eaps primary-port 1 xe1/11
eaps secondary-port 1 xe1/12
eaps control-vlan 1 2
eaps protected-vlan 1 1
eaps hello-time 1 2
eaps fail-time 1 2
eaps enable 1
```

14.2 EAPS Information

Displaying EAPS configuration information and operating status

■ EAPS Information in CLI

```
Switch#show eaps <EAPS Ring_ID>

Switch#show eaps 1
%  EAPS Ring 1 - enable, Version 1, Mode - Master,  State - Complete.
%  Hello Time Interval            - 1 secs, Current - on.
%  Fail Time Age                  - 2 secs, Current - on.
%  Pre-forwarding Time Age        - 0 secs, Current - off.
%  Primary Port                    - ge1/9, State - Forwarding.
%  Secondary Port                  - ge1/10, State - Blocking.
%  Extreme interoperability admin - on, oper - on.
%  Data spanning with rings        - off.
%  Bridge Id                       - 24:72:60:F0:A3:58.
%  Control Vlan ID                 - 2.
%  Protected Vlan list             - 1.
%  Last LinkDown Bridge            - 00:28:24:13:5D:17.  2020/01/01 02:36:17
```

15 RMON Configuration

RMON (The Remote Network Monitoring) is an extension of SNMP that allows for the analysis and monitoring of traffic from devices installed throughout a network. The RMON Management Information Base (MIB) is defined in RFC 1757 and describes the interaction between an SNMP management station and an RMON monitoring agent. Protocol analyzers and RMON probes enhance the monitoring capabilities of the RMON agent by collecting packet data from the monitored LAN. Probes send the collected data to an NMS device via SNMP. Additionally, NMS applications can process the collected data and display it in a complete report format.

15.1 Statistics Configuration

You can check the transmission and reception status of each port.
You can check data such as broadcast data, multicast data, and undersize data for the port.

Statistics Configuration

Item	Description
Port	Port to write statistics to
Index	A unique number that identifies each RMON Statistics Entry.
Owner	RMON Statistics Author
etherStatsDropEvents	Number of dropped events due to the device's inability to properly process packet
etherStatsOctets	Total number of bytes in all packets traversing the interface
etherStatsPkts	Total number of Ethernet frames received
etherStatsBroadcastPkts	Number of packets addressed to the broadcast MAC address
etherStatsMulticastPkts	Number of packets addressed to the multicast MAC address

etherStatsCRCAlignErrors	Number of frames with CRC or alignment errors
etherStatsUndersizePkts	Frames less than 64 bytes long but with a normal FCS
etherStatsOversizePkts	Frames longer than 1518 bytes (based on the standard MTU) and with a normal FCS
etherStatsFragments	Small frames less than 64 bytes with a broken FCS (= CRC)
etherStatsJabbers	Large frames greater than 1518 bytes with a broken FCS
etherStatsCollisions	Number of collisions in a half-duplex environment
etherStatsPkts64Octets	Frames of exactly 64 bytes
etherStatsPkts65to127Octets	Frames of 65 to 127 bytes
etherStatsPkts128to255Octets	Frames of 128 to 255 bytes
etherStatsPkts256to511Octets	Frames of 256 to 511 bytes Frames
etherStatsPkts512to1023Octets	512-1023 byte frames
etherStatsPkts1024to1518Octets	1024-1518 byte frames

■ Statistics Configuration in CLI

● RMON Statistics Configuration

```
Switch(config)#interface <IF_Name>
Switch(config-ge1/1)#rmon statistics <Index Num> owner <Owner>
    ▪ Index Num :  Statistics entry number
    ▪ Owner: Statistics Owner name

Switch(config)#int ge1/1
Switch(config-ge1/1)#rmon statistics 1 owner admin
```

● Displaying RMON statistics configuration

```
Switch#show rmon statistics config
RMON statistics configuration

Index              :1
DataSource         :2001
Owner               :admin
```

● Displaying RMON statistics

```
Switch#show rmon statistics-data interface <IN_Name>

Switch#show rmon statistics-data inter ge1/1
DropEvents                  :0
Octets                      :24557011
Pkts                        :148336
BroadcastPkts               :5436
MulticastPkts              :3353
CRCAlignErrors              :0
UndersizePkts               :0
OversizePkts                :0
Fragments                    :0
Jabbers                     :0
Collisions                 :0
Pkts64Octets                :90837
Pkts65to127Octets           :29232
Pkts128to255Octets          :11939
Pkts256to511Octets          :3386
Pkts512to1023Octets         :6830
Pkts1024to1518Octets        :6112
```

15.2 History Configuration

The RMON feature enables monitoring statistics per interface. The History page defines the sampling frequency, the number of samples to store, and the ports from which data will be collected. To configure RMON History on the switch, perform the following steps:

The table displays the History data collected since setup was successfully completed.

History Configuration

Item	Description
Port	Port to which RMON History will be applied.
Index	A unique ID that identifies a specific RMON History Entry.
Interval	The time interval (in seconds) for collecting each history bucket (sample)
Request bucket	The number of samples (buckets) stored in the history entry. When the bucket is full, the oldest entry is deleted and new data is stored.
Owner	History Entry Creator
Time Interval Start	The time (timestamp) when the sample (bucket) started. The starting point of the interval.
Drop Events	The number of packets dropped on the interface during the interval.
Octets	he total number of bytes passed during the interval (including FCS).
Broadcast Pkts	Number of broadcast frames received during the interval
Multicast Pkts	Number of multicast frames received during the interval
CRC Align Errors	CRC errors + alignment errors occurred during the interval
Undersize Pkts	Number of normal frames received less than 64 bytes + FCS during the interval

Oversize Pkts	Number of normal frames received more than 1518 bytes + FCS during the interval
Fragments	Length < 64 bytes + FCS error
Jabbers	Length > 1518 bytes + FCS error
Collisions	The number of frames received during the interval CSMA/CD Collision Count Occurred only in half-duplex mode
Utilization	Percentage of bandwidth used by the interface during the interval

■ History Configuration in CLI

● RMON History Configuration

```
Switch(config)#interface <IF_Name>
Switch(config-ge1/1)#rmon history <Index Num> buckets <buckets Number>
 interval <interval> owner <Owner>
      ■ Index Num :  History entry number
      ■ buckets Number :  History buckets number
      ■ interval: History sampling interval in seconds
      ■ Owner:History Owner name

Switch(config)#int ge1/1
Switch(config-ge1/1)#rmon history 1 buckets 20 interval 10 owner admin
```

● Displaying RMON History configuration

```
Switch#show rmon history-control config
RMON history control configuration

Index                    :1
DataSource               :2001
BucketsRequested         :20
Interval                 :10
Owner                    :admin
```

● Displaying RMON History-Data

```
Switch#show rmon history-data interface <IF_Name>

Switch#show rmon history-data interface ge1/1
Index                    :1
SampleIndex              :1
IntervalStart            :2020/01/01 13:11:02
DropEvents               :0
Octets                   :6343
Pkts                     :52
BroadcastPkts            :16
MulticastPkts            :0
CRCAlignErrors           :0
UndersizePkts            :0
OversizePkts             :0
Fragments                :0
Jabbers                  :0
Collisions               :0
Utilization              :0
```

15.3 Alarm Configuration

RMON alarm is one of the functions of RMON (Remote Network Monitoring), a network management protocol, and is a mechanism that automatically generates an alarm when a network device exceeds or falls below a specific performance threshold defined in advance by the administrator.

Alarm Configuration

Item	Description
Index	The unique identification number (ID) of the RMON Alarm entry.
Interval	The time interval (in seconds) at which the Alarm will periodically monitor.
Variable	The SNMP OID (specific RMON Statistics variable) monitored by the Alarm. This specifies which data to monitor.
Sample Type	This indicates the sampling method.
Alarm Value	The current value (or increment) calculated from the most recent interval sampling results.
Rising Threshold	A rising event occurs when the variable (or delta value) exceeds this value.
Falling Threshold	A falling event occurs when the variable falls below this value.
Rising Event Index	The index of the event entry to be executed when the rising threshold is reached.
Falling Event Index	The index of the event entry to be executed when the falling threshold is met.
Owner	The entity that created the alarm entry.

◎ Sample Type

- *Absolute (absolute value comparison):Compares the read value against the rising/falling threshold.*

→ If the cumulative counter increases and exceeds the threshold once, an event is continuously generated.

- *Delta (incremental value comparison) : Calculates the difference (increment) between the current sample value and the previous sample value and compares it to the threshold. Suitable for monitoring traffic growth and error growth.*

■ Alarm Configuration in CLI

● RMON Alarm Configuration

Switch(config)#rmon alarm *<Index> <Variable> <Interval> <Sample_type>*
rising-threshold *<rising-threshold > <Rising Event Index>*
falling-threshold *<falling-threshold> <Event Index>* owner *<Owner>*

<Index>: Alarm entry number
<Variable> : Alarm MIB variable
<Interval> : Sampling interval in seconds
<Sample_type>: absolute(Alarm by absolute value), delta(Alarm by delta value)
<rising-threshold> : Rising threshold value
<Rising Event Index> Event entry number by rising threshold
<falling-threshold> : Falling threshold value
<Falling Event Index> : Event entry number by falling threshold
<Event Index>: Event entry number by falling threshold
<Owner> : Set alarm owner

Switch(config)#rmon alarm 5 1.3.6.1.2.1.2.2.1.10 30 delta rising-threshold 1000 3
falling-threshold 10 1

15.4 Event Configuration

An RMON event is a notification or record generated when a critical situation, such as exceeding a certain threshold or an error, is detected on a network device using the RMON (Remote Network Monitoring) protocol. This is a key feature that helps network managers proactively identify and respond to network issues remotely.

Event Configuration

Item	Description
Index	A unique identification number (ID) for the RMON Event entry.
Description	A string (text) describing the purpose and content of the event.
Type	A behavioral method that determines how notifications are sent when an Event Alarm occurs.
Community	An SNMP Community String (SNMPv1/v2) used when sending SNMP Traps..
Last Time Sent	The timestamp of the last occurrence (transmission) of the Event.
Owner	The entity that generated the Event.

Type : This behavior determines how notifications are sent when an event triggers an alarm.

- log
  Logs only to the RMON Event Log Table (LCL log)
  Does not send SNMP Traps.
  Events can only be viewed locally.
- snmp-trap
  Sends a Trap message to the SNMP Manager.
  May not be logged in the Event Log Table (varies by device).
- log-and-trap
  Logs both Traps and local logs.
  Events are logged on both the management system and the device.

■ Event Configuration in CLI

● RMON Event Configuration

Switch(config)#rmon event *<Index Num>* *<Type>* *<Community>*
description *<description>* owner *<Owner>*

- *Index Num : RMON Event entry.*
- *<Type> : Action when an event occurs*
- *<Community> : SNMP Community String (SNMPv1/v2)*
- *<description> : string describing the purpose and content of the event.*
- *<Owner> : Owner name*

Switch(config)#rmon event 1 log-trap private description RMON_Event owner admin

● Displaying RMON Event configuration

```
Switch#show rmon event config
RMON event configuration
Index              :1
Description        :RMON Event
Type               :log-trap
Community          :private
Owner              :admin
```

16 Cluster Management

Provides the ability to request or provide information to discover, explore, detect changes/maintain surrounding (adjacent) nodes.

16.1 NDP Configuration

The Neighbor Discovery Protocol (NDP), or simply Neighbor Discovery (ND), is a protocol of the Internet protocol suite used with Internet Protocol Version 6 (IPv6).[1]: § 1 It operates at the internet layer of the Internet model, and is responsible for gathering various information required for network communication, including the configuration of local connections and the domain name servers and gateways.

The protocol defines five ICMPv6 packet types to perform functions for IPv6 similar to the Address Resolution Protocol (ARP) and Internet Control Message Protocol (ICMP) Router Discovery and Router Redirect protocols for IPv4. It provides many improvements over its IPv4 counterparts. For example, it includes Neighbor Unreachability Detection (NUD), thus improving robustness of packet delivery in the presence of failing routers or links, or mobile nodes.

The Inverse Neighbor Discovery (IND) protocol extension allows nodes to determine and advertise an IPv6 address corresponding to a given link-layer address, similar to Inverse ARP for IPv4.[3]

The Secure Neighbor Discovery Protocol (SEND), a security extension of NDP, uses Cryptographically Generated Addresses (CGA) and the Resource Public Key Infrastructure (RPKI) to provide an alternative mechanism for securing NDP with a cryptographic method that is independent of IPsec. Neighbor Discovery Proxy (ND Proxy) provides a service similar to IPv4 Proxy ARP and allows bridging multiple network segments within a single subnet prefix when bridging cannot be done at the link layer.

NDP Configuration

Item	Description
Port	Select the port on which you want to enable the NDP feature.
Port Enable	Select Enable/Disable the NDP feature for the selected port.
Global Enable	Select Enable/Disable the NDP feature globally.
Hello-time	Enter the retransmission interval for resending NS messages.
Aging-time	Enter the amount of time the host will keep the neighboring node in the “Reachable“ state.

■ NDP Configuration in CLI

● Global Enable/disalbe

- Enable

```
Switch(config)#ndp global enable
```

- Disable

```
Switch(config)#no ndp global enable
```

● aging-timer Configuration

```
Switch(config)#ndp aging-timer <time>

Switch(config)#ndp aging-timer 60
```

● hello-timer Configuration

```
Switch(config)#ndp  hello-timer <time>

Switch(config)#ndp  hello-timer 180
```

● Port Configuration

```
Switch(config)#interface <IF_Name>
Switch(config-ge1/1)#ndp enable

Switch(config)#interface ge1/1
Switch(config-ge1/1)#ndp enable
```

16.2 NTDP Configuration

The Neighbor Topology Discovery Protocol (NTDP) routing exchange is a protocol used to gather network topology information. NTDP collects topology information about switches within a specified number of hops, providing device information for clustered management. NDP provides neighbor table information to NTDP. Based on the neighbor information, NTDP sends and receives NTDP topology collection requests, collects NDP information for each device within a specified network range, and collects connection information for all neighboring devices.

After collecting this information, the management device or network administrator can use the information to complete any necessary functions. When the NDP on a member device detects a change in neighbors, it notifies the management device of the change via a handshake message. The management device can then initiate NTDP for a specified topology collection, allowing NTDP to immediately reflect any changes in the network topology. The Neighbor Discovery Protocol (NDP) is a protocol used to discover information about neighbors. Because NDP runs at the data link layer, it can support different network layer protocols. You can configure NTDP global settings. Information you can configure includes ports, port NTDP activation, global NDP activation, information collection scope, and information collection interval.

NTDP Configuration

Item	Description
Port	Select the port on which you want to enable the NTDP feature.
Port Enable	Select Enable/Disable the NTDP feature for the selected port.
Global Enable	Enables the NTDP protocol on all devices. This command initiates network topology collection.
Hops	This command manages the device distance in a multi-hop network by setting the maximum number of hops between neighboring devices.
Interval-time	This sets the interval for periodically checking the status of neighboring devices. This is the device status update cycle.
Hop-delay	This command sets the delay time that occurs during hop-to-hop communication. This command manages data transmission delays in multi-hop paths.
Port-delay	This command sets the delay time that occurs on a port. This command manages delays at the port level to improve data transmission efficiency.

■ NTDP Configuration in CLI

● Global Enable/disalbe

```
▪ Enable
Switch(config)#ntdp global enable

▪ Disable
Switch(config)#no ntdp global enable
```

● Hops Configuration

```
Switch(config)#ntdp hop <hops number?

Switch(config)#ntdp hop 3
```

● Interval timer Configuration

```
Switch(config)#ntdp timer <interval time>

Switch(config)#ntdp timer 1
```

● Hop-delay Configuration

```
Switch(config)#ntdp timer hop-delay <Hop-delay>

Switch(config)#ntdp timer hop-delay 200
```

● Port-delay Configuration

```
Switch(config)#ntdp timer port-delay <port-delay>

Switch(config)#ntdp timer port-delay 100 ?
```

● Port Configuration

```
Switch(config)#interface <IF_Name>
Switch(config-ge1/1)#ntdp enable

Switch(config)#interface ge1/1
Switch(config-ge1/1)#ntdp enable
```

16.3 Cluster Configuration

Network device clustering is a technology that achieves high availability and scalability by combining multiple network devices (switches, routers, firewalls, etc.) into a single logical system. Multiple devices function as a single virtual computer, sharing tasks and responding to failures.

If a device fails, another device within the cluster immediately takes over, preventing service interruptions.

Traffic loads can be distributed across multiple devices, overcoming the processing capacity limitations of a single device and efficiently managing large volumes of traffic.

Incoming requests and traffic are evenly distributed across multiple devices within the cluster, preventing load concentration on specific devices and optimizing overall performance.

Equipment replacement or maintenance can be performed without affecting operating services.

NTDP Configuration

Item	Description
Cluster Enable	Enables clustering functionality, allowing devices to operate as a single device.

Management-vlan	This is the VLAN through which the cluster's management traffic flows.
IP-Pool	This setting manages the IP addresses dynamically assigned to each device in the cluster. This setting is used when multiple devices are dynamically assigned IP addresses or when setting virtual IP addresses in a cluster environment.
Handshake time	This setting determines the time it takes for devices within the cluster to establish a connection.
Handshake hold-time	This setting determines the retry wait time after a connection failure.
Cluster Name	This setting identifies the cluster.
Type	This setting determines how clustering is configured.

■ Cluster Configuration in CLI

● Cluster Enable/Disable

```
▪ Enable
Switch(config)#cluster enable

▪ Disable
Switch(config)#no cluster enable
```

● Management-Vlan Configuration

```
Switch(config)#cluster management-vlan <Vlan_ID>

Switch(config)#cluster management-vlan 1
```

● IP-Pool Configuration

```
Switch(config)#cluster ip-pool <IP-Pool>
  IP-Pool format : A.B.C.D/M

Switch(config)#cluster ip-pool 192.168.10.0/24
```

● Handshake time Configuration

```
Switch(config)#cluster time <Handshake time>

Switch(config)#cluster ip-pool 192.168.10.0/24
```

● Handshake time Hole time configuration

```
Switch(config)#cluster holdtime <Hold-time>

Switch(config)#cluster holdtime 255
```

● Cluster Name configuration

```
 ■ Autobuild
Switch(config)#cluster autobuild <cluster name>
Switch(config)#cluster autobuild  Cluster-Auto

 ■ Manual Build
Switch(config)#cluster build <cluster name>
Switch(config)#cluster autobuild  Cluster-Manual
```

● Display Cluster

```
Switch#show cluster

Cluster name:Cluster-2
Role:Administrator
Management-vlan:100
Handshake timer:10 sec
Handshake hold-time:60 sec
IP-Pool:192.168.100.39/24
Cluster-mac:0180-c200-000a
0 member(s) in the cluster, and 0 of them down.
```

17 ERPS Configuration

Ethernet Ring Protection Switching (ERPS) is a protocol developed by the ITU-T based on the G.8032 recommendation to provide protection and recovery switching of less than 50 ms for Ethernet traffic in a ring topology while preventing loops from forming at the Ethernet layer. G.8032v1 supports single-ring topologies, while G.8032v2 supports multi-ring/ladder topologies. ERPS specifies protection switching mechanisms and protocols for Ethernet-layer network rings. Ethernet rings can provide wide-area multipoint connections more economically due to their reduced number of links. The mechanisms and protocols defined in this recommendation achieve highly reliable and robust protection, preventing loops from forming, which can have a detrimental impact on network operation and service availability. Each Ethernet ring node uses two independent links to connect to adjacent Ethernet ring nodes participating in the same Ethernet ring. A ring link is tied to two adjacent Ethernet ring nodes, and the ports for the ring links are called ring ports. The minimum number of Ethernet ring nodes in an Ethernet ring is three.

17.1 ERPS Configuration

ERPS Domain

Item	Description
ERPS Domain	Select an ERPS domain ID to create or delete an ERPS domain. Up to eight RPS domains can be configured.
ERPS Domain Status	ERPS domain creation status (Created or Not Created)
ERPS Domain Node Role	Select the ERPS domain role: interconnection 또는 none-interconnection
ERPS Ring	ERPS Ring Select the ERPS Ring ID you want to use from the drop-down list. The range is 1 to 32.
Ring Status	ERPS Ring Creation Status (Created or Not Created) When an ERPS Ring is created, the Ring Status changes from Not Created to Created.
Ring Mode	Select the Ring Mode (Major-Ring or Sub-Ring)
Node Mode	Select the Node Mode (rpl-owner-node, rpl-neighbor-node, ring-node)

Raps VLAN	The VLAN ID to which ERPS traffic will be transmitted. Range: 2-4094
Traffic VLAN	The VLAN ID to which data traffic will be transmitted. Range: 1-4094.
RPL Port	Select an RPL port. RPL (Ring Protection Link) – A link designated by a blocking mechanism during idle state to prevent loops in the switch ring.
RL Port	Select an RL port.
Revertive Behaviour	Select revertive or non-revertive.
Hold-off Time	When a failure occurs, the time to wait before resuming data transmission after the link is restored. Range: 0-10000, Unit: ms, Default: 0
Guard Time	When a failure occurs, all nodes use the time to change state to indicate whether the failure is actually ongoing. The Guard Time prevents old potential messages from causing unnecessary state changes. Default: 500, Input range: 10-2000ms.
WTR Time	Enter the WTR time. Default: 5, Input range: 1-12min.
WTB Time	The wait time before a link is restored after being blocked due to a failure. The WAIT-TO-BLOCK TIMER is used by the root node. This timer is used when the ring is restored from an operator command. When the WAIT-TO-BLOCK TIMER expires, the ring protection link is blocked. Default: 5. Input range: 1-10sec.
Raps-send Time	Rapse-send time. Default: 5. Range: 1-10 sec
ERPS Ring Enable	ERPS Ring Enable or Disable
Forced Switch RPL Port and RL Port	Configures a feature to force a specific port to switch. This feature forces a RPL port / RL port switch.
Manual Switch Port:	Blocks or unblocks the port.

◎ Ring Mode (Major-Ring or Sub-Ring)

- Major-Ring: An Ethernet ring that controls the entire physical ring and is connected to an interconnect node on two ports.
- Sub-Ring: An Ethernet ring connected to the main ring of an interconnect node. A sub-ring does not form a closed ring itself. A sub-ring is connected to an interconnect node on only one port.

◎ Node Mode (rpl-owner-node, rpl-neighbor-node, ring-node)

- rpl-owner-node: An ERPS ring has only one user-configured RPL owner port. Blocking the RPL owner port prevents loops in the ERPS ring. The node that owns the RPL owner port becomes the RPL owner node.
- rpl-neighbor-node: An ERPS ring has only one user-configured RPL neighbor port. This port must be connected to an RPL owner port. If the network is normal, it is blocked along with the RPL owner port to prevent loops in the ERPS ring. A node with an RPL Neighbor port becomes an RPL Neighbor node.
- Ring-node: A public port. Ports other than the RPL owner and adjacent ports are ring node ports. If a node only has common ports, it becomes a ring node.

◎ Raps VLAN: VLAN ID to which ERPS traffic will be forwarded.

Nodes in a ring coordinate the turning on and off of the Ring Protection Link (RPL) using control messages called Ring Automatic Protection Switching (R-APS) messages. After a node blocks a port facing a failed link, any failure along the ring triggers an R-APS Signaling Failure (R-APS SF) message in both directions to the nodes adjacent to the failed link. Upon receiving this message, the RPL owner unblocks the RPL port.

◎ Revertive Behavior

- Revertive: When a link fails, the RPL link is in the Disabled Protection state. After the failure is recovered, the RPL link transitions back to the Protected state to prevent loops.
- Non-revertive: After the failure is recovered, the failed node does not transition to the Forwarding state, and the RPL link remains in the Disabled Protection state.

■ ERPS Configuration in CLI

● Create ERPS Domain

```
Switch(config)#erps   <Domain_ID>
Switch(config)#erps   1
```

● Delete ERPS Domain

```
Switch(config)#no erps  <Domain_ID>
Switch(config)#no erps  1
```

● ERPS Domain None-interconnection configuration

```
Switch(config-erps)#node-role none-interconnection
```

● ERPS Domain interconnection configuration

```
Switch(config-erps)#node-role interconnection
```

● Displaying ERPS Domain Creation

```
Switch#show erps  <Domain_ID>
Switch#show erps 1
domain 1 information
instance: 1
node role: none interconnection
```

● Ring Configuration

```
Switch(config-erps)#ring <Ring_ID> <ERPS Ring Parameter>
                        <ERPS Ring Parameter_Value>
```

● Ring enable configuration

```
Switch(config-erps)#ring 1 enable
```

● Ring Mode configuration

```
Major Ring configuration
Switch(config-erps)#ring 1 ring-mode major-ring

Sub Ring configuration
Switch(config-erps)#ring 1 ring-mode sub-ring
```

● Node Mode configuration

```
RPL-Owner Node configuration
Switch(config-erps)#ring 1 node-mode rpl-owner-node

RPL-Neighbor-Node configuration
Switch(config-erps)#ring 1 node-mode rpl-neighbor-node

Ring-node configuration
Switch(config-erps)#ring 1 node-mode ring-node
```

● Ring Raps VLAN configuration

```
Switch(config-erps)#ring 1 raps-vlan 3001
```

● Ring Traffic VLAN configuration

```
Switch(config-erps)#ring 1 traffic-vlan 2,3
```

● Ring RPL Port configuration

```
Switch(config-erps)#ring 1 rpl-port ge1/11
```

● Ring RL Port configuration

```
Switch(config-erps)#ring 1 rl-port ge1/12
```

● Revertive-Behaviour configuration

```
Non-Revertive Configuration
Switch(config-erps)#ring 1 revertive-behaviour non-revertive

Revertive Configuration
Switch(config-erps)#ring 1 revertive-behaviour revertive
```

● Hold-off-Time configuration

```
Switch(config-erps)#ring 1 hold-off-time 100
```

● Guard-Time configuration

```
Switch(config-erps)#ring 1 guard-time 500
```

● WTR-Time configuration

```
Switch(config-erps)#ring 1 wtr-time 5
```

● WTB-Time configuration

```
Switch(config-erps)#ring 1 wtb-time 5
```

- RAPS-Send-Time configuration

```
Switch(config-erps)#ring 1 raps-send-time 5
```

- Forced Switch configuration

```
Switch(config-erps)#ring 1 forced-switch ge1/11
```

- Manual Switch configuration

```
Switch(config-erps)#ring 1 manual-switch ge1/10
```

17.2 ERPS Information

Displaying RPS configuration and operating status

■ ERPS Information in CLI

```
Switch#show erps <ERPS_ID>

Switch#show erps 1
domain 1 information
instance: 1
node role: none interconnection
 ring 1 information:
  ring mode: major ring
  node mode: rpl owner node
  rpl port: 2011
  rl port: 2012
  revertive behaviour: revertive
```

```
    hold off time: 0s, 0ms
    guard time: 0s, 500ms
    wtr time: 5min
    wtb time: 5s
    raps send time: 5s
    raps vlan: 3001
    traffic vlan list: 1
    enable state: enable
    node state: protection
    port list:
     ring port: xe1/12, port mode: rl port, port state: blocking
     ring port: xe1/11, port mode: rpl port, port state: forwarding
!
```

18 LLDP Configuration

LLDP (Link Layer Discovery Protocol) is a critical data link layer protocol that helps adjacent network devices exchange device information and automatically identify network conditions. LLDP uses the Type, Length, and Value attributes (called TLVs) to discover neighboring network devices.

LLDP significantly assists network administrators in efficiently understanding network configurations and resolving compatibility issues between devices. Because the protocol is standardized, it facilitates interoperability across various devices. Its high scalability makes it useful for exchanging a variety of information.

18.1 LLDP Global Configuration

LLDP Global Configuration

Item	Description
LLDP Global	LLDP Enable/Disable
Hold-multiplier <1-10>	LLDP PDU Validity Time: The value used to calculate the LLDP Time-to-Live (TTL) value.
Reinit-delay <1-10s>	The delay (in seconds) a device must wait before retransmitting LLDP information on the interface.
Tx-Delay <1-10s>	The delay (in seconds) for transmitting LLDP Protocol Data Units (PDUs).
Tx-interval <5-300s>	The frequency (in seconds) at which a device periodically transmits LDP Protocol Data Units (PDUs), which contain information about itself, to neighboring network devices. The minimum configuration must be at least four times the LLDP Tx-Delay value.

Note:

◎ Hold Time: Each LLDP PDU contains a Time to Live (TTL) or Hold Time value. This value indicates how long the device will keep the information in an LLDP PDU received from another device valid. By default, the device discards the information when the TTL expires and waits until a new LLDP PDU is received.

◎ Hold Multiplier: LLDP determines the Hold Time by configuring the Hold Multiplier value. Typically, the Hold Multiplier is configured as a multiple of the Time Interval (the frequency at which LLDP PDUs are transmitted).

■ LLDP Global Configuration in CLI

● Enable LLDP globally

```
Switch(config)#lldp global enable
```

● Disable LLDP globally

```
Switch(config)#no lldp global enable
```

● LLDP hold-multiplier configuration

```
Switch(config)#lldp hold-multiplier <Hold Multiplier_Value>
Switch(config)#lldp hold-multiplier 10
```

● LLDP reinit-delay configuration

```
Switch(config)#lldp timer reinit-delay <Reinit-Delay_Value>
Switch(config)#lldp timer reinit-delay 10
```

● LLDP tx-delay configuration

```
Switch(config)#lldp timer tx-delay <Tx-Delay_Value>
Switch(config)#lldp timer tx-delay 3
```

● LLDP tx-interval configuration

```
Switch(config)#lldp timer tx-interval<Tx-Interval_Value>
Switch(config)#lldp timer tx-interval 3
```

● Displaying LLDP Global Configuration

```
Switch#show running-config
!
lldp timer tx-interval 20
lldp timer tx-delay 3
lldp timer reinit-delay 5
lldp hold-multiplier 10
lldp global enable
!


Switch#show lldp configuration

LLDP global status: Enable
LLDP tx interval: 20
LLDP tx hold: 10
LLDP tx delay: 3
LLDP reinit delay: 5
```

18.2 LLDP Ports Configuration

LLDP Port Configuration

Item	Description
Selected Port	Ports to which LLDP will be applied
LLDP Status	Select whether to enable or disable the LLDP protocol on the physical port
Admin Status	Select whether to transmit (Tx) and receive (Rx) the LLDP protocol
Manage IP	Management Address TLV to be included in LLDP packets transmitted by the target switch port

Check Change Interval	Interval for transmitting LLDP advertisements on the port
DOT1-TLV	TLV (Type-Length-Value) type containing IEEE 802.1Q VLAN information
DOT3-TLV	TLV containing information about Ethernet characteristics
MED-TLV	Information related to Multimedia Educational Applications (MED)

- DOT1-TLV: DOT1-TLV is an extension of LLDP and represents a TLV (Type-Length-Value) type that includes IEEE 802.1Q VLAN information. It can automatically identify connection status, device type, port identifier, VLAN information, etc. between devices.
- DOT3-TLV: One of the LLDP TLVs, this TLV contains information about Ethernet characteristics. DOT3-TLV represents information related to IEEE 802.3 Ethernet connections and primarily provides details related to the physical link. It can include information such as the link status, speed, and duplex mode of the Ethernet connection.
- MED-TLV: Used to exchange information related to MED (Multimedia Educational Applications). LLDP MED is an extension of LLDP that helps optimize device-to-device interaction in network environments, particularly for multimedia applications such as VoIP (Voice over IP).

■ LLDP Ports Configuration in CLI

● Enable LLDP Port

```
Switch(config)#interface <IF_Name>
Switch(config)#interface ge1/1

Switch(config-ge1/1)#lldp enable
```

● Disable LLDP Port

```
Switch(config)#interface <IF_Name>
Switch(config)#interface ge1/1

Switch(config-ge1/1)#no lldp enable
```

● LLDP Port admin-status configuration

```
Switch(config)#interface <IF_Name>
Switch(config)#interface ge1/1

Switch(config-ge1/1)#lldp admin-status {disable ¦ rx ¦ rx ¦ txrx}
Switch(config-ge1/1)#lldp admin-status txrx
```

● LLDP Port Management-address configuration

```
Switch(config)#interface <IF_Name>
Switch(config)#interface ge1/1

Switch(config-ge1/1)#lldp management-address <Management Address>
Switch(config-ge1/1)#lldp management-address 192.168.192.100
```

● LLDP Port Check-change-Interval configuration

```
Switch(config)#interface <IF_Name>
Switch(config)#interface ge1/1

Switch(config-ge1/1)#lldp check-change-interval <Check-change-Interval>
Switch(config-ge1/1)#lldp check-change-interval 5
```

● Enable LLDP Port dot1-tlv, dot3-tlv, med-tlv

```
Switch(config)#interface <IF_Name>
Switch(config)#interface ge1/1

Switch(config-ge1/1)#lldp tlv-enable {dot1-tlv ¦ dot3-tlv ¦ med-tlv}
Switch(config-ge1/1)#lldp tlv-enable dot1-tlv
```

● Disable LLDP Port dot1-tlv, dot3-tlv, med-tlv

```
Switch(config)#interface <IF_Name>
Switch(config)#interface ge1/1

Switch(config-ge1/1)#no lldp tlv-enable {dot1-tlv ¦ dot3-tlv ¦ med-tlv}
Switch(config-ge1/1)#no lldp tlv-enable dot1-tlv
```

● Displaying LLDP Port Configuration

```
Switch#show lldp configuration <IF_Name>

Switch#show lldp configuration  ge1/1

LLDP global status: Enable
LLDP tx interval: 20
LLDP tx hold: 10
LLDP tx delay: 3
LLDP reinit delay: 5

Port ge1/1 Configuration:
LLDP status: Enable
Admin status: enabled RxTx
Check local change: Enable
Check local change interval: 5
Management address: 192.168.10.100
Dot1-tlv: Enable
Dot3-tlv: Enable
Med-tlv: Enable

Switch#show running-config
!
lldp timer tx-interval 20
lldp timer tx-delay 3
lldp timer reinit-delay 5
lldp hold-multiplier 10
lldp global enable
!
interface ge1/1
 qos apply-policy 10
 qos user-priority 3
 qos qosprofile qp0 weight 0
 qos qosprofile qp7 weight 100
 lldp management-address 192.168.10.100
 lldp check-change-interval 5
 poe high-power bt
!
```

18.3 LLDP Neighbor

LLDP Neighbor Table

Item	Description
Local Port	Port receiving the neighbor LLDP PDU
Device ID	Information transmitted in an LLDP PDU that identifies a specific component of the device. Typically, the device's hostname is used.
Chassis ID	An identifier that uniquely identifies the device. Transmitted in an LLDP PDU, this information typically uses the MAC address.
Port ID	Port connected to the neighbor device.
Manage IP	Management IP address transmitted by network devices to each other via LLDP.
VLAN	VLAN ID of the neighbor device.
TTL(S)	Time (in seconds) that the LLDP message remains valid on the network.
Capability	Information indicating the function or role provided by the device.

■ LLDP Neighbor in CLI

```
Switch#show lldp neighbor-information xe1/12

Local Port xe1/12:
Neighbor ID: 00 82 44 26 e7 82 78 65 31 2f 31 31
rxInfoTTL: 108
--Chassis ID TLV--:
  chassis ID subtype: MAC address(4); chassis ID: 00:82:44:26:e7:82
--Port ID TLV--:
  port ID subtype: Interface name(5); port ID: xe1/11
--Time To Live TLV--:
  time to live (TTL): 120
--Port Description TLV--:
  port description: xe1/11
```

```
--System Name TLV--:
  system name: Switch
--System Description TLV--:
  system description: Switch 6.5.1
--System Capabilities TLV--:
  system capabiltiies: Bridge (00 04); enabled capabilities: Bridge (00 04)
--Management Address TLV--:
  management address subtype: IPv4 address(1); management address:
192.168.10.100; interface numbering subtype: Unknown(1); interface number: 0; OID
string length: 0
--Port VLAN ID TLV--:
  port VLAN identifier (PVID): 1
--Port And Protocol VLAN ID TLV--:
  flags: Port and protocol VLAN not supported, Port and protocol VLAN not enabled;
port and protocol VLAN ID (PPVID): 0
--VLAN Name TLV--:
  VLAN ID (VID): 1;  VLAN name: vlan1
--MAC/PHY Configuration/Status TLV--:
  auto-neGTWaveiation support/status: Auto-neGTWaveiation supported,
Auto-neGTWaveiation enabled; PMD auto-neGTWaveiation advertised capability:
1000BASE-T full duplex mode(15); operational MAU type:
dot3MauType1000BaseTFD(30)
--Link Aggregation TLV--:
  Aggregation capability: capable of being aggregated;  Aggregation status: not
currently in aggregation;  aggregated port ID: 0
--Maximum Frame Size TLV--:
  maximum 802.3 frame size: 1522
--LLDP-MED Capabilities TLV--:
  LLDP-MED Capabilities: LLDP-MED Capabilities, Inventory(00 21);  LLDP-MED Device
Type: Network Connectivity(4)
--Hardware Revision TLV--:
  Hardware revision: 1.0.0
--Firmware Revision TLV--:
  Firmware revision: 6.5.1
--Software Revision TLV--:
  Software revision: 6.5.1
--Serial Number TLV--:
  Serial number: 02880000001
--Model Name TLV--:
  Model Name: Switch
```

19 Log Management

19.1 Log Configuration

Log

Item	Description
Syslog	When a log is generated, it is sent to a Syslog server. To send to a Syslog server, communication with the Syslog server must be possible.
First/Second Syslog Server IP	Enter the Syslog Server IP address.
Syslog UDP Port	Enter the port number to use in Syslog. (Default : 514)
Level	Select the lowest level to save or display in the log. Display or log levels higher than the selected level. - Error: Save or display error information and higher. - Warning: Save or display warning information and higher. - Informational: Save or display general information and higher. - Debugging: Save or display debug information and higher

■ **Log Configuration in CLI**

● Send logs to syslog server

```
Switch(config)#log syslog
Switch(config)#syslog open <syslog server IP address> <server udp port 1-65535>
Switch(config)#syslog source-interface <IF_Name>

ex)
Switch(config)#syslog open 192.168.10.1 514
Switch(config)#syslog source-interface ge1/1
```

Note: Source-interface is the port that the Syslog server is connected to.

19.2 Log Information

■ Log Information in CLI

```
show log <log level>
  - audit : Audit log,  debugging : Debugging log,  errors : Errors log,
    informational : Informational log,  warnings : Warnings

Switch#show log audit
2025/07/23 14:51:37 audit: IMI: Console user admin logins to this switch successfully.
2025/07/23 14:51:32 audit: IMI: Console user admin trys to login this switch,
 but entered incorrect username or password.
2025/07/23 14:39:39 audit: IMI: Console user admin logins to this switch successfully.
2025/07/23 14:39:35 audit: IMI: Console user trys to login this switch, but entered
incorrect username or password.
2025/07/23 14:26:26 audit: IMI: Console user admin logins to this switch successfully.
2025/07/23 14:21:04 audit: IMI: Web user admin logins to this switch successfully.
```

20 PoE

Power over Ethernet (PoE) is a networking feature defined by the IEEE 802.3af and 802.3at standards. PoE allows network devices to be powered via Ethernet cables over existing data connections. PoE-capable devices are either power sourcing equipment (PSEs) or powered devices (PDs), sometimes both. The device that supplies power is a PSE, and the device that receives power is a PD. Most PSEs are network switches or PoE injectors used with non-PoE switches. Common examples of PDs include VoIP phones, wireless access points, and IP cameras. Using a PoE switch, you can configure the use of PoE power, power supply method, and monitor power supply status.

20.1 PoE Port Configuration

You can configure the switch's total PoE power, single-port PoE power, and turn PoE devices on and off. You can also display the current status of each port.

The web user interfaces for models supporting IEEE 802.3af/at and models supporting IEEE 802.3af/at/bt differ slightly.

PoE Port Configuration

Item	Description
Selected Port(s)	The port that you want to configure PoE
PoE Mode	Select PoE power supply mode.
PoE Admin Status	Select whether to use PoE power supply.
Active Voltage (V)	The voltage currently being supplied by the PoE port.
Active PSE Type	The Active PSE Type indicates the PoE standard currently being used by this port.
PoE Power Type	Select whether PoE power supply is automatic or configured manually by the administrator.

PoE Protocol Type	This is the case when you configure Auto in the PoE power type. You can select AT or AF.
Port Max Power(W)	The maximum power(W) that can be supplied to the selected port's PoE device. This applies when the PoE power type is set to Manual. Enter the maximum power that can be supplied to the PoE device.
PoE Voltage(V):	Voltage supplied to the PoE device (V)
Total Power(W):	Maximum power supplied to the PoE device (W)
Power Consumption(W)	Current power supplied to the PoE device (W)
Power Usage(%):	Current PoE power usage (%)

■ Configuring a PoE Port in the CLI

● Configuring PoE Admin Status

- Enable Port PoE

```
Switch(config)#interface <IFNAME>
Switch(config-ge1/2)#poe enable

Switch(config)#interface ge1/2
Switch(config-ge1/2)#poe enable
```

- Disable Port PoE

```
Switch(config)#interface <IFNAME>
Switch(config-ge1/2)#no poe enable

Switch(config)#interface ge1/2
Switch(config-ge1/2)#no poe enable
```

● **PoE Power Type Configuration**

```
Switch(config)#interface <IFNAME>
Switch(config-ge1/2)##poe high-power {hipoe, bt}
Switch(config)#interface ge1/2
Switch(config-ge1/2)#poe high-power hipoe
```

● Port Max Power Configuration

```
Switch(config)#interface <IFNAME>
Switch(config-ge1/2)#poe max-power <MAX-POWER>
Switch(config)#interface ge1/2
Switch(config-ge1/2)#poe max-power 30
```

● PoE Total Power Configuration

```
Switch(config)#poe max-power <Total-Max-Power>
Switch(config)#poe max-power 370
```

● PoE Port Status Display

```
Switch#show poe

 Port    Status    Oper  48V-Type 24V-Type Curr(mA) Volt(V) Power(W) Class
------ -------- ------ -------- -------- -------- ------- -------- -----
 ge1/1   Enable     ON       AF      N/A       84   51.59     4.33     9
 ge1/2   Enable    OFF       BT      N/A      N/A     N/A      N/A     0
 ge1/3   Enable    OFF       AT      N/A      N/A     N/A      N/A     0
   .
   .
```

20.2 PoE Policy Configuration

Scheduling management allows you to enable or disable POE power supplies based on actual requirements. Control modes include time and week modes.

PoE Policy Configuration

Item	Description
PoE Port	Select the port for which you want to configure a PoE policy.
Policy Status	Select whether to enable PoE policy.

■ Configuring PoE Policy in CLI

● Enable PoE policy

```
Switch(config)#interface <IFNAME>
Switch(config-ge1/2)#poe policy enable

Switch(config)#interface ge1/2
Switch(config-ge1/2)#poe policy enable
```

● Disable PoE policy

```
Switch(config)#interface <IFNAME>
Switch(config-ge1/2)#no poe policy enable

Switch(config)#interface ge1/2
Switch(config-ge1/2)#no poe policy enable
```

● Configuring PoE policies

```
Switch(config)#interface <IFNAME>
Switch(config-ge1/2)#poe policy shutdown clock <clock> week-day <week>

Switch(config)#interface ge1/2
Switch(config-ge1/2)#poe policy shutdown clock 20-23 week-day 1-7
```

● Remove PoE policy

```
Switch(config)#interface <IFNAME>
Switch(config-ge1/2)#no poe policy shutdown clock <clock> week-day <week>

Switch(config)#interface ge1/2
Switch(config-ge1/2)#no poe policy shutdown clock 20-23 week-day 1-7
```

● Display PoE port policy

```
Switch#show poe policy <IFNAME>
Switch#show poe policy ge1/2
Policy Status: Enable
(S --- shutdown  - --- no shutdown)
Clock   Mon  Tues   Wed  Thur   Fri   Sat   Sun
-----  ----  ----  ----  ----  ----  ----  ----
    0     S     S     S     S     S     S     S
    1     S     S     S     S     S     S     S
    2     S     S     S     S     S     S     S
    3     -     -     -     -     -     -     -
    4     -     -     -     -     -     -     -
    .
    .
```

20.3 PD Query Configuration

Intelligent auto-recovery configuration allows you to restart PoE devices when abnormal behavior is detected.

PD Query Configuration

Item	Description
PoE Port	Select the port on which you want to use the PoE device query feature.
PD IP Address	Enter the IP address of the PoE device.
PD Query Interval	Enter the interval at which the PoE device queries are sent.
PD Timeout Number	Enter the number of failed responses from the PoE device.
PD Boot Time	Enter the wait time after PoE power is applied to the PoE device before sending the first query.
PD Reboot Times	The number of times the PoE device will restart.

■ Configuring PD Query in CLI

● PD IP Address Configuration

```
Switch(config)#interface <IF_NAME>
Switch(config-ge1/2)#poe pd-ip-address <IP Address>
  /* IP Address of the PD device connected to the selected interface

Switch(config)#interface ge1/2
Switch(config-ge1/2)#poe pd-ip-address 192.168.10.1
```

Note : The IP Address must be the IP address of the directly connected PD device.
Entering a different IP address may cause the system to repeatedly restart.

● PD Query Interval Configuration

```
Switch(config)#interface <IFNAME>
Switch(config-ge1/2)#poe pd-query-interval <pd-query-interval>

Switch(config)#interface ge1/2
Switch(config-ge1/2)#poe pd-query-interval 20
```

● PD Timeout Number configuration

```
Switch(config)#interface <IFNAME>
Switch(config-ge1/2)#poe pd-timeout-number <pd-timeout-number >

Switch(config)#interface ge1/2
Switch(config-ge1/2)#poe pd-timeout-number 10
```

● PD Boot Time Configuration

```
Switch(config)#interface <IFNAME>
Switch(config-ge1/2)#poe pd-boot-time <pd-boot-time>

Switch(config)#interface ge1/2
Switch(config-ge1/2)#poe pd-boot-time 300
```

● Displaying PD Query Configuration in CLI

```
Switch#show running-config
!
interface ge1/1
 poe pd-ip-address 192.168.10.1
 poe pd-query-interval 20
 poe pd-timeout-number 10
 poe pd-boot-time 300
!
```

21 Industrial Switch Monitoring

The system can be configured to monitor power and temperature, as well as ambient temperature and humidity. When temperature, humidity, or other values reach their threshold, the system can notify the administrator through alarms.

In addition, by connecting to the I/O interface, it can be configured to start or stop the HVAC (heating, ventilation, and air-conditioning) or environmental control equipment.

Note: The system monitoring feature is supported only on industrial switches that include monitoring capabilities.

Industry Monitoring

Item	Description
Ring Control & Ring Status	When using a physical ring, monitor the ring's status. Ring Control: Select whether to enable ring status monitoring. Ring Status: Displays the ring's inspection operation status
System Temperature (° C)	Displays the current system temperature.
System Temperature Upper(° C)	Configures the maximum temperature allowed by the system.
System Temperature Lower(° C)	Configures the minimum temperature allowed by the system.
Ambient Temperature (° C)	Displays the current ambient temperature.
Ambient Temperature Upper(° C)	Configures the maximum allowable ambient temperature.
Ambient Temperature Lower(° C)	Configures the minimum allowable ambient temperature.
Ambient Humidity (%)	Displays the current ambient humidity.
Ambient Humidity Upper	Configures the maximum allowable ambient humidity.
System Power Upper	Enters the maximum power available to the system.

Power Type	Support PoE
Power In (Master V1, Slave V2)	Displays the system's power input port.
System Current (A)	Displays the current current being used.
Master V1 Voltages (V)	Displays the voltage input to Master V1.
Slave V2 Voltages (V)	Displays the voltage input to Master V2.
System Power (W)	Displays the power being used by the system.
System 3.3V	Displays the input voltage status of the DC 3.3V power used by the system. Power error or no input: The system is not using the corresponding voltage or power is not being supplied. Normal: The power is being input normally.
System 1.5V	Displays the input voltage status of the DC 1.5V power used by the system. Power Error and No Input: The system does not use the corresponding voltage or power is not supplied. Normal: Power is being supplied normally.
System 1.2V	Power Error and No Input: The system is not using the corresponding voltage or power is not being supplied. Normal: Power is being supplied normally.
Alarm Detection Method	Configure the alarm detection type: Close, Low Level, High Level
Close Port	Select the port to close when an alarm is detected.
Reboot Port	Select the port to reboot when an alarm is detected.
Alarm Output Mode	Configure the output when an alarm occurs. Alarm Output Mode: Select the alarm output mode: Close, Alarm (Often Closed), Alarm (Often Open), Alarm Impulse
Port Failure	Select the port that will generate an alarm when an error occurs.
System Condition Failure	Select the system error type that will generate an alarm when a system error occurs.

■ Configure System monitoring in CLI

● System environment configuration

- System Temperature Upper configuration

```
industry max-system-temperature <1-100>
Switch(config)#industry max-system-temperature 70
```

- System Temperature Lower configuration

```
industry max-ambient-temperature <-60 - 100>
Switch(config)#industry min-system-temperature 0
```

- Ambient Temperature Upper configuration

```
industry max-ambient-temperature <-60-100>
Switch(config)#industry max-ambient-temperature 60
```

- Ambient Temperature Lower configuration

```
industry min-system-temperature <-60-100>
Switch(config)#industry min-ambient-temperature -10
```

- Ambient Humidity Upper configuration

```
industry max-ambient-humidity  <0-100>
Switch(config)#industry max-ambient-humidity 80
```

- System Power Upper configuration

```
industry max-power 370  <0-3000>
Switch(config)#industry max-power 370
```

● Configuring the alarm port input method

- Alarm Detection Method Configuration

```
industry in-alarm action [close-port ¦ high-level ¦ Low-level]
Switch(config)#industry in-alarm close
Switch(config)#industry in-alarm high-level
Switch(config)#industry in-alarm low-level
```

- Close Port Configuration

```
industry in-alarm action close-port IFNAME
Switch(config)#industry in-alarm action close-port ge1/1
```

- Reboot Port Configuration

```
industry in-alarm action reboot-port IFNAME
Switch(config)#industry in-alarm action reboot-port ge1/1
```

● Configuring the alarm port output method

- Alarm Output Mode Configuration

```
industry out-alarm-2 [close: impulse-level: low-open]
Switch(config)#industry out-alarm-2 close
Switch(config)#industry out-alarm-2 impulse-level
Switch(config)#industry out-alarm-2 low-open
```

- Port-Failure Configuration

```
industry out-alarm link-port IFNAME
Switch(config)#industry out-alarm link-port ge1/1

industry out-alarm poe-port IFNAME
Switch(config)#industry out-alarm poe-port ge1/1
```

- System Condition Failure Configuration

```
industry out-alarm alarm-input [System Condition]
Switch(config)#industry out-alarm system-temperature ?
Switch(config)#industry out-alarm ambient-temperature
Switch(config)#industry out-alarm ambient-humidity
Switch(config)#industry out-alarm system-power
Switch(config)#industry out-alarm master-v1-voltages
Switch(config)#industry out-alarm slave-v2-voltages
Switch(config)#industry out-alarm system-3p3v
Switch(config)#industry out-alarm system-1p5v
Switch(config)#industry out-alarm system-1p2v
Switch(config)#industry out-alarm close
Switch(config)#industry out-alarm high-open
Switch(config)#industry out-alarm low-open
Switch(config)#industry out-alarm impulse-level
```

- Upload Fault Message Configuration

```
Switch(config)#industry in-alarm upload-fault-message
Switch(config)#industry out-alarm upload-fault-message
```

Note) This feature also requires configuration of the Syslog server.

Ⅴ Troubleshooting

Issues	check
Device power issues	・ Check that the power cable is properly connected. ・ If a power switch is present, check that the switch is turned on and off. ・ Check that the source power is normal. ■ AC Input Switch Input Voltage: AC110~220V ■ Industrial Switch: DC12V (Network Only) DC48V (PoE Switch)
Device booting issues	・Power LED On/Off (Normal Operation: On) - If Off If power is supplied properly from the source -> Refer to the manufacturer for a power supply issue. - If On but not booting Check the Sys LED ・ SYS LED (Normal: Slow blinking after booting) - If the SYS LED remains On after powering on the device -> Refer to the manufacturer for a bootloader issue. - If the SYS LED continues to blink rapidly -> Refer to the manufacturer for a firmware error. *Note: After powering on, the system performs a hardware self-check (including the power supply, CPU, memory, flash, and TCAM). It then performs a kernel check and load, followed by a firmware integrity check and load.* *- If a problem occurs during the self-check, the device cannot proceed to the next step and the booting process will be halted.* *- If booting is successful, the PWR LED will be On and the SYS LED will blink slowly. If this LED status does not match, contact the manufacturer for inspection and repair.*

After system boot completes, data communication issues occur.	▪ Interface LED display Normal: On: No data traffic Blink: Data traffic ▪ If the network interface LED is off, Check if the device is properly connected to the switch. ▪ If the device and switch are properly connected, check the cable. ▪ If the cable is normal, Check the network interface of the connected device. ▪ If the network interface of the connected device is normal, Check if the port has been disabled by the system administrator. - Refer to the port section of the manual. ▪ If the port is enabled but communication is not possible, - If there is a port problem, contact the manufacturer for inspection and repair.
Management Access Service Connection Issues	① Console connection issue - Check the cable connection - If using USB-to-Serial, check the converter as well - Check the emulator configuration (COM port, baud rate, data bit, parity, stop bit) - Contact the manufacturer ② SSH/Telnet connection issue - Check the connection status between the computer and the switch - Check the IP address scheme of the computer and the switch - Check the emulator configuration - Check the administrator's activation status of related services - Check allowed and blocked IP addresses -> Contact the manufacturer ③ HTTPS/HTTP Connection Issues - Check the connection status between the computer and the switch - Check the IP address system of the computer and the switch - Check the web browser's normal operation - Check the administrator's activation status of related services - Check allowed and blocked IP addresses -> Contact the manufacturer