

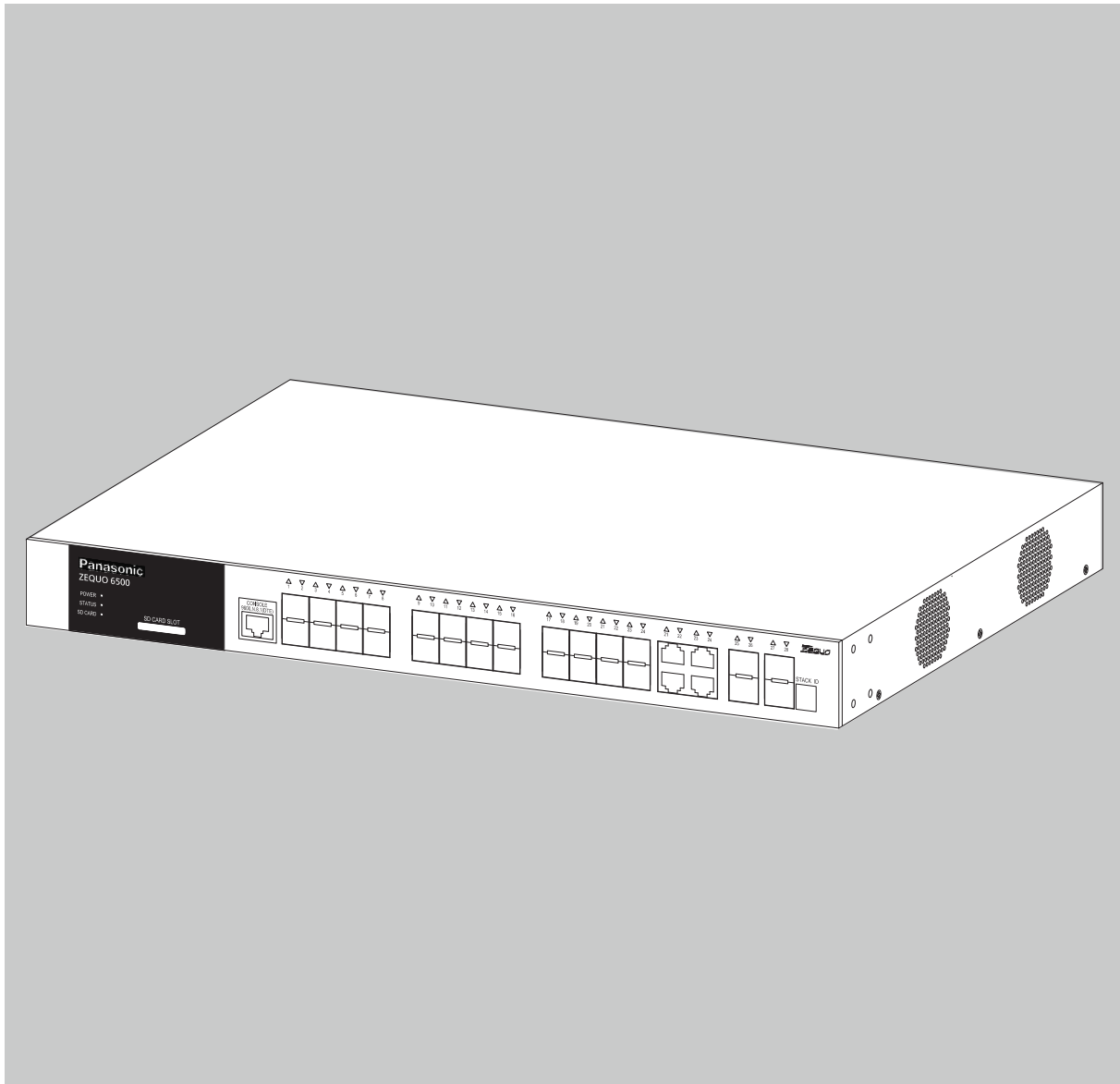


## **ZEQUO 6500**

### **Operating Instructions**

**Model Number: PN36242E**

- Thank you for purchasing our product.
- This manual provides important information about safe and proper operations of this Switching Hub.
- Please read "Important Safety Instructions" on pages 6 to 8 before use.
- Under all circumstances, customer disassembling of this Switching Hub voids the warranty.



The target model for this Operating Instruction is as follows.

| Model name | Model number | Firmware version |
|------------|--------------|------------------|
| ZEQUO 6500 | PN36242E-ID  | 1.0.1.34         |
|            | PN36242E-TH  |                  |
|            | PN36242E-MY  |                  |
|            | PN36242E-SG  |                  |

---

# Table of Contents

---

|                                                                       |     |
|-----------------------------------------------------------------------|-----|
| 1. Product Outline .....                                              | 11  |
| 2. Installation .....                                                 | 18  |
| 3. Connection .....                                                   | 19  |
| 4. Using Command Line Interface .....                                 | 23  |
| 5. Basic Management Commands .....                                    | 30  |
| 6. 802.1X Commands .....                                              | 54  |
| 7. Access Control List (ACL) Commands .....                           | 88  |
| 8. Access Control List (ACL) Egress Command List .....                | 117 |
| 9. ARP Commands .....                                                 | 143 |
| 10. Asymmetric VLAN Commands .....                                    | 150 |
| 11. Auto Configuration Commands .....                                 | 153 |
| 12. Basic IP Commands .....                                           | 156 |
| 13. Bootup Function Commands .....                                    | 171 |
| 14. BPDU Attack Protection Commands .....                             | 174 |
| 15. Cable Diagnostics Commands .....                                  | 180 |
| 16. Command List History Commands .....                               | 183 |
| 17. Command Logging Command List .....                                | 187 |
| 18. Network Access Authentication Command List .....                  | 191 |
| 19. Digital Diagnostic Monitoring (DDM) Commands .....                | 200 |
| 20. Debug Software Command List .....                                 | 218 |
| 21. DHCP Local Relay Commands .....                                   | 263 |
| 22. DHCP Relay Commands .....                                         | 268 |
| 23. DHCP Server Commands .....                                        | 287 |
| 24. DHCP Snooping Commands .....                                      | 310 |
| 25. DHCPv6 Relay Command List .....                                   | 315 |
| 26. DHCPv6 Server Commands .....                                      | 321 |
| 27. Distance Vector Multicast Routing Protocol (DVMRP) Commands ..... | 337 |
| 28. Domain Name System (DNS) Relay Commands .....                     | 345 |
| 29. DNS Resolver Commands .....                                       | 351 |
| 30. FDB Commands .....                                                | 359 |
| 31. File System Management Commands .....                             | 370 |
| 32. Filter Commands .....                                             | 382 |
| 33. Gratuitous ARP Commands .....                                     | 389 |
| 34. Internet Group Management Protocol (IGMP) Commands .....          | 396 |
| 35. IGMP Proxy Commands .....                                         | 405 |
| 36. IGMP Snooping Commands .....                                      | 411 |
| 37. IP Multicasting Commands .....                                    | 433 |
| 38. IP Routing Commands .....                                         | 436 |
| 39. IP Source Address Verify Commands .....                           | 446 |
| 40. IPv6 NDP Commands .....                                           | 460 |
| 41. Jumbo Frame Commands .....                                        | 469 |
| 42. LACP Configuration Commands .....                                 | 473 |
| 43. Layer 2 Protocol Tunneling (L2PT) Command List .....              | 476 |
| 44. Limited Multicast IP Address Commands .....                       | 481 |
| 45. Link Aggregation Commands .....                                   | 491 |

|                                                                            |      |
|----------------------------------------------------------------------------|------|
| 46. LLDP Commands .....                                                    | 497  |
| 47. Loopback Interface Commands .....                                      | 525  |
| 48. MAC Notification Commands .....                                        | 529  |
| 49. MAC-based Access Control Commands .....                                | 534  |
| 50. MD5 Commands .....                                                     | 556  |
| 51. Mirror Commands .....                                                  | 560  |
| 52. MLD Proxy Commands .....                                               | 567  |
| 53. MLD Snooping Commands .....                                            | 573  |
| 54. Login Banner and Prompt Commands .....                                 | 594  |
| 55. Multicast Listener Discovery (MLD) Commands .....                      | 595  |
| 56. Network Load Balancing (NLB) Commands .....                            | 601  |
| 57. Network Management Commands .....                                      | 605  |
| 58. Network Monitoring Commands .....                                      | 624  |
| 59. Open Shortest Path First (OSPF) Command List .....                     | 646  |
| 60. OSPFv3 Commands .....                                                  | 672  |
| 61. Packet Storm Commands .....                                            | 696  |
| 62. Protocol Independent Multicast (PIM) Commands .....                    | 702  |
| 63. PIM for IPv6 Command List .....                                        | 724  |
| 64. Policy Route Commands .....                                            | 747  |
| 65. Port Security Commands .....                                           | 751  |
| 66. Power Saving Commands .....                                            | 761  |
| 67. Precision Time Protocol (PTP) Commands .....                           | 764  |
| 68. Protocol VLAN Commands .....                                           | 785  |
| 69. QoS Commands .....                                                     | 792  |
| 70. Ring Redundant Protocol (RRP) Commands .....                           | 814  |
| 71. Routing Information Protocol (RIP) Command List .....                  | 824  |
| 72. RSPAN Commands .....                                                   | 830  |
| 73. SNMPv1/v2/v3 Commands .....                                            | 838  |
| 74. Spanning Tree Protocol (STP) commands .....                            | 859  |
| 75. SSH Commands .....                                                     | 876  |
| 76. Stacking Commands .....                                                | 886  |
| 77. Static MAC-based VLAN Commands .....                                   | 895  |
| 78. Subnet VLAN Commands .....                                             | 899  |
| 79. Switch Port Commands .....                                             | 906  |
| 80. System Severity Commands .....                                         | 912  |
| 81. Tech Support Commands .....                                            | 914  |
| 82. Time and SNTP Commands .....                                           | 917  |
| 83. Traffic Segmentation Commands .....                                    | 925  |
| 84. Utility Commands .....                                                 | 927  |
| 85. Virtual Router Redundancy Protocol (VRRP) Command List .....           | 956  |
| 86. Voice VLAN Commands .....                                              | 967  |
| 87. VLAN Commands .....                                                    | 978  |
| 88. VLAN Trunking Commands .....                                           | 996  |
| 89. Web-based Access Control (WAC) Commands .....                          | 1001 |
| 90. Weighted Random Early Detection (WRED) Commands .....                  | 1018 |
| 91. System Log Lists .....                                                 | 1026 |
| 92. Appendix A. Specifications .....                                       | 1052 |
| 93. Appendix B. Procedures for Configuration Using ZEQUO assist Plus ..... | 1056 |
| 94. Troubleshooting .....                                                  | 1057 |
| 95. Warranty and After-sales Service .....                                 | 1058 |



## Important Safety Instructions

This chapter contains important safety instructions for preventing bodily injury and/or property damage. You are required to follow them.

- Severity of bodily injury and/or property damage, which could result from incorrect use of the Switching Hub, are explained below.



**WARNING** This symbol indicates a potential hazard that could result in serious injury or death.



**CAUTION** This symbol indicates safety instructions. Deviation from these instructions could lead to bodily injury and/or property damage.

- The following symbols are used to classify and describe the type of instructions to be observed.



This symbol is used to alert users to what they must not do.



This symbol is used to alert users to what they must do.



**WARNING**



- Do not use power supply other than AC 100 - 240 V.  
Deviation could lead to fire, electric shock, and/or equipment failure.
- Do not handle the power cord with wet hand.  
Deviation could lead to electric shock, and/or equipment failure.
- Do not handle this Switching Hub and connection cables during a thunderstorm.  
Deviation could lead to electric shock.
- Do not disassemble and/or modify this Switching Hub.  
Deviation could lead to fire, electric shock, and/or equipment failure.
- Do not damage the power cord. Do not bend too tightly, stretch, twist, bundle with other cord, pinch, put under a heavy object, and/or heat it.  
A damaged power cord could lead to fire, short, and/or electric shock.
- Do not put foreign objects (such as metal or combustibles) into the opening (such as twisted pair port, console port, SFP extension slot, SFP+ extension slot, or SD card slot), and/or do not drop them into the inside of the Switching Hub.  
Deviation could lead to fire, electric shock, and/or equipment failure.

## **WARNING**



- **Do not connect equipments other than 10BASE-T/100BASE-TX/1000BASE-T to twisted pair port.**  
Deviation could lead to fire, electric shock, and/or equipment failure.
- **Do not place this Switching Hub in harsh environment such as near water, high humid, and/or high dust.**  
Deviation could lead to fire, electric shock, and/or equipment failure.
- **Do not place this Switching Hub under direct sun light and/or high temperature.**  
Deviation could lead to high internal temperature and fire.
- **Do not install this Switching Hub at the location with continuous vibration or strong shock, or at an unstable location.**  
Deviation could lead to injury and/or equipment failure.
- **Do not install any module other than our optional SFP modules (PN54021K/PN54023K) to SFP extension slot.**  
Deviation could lead to fire, electric shock, and/or equipment failure.
- **Do not install any module other than our optional SFP+ modules (PN59021/PN59023) and SFP modules (PN54021K/PN54023K) to SFP+ extension slot.**  
Deviation could lead to fire, electric shock, and/or equipment failure.
- **Do not install any module other than our optional SFP+ direct attach cable to stacking port.**  
Deviation could lead to fire, electric shock, and/or equipment failure.
- **Do not put this Switching Hub into fire.**  
Deviation could lead to explosion and/or fire.
- **Do not use the supplied power cord for anything other than this product.**  
Deviation could lead to fire, electric shock, and/or equipment failure.



## CAUTION



- **Use the bundled power cord (AC 100 - 240 V specifications).**  
Deviation could lead to electric shock, malfunction, and/or equipment failure.
- **Unplug the power cord in case of equipment failure.**  
Deviation, such as keeping connected for a long time, could lead to fire.
- **Connect this Switching Hub to ground.**  
Deviation could lead to electric shock, malfunction, and/or equipment failure.
- **Connect the power cord firmly to the power port.**  
Deviation could lead to electric shock, and/or malfunction.
- **Unplug the power plug if the STATUS LED blinks in orange (system fault).**  
Deviation, such as keeping connected for a long time, could lead to fire.
- **Handle the Switching Hub carefully so that fingers or hands may not be damaged by twisted pair ports, SFP/SFP+ extension slots, console port, SD card slot, or power cord hook block.**

## Basic Instructions for the Use of This Product

- For internal inspection and/or repair, please contact the shop.
- Use commercial power supply from a wall socket, which is close and easily accessible to this Switching Hub.
- Unplug the power cord when installing, moving, or cleaning this Switching Hub.
- Use this Switching Hub within the specifications. Deviation could lead to malfunctions.
- Do not touch the metal terminal of the RJ45 connector, the modular plug of connected twisted pair cable and serial port, or the metal terminal of the SFP/SFP+ extension slot. Do not place charged objects in the proximity of them. Static electricity could lead to equipment failure.
- Do not put the modular plug of the connected twisted pair cable on objects that can carry static charge, such as a carpet. Do not place it in the proximity. Static electricity could lead to equipment failure.
- Before connecting a console cable to the console port, discharge static electricity, for example by touching metal appliance (do not discharge by touching this Switching Hub).
- Do not put a strong shock, including dropping, to this Switching Hub. Deviation could lead to equipment failure.
- Do not store and/or use this Switching Hub in the environment with the characteristics listed below.  
(Store and/or use this Switching Hub in the environment in accordance with the specification.)
  - High humidity. Possible spilled liquid (water).
  - Dusty. Possible static charge (such as carpet).
  - Under direct sunlight.
  - Possible condensation. High/low temperature exceeding the environment specifications.
  - Strong vibration and/or strong shock.
- Please use this Switching Hub in place where ambient temperature is from 0 to 40 degrees C. Failure to meet the above conditions may result in fire, electric shock, breakdown, and/or malfunction. Please take notice because such cases are out of guarantee. Additionally, do not cover the bent hole of this Switching Hub. Deviation could lead to high internal temperature, equipment failure and/or malfunction.
- When stacking Switching Hubs, leave a minimum of 20 mm space between them.
- When connecting the stacks, be sure to use firmware versions that are identical for all of the devices. Please note that operations are not guaranteed if the firmware versions are different.
- Please note that operation will not be guaranteed if any SD card other than the separately sold Panasonic SD card is installed into the SD card slot. Format the card with this Switching Hub.

1. Panasonic will not be liable for any damage resulting from the operation not in accordance with this operation manual or loss of communications, which may or may not be caused by failure and/or malfunction of this product.
2. The contents described in this document may be changed without prior notice.

The latest version is available on our web site.

3. For any questions, please contact the shop where you purchased the product.

\* Brands and product names in this document are trademarks or registered trademarks of their respective holders.

---

# 1. Product Outline

---

ZEQUO 6500 is a Layer-3 All Gigabit Ethernet Switching Hub with management functions, equipped with 24 1000BASE-X SFP extension slots, four 10/100/1000BASE-T ports, and four 1000BASE-X/10GBASE-X extension slots.

## 1.1. Features

---

- Ports 1 to 24 (fiber ports) are SFP extension ports. Capable of 1 Gbps communications with SFP module.
- Ports 21 to 24 (copper ports) are 10BASE-T/100BASE-TX/1000BASE-T ports corresponding to auto negotiation. You can select either of 1000BASE-T supported copper port or SFP port for use.
- Ports 25 to 28 are SFP/SFP+ extension ports. Capable of 10 Gbps communications with SFP+ module.
- Ports 27 to 28 can also be used as stack ports.  
Up to four units of ZEQUO 6500 or ZEQUO6400 can be connected in a stack with SFP+ modules and optical fiber cables, or SFP+ direct attach cables.
- A SD card can be used to change and save configuration and firmware.
- All copper ports support the straight/cross cable via auto sensing function.  
You can simply connect devices with straight cables, whether the target is a terminal or a network device.
- The Power Saving Mode detects the connection status automatically and saves power consumption to minimum.
- The auto negotiation function is supported, allowing to easily support a heterogeneous environment of 10BASE-T, 100BASE-TX, and 1000BASE-T. The speed and communication mode can be set at Fixed.
- The Ping command can be used to verify communications.
- The standard MIB (MIB II, Bridge MIB, RMON four groups, etc.) is supported, allowing to manage the Switching Hub from the SNMP manager. (For details, refer to Appendix A.)
- The support application “ZEQUO assist Plus” supports GUI-based easy configuration for installation.
- RIP is supported, allowing to dynamically build a network.
- OSPF is supported, allowing for efficient routing even in a large-size network.
- PIM-SM/PIM-DM/PIM-SM-DM/PIM-SSM are supported, allowing for efficient multicast routing.

## 1. Product Outline

- Policy-based routing is supported, allowing for routing according to the access conditions.
- The Access Control function is supported, allowing to filter by IP address, MAC address, protocol number, and L4 port number.
- VRRP is supported, allowing for layer-3 Switching Hub redundancy.
- Spanning Tree Protocol is supported, allowing to build a redundant system.
- IEEE802.1Q tagged VLAN is supported, allowing to register up to 4094 VLANs.
- The IEEE802.1p QoS function is supported.
- The IEEE802.3ad Link Aggregation function is supported, allowing to configure up to 8 ports and 48 groups.
- The IEEE802.1X authentication function is supported, allowing to block network access from unregistered users.
- The IGMP Snooping function is supported, allowing to prevent multicast packets from monopolizing bandwidth.
- The Ring Redundant Protocol (RRP) is supported, allowing to make a redundant network via ring topology.

## 1.2. Accessories

Please be sure to confirm the contents. Please contact your distributor if any of the contents are insufficient.

- ZEQUO 6500 main unit.....1
- Installation Guide.....1
- CD-ROM (including this Operating Instructions).....1
- Mounting brackets (for 19-inch rack).....2
- Screws (for 19-inch rack).....4
- Screws (for fixing the main unit and the mounting bracket).....8
- SFP+ direct attach cable (OPSFPP-T01:1m).....1
- Rubber foot.....4
- Dummy SD card.....1
- Power cord (\*)......1

(\*) Just the PN36242E-TH has 1 Installation Guide in Thai (a total of 2 guides) .

[Power Code]

The following power cords are supplied as per the intended nation of delivery.

| Product Number | Locale    | Power Code Rating | FUSE Rated Current | Plug Type   |
|----------------|-----------|-------------------|--------------------|-------------|
| PN36242E-ID    | Indonesia | 250VAC 10A        | -                  | CEE7/7      |
| PN36242E-TH    | Thailand  | 250VAC 6A         | -                  | TIS166-2549 |
| PN36242E-MY    | Malasia   | 250VAC 10A        | 13A                | BS1363      |
| PN36242E-SG    | Singapore | 250VAC 5A         | 5A                 | BS1363      |

## 1.3. Optional Accessories

- PN54021K-XX                      1000BASE-SX SFP Module
- PN54023K-XX                      1000BASE-LX SFP Module
- PN59021-XX                        10GBASE-SR SFP+ Module
- PN59023-XX                        10GBASE-LR SFP+ Module

The XXs are identical to the intended nation of delivery codes.



## 1.4. Part Names and Functions

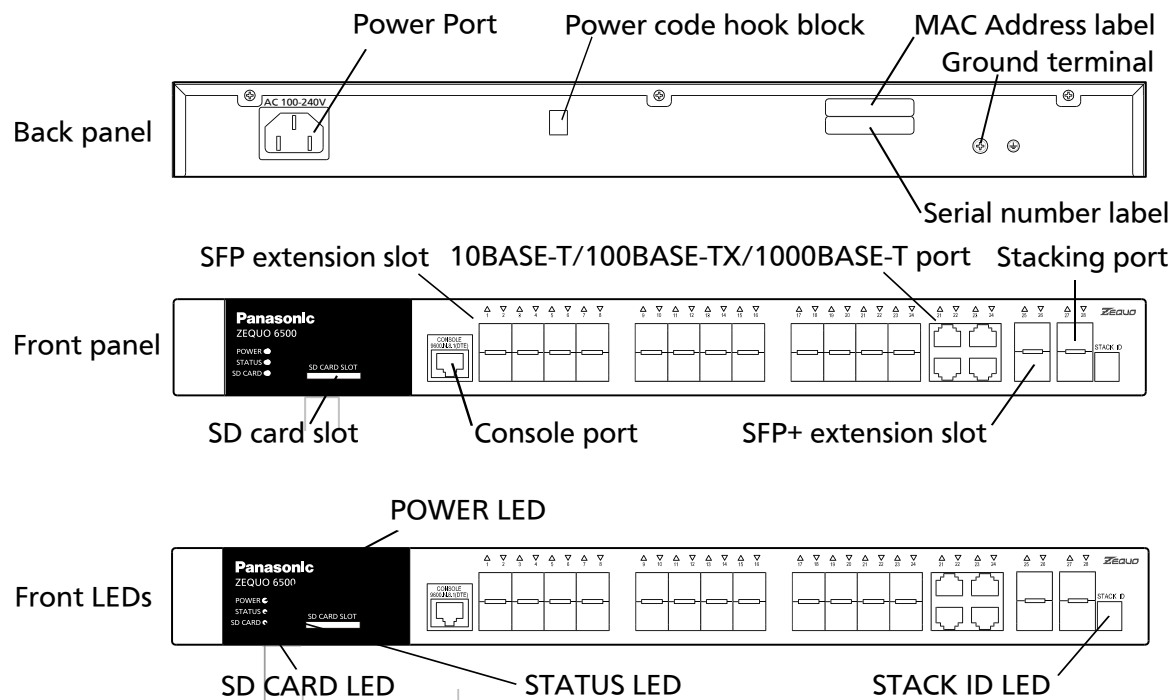


Fig. 1-1 Back, Front, LEDs

### ● Power port

Connect the supplied power cord into the port and connect the other end into an electric outlet.

### ● Power cord hook block

If the supplied power cord is hanged to this block, the cord becomes hard to pull out from the power port.

### ● Ground terminal

Only qualified Personnel should install minimum 18AWG green-and-yellow stranded copper wire to Ground terminal screw.

### ● SD card slot

Insert a SD card to change configuration information and change and save firm-ware.

● **SFP extension port (Ports 1 to 24)**

SFP module can be implemented. (ports 21-24 are exclusive usage with twisted pair ports.)

When SFP extension slot is linked, the port is automatically switched to fiber port mode. SFP port supports only the full-duplex mode.

● **10BASE-T/100BASE-TX/1000BASE-T port (Ports 21 to 24)**

Connect 10BASE-T/100BASE-TX/1000BASE-T terminals, hubs, repeaters, bridges, and switching hubs, etc.

Set the twisted-pair cable (CAT5e or higher) , connecting this Switching Hub and a device must be 100 m or shorter.

● **SFP+ extension port (Ports 25 to 28)**

An SFP or SFP+ module can be connected .

When the stacking function is enabled, port 27 and 28 become the stack-specific ports.

● **Stacking port (Ports 27 to 28)**

Up to four units can be stacked by connecting the SFP+ module and optical fiber cables, or SFP+ direct attach cables when the stacking function is enabled.

● **Console port**

Used to connect a VT100 compatible terminal to configure and manage this Switching Hub.

|                    |             |                         |          |
|--------------------|-------------|-------------------------|----------|
| Transmission mode  | : RS-232C   | Emulation mode          | : VT100  |
| Transmission speed | : 9,600 bps | Data length             | : 8 bits |
| Stop bit           | : 1 bit     | Parity control          | : None   |
| Flow control       | : None      | Communication connector | : RJ45   |

Use an RJ45-Dsub 9 pin console cable for connection.

## 1.5. LED Behavior

---

### 1.5.1. LED Behavior at Starting-up

When you turn on this Switching Hub, all LEDs are lit momentarily. POWER LED lights green and STATUS LED lights orange, and then the hardware self diagnosis is executed. Upon finishing the diagnosis, both POWER and STATUS LEDs light green.

### 1.5.2. LED Behavior while Operating

This Switching Hub has a set of LEDs for each port. These LEDs indicate the operation status of each port.

#### ● System LED

| LED          | Behavior                                    | Description                       |
|--------------|---------------------------------------------|-----------------------------------|
| POWER LED    | Green Light                                 | Power is ON                       |
|              | Off                                         | Power is OFF                      |
| STATUS LED   | Green Light                                 | The system is operating normally. |
|              | Orange Light                                | The system is starting up.        |
|              | Orange Blink                                | Malfunction<br>(Contact the shop) |
| SD CARD LED  | Green Light                                 | SD card is inserted               |
|              | Green Blink                                 | Accessing to SD card              |
|              | Orange Light                                | SD card error                     |
|              | Off                                         | Not inserted                      |
| STACK ID LED | "H" and STACK ID are displayed alternately. | Master device                     |
|              | "h" and STACK ID are displayed alternately. | Backup-master device              |
|              | STACK ID only                               | Slave device                      |

### ● SFP extension slot LED (Ports 1 to 24)

| LED       | Behavior    | Description                                             |
|-----------|-------------|---------------------------------------------------------|
| LINK/ACT. | Green Light | 1000Mbps link established at full-duplex.               |
|           | Green Blink | Transmitting/receiving packets at 1000Mbps full-duplex. |
|           | Off         | No device are connected.                                |

### ● 10/100/1000BASE-T port LED (Ports 21 to 24)

| LED       | Behavior     | Description                                             |
|-----------|--------------|---------------------------------------------------------|
| LINK/ACT. | Green Light  | 1000Mbps link established at full-duplex.               |
|           | Green Blink  | Transmitting/receiving packets at 1000Mbps full-duplex. |
|           | Orange Light | 10/100Mbps link are established.                        |
|           | Orange Blink | Transmitting/receiving packets at 10/100Mbps.           |
|           | Off          | No device are connected.                                |

### ● SFP+ extension slot LED (Ports 25 to 28)

| LED       | Behavior     | Description                                 |
|-----------|--------------|---------------------------------------------|
| LINK/ACT. | Green Light  | 10Gbps link established at full-duplex.     |
|           | Green Blink  | Transmitting packets at 10Gbps full-duplex. |
|           | Orange Light | 1000Mbps link are established.              |
|           | Orange Blink | Transmitting/receiving packets at 1000Mbps. |
|           | Off          | No device are connected.                    |

---

## 2. Installation

---

### 2.1. Installing in a 19-inch Rack

---

Take out two mount brackets and eight screws (for securing the mount brackets to the Switching Hub) from accessories, and secure a bracket to each of the right and left sides of the Switching Hub via four screw holes.

Then, by using four supplied screws (for 19-inch rack mount) or screws included with the rack, firmly mount the Switching Hub in the rack.

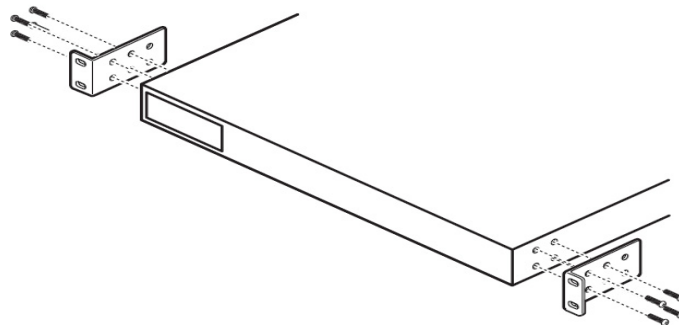


Fig. 2-1 Installing in 19-inch Rack

The main unit can be placed 20 mm back on the rack by changing the bracket fixing position.

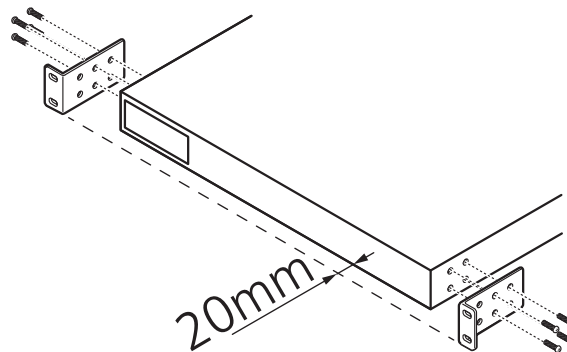


Fig. 2-2 Installing in 19-inch Rack (20 mm backward mounting)

## 3. Connection

### 3.1. Connecting a Copper Cable Port

#### ● Connection Cable

Use a CAT5e or higher compliant straight cable (copper cabling) with 8P8C RJ45 modular plugs.

#### ● Network Configuration

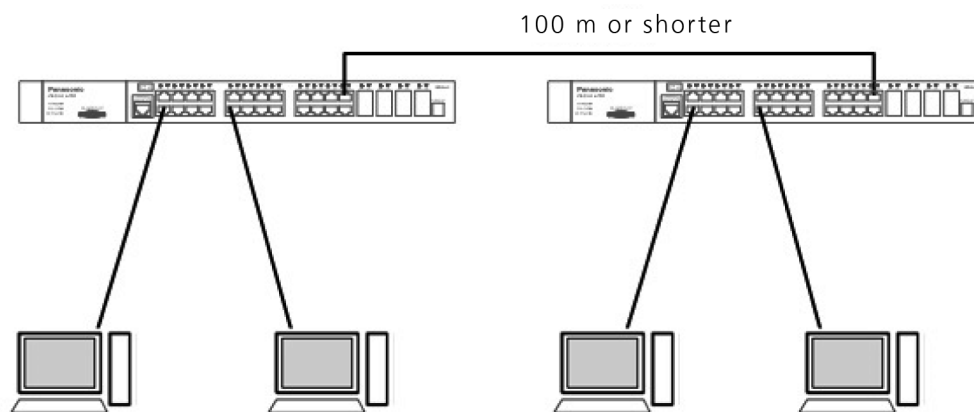


Fig. 3-1 Connection Configuration Example

The length of the cable connecting this Switching Hub and a device must be 100 m or shorter. When a terminal or a LAN device with auto negotiation function is connected to a port, the port is automatically configured to the most appropriate performance mode. When a terminal or a device without auto negotiation function is connected to a port, this Switching Hub automatically determines and sets the communication speed; however, the full-duplex/half-duplex configuration is set at half-duplex because the full-duplex/half-duplex capability cannot be determined. When connecting a terminal or a device without auto negotiation function, set the connection mode of the port to Fixed.

**Note:** If connection mode is set to a fixed value, Auto MDI/MDI-X function does not work. Therefore, you need to use a cross cable for connections between Switching Hubs.

## 3.2. Connecting with an SFP Extension Slot

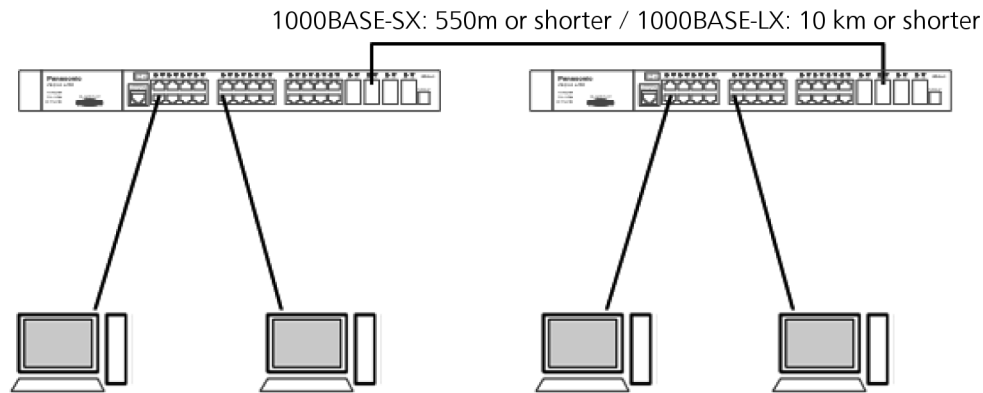


Fig. 3-2 Optical Fiber Cable Connection Example

Plugging an SFP module (optional) into an SFP extension slot enables an optical fiber connection. By factory default, the copper cable port is enabled, but the SFP extension port is automatically enabled when a link is established.

Connect this Switching Hub's TX port to the RX port of the connected device and this Switching Hub's RX port to the TX port of the connected device.

The following SFP modules are optionally available:

- 1000BASE-SX SFP module (Part number: PN54021K)
- 1000BASE-LX SFP module (Part number: PN54023K)

### 3.3. Connecting with an SFP+ Extension Slot

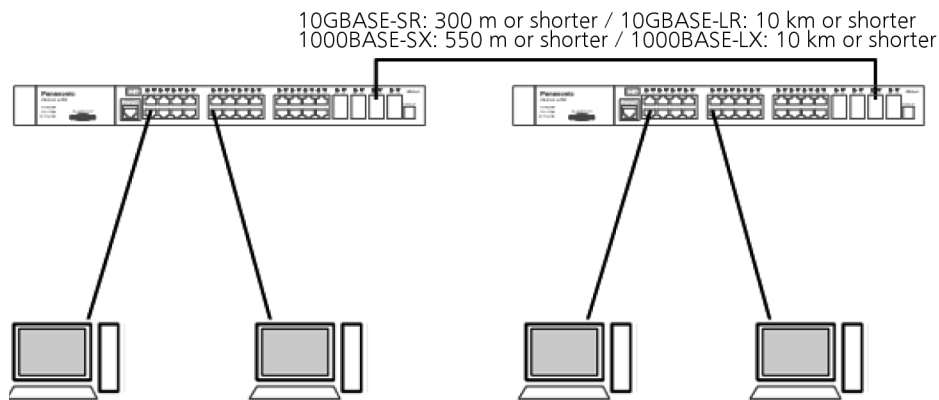


Fig. 3-3 Optical Fiber Cable Connection Example

Plugging an SFP/SFP+ module (optional) into an SFP+ extension slot enables an optical fiber connection.

Connect this Switching Hub's TX port to the RX port of the connected device and this Switching Hub's RX port to the TX port of the connected device.

The following SFP+ modules are optionally available:

- 10GBASE-SR SFP+ module (Part number: PN59021)
- 10GBASE-LR SFP+ module (Part number: PN59023)



## **3.4. Connecting to Power**

---

Connect the supplied power cord to the power port of this Switching Hub, and connect the power plug into an electric outlet. The Switching Hub operates at AC 100 - 240 V (50/60 Hz).

It does not have a power switch. When you connect the power plug, the Switching Hub turns on and starts operating. To power off, unplug the power plug from the electric outlet.

---

## 4. Using Command Line Interface

---

The Command Line Interface (CLI) is an operation screen to configure and manage this Switching Hub.

You can use the CLI by connecting a VT-100 compatible terminal to the serial port of this Switching Hub or through a remote connection such as telnet.

This chapter describes the following CLI procedures.

- Overview of connecting to the serial port
- How to configure the IP address of this Switching Hub
- Overview of how to use commands
  - "?" command, which displays the command help
  - Operations when parameters are omitted
  - Using command autocomplete function and input history
  - Operations when making a typo
- Syntax rules
- Available input editing keys and page operation keys

### 4.1. Accessing the Switch via the Serial Port

---

The Switch's serial port's default settings are as follows:

- 9600 baud
- no parity
- 8 data bits
- 1 stop bit

A computer running a terminal emulation program capable of emulating a VT-100 terminal and a serial port configured as above is then connected to the Switch's serial port via an RJ-45 to RS-232 DB-9 convertor cable.

With the serial port properly connected to a management computer, the following screen should be visible.

```
Zxxx0 Gigabit Ethernet Switch
Command Line Interface

Firmware: Build 1.0.x.xx

UserName:
```

## 4. Using Command Line Interface

There is no initial username or password. Just press the Enter key twice to display the CLI input cursor - **Zxxx0:admin#**. This is the command line where all commands are input.

### 4.2. Setting the Switch's IP Address

Each Switch must be assigned its own IP Address, which is used for communication with an SNMP network manager or other TCP/IP application (for example BOOTP, TFTP). The Switch's default IP address is 10.90.90.90. You can change the default Switch IP address to meet the specification of your networking address scheme.

The Switch is also assigned a unique MAC address by the factory. This MAC address cannot be changed, and can be found on the initial boot console screen - shown below or the command **show switch**.

```
Boot Procedure                                     V1.0.x.xx
-----
Power On Self Test ..... 100 %

MAC Address   : 00-01-02-03-04-00
H/W Version   : A1

Please Wait, Loading V1.0.0.xx Runtime Image ..... 100 %
UART init ..... 100 %
Starting runtime image
Device Discovery ..... 100 %
Configuration init ..... 100 %
```

The Switch's MAC address can also be found in the Web management program on the Device Information (Basic Settings) window on the Configuration menu.

The IP address for the Switch must be set before it can be managed with the Web-based manager. The Switch IP address can be automatically set using BOOTP or DHCP protocols, in which case the actual address assigned to the Switch must be known.

Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**. Where the x's represent the IP address to be assigned to the IP interface named **System** and the y's represent the corresponding subnet mask.

Alternatively, you can enter **config ipif System ipaddress xxx.xxx.xxx.xxx/z**. Where the x's represent the IP address to be assigned to the IP interface named **System** and the z represents the corresponding number of subnets in CIDR notation.

The IP interface named **System** on the Switch can be assigned an IP address and subnet mask which can then be used to connect a management station to the Switch's Telnet or Web-based management agent

```
Zxxx0:admin# config ipif System ipaddress 10.24.22.100/255.0.0.0
Command: config ipif System ipaddress 10.24.22.100/8

Success.

Zxxx0:admin#
```

## 4. Using Command Line Interface

In the above example, the Switch was assigned an IP address of 10.24.22.100 with a subnet mask of 255.0.0.0. The system message **Success** indicates that the command was executed successfully. The Switch can now be configured and managed via Telnet, SNMP MIB browser and the CLI or via the Web-based management agent using the above IP address to connect to the Switch.

There are a number of helpful features included in the CLI. Entering the ? command will display a list of all of the top-level commands.

```
Zxxx0:admin#?  
Command: ?  
  
..  
?  
cable_diag ports  
cd  
change drive  
clear  
clear address_binding dhcp_snoop binding_entry ports  
clear address_binding nd_snoop binding_entry ports  
clear arptable  
clear attack_log  
clear counters  
clear dhcp binding  
clear dhcp conflict_ip  
clear dhcpv6 binding  
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

When entering a command without its required parameters, the CLI will prompt you with a **Next possible completions:** message.

```
Zxxx0:admin#config account  
Command: config account  
Next possible completions:  
<username>  
  
Zxxx0:admin#
```

In this case, the command config account was entered with the parameter <username>. The CLI will then prompt to enter the <username> with the message, **Next possible completions:**. Every command in the CLI has this feature, and complex commands have several layers of parameter prompting.

In addition, after typing any given command plus one space, users can see all of the next possible sub-commands, in sequential order, by repeatedly pressing the **Tab** key.

To re-enter the previous command at the command prompt, press the up arrow cursor key. The previous command will appear at the command prompt.

```
Zxxx0:admin# config account  
Command: config account  
Next possible completions:  
<username>  
  
Zxxx0:admin# config account
```

## 4. Using Command Line Interface

In the above example, the command **config account** was entered without the required parameter **<username>**, the CLI returned the **Next possible completions: <username>** prompt. The up arrow cursor control key was pressed to re-enter the previous command (**config account**) at the command prompt. Now the appropriate username can be entered and the **config account** command re-executed.

All commands in the CLI function in this way. In addition, the syntax of the help prompts are the same as presented in this manual - angle brackets **< >** indicate a numerical value or character string, braces **{ }** indicate optional parameters or a choice of parameters, and brackets **[ ]** indicate required parameters.

If a command is entered that is unrecognized by the CLI, the top-level commands will be displayed under the **Available commands:** prompt.

```
Zxxx0:admin#the
Available commands:
..                ?                cable_diag        cd
                  change            clear             config
copy              create            debug            del
delete            dir              disable           download
enable            erase              format           login
logout            md                move             no
ping              ping6            rd               reboot
reconfig          rename           reset            save
show              telnet          traceroute       traceroute6
upload

Zxxx0:admin#
```

The top-level commands consist of commands such as **show** or **config**. Most of these commands require one or more parameters to narrow the top-level command. This is equivalent to **show** what? or **config** what? Where the what? is the next parameter. For example, entering the **show** command with no additional parameters, the CLI will then display all of the possible next parameters.

## 4. Using Command Line Interface

```
Zxxx0:admin#show
Command: show

Next possible completions:
802.1p          802.1x          access_profile  account
accounting      acct_client     address_binding
arpentry        asymmetric_vlan
attack_log      auth_client     auth_diagnostics
auth_session_statistics
authen_enable   authen_login    auth_statistics  authen
authorization    autoconfig     authen_policy
boot_file       bpdu_protection bandwidth_control
                command        broadcast_ping_reply
                command_history
community_encryption
current_config  ddm            device_status    dhcp
dhcp_local_relay dhcp_relay      dhcp_server      dhcpv6
dhcpv6_relay    dhcpv6_server  dnsr
dot1lv_protocol_group
dvmrp          ecmp           dscp
egress_flow_meter environment     egress_access_profile
                fdb                error
gratuitous_arp  greeting_message
host_name       igmp           filter            flow_meter
ip              ipfdb          gvrp              hol_prevention
ipif_ipv6_link_local_auto
iproute         ipv6           igmp_proxy        igmp_snooping
                l2protocol_tunnel
limited_multicast_addr
lldp_med        log            ipif              ipmc
log_software_module
mac_based_access_control
mac_based_vlan  mac_notification
mcast_filter_profile
mld             mld_proxy      ipv6route         jumbo_frame
multicast_fdb   name_server    lacp_port
ospfv3          nlb            link_aggregation  lldp
per_queue       pim            log_save_timing
policy_route    port           loopback
port_security_entry
power_saving    private_vlan   mac_based_access_control_local
                radius          max_mcast_group
router_ports    rmon           mirror
scheduling_mechanism
snmp            snmp           mld_snooping      multicast
stack_information
sub_vlan        subnet_vlan    nlb                ospf
syslog          system_severity
time            time_range     packet
traffic_segmentation
utilization     vlan           pim-ssm
vlan_trunk      voice_vlan     port_group         port_security
                vrrp           port_vlan          ports
                wac           ptp               pvid
                route_map
                session
                stack_device
                stp
                terminal
                trusted_host
                vlan_translation
                wac
```

## 4. Using Command Line Interface

In the above example, all of the possible next parameters for the **show** command are displayed. At the next command prompt, the up arrow was used to re-enter the **show** command, followed by the **account** parameter. The CLI then displays the user accounts configured on the Switch.

### 4.3. Command Syntax Symbols

The following symbols are used to describe how command entries are made and values and arguments are specified in this manual. The online help contained in the CLI and available through the console interface uses the same syntax.

**NOTE** All commands are case-sensitive. Be sure to disable Caps Lock or any other unwanted function that changes text case.

| Syntax                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| angle brackets < >                         | Encloses a variable or value. Users must specify the variable or value. For example, in the syntax<br><b>create ipif &lt;ipif_name 12&gt; {&lt;network_address&gt;} &lt;vlan_name 32&gt; {secondary   state [enable   disable]   proxy_arp [enable   disable] {local [enable   disable]}}</b><br>users must supply an IP interface name for <b>&lt;ipif_name 12&gt;</b> and a VLAN name for <b>&lt;vlan_name 32&gt;</b> when entering the command. DO NOT TYPE THE ANGLE BRACKETS. |
| square brackets [ ]                        | Encloses a required value or list of required arguments. Only one value or argument must be specified. For example, in the syntax<br><b>create account [admin   operator   power_user   user] &lt;username 15&gt; {encrypt [plain_text   sha_1] &lt;password&gt;}</b><br>users must specify either the admin-, operator-, power_user-level or user-level account when entering the command. DO NOT TYPE THE SQUARE BRACKETS.                                                       |
| vertical bar                               | Separates mutually exclusive items in a list. For example, in the syntax<br><b>reset {[config   system]} {force_agree}</b><br>users may choose config or system in the command. DO NOT TYPE THE VERTICAL BAR.                                                                                                                                                                                                                                                                      |
| braces { }                                 | Encloses an optional value or a list of optional arguments. One or more values or arguments can be specified. For example, in the syntax<br><b>config dhcp_relay {hops &lt;int 1-16&gt;   time &lt;sec 0-65535&gt;}(1)</b><br>users may choose config or system in the command. DO NOT TYPE THE BRACES.                                                                                                                                                                            |
| parentheses ( )                            | Indicates at least one or more of the values or arguments in the preceding syntax enclosed by braces must be specified. For example, in the syntax<br><b>config dhcp_relay {hops &lt;int 1-16&gt;   time &lt;sec 0-65535&gt;}(1)</b><br>users have the option to specify hops or time or both of them. The "(1)" following the set of braces indicates at least one argument or value within the braces must be specified. DO NOT TYPE THE PARENTHESES.                            |
| ipif <ipif_name 12><br>metric <value 1-31> | <b>12</b> means the maximum length of the IP interface name.<br><b>1-31</b> means the legal range of the metric value.                                                                                                                                                                                                                                                                                                                                                             |

## 4.4. Line Editing Keys

| Keys        | Description                                                                                                                                                                                                                                                                                     |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Delete      | Delete character under cursor and shift remainder of line to left.                                                                                                                                                                                                                              |
| Backspace   | Delete character to left of cursor and shift remainder of line to left.                                                                                                                                                                                                                         |
| Ctrl+R      | Toggle on and off. When toggled on, inserts text and shifts previous text to right.                                                                                                                                                                                                             |
| Up Arrow    | Repeats the previously entered command. Each time the up arrow is pressed, the command previous to that displayed appears. This way it is possible to review the command history for the current session. Use the down arrow to progress sequentially forward through the command history list. |
| Down Arrow  | The down arrow will display the next command in the command history entered in the current session. This displays each command sequentially as it was entered. Use the up arrow to review previous commands.                                                                                    |
| Left Arrow  | Move cursor to left.                                                                                                                                                                                                                                                                            |
| Right Arrow | Move cursor to right                                                                                                                                                                                                                                                                            |
| Tab         | Help user to select appropriate token.                                                                                                                                                                                                                                                          |

The screen display pauses when the show command output reaches the end of the page.

## 4.5. Multiple Page Display Control Keys

| Keys   | Description                                                                   |
|--------|-------------------------------------------------------------------------------|
| Space  | Displays the next page.                                                       |
| Ctrl+C | Stops the display of remaining pages when multiple pages are to be displayed. |
| Esc    | Stops the display of remaining pages when multiple pages are to be displayed. |
| n      | Displays the next page.                                                       |
| p      | Displays the previous page.                                                   |
| q      | Stops the display of remaining pages when multiple pages are to be displayed. |
| r      | Refreshes the pages currently displayed.                                      |
| a      | Displays the remaining pages without pausing between pages.                   |
| Enter  | Displays the next line or table entry.                                        |



---

## 5. Basic Management Commands

---

This chapter describes the basic management commands for this Switching Hub.

- Creating, editing, displaying, and deleting the accounts of users to manage this Switching Hub

---

**NOTE** Up to eight user accounts can be created.

---

- Encrypting the login password and configuration file
- Displaying users who are currently logged in to the console
- Displaying and managing the status of power, temperature, and fan on this Switching Hub
- Configuring the serial port (serial port) setting
- Pausing the screen page feed, configuring the terminal width, and clearing the screen
- Using Telnet
- Saving configuration and log files to NV-RAM
- Resetting and rebooting
- Logging in and logging out

---

```
create account [admin | operator | power_user | user] <username 15> {encrypt [plain_text |
    sha_1] <password>}
enable password encryption
disable password encryption
config account <username> {encrypt [plain_text | sha_1] <password>}
show account
delete account <username>
show session
show switch
show environment
config temperature [trap | log] state [enable | disable]
config temperature threshold {high <temperature -500-500> | low <temperature -500-500>}(1)
show serial_port
config serial_port {baud_rate [9600 | 19200 | 38400 | 115200] | auto_logout [never |
    2_minutes | 5_minutes | 10_minutes | 15_minutes]}(1)
enable clipaging
disable clipaging
enable telnet {<tcp_port_number 1-65535>}
disable telnet
save {[config <pathname> | log | all]}
reboot {force_agree}
reset {[config | system]} {force_agree}
login
logout
```

---

---

```
clear
config terminal width [default | <value 80-200>]
show terminal width
show device_status
```

---

## 5.1. create account

---

### ● Description

This command creates user accounts. The username is between 1 and 15 characters, the password is between 0 and 15 characters. The number of accounts (including admin, operator, and user) is up to eight.

### ● Format

```
create account [admin | operator | power_user | user] <username 15> {encrypt
[plain_text | sha_1] <password>}
```

### ● Parameters

---

**admin** Specify the name of the admin account.

---

**operator** Specify the name of the operator account.

---

**power\_user**

Specify a power user level account. The power user level is lower than the operator level and higher than the user level.

---

**user** Specify the name of the user account.

---

**<username 15>**

Specify a username of up to 15 characters.

---

**encrypt** Specifies the encryption used.

**plain\_text**

Specify the password in plain text form.

**sha\_1** Specify the password in SHA-1 encrypted form.

**<password>**

The password for the user account. The length of a password in plain-text form and encrypted form are different. For a plain-text form password, the password must be a minimum of 0 characters and a maximum of 15 characters. For an encrypted form password, the length is fixed to 35 bytes long. The password is case-sensitive.

---

### ● Restrictions

Only Administrator-level users can issue this command.

## 5. Basic Management Commands

### ● Example

To create the Administrator-level user "panasonic":

```
Zxxx0:admin#create account admin manager
Command: create account admin manager

Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success.

Zxxx0:admin#
```

To create the Operator-level user "Sales":

```
Zxxx0:admin##create account operator Sales
Command: create account operator Sales

Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success.

Zxxx0:admin#
```

To create the User-level user "System":

```
Zxxx0:admin##create account user System
Command: create account user System

Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success.

Zxxx0:admin#
```

## 5.2. enable password encryption

---

### ● Description

The user account configuration information will be stored in the configuration file, and can be applied to the system later. If the password encryption is enabled, the password will be in encrypted form when it is stored in the configuration file. When password encryption is disabled, the password will be in plain text form when it is stored in the configuration file. However, if the created user account directly uses the encrypted password, the password will still be in the encrypted form.

### ● Format

enable password encryption

### ● Parameters

None.

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To enable password encryption:

```
Zxxx0:admin#enable password encryption
Command: enable password encryption

Success.

Zxxx0:admin#
```

## 5.3. disable password encryption

---

### ● Description

The user account configuration information will be stored in the configuration file, and can be applied to the system later. If the password encryption is enabled, the password will be in encrypted form when it is stored in the configuration file. When password encryption is disabled, the password will be in plain text form when it is stored in the configuration file. However, if the created user account directly uses the encrypted password, the password will still be in the encrypted form.

### ● Format

disable password encryption

### ● Parameters

None.

### ● Restrictions

Only Administrator-level users can issue this command.

## 5. Basic Management Commands

### ● Example

To disable password encryption:

```
Zxxx0:admin#disable password encryption
Command: disable password encryption

Success.

Zxxx0:admin#
```

## 5.4. config account

---

### ● Description

When the password information is not specified in the command, the system will prompt the user to input the password interactively. For this case, the user can only input the plain text password. If the password is present in the command, the user can select to input the password in the plain text form or in the encrypted form. The encryption algorithm is based on SHA-1.

### ● Format

**config account <username> {encrypt [plain\_text | sha\_1] <password>}**

### ● Parameters

---

**<username>**

Specify the name of the account. The account must already be defined.

---

**encrypt** (Optional) Specify the encryption type, plain\_text or sha\_1.

**plain\_text**

Specify the password in plain text form. For the plain text form, passwords must have a minimum of 0 and a maximum of 15 characters. The password is case-sensitive

**sha\_1** Specify the password in the SHA-1 encrypted form. For the encrypted form password, the length is fixed to 35 bytes long. The password is case-sensitive.

---

**<password>**

Specify the password.

---

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To configure the user password of the "panasonic" account:

```
Zxxx0:admin#config account manager
Command: config account manager

Enter a old password:****
Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success.

Zxxx0:admin#
```

To configure the user password of the "administrator" account:

```
Zxxx0:admin#config account administrator encrypt sha_1
*@&NWozK3kTsExUV00Ywo1G5jlUKKv+toYg
Command: config account administrator encrypt sha_1
*@&NWozK3kTsExUV00Ywo1G5jlUKKv+toYg
Success.

Zxxx0:admin#
```

## 5.5. show account

---

### ● Description

This command is used to display user accounts that have been created.

### ● Format

**show account**

### ● Parameters

None.

### ● Restrictions

Only Administrator-level users can issue this command.

## 5. Basic Management Commands

### ● Example

To display accounts that have been created:

```
Zxxx0:admin#show account
Command: show account

Current Accounts:
Username          Access Level
-----
System            User
Sales             Operator
manager           Admin

Zxxx0:admin#
```

## 5.6. delete account

---

### ● Description

This command is used to delete an existing account.

### ● Format

**delete account <username>**

### ● Parameters

---

**<username>**  
Specify the name of the user who will be deleted.

---

### ● Restrictions

Only Administrator-level users can issue this command. One active admin user must exist.

### ● Example

To delete the user account "System":

```
Zxxx0:admin#delete account System
Command: delete account System

Success.

Zxxx0:admin#
```

## 5.7. show session

---

### ● Description

This command is used to display a list of current users which are logged in to CLI sessions.

### ● Format

show session

### ● Parameters

None.

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To display accounts a list of currently logged-in users:

```
Zxxx0:admin#show session
Command: show session

ID   Live Time      From           Level   User
--   -
8    23:37:42.270   Serial Port    admin   Anonymous

Total Entries: 1

CTRL+C  ESC  q  Quit  SPACE  n  Next Page  p  Previous Page  r  Refresh
```

## 5.8. show switch

---

### ● Description

This command is used to display the Switching Hub information.

### ● Format

show switch

### ● Parameters

None.



## 5. Basic Management Commands

### ● Restrictions

None.

### ● Example

To display the Switching Hub information:

```
Zxxx0:admin#show switch
Command: show switch

Device Type           : Zxxx0 Gigabit Ethernet Switch
MAC Address           : 00-01-02-03-04-00
IP Address             : 10.90.90.90 (Manual)
VLAN Name              : default
Subnet Mask            : 255.0.0.0
Default Gateway        : 0.0.0.0
Boot PROM Version     : Build 1.0.x.xx
Firmware Version       : Build 1.0.x.xx
Hardware Version       : A1
Serial Number          :
System Name            :
System Location        :
System Uptime          : 0 days, 0 hours, 38 minutes, 12 seconds
System Contact         :
Spanning Tree          : Disabled
GVRP                   : Disabled
IGMP Snooping          : Disabled
MLD Snooping           : Disabled
RIP                    : Disabled
DVMRP                  : Disabled
PIM                    : Disabled
OSPF                   : Disabled
OSPFv3                 : Disabled
VLAN Trunk             : Disabled
Telnet                 : Enabled (TCP 23)
SNMP                   : Disabled
SSH Status             : Disabled
802.1X                 : Disabled
Jumbo Frame           : Off
CLI Paging             : Enabled
MAC Notification       : Disabled
Port Mirror            : Disabled
SNTP                   : Disabled
DHCP Relay             : Disabled
DNSR Status            : Disabled
VRRP                   : Disabled
HOL Prevention State   : Enabled
Syslog Global State    : Disabled
Single IP Management   : Disabled
Password Encryption Status : Disabled
DNS Resolver           : Disabled

Zxxx0:admin#
```

## 5.9. show environment

---

- Description

This command is used to display the device's internal and external power and internal temperature status.

- Format

show environment

- Parameters

None.

- Restrictions

None.

- Example

To display the Switching Hub hardware status:

```
Zxxx0:admin#show environment
Command: show environment

Internal Power      : Active
Right Fan           : Speed Low
Current Temperature(Celsius) : 56
High Warning Temperature Threshold(Celsius) : 79
Low Warning Temperature Threshold(Celsius) : 11

CTRL+C  ESC  c  Quit  SPACE  n  Next Page  p  Previous Page  r  Refresh
```

## 5.10. config temperature

---

- Description

This command is used to configure the warning trap or log state of the system internal temperature.

- Format

config temperature [trap | log] state [enable | disable]

## 5. Basic Management Commands

### ● Parameters

|              |                                                                                                                                                                                                                                                                                            |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>trap</b>  | Specify to configure the warning temperature trap.                                                                                                                                                                                                                                         |
| <b>log</b>   | Specify to configure the warning temperature log.                                                                                                                                                                                                                                          |
| <b>state</b> | Enable or disable either the trap or log state for a warning temperature event. The default is enable.<br><b>enable</b><br>Enable either the trap or log state for a warning temperature event.<br><b>disable</b><br>Disable either the trap or log state for a warning temperature event. |

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To enable the warning temperature trap state:

```
Zxxx0:admin#config temperature trap state enable
Command: config temperature trap state enable

Success.

Zxxx0:admin#
```

To enable the warning temperature log state:

```
Zxxx0:admin#config temperature log state enable
Command: config temperature log state enable

Success.

Zxxx0:admin#
```

## 5.11. config temperature threshold

### ● Description

This command is used to configure the warning temperature high threshold or low threshold. When temperature is above the high threshold or below the low threshold, SW will send alarm traps or keep the logs.

### ● Format

config temperature threshold {high <temperature -500-500> | low <temperature -500-500>}(1)

## ● Parameters

|             |                                                                                                                                                                                                               |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>high</b> | Specify the high threshold value. The high threshold must bigger than the low threshold.<br><b>&lt;temperature -500-500&gt;</b><br>Specify the high threshold value. This value must be between -500 and 500. |
| <b>low</b>  | Specify the low threshold value.<br><b>&lt;temperature -500-500&gt;</b><br>Specify the low threshold value. This value must be between -500 and 500.                                                          |

## ● Restrictions

Only Administrator and Operator-level users can issue this command.

## ● Example

To configure a warming temperature threshold high of 80:

```
Zxxx0:admin#config temperature threshold high 80
Command: config temperature threshold high 80

Success.

Zxxx0:admin#
```

# 5.12. show serial\_port

## ● Description

This command is used to display the current console port setting.

## ● Format

show serial\_port

## ● Parameters

None.

## ● Restrictions

None.

## 5. Basic Management Commands

### ● Example

To display the console port setting:

```
Zxxx0:admin#show serial_port
Command: show serial_port

Baud Rate      : 9600
Data Bits      : 8
Parity Bits     : None
Stop Bits      : 1
Auto-Logout    : 10 mins

Zxxx0:admin#
```

## 5.13. config serial\_port

---

### ● Description

This command is used to configure the serial bit rate that will be used to communicate with the management host and the auto logout time for idle connections.

### ● Format

**config serial\_port {baud\_rate [9600 | 19200 | 38400 | 9600] | auto\_logout [never | 2\_minutes | 5\_minutes | 10\_minutes | 15\_minutes]}(1)**

### ● Parameters

---

#### **baud\_rate**

Specify the baud rate value. The default baud rate is 9600.

**9600** Specify a baud rate of 9600.

**19200**

Specify a baud rate of 19200.

**38400**

Specify a baud rate of 38400.

**115200**

Specify a baud rate of 115200.

---

#### **auto\_logout**

Specify the timeout value. The default timeout is 10\_minutes.

**never** Specify to never timeout.

**2\_minutes**

Specify when the idle value is over 2 minutes, the device will auto logout.

**5\_minutes**

Specify when the idle value is over 5 minutes, the device will auto logout.

**10\_minutes**

Specify when the idle value is over 10 minutes, the device will auto logout.

**15\_minutes**

Specify when the idle value is over 15 minutes, the device will auto logout.

---

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To configure the baud rate:

```
Zxxx0:admin# config serial_port baud_rate 9600
Command: config serial_port baud_rate 9600

Success.

Zxxx0:admin#
```

## 5.14. enable clipaging

---

### ● Description

This command is used to enable pausing of the screen display when show command output reaches the end of the page. The default setting is enabled.

### ● Format

enable clipaging

### ● Parameters

None.

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

Only Administrator and Operator-level users can issue this command.

```
Zxxx0:admin#enable clipaging
Command: enable clipaging

Success.

Zxxx0:admin#
```

## 5.15. disable clipaging

---

### ● Description

This command is used to disable pausing of the screen display when show command output reaches the end of the page. The default setting is enabled.

### ● Format

`disable clipaging`

### ● Parameters

None.

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To disable pausing of the screen display when show command output reaches the end of the page:

```
Zxxx0:admin#disable clipaging
Command: disable clipaging

Success.

Zxxx0:admin#
```

## 5.16. enable telnet

---

### ● Description

This command is used to enable Telnet and configure a port number. The default setting is enabled and the port number is 23.

### ● Format

`enable telnet {<tcp_port_number 1-65535>}`

### ● Parameters

---

`<tcp_port_number 1-65535>`

(Optional) Specify the TCP port number. TCP ports are numbered between 1 and 65535. The "well-known" TCP port for the Telnet protocol is 23.

---

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To enable Telnet and configure a port number:

```
Zxxx0:admin#enable telnet 23
Command: enable telnet 23

Success.

Zxxx0:admin#
```

## 5.17. disable telnet

---

### ● Description

This command is used to disable Telnet.

### ● Format

disable telnet

### ● Parameters

None.

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To disable Telnet:

```
Zxxx0:admin#disable telnet
Command: disable telnet

Success.

Zxxx0:admin#
```

## 5.18. save

---

### ● Description

This command is used to save the current configuration or log in non-volatile RAM.



## 5. Basic Management Commands

### ● Format

**save** {[config <pathname> | log | all]}

### ● Parameters

|               |                                                                                                                 |
|---------------|-----------------------------------------------------------------------------------------------------------------|
| <b>config</b> | (Optional) Specify to save configuration.<br><pathname><br>Specify the path name of the indicated configuration |
| <b>log</b>    | (Optional) Specify to save log.                                                                                 |
| <b>all</b>    | (Optional) Specify to save changes to currently active configuration and save logs.                             |

**NOTE** If no keyword is specified, all changes will be saved to bootup configuration file.

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To save the current configuration to the bootup configuration file:

```
Zxxx0:admin#save
Command: save

Saving all configurations to NV-RAM..... Done.

Zxxx0:admin#
```

To save the current configuration to destination file, named 1:

```
Zxxx0:admin#save config 1
Command: save config 1

Saving all configurations to NV-RAM..... Done.

Zxxx0:admin#
```

To save a log to NV-RAM:

```
Zxxx0:admin#save log
Command: save log

Saving all system logs to NV-RAM..... Done.

Zxxx0:admin#
```

To save all the configurations and logs to NV-RAM:

```
Zxxx0:admin#save all
Command: save all

Saving configuration and logs to NV-RAM..... Done.

Zxxx0:admin#
```

## 5.19. reboot

---

### ● Description

This command is used to restart the Switching Hub.

### ● Format

**reboot {force\_agree}**

### ● Parameters

---

**force\_agree**  
(Optional) Specify to immediately execute the reboot command without further confirmation.

---

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To restart the Switching Hub:

```
Zxxx0:admin#reboot
Command: reboot

Are you sure you want to proceed with the system reboot?(y/n)
Please wait, the switch is rebooting..
```

## 5.20. reset

---

### ● Description

This command is used to reset all Switching Hub parameters to the factory defaults.

### ● Format

**reset {[config | system]} {force\_agree}**

## 5. Basic Management Commands

### ● Parameters

---

**config** (Optional) Specify this keyword and all parameters are reset to default settings. However, the device will neither save nor reboot.

---

**system** (Optional) Specify this keyword and all parameters are reset to default settings. Then the Switching Hub will do factory reset, save, and reboot.

---

**force\_agree**  
(Optional) Specify and the reset command will be executed immediately without further confirmation.

---

---

**NOTE** If no keyword is specified, all parameters will be reset to default settings except IP address, user account, and history log, but the device will neither save nor reboot.

---

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To reset all the Switching Hub parameters except the IP address:

```
Zxxx0:admin#reset
Command: reset

Are you sure to proceed with system reset except IP address?(y/n)
Success.

Zxxx0:admin#
```

To reset the system configuration settings:

```
Zxxx0:admin#reset config
Command: reset config

Are you sure to proceed with system reset?(y/n)
Success.

Zxxx0:admin#
```

To reset all system parameters, save, and restart the Switching Hub:

```
Zxxx0:admin#reset system
Command: reset system

Are you sure to proceed with system reset, save and reboot?(y/n)
Loading factory default configuration... Done.
Saving all configuration to NV-RAM... Done.
Please wait, the switch is rebooting...
```

## 5.21. login

---

- **Description**

This command is used to log in to the Switching Hub.

- **Format**

login

- **Parameters**

None.

- **Restrictions**

None.

- **Example**

To login to the Switching Hub:

```
Zxxx0:admin#login
Command: login

UserName:
```

## 5.22. logout

---

- **Description**

This command is used to log out of the Switching Hub.

- **Format**

logout

- **Parameters**

None.

- **Restrictions**

None.

## 5. Basic Management Commands

### ● Example

To logout of the Switching Hub:

```
Zxxx0:admin#logout
Command: logout

*****
* Logout *
*****

                Zxxx0 Gigabit Ethernet Switch
                Command Line Interface

                Firmware: Build 1.0.x.xx

UserName:
```

## 5.23. clear

---

### ● Description

This command is used to clear the terminal screen.

### ● Format

clear

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To clear the terminal screen:

```
Zxxx0:admin#clear
Command: clear
```

## 5.24. config terminal width

---

### ● Description

This command is used to configure the terminal width.

### ● Format

config terminal width [default | <value 80-200>]

### ● Parameters

---

**default** Specify the default terminal width value.

**<value 80-200>**

Specify a terminal width value between 80 and 200 characters. The default value is 80.

---

### ● Restrictions

None.

### ● Example

To configure the terminal width:

```
Zxxx0:admin#config terminal width 90
Command: config terminal width 90

Success.

Zxxx0:admin#
```

## 5.25. show terminal width

---

### ● Description

This command is used to display the configuration of the current terminal width.

### ● Format

show terminal width

### ● Parameters

None.

### ● Restrictions

None.

## 5. Basic Management Commands

### ● Example

To display the configuration of the current terminal width:

```
Zxxx0:admin#show terminal width
Command: show terminal width

Global terminal width      : 80
Current terminal width     : 80

Zxxx0:admin#
```

## 5.26. show device\_status

---

### ● Description

This command displays current status of power(s) and fan(s) on the system.

Within fan(s) status display, for example, there are three fans on the left of the Switching Hub, if three fans is working normally, there will display "OK" in the Left Fan field. If some fans work failed, such as fan 1,3 , there will only display the failed fans in the Left Fan field, such as "1,3 Fail".

In the same way, the Right Fan, Back Fan is same to Left Fan. Because there is only one CPU Fan, if it is working failed, display "Fail", otherwise display "OK".

### ● Format

**show device\_status**

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To show device status, the number 1, 2, 3 etc represent the fan number:

```
Zxxx0:admin# show device_status
Command: show device_status

Unit 1:
  Internal Power: Active
  External Power: Fail
  Left Fan      : 1, 3 Fail
  Right Fan     : 2 Fail
  Back Fan      : OK
  CPU Fan       : Fail

Unit 2:
  Internal Power: Active
  External Power: Fail
  Left Fan      : 1 Fail
  Right Fan     : OK
  Back Fan      : 2, 4 Fail
  CPU Fan       : OK

Zxxx0:admin#
```



## 6. 802.1X Commands

IEEE802.1X provides user authentication when clients access the network and blocks connections to the network from unregistered clients. It prevents the access by unauthorized users or devices to protect information assets security.

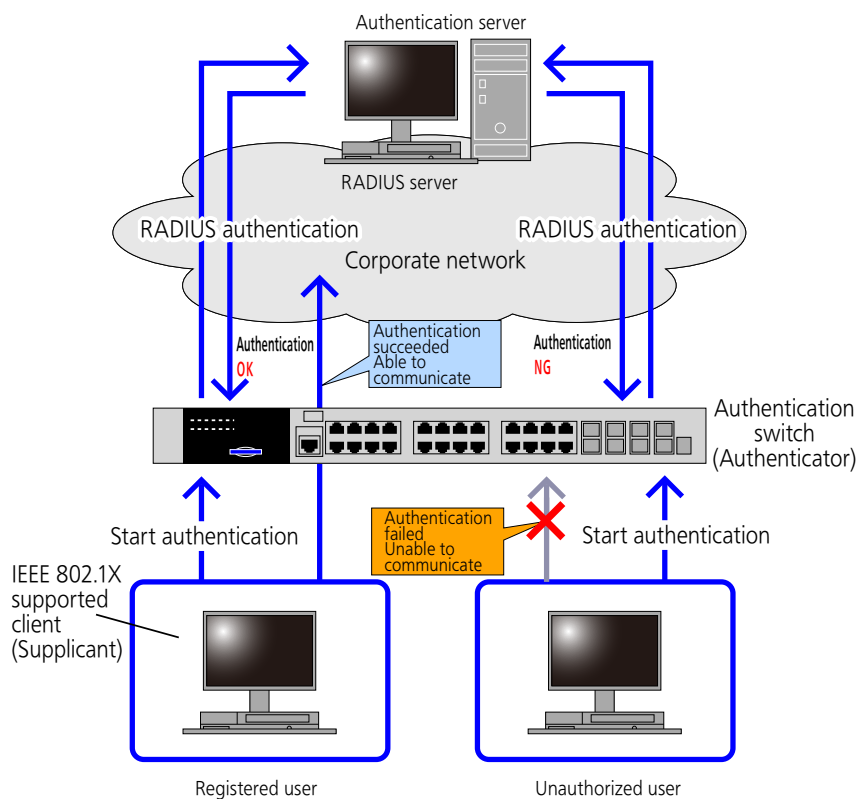


Figure 6-1 IEEE 802.1X overview

To use IEEE 802.1X authentication, there must be a client, authentication Switching Hub, and authentication server as shown above.

- The client requires IEEE 802.1X compatible software (An IEEE 802.1X supported client is called Supplicant). The client sends an authentication request when connecting to the network and is able to access when authorized.
- The authentication Switching Hub intermediates an authentication process between the client and authentication server. It blocks connections to the network from unauthorized clients (The authentication Switching Hub is also called Authenticator). This Switching Hub allows you to enable/disable authentication for each port and configure the authentication settings.
- A RADIUS server is usually used for the authentication server. It only approves an authentication request from registered users. Up to three authentication servers can be registered in the authentication Switching Hub.

**NOTE** You can register users in a local database in the authentication Switching Hub and use the database in place of a RADIUS server or as a RADIUS server failover.

## ● Port-based authentication and MAC-based authentication

You need to change the authentication method depending on how you connect the client to the port for the authentication Switching Hub. This Switching Hub allows you to select port-based or MAC-based authentication.

- **Port-based authentication:** Authorize a port to which the client is connected.
- **MAC-based authentication:** Authorize based on the MAC address of the client connected. It authorizes even in an environment where multiple clients communicate on a single port of the authentication Switching Hub (e.g. using an island hub). You can register up to 448 MAC addresses per port.

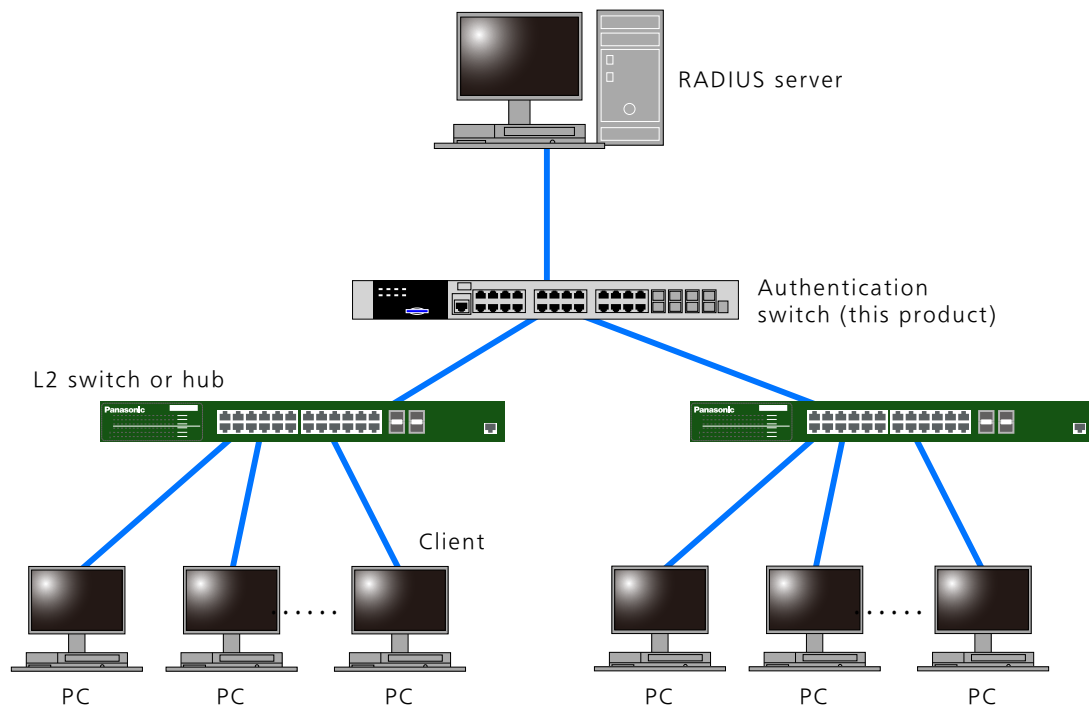


Figure 6-2 Authentication in edge hub

**NOTE** For authentication in an edge hub, a Switching Hub acting as an edge hub requires the EAP packet forwarding function. An EAP frame is communication data used for an authentication process. If devices are connected via a Switching Hub not supporting the EAP packet forwarding function, EAP frames are discarded and authentication is not performed (This Switching Hub supports the EAP packet forwarding function).

## 6. 802.1X Commands

### ● Guest VLAN

Combining the IEEE 802.1X and guest VLAN functions allows for restricted access, such as authorizing connection to the Internet only instead of completely blocking communications from unauthorized clients.

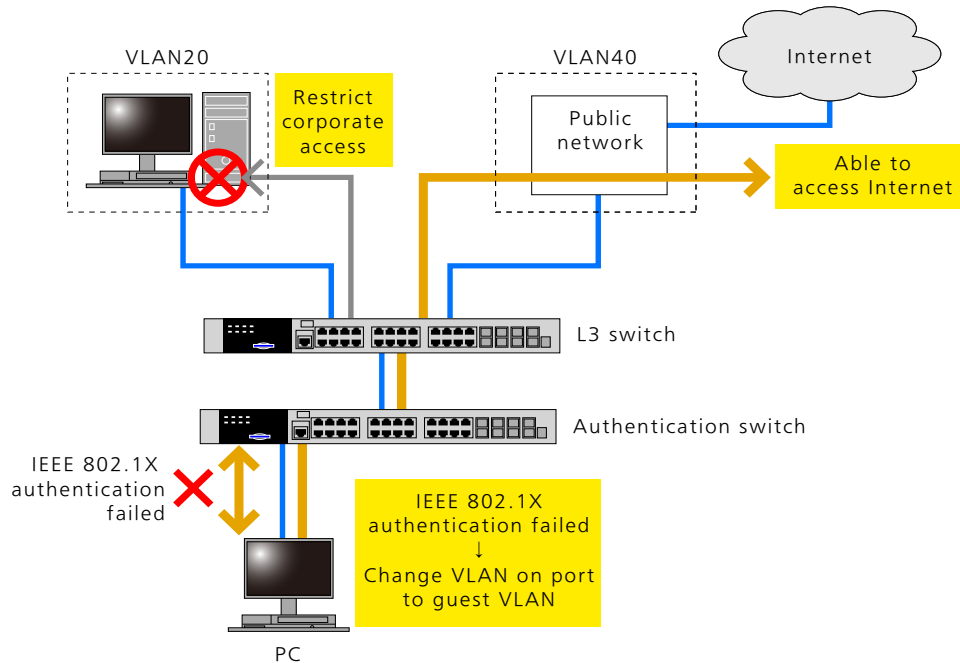


Figure 6-3 Connection through guest VLAN

---

**NOTE** Only one VLAN can be assigned to a guest VLAN.

---

## ● Dynamic VLAN using IEEE 802.1X

In a static VLAN, the destination VLAN is fixed for each port. Meanwhile, in a dynamic VLAN, the destination VLAN is determined based on the client MAC address information regardless of a port to be connected.

There are several ways to configure dynamic VLAN. One of them is to use IEEE 802.1X RADIUS server information. If the client's VLAN information is registered in the RADIUS server, the VLAN information is retrieved during authentication, allowing for accessing the VLAN to which the client belongs from any port.

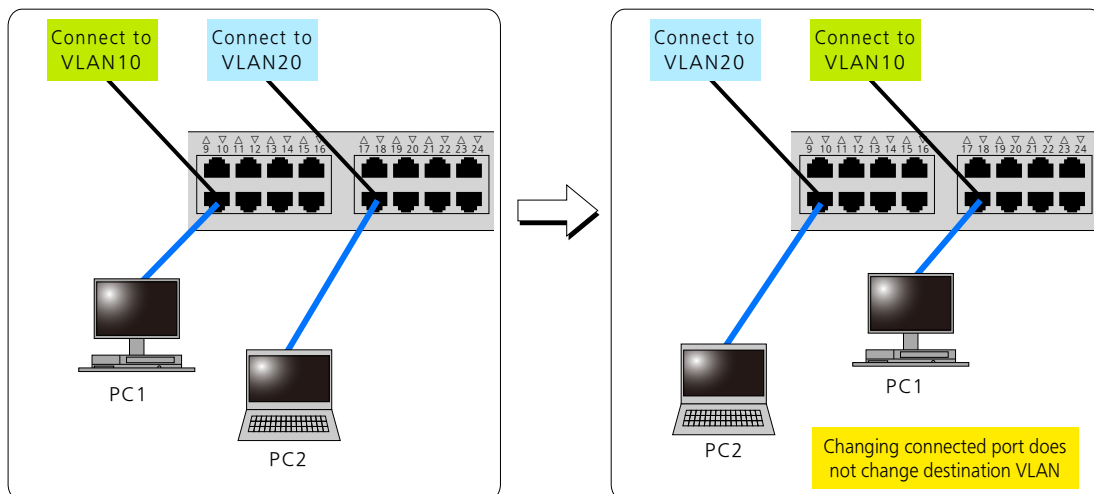


Figure 6-4 Dynamic VLAN

```
enable 802.1x
disable 802.1x
create 802.1x user <username 15>
delete 802.1x user <username 15>
show 802.1x user
config 802.1x auth_protocol [local | radius_eap]
show 802.1x {[auth_state | auth_configuration] ports {<portlist>}}
config 802.1x capability ports [<portlist> | all] [authenticator | none]
config 802.1x fwd_pdu ports [<portlist> | all] [enable | disable]
config 802.1x fwd_pdu system [enable | disable]
config 802.1x auth_parameter ports [<portlist> | all] [default | {direction [both | in] | port_control
    [force_unauth | auto | force_auth] | quiet_period <sec 0-65535> | tx_period <sec 1-65535>
    | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req <value 1-10> |
    reauth_period <sec 1-65535> | max_users [<value 1-448> | no_limit] | enable_reauth [enable
    | disable]}(1)]
config 802.1x authorization attributes radius [enable | disable]
config 802.1x init [port_based ports [<portlist> | all] | mac_based ports [<portlist> | all]
    {mac_address <macaddr>}]
config 802.1x max_users [<value 1-448> | no_limit]
config 802.1x reauth [port_based ports [<portlist> | all] | mac_based ports [<portlist> | all]
    {mac_address <macaddr>}]
create 802.1x guest_vlan <vlan_name 32>
delete 802.1x guest_vlan <vlan_name 32>
config 802.1x guest_vlan ports [<portlist> | all] state [enable | disable]
```

## 6. 802.1X Commands

---

```
show 802.1x guest_vlan
config radius add <server_index 1-3> [<server_ip> | <ipv6addr>] key <password 32> [default |
    {auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | timeout
    <sec 1-255> | retransmit <int 1-20>}(1)]
config radius delete <server_index 1-3>
config radius <server_index 1-3> {ipaddress [<server_ip> | <ipv6addr>] | key <password 32> |
    auth_port [<udp_port_number 1-65535> | default] | acct_port [<udp_port_number 1-
    65535> | default] | timeout [<sec 1-255> | default] | retransmit [<int 1-20> | default]}(1)
show radius
show auth_statistics {ports <portlist>}
show auth_diagnostics {ports <portlist>}
show auth_session_statistics {ports <portlist>}
show auth_client
show acct_client
config accounting service [network | shell | system] state [enable | disable]
show accounting service
```

---

### 6.1. enable 802.1x

---

#### ● Description

This command is used to enable the 802.1X function.

#### ● Format

**enable 802.1x**

#### ● Parameters

None.

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To enable the 802.1X function:

```
Zxxx0:admin#enable 802.1x
Command: enable 802.1x

Success.

Zxxx0:admin#
```

## 6.2. disable 802.1x

---

- **Description**

This command is used to disable the 802.1X function.

- **Format**

disable 802.1x

- **Parameters**

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To disable the 802.1X function:

```
Zxxx0:admin#disable 802.1x
Command: disable 802.1x

Success.

Zxxx0:admin#
```

## 6.3. create 802.1x user

---

- **Description**

This command is used to create an 802.1X user.

- **Format**

create 802.1x user <username 15>

- **Parameters**

---

<username 15>  
Specify to add a user name.

---

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

## 6. 802.1X Commands

### ● Example

To create a user named "ctsnow":

```
Zxxx0:admin#create 802.1x user ctsnow
Command: create 802.1x user ctsnow

Enter a case-sensitive new password:
Enter the new password again for confirmation:

Success.

Zxxx0:admin#
```

## 6.4. delete 802.1x user

---

### ● Description

This command is used to delete a specified user.

### ● Format

delete 802.1x user <username 15>

### ● Parameters

---

<username 15>  
Specify to delete a user name.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete the user named "Tiberius":

```
Zxxx0:admin#delete 802.1x user Tiberius
Command: delete 802.1x user Tiberius

Success.

Zxxx0:admin#
```

## 6.5. show 802.1x user

---

### ● Description

This command is used to display 802.1X local user account information.

### ● Format

show 802.1x user

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display 802.1X user information:

```
Zxxx0:admin#show 802.1x user
Command: show 802.1x user

Current Accounts:
Username          Password
-----          -
ctsnow            gallinari

Total Entries : 1

Zxxx0:admin#
```

## 6.6. config 802.1x auth\_protocol

---

### ● Description

This command is used to configure the 802.1X authentication protocol.

### ● Format

config 802.1x auth\_protocol [local | radius\_eap]

### ● Parameters

---

**local**      Specify the authentication protocol as local.

---

**radius\_eap**  
Specify the authentication protocol as RADIUS EAP.

---



## 6. 802.1X Commands

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the 802.1X RADIUS EAP:

```
Zxxx0:admin#config 802.1x auth_protocol radius_eap
Command: config 802.1x auth_protocol radius_eap

Success.

Zxxx0:admin#
```

## 6.7. show 802.1x

---

### ● Description

This command is used to display the 802.1X state or configurations.

### ● Format

**show 802.1x** {[auth\_state | auth\_configuration] ports {<portlist>}}

### ● Parameters

|                           |                                                                                                                 |
|---------------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>auth_state</b>         | (Optional) Specify to display the 802.1X authentication state of some or all ports.                             |
| <b>auth_configuration</b> | (Optional) Specify to display 802.1X configuration of some or all ports.                                        |
| <b>ports</b>              | (Optional) Specify a range of ports to be displayed.<br><portlist><br>Specify a range of ports to be displayed. |

### ● Restrictions

None.

### ● Example

To display 802.1X information:

```
Zxxx0:admin#show 802.1x
Command: show 802.1x

802.1X                : Disabled
Authentication Protocol : RADIUS_EAP
Forward EAPOL PDU      : Disabled
Max User               : 448
RADIUS Authorization    : Enabled

Zxxx0:admin#
```

To display the 802.1x state for ports 1 to 5:

```
Zxxx0:admin# show 802.1x auth_state ports 1-4
Command: show 802.1x auth_state ports 1-4

Status:  A - Authorized; U - Unauthorized; (P): Port-Based 802.1X Pri: Priority
Port  MAC Address          Auth  PAE State      Backend      Status VID  Pri
-----
1      00-00-00-00-00-01     10    Authenticated  Idle         A    4004  3
1      00-00-00-00-00-02     10    Authenticated  Idle         A    1234  -
1      00-00-00-00-00-04     30    Authenticating Response  U    -    -
2      -                    (P) - Authenticating Request  U    -    -
3      -                    (P) - Connecting      Idle         U    -    -
4      -                    (P) - Held           Fail         U    -    -

Total Authenticating Hosts: 3
Total Authenticated Hosts : 2

Zxxx0:admin#
```

To display the 802.1x configuration for port 1:

```
Zxxx0:admin# show 802.1x auth_configuration ports 1
Command: show 802.1x auth_configuration ports 1

Port number           : 1
Capability             : None
AdminCrlDir           : Both
OpenCrlDir            : Both
Port Control          : Auto
QuietPeriod           : 60 Seconds
TxPeriod              : 30 Seconds
SuppTimeout           : 30 Seconds
ServerTimeout         : 30 Seconds
MaxReq                : 2 Times
ReAuthPeriod          : 3600 Seconds
ReAuthenticate        : Disabled
Forward EAPOL PDU On Port : Disabled
Max User On Port      : 16

Zxxx0:admin#
```

## 6.8. config 802.1x capability ports

---

### ● Description

This command is used to configure port capability.

### ● Format

config 802.1x capability ports [<portlist> | all] [authenticator | none]

### ● Parameters

|               |                                                                                                                                                    |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <portlist>    | Specify a range of ports to be configured.                                                                                                         |
| all           | Specify to configure all ports.                                                                                                                    |
| authenticator | The port that wishes to enforce authentication before allowing access to services that are accessible via that port adopts the authenticator role. |
| none          | Disable authentication on specified port.                                                                                                          |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure port capability for ports 1 to 10:

```
Zxxx0:admin#config 802.1x capability ports 1-10 authenticator
Command: config 802.1x capability ports 1-10 authenticator

Success.

Zxxx0:admin#
```

## 6.9. config 802.1x fwd\_pdu ports

---

### ● Description

This command is used to configure the 802.1X PDU forwarding state on specific ports of the Switching Hub.

### ● Format

config 802.1x fwd\_pdu ports [<portlist> | all] [enable | disable]

## ● Parameters

|                         |                                            |
|-------------------------|--------------------------------------------|
| <b>&lt;portlist&gt;</b> | Specify a range of ports to be configured. |
| <b>all</b>              | Specify all ports.                         |
| <b>enable</b>           | Enable the 802.1X PDU forwarding state.    |
| <b>disable</b>          | Disable the 802.1X PDU forwarding state.   |

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure the 802.1X PDU forwarding state on ports 1 to 2:

```
Zxxx0:admin#config 802.1x fwd_pdu ports 1-2 enable
Command: config 802.1x fwd_pdu ports 1-2 enable

Success.

Zxxx0:admin#
```

# 6.10. config 802.1x fwd\_pdu system

## ● Description

This command is used to configure the 802.1X PDU forwarding state.

## ● Format

**config 802.1x fwd\_pdu system [enable | disable]**

## ● Parameters

|                |                                          |
|----------------|------------------------------------------|
| <b>enable</b>  | Enable the 802.1X PDU forwarding state.  |
| <b>disable</b> | Disable the 802.1X PDU forwarding state. |

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure the 802.1X PDU forwarding state:

## 6. 802.1X Commands

```
Zxxx0:admin#config 802.1x fwd_pdu system enable
Command: config 802.1x fwd_pdu system enable

Success.

Zxxx0:admin#
```

### 6.11. config 802.1x auth\_parameter ports

#### ● Description

This command is used to configure the parameters that control the operation of the authenticator associated with a port.

#### ● Format

```
config 802.1x auth_parameter ports [<portlist> | all] [default | {direction [both | in] |
port_control [force_unauth | auto | force_auth] | quiet_period <sec 0-65535> |
tx_period <sec 1-65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535>
| max_req <value 1-10> | reauth_period <sec 1-65535> | max_users [<value 1-448> |
no_limit] | enable_reauth [enable | disable]}(1)]
```

#### ● Parameters

---

**<portlist>**

Specify a range of ports to be configured.

---

**all**

Specify to configure all ports.

---

**default** Set all parameters to the default value.

---

**direction**(Optional) Set the direction of access control.

**both** For bidirectional access control.

**in** For ingress access control.

---

**port\_control**

(Optional) Force a specific port to be unconditionally authorized or unauthorized by setting the parameter of port\_control to be force\_authorized or force\_unauthorized. Besides, the controlled port will reflect the outcome of authentication if port\_control is auto.

**force\_authorized**

The port transmits and receives normal traffic without 802.1X-based authentication of the client.

**auto** The port begins in the unauthorized state, and relays authentication messages between the client and the authentication server.

**force\_unauthorized**

The port will remain in the unauthorized state, ignoring all attempts by the client to authenticate.

---

---

**quiet\_period**

(Optional) The initialization value of the quietWhile timer. The default value is 60 s and can be any value from 0 to 65535.

**<sec 0-65535>**

The quiet period value must be between 0 and 65535 seconds.

---

**tx\_period**

(Optional) The initialization value of the txWhen timer. The default value is 30 s and can be any value from 1 to 65535.

**<sec 1-65535>**

The transmit period value must be between 1 and 65535 seconds.

---

**supp\_timeout**

(Optional) The initialization value of the aWhile timer when timing out the supplicant. Its default value is 30 s and can be any value from 1 to 65535.

**<sec 1-65535>**

The timeout value must be between 1 and 65535 seconds.

---

**server\_timeout**

(Optional) The initialization value of the aWhile timer when timing out the authentication server. Its default value is 30 and can be any value from 1 to 65535.

**<sec 1-65535>**

The server timeout value must be between 1 and 65535 seconds.

---

**max\_req** (Optional) The maximum number of times that the authentication PAE state machine will retransmit an EAP Request packet to the supplicant. Its default value is 2 and can be any number from 1 to 10.

**<value 1-10>**

The maximum require number must be between 1 and 10.

---

**reauth\_period**

(Optional) It's a non-zero number of seconds, which is used to be the re-authentication timer. The default value is 3600.

**<sec 1-65535>**

The reauthentication period value must be between 1 and 65535 seconds.

---

**max\_users**

(Optional) Set the maximum number of users between 1 and 448.

**<value 1-448>**

The maximum users value must be between 1 and 448.

**no\_limit**

Set an unlimited number of users.

---

**enable\_reauth**

(Optional) Enable or disable the re-authentication mechanism for a specific port.

**enable**

Enable the re-authentication mechanism for a specific port.

**disable**

Disable the re-authentication mechanism for a specific port.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure the parameters that control the operation of the authenticator associated with a port:

## 6. 802.1X Commands

```
Zxxx0:admin# config 802.1x auth_parameter ports 1-20 direction both
Command: config 802.1x auth_parameter ports 1-20 direction both

Success.

Zxxx0:admin#
```

## 6.12. config 802.1x authorization attributes radius

---

### ● Description

This command is used to enable or disable the acceptance of an authorized configuration. (To configure that attributes, regarding VLAN, 802.1p, ACL and Ingress/Egress Bandwidth, please refer to the Appendix section at the end of this document.)

### ● Format

**config 802.1x authorization attributes radius [enable | disable]**

### ● Parameters

---

|               |                                                                                                                                                                                                         |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>enable</b> | The authorization attributes such as VLAN, 802.1p default priority, and ACL assigned by the RADUIS server will be accepted if the global authorization status is enabled. The default state is enabled. |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

|                |                                                                                  |
|----------------|----------------------------------------------------------------------------------|
| <b>disable</b> | The authorization attributes assigned by the RADUIS server will not be accepted. |
|----------------|----------------------------------------------------------------------------------|

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the 802.1X state of acceptance of an authorized configuration:

```
Zxxx0:admin#config 802.1x authorization attributes radius enable
Command: config 802.1x authorization attributes radius enable

Success.

Zxxx0:admin#
```

## 6.13. config 802.1x init

---

### ● Description

This command is used to initialize the authentication state machine of some or all.

### ● Format

**config 802.1x init** [port\_based ports [<portlist> | all] | mac\_based ports [<portlist> | all] {mac\_address <macaddr>}]

### ● Parameters

---

#### port\_based ports

Used to configure authentication in port-based mode.

**<portlist>**

Specify a range of ports to be configured.

**all** Specify to configure all ports.

---

#### mac\_based ports

To configure authentication in host-based 802.1X mode.

**<portlist>**

Specify a range of ports to be configured.

**all** Specify to configure all ports.

---

#### mac\_address

(Optional) Specify the MAC address of the host.

**<macaddr>**

Enter the MAC address here.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To initialize the authentication state machine of some or all:

```
Zxxx0:admin# config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

Zxxx0:admin#
```



## 6.14. config 802.1x max\_users

---

### ● Description

This command is used to configure the 802.1X maximum number of users of the system.

### ● Format

config 802.1x max\_users [<value 1-448> | no\_limit]

### ● Parameters

---

<value 1-448>

Specify the maximum number of users.

---

no\_limit Specify an unlimited number of users.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the 820.1X maximum numbers of the system:

```
Zxxx0:admin# config 802.1x max_users 2
Command: config 802.1x max_users 2

Success.

Zxxx0:admin#
```

## 6.15. config 802.1x reauth

---

### ● Description

This command is used to reauthenticate the device connected with the port. During the reauthentication period, the port status remains authorized until failed reauthentication.

### ● Format

config 802.1x reauth [port\_based ports [<portlist> | all] | mac\_based ports [<portlist> | all] {mac\_address <macaddr>}]

## ● Parameters

---

### port\_based ports

The Switching Hub passes data based on its authenticated port.

**<portlist>**

Specify a range of ports to be configured.

**all** Specify to configure all ports.

---

### mac\_based ports

The Switching Hub passes data based on the MAC address of authenticated RADIUS client.

**<portlist>**

Specify a range of ports to be configured.

**all** Specify to configure all ports.

---

### mac\_address

(Optional) Specify the MAC address of the authenticated RADIUS client.

**<macaddr>**

Enter the MAC address here.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To reauthenticate the device connected with the port:

```
Zxxx0:admin# config 802.1x reauth port_based ports all
Command: config 802.1x reauth port_based ports all

Success.

Zxxx0:admin#
```

## 6.16. create 802.1x guest\_vlan

---

### ● Description

This command is used to assign a static VLAN to be a guest VLAN. The specific VLAN which is assigned to a guest VLAN must already exist. The specific VLAN which is assigned to the guest VLAN can't be deleted.

### ● Format

**create 802.1x guest\_vlan <vlan\_name 32>**

### ● Parameters

---

**<vlan\_name 32>**

Specify the static VLAN to be a guest VLAN.

---

## 6. 802.1X Commands

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To assign a static VLAN to be a guest VLAN:

```
Zxxx0:admin# create 802.1x guest_vlan guestVLAN
Command: create 802.1x guest_vlan guestVLAN

Success.

Zxxx0:admin#
```

## 6.17. delete 802.1x guest\_vlan

### ● Description

This command is used to delete a guest VLAN setting, but not to delete the static VLAN itself.

### ● Format

delete 802.1x guest\_vlan <vlan\_name 32>

### ● Parameters

---

<vlan\_name 32>  
Specify the guest VLAN name.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete a guest VLAN configuration:

```
Zxxx0:admin# delete 802.1x guest_vlan guestVLAN
Command: delete 802.1x guest_vlan guestVLAN

Success.

Zxxx0:admin#
```

## 6.18. config 802.1x guest\_vlan ports

---

### ● Description

This command is used to configure a guest VLAN setting.

### ● Format

config 802.1x guest\_vlan ports [<portlist> | all] state [enable | disable]

### ● Parameters

|            |                                                            |
|------------|------------------------------------------------------------|
| <portlist> | Specify a range of ports to be configured.                 |
| all        | Specify to configure all ports.                            |
| state      | Specify the guest VLAN port state of the configured ports. |
| enable     | Join the guest VLAN.                                       |
| disable    | Remove from guest VLAN.                                    |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure a guest VLAN setting for ports 1 to 8:

```
Zxxx0:admin# config 802.1x guest_vlan ports 1-8 state enable
Command: config 802.1x guest_vlan ports 1-8 state enable

Warning, The ports are moved to Guest VLAN.

Success.

Zxxx0:admin#
```

## 6.19. show 802.1x guest\_vlan

---

### ● Description

This command is used to display guest VLAN information.

### ● Format

show 802.1x guest\_vlan

## 6. 802.1X Commands

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display guest VLAN information:

```
Zxxx0:admin#show 802.1x guest_vlan
Command: show 802.1x guest_vlan

Guest Vlan Setting
-----
Guest vlan : guest
Enable guest vlan ports : 1-10

Zxxx0:admin#
```

## 6.20. config radius add

### ● Description

This command is used to add a new RADIUS server. The server with a lower index has higher authenticative priority.

### ● Format

```
config radius add <server_index 1-3> [<server_ip> | <ipv6addr>] key <password 32>
[default | {auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | timeout <sec 1-255> | retransmit <int 1-20>}(1)]
```

### ● Parameters

---

**<server\_index 1-3>**

Specify the RADIUS server index.

---

**<server\_ip>**

Specify the IP address of the RADIUS server.

---

**<ipv6addr>**

Specifies the IPv6 address used.

---

**key**

Specify the key pre-negotiated between Switching Hub and the RADIUS server. It is used to encrypt user's authentication data before being transmitted over the Internet. The maximum length of the key is 32.

**<passwd 32>**

The maximum length of the password is 32 characters long.

---

**default** Sets the auth\_port to be 1812 and acct\_port to be 1813.

---

---

**auth\_port**

Specify the UDP port number which is used to transmit RADIUS authentication data between the Switching Hub and the RADIUS server. The range is 1 to 65535.

**<udp\_port\_number 1-65535>**

The authentication port value must be between 1 and 65535.

---

**acct\_port**

Specify the UDP port number which is used to transmit RADIUS accounting statistics between the Switching Hub and the RADIUS server. The range is 1 to 65535.

**<udp\_port\_number 1-65535>**

The accounting statistics value must be between 1 and 65535.

---

**timeout** Specify the time, in seconds, for waiting server reply. The default value is 5 seconds.

**<int 1-255>**

The timeout value must be between 1 and 255.

---

**retransmit**

Specify the count for re-transmit. The default value is 2.

**<int 1-20>**

The re-transmit value must be between 1 and 20.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To add a new RADIUS server:

```
Zxxx0:admin#config radius add 1 10.48.74.121 key manager default
Command: config radius add 1 10.48.74.121 key manager default

Success.

Zxxx0:admin#
```

## 6.21. config radius delete

---

### ● Description

This command is used to delete a RADIUS server.

### ● Format

**config radius delete <server\_index 1-3>**

### ● Parameters

---

**<server\_index 1-3>**

Specify the RADIUS server index. The range is from 1 to 3.

---

## 6. 802.1X Commands

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete a RADIUS server:

```
Zxxx0:admin#config radius delete 1
Command: config radius delete 1

Success.

Zxxx0:admin#
```

## 6.22. config radius

---

### ● Description

This command is used to configure a RADIUS server.

### ● Format

config radius <server\_index 1-3> {ipaddress [<server\_ip> | <ipv6addr>] | key <password 32> | auth\_port [<udp\_port\_number 1-65535> | default] | acct\_port [<udp\_port\_number 1-65535> | default] | timeout [<sec 1-255> | default] | retransmit [<int 1-20> | default]}(1)

### ● Parameters

---

**<server\_index 1-3>**

Specify the RADIUS server index.

---

**ipaddress**

Specify the IP address of the RADIUS server.

**<server\_ip>**

Enter the RADIUS server IP address here.

**<ipv6addr>**

Enter the IPv6 address here.

---

**key**

Specify the key pre-negotiated between the Switching Hub and the RADIUS server. It is used to encrypt user's authentication data before being transmitted over the Internet. The maximum length of the key is 32.

**<passwd 32>**

Specify the key pre-negotiated between the Switching Hub and the RADIUS server. It is used to encrypt user's authentication data before being transmitted over the Internet. The maximum length of the key is 32.

---

---

**auth\_port**

Specify the UDP port number which is used to transmit RADIUS authentication data between the Switching Hub and the RADIUS server. The default is 1812.

**<udp\_port\_number 1-65535>**

The authentication port value must be between 1 and 65535.

**default**

Specify to use the default value.

---

**acct\_port**

Specify the UDP port number which is used to transmit RADIUS authentication data between the Switching Hub and the RADIUS server. The default is 1812.

**<udp\_port\_number 1-65535>**

The authentication port value must be between 1 and 65535.

**default**

Specify to use the default value.

---

**timeout** Specify the time in seconds for waiting for a server reply. The default value is 5 seconds.

**<int 1-255>**

Specify the time in seconds for waiting for a server reply. The timeout value must be between 1 and 255. The default value is 5 seconds.

**default**

Specify to use the default value.

---

**retransmit**

Specify the count for re-transmission. The default value is 2.

**<int 1-20>**

The re-transmit value must be between 1 and 20.

**default**

Specify to use the default value.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure a RADIUS server:

```
Zxxx0:admin#config radius 1 ipaddress 10.48.74.121 key manager
Command: config radius 1 ipaddress 10.48.74.121 key manager

Success.

Zxxx0:admin#
```



## 6.23. show radius

---

### ● Description

This command is used to display RADIUS server configurations.

### ● Format

**show radius**

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display RADIUS server configurations:

```
Zxxx0:admin#show radius
Command: show radius

Index 1
  IP Address      : 192.168.69.1
  Auth-Port       : 1812
  Acct-Port       : 1813
  Timeout         : 5
  Retransmit      : 2
  Key             : 123456

Total Entries : 1

Zxxx0:admin#
```

## 6.24. show auth\_statistics

---

### ● Description

This command is used to display authenticator statistics information

### ● Format

**show auth\_statistics {ports <portlist>}**

### ● Parameters

---

|                         |                                                      |
|-------------------------|------------------------------------------------------|
| <b>ports</b>            | (Optional) Specify a range of ports to be displayed. |
| <b>&lt;portlist&gt;</b> | Specify a range of ports to be displayed.            |

---

### ● Restrictions

None.

### ● Example

To display authenticator statistics information for port 3:

```
Zxxx0:admin# show auth_statistics ports 3
Command: show auth_statistics ports 3

Auth VID      : 100
MAC Address   : 00-00-00-00-00-03
Port number   : 3

EapolFramesRx          0
EapolFramesTx          6
EapolStartFramesRx     0
EapolReqIdFramesTx     6
EapolLogoffFramesRx    0
EapolReqFramesTx       0
EapolRespIdFramesRx    0
EapolRespFramesRx      0
InvalidEapolFramesRx   0
EapLengthErrorFramesRx 0
LastEapolFrameVersion  0
LastEapolFrameSource   00-00-00-00-00-03

CTRL+C  ESC  q  Quit  SPACE  n  Next Page  p  Previous Page  r  Refresh
```

## 6.25. show auth\_diagnostics

---

### ● Description

This command is used to display authenticator diagnostics information.

### ● Format

**show auth\_diagnostics {ports <portlist>}**

### ● Parameters

---

|                         |                                                      |
|-------------------------|------------------------------------------------------|
| <b>ports</b>            | (Optional) Specify a range of ports to be displayed. |
| <b>&lt;portlist&gt;</b> | Specify a range of ports to be displayed.            |

---

### ● Restrictions

None.

### ● Example

To display authenticator diagnostics information for port 3:

```
Zxxx0:admin# show auth_diagnostics ports 3
Command: show auth_diagnostics ports 3

Auth VID                               100
MAC Address                           00-00-00-00-00-03
Port number : 1

EntersConnecting                       20
EapLogoffsWhileConnecting              0
EntersAuthenticating                  0
SuccessWhileAuthenticating             0
TimeoutsWhileAuthenticating            0
FailWhileAuthenticating                0
ReauthsWhileAuthenticating             0
EapStartsWhileAuthenticating           0
EapLogoffWhileAuthenticating           0
ReauthsWhileAuthenticated              0
EapStartsWhileAuthenticated            0
EapLogoffWhileAuthenticated            0
BackendResponses                       0
BackendAccessChallenges                0
BackendOtherRequestsToSupPLICant       0
BackendNonNakResponsesFromSupPLICant    0
BackendAuthSuccesses                   0
BackendAuthFails                       0

CTRL+C  ESC  q  Quit  SPACE  n  Next Page  p  Previous Page  r  Refresh
```

## 6.26. show auth\_session\_statistics

---

### ● Description

This command is used to display authenticator session statistics information.

### ● Format

**show auth\_session\_statistics {ports <portlist>}**

### ● Parameters

---

|                         |                                                      |
|-------------------------|------------------------------------------------------|
| <b>ports</b>            | (Optional) Specify a range of ports to be displayed. |
| <b>&lt;portlist&gt;</b> | Specify a range of ports to be displayed.            |

---

### ● Restrictions

None.

### ● Example

To display authenticator session statistics information for port 1:

```
Zxxx0:admin# show auth_session_statistics ports 3
Command: show auth_session_statistics ports 3

Auth VID      : 100
MAC Address   : 00-00-00-00-00-03
Port number   : 3

SessionOctetsRx      0
SessionOctetsTx      0
SessionFramesRx      0
SessionFramesTx      0
SessionId
SessionAuthenticMethod Remote Authentication Server
SessionTime          0
SessionTerminateCause SupplicantLogoff
SessionUserName
```

```
CTRL+C  ESC  q  Quit  SPACE  n  Next Page  p  Previous Page  r  Refresh
```

## 6.27. **show auth\_client**

---

- **Description**

This command is used to display authentication client information.

- **Format**

`show auth_client`

- **Parameters**

None.

- **Restrictions**

None.

- **Example**

To display authentication client information:

```

Zxxx0:admin# show auth_client
Command: show auth_client

radiusAuthClient ==>
radiusAuthClientInvalidServerAddresses    0
radiusAuthClientIdentifier                 Manager

radiusAuthServerEntry ==>
radiusAuthServerIndex :1

radiusAuthServerAddress                    0.0.0.0
radiusAuthClientServerPortNumber          X
radiusAuthClientRoundTripTime             0
radiusAuthClientAccessRequests            0
radiusAuthClientAccessRetransmissions     0
radiusAuthClientAccessAccepts             0
radiusAuthClientAccessRejects             0
radiusAuthClientAccessChallenges          0
radiusAuthClientMalformedAccessResponses  0
radiusAuthClientBadAuthenticators         0
radiusAuthClientPendingRequests           0
radiusAuthClientTimeouts                  0
radiusAuthClientUnknownTypes              0
radiusAuthClientPacketsDropped            0

radiusAuthClient ==>
radiusAuthClientInvalidServerAddresses    0
radiusAuthClientIdentifier                 MANAGER

radiusAuthServerEntry ==>
radiusAuthServerIndex :2

radiusAuthServerAddress                    0.0.0.0
radiusAuthClientServerPortNumber          X
radiusAuthClientRoundTripTime             0
radiusAuthClientAccessRequests            0
radiusAuthClientAccessRetransmissions     0
radiusAuthClientAccessAccepts             0
radiusAuthClientAccessRejects             0
radiusAuthClientAccessChallenges          0
radiusAuthClientMalformedAccessResponses  0
radiusAuthClientBadAuthenticators         0
radiusAuthClientPendingRequests           0
radiusAuthClientTimeouts                  0
radiusAuthClientUnknownTypes              0
radiusAuthClientPacketsDropped            0

```

## 6. 802.1X Commands

```
radiusAuthClient ==>
radiusAuthClientInvalidServerAddresses    0
radiusAuthClientIdentifier                 MANAGER

radiusAuthServerEntry ==>
radiusAuthServerIndex :3

radiusAuthServerAddress                    0.0.0.0
radiusAuthClientServerPortNumber          X
radiusAuthClientRoundTripTime             0
radiusAuthClientAccessRequests            0
radiusAuthClientAccessRetransmissions     0
radiusAuthClientAccessAccepts             0
radiusAuthClientAccessRejects             0
radiusAuthClientAccessChallenges          0
radiusAuthClientMalformedAccessResponses  0
radiusAuthClientBadAuthenticators         0
radiusAuthClientPendingRequests           0
radiusAuthClientTimeouts                  0
radiusAuthClientUnknownTypes              0
radiusAuthClientPacketsDropped            0

Zxxx0:admin#
```

### 6.28. show acct\_client

---

#### ● Description

This command is used to display account client information

#### ● Format

show acct\_client

#### ● Parameters

None.

#### ● Restrictions

None.

#### ● Example

To display account client information:

```

Zxxx0:admin# show acct_client
Command: show acct_client

radiusAcctClient ==>
radiusAcctClientInvalidServerAddresses    0
radiusAcctClientIdentifier                MANAGER

radiusAuthServerEntry ==>
radiusAccServerIndex : 1

radiusAccServerAddress                    0.0.0.0
radiusAccClientServerPortNumber          X
radiusAccClientRoundTripTime             0
radiusAccClientRequests                  0
radiusAccClientRetransmissions           0
radiusAccClientResponses                 0
radiusAccClientMalformedResponses        0
radiusAccClientBadAuthenticators         0
radiusAccClientPendingRequests           0
radiusAccClientTimeouts                  0
radiusAccClientUnknownTypes              0
radiusAccClientPacketsDropped            0

radiusAcctClient ==>
radiusAcctClientInvalidServerAddresses    0
radiusAcctClientIdentifier                MANAGER

radiusAuthServerEntry ==>
radiusAccServerIndex : 2

radiusAccServerAddress                    0.0.0.0
radiusAccClientServerPortNumber          X
radiusAccClientRoundTripTime             0
radiusAccClientRequests                  0
radiusAccClientRetransmissions           0
radiusAccClientResponses                 0
radiusAccClientMalformedResponses        0
radiusAccClientBadAuthenticators         0
radiusAccClientPendingRequests           0
radiusAccClientTimeouts                  0
radiusAccClientUnknownTypes              0
radiusAccClientPacketsDropped            0

radiusAcctClient ==>
radiusAcctClientInvalidServerAddresses    0
radiusAcctClientIdentifier                MANAGER

```



## 6. 802.1X Commands

```
radiusAuthServerEntry ==>
radiusAccServerIndex : 3

radiusAccServerAddress          0.0.0.0
radiusAccClientServerPortNumber X
radiusAccClientRoundTripTime    0
radiusAccClientRequests         0
radiusAccClientRetransmissions  0
radiusAccClientResponses        0
radiusAccClientMalformedResponses 0
radiusAccClientBadAuthenticators 0
radiusAccClientPendingRequests  0
radiusAccClientTimeouts         0
radiusAccClientUnknownTypes     0
radiusAccClientPacketsDropped   0

Zxxx0:admin#
```

## 6.29. config accounting service

### ● Description

This command is used to configure the state of the specified RADIUS accounting service.

### ● Format

**config accounting service [network | shell | system] state [enable | disable]**

### ● Parameters

|                |                                                                                                                                                                                                                                                                              |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>network</b> | Specify the accounting service for 802.1X port access control. By default, the service is disabled.                                                                                                                                                                          |
| <b>shell</b>   | Specify the accounting service for shell events. When a user logs in or logouts of the Switching Hub (via the console, Telnet, or SSH) and when timeout occurs, accounting information will be collected and sent to the RADIUS server. By default, the service is disabled. |
| <b>system</b>  | Specify the accounting service for system events: reset and reboot. By default, the service is disabled.                                                                                                                                                                     |
| <b>state</b>   | Specify the state of the accounting service.<br><b>enable</b><br>Enable the specified accounting service.<br><b>disable</b><br>Disable the specified accounting service.                                                                                                     |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To configure the state of the RADIUS accounting service shell to enable:

```
Zxxx0:admin# config accounting service shell state enable
Command: config accounting service shell state enable

Success

Zxxx0:admin#
```

## **6.30. show accounting service**

---

- **Description**

This command is used to display RADIUS accounting service information.

- **Format**

**show accounting service**

- **Parameters**

None.

- **Restrictions**

None.

- **Example**

To display accounting service information:

```
Zxxx0:admin#show accounting service
Command: show accounting service

Accounting State
-----
Network : Disabled
Shell   : Disabled
System  : Disabled

Zxxx0:admin#
```

# 7. Access Control List (ACL) Commands

For network security protection, blocking unauthorized access from internal and external sources is important.

Access Control is a function to filter packet transfer by setting rules after checking the header information of packets that reach the Switching Hub. To use the Access Control function, you need to create an Access Control List (ACL), which defines filtering targets, conditions, and actions, and configure target ports and VLANs.

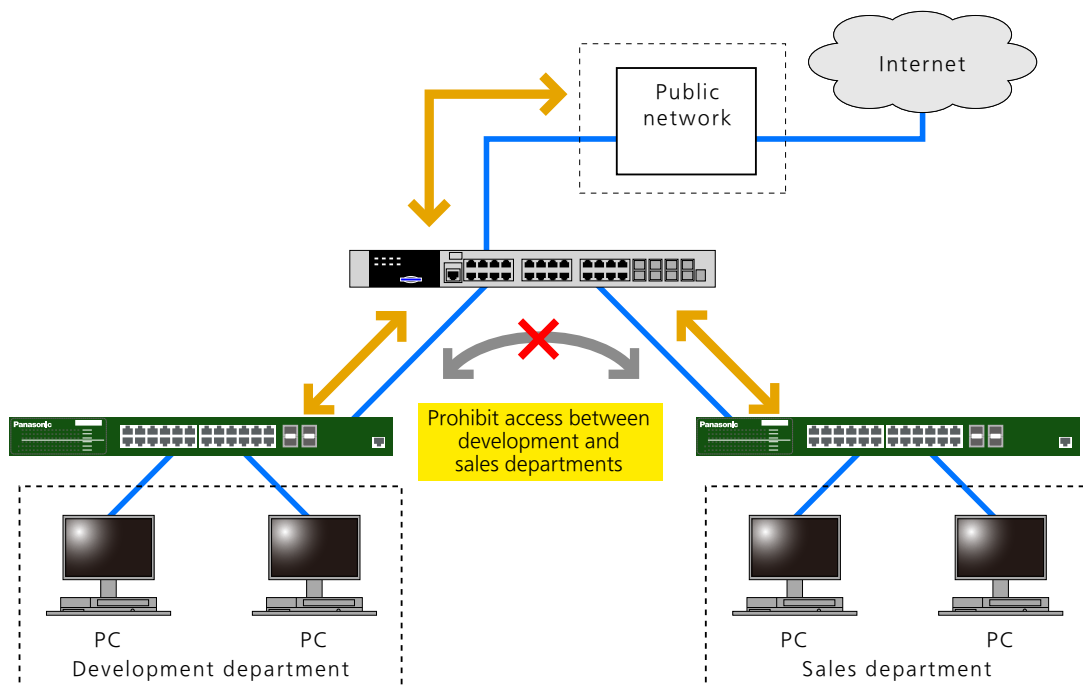


Figure 7-1 Access Control overview

## ● Access List Profile

This Switching Hub allows you to create an ACL named as "access list profile" with IDs 1 to 6.

In a profile, you can configure filtering targets from the following various categories.

- IEEE 802.1p priority
- VLAN name, VLAN number
- MAC address
- Ether type
- IP address
- DSCP (Differentiated Services Code Point)

- Protocol type
- TCP/UDP port number
- IPv6 traffic class, flow label
- Any packet contents (specified with the packet byte offset and mask, up to four contents)

In addition, you can create rules that define packet detail information and filtering actions with IDs 1 to 256 for each profile.

---

**NOTE** Profiles and rules are applied in the order starting from the lowest ID number.

---

You can also set the range of time to change rules applied according to the date and time or day of the week.

---

**NOTE** To use the range of time, you need to correctly adjust the internal clock of the Switching Hub. For the settings, refer to the sections in "75. Time and SNTP Commands."

---

### ● Applicable actions

The following actions can be applied to packets that match the rules.

- Permit: Start transferring.

---

**NOTE** IEEE 802.1p priority, DSCP, and output packet IP priority can also be changed.

---

- Deny: Discard without transmitting.
- Mirror: Copy packets and transfer them to a mirroring port set separately.

---

**NOTE** For the mirroring settings, refer to the sections in "Mirror Commands."

---

- Counter: Record the number of packets that match.

### ● Flow Meter

The function filters according to the number of bytes in a target packet. It allows you to configure the thresholds of bandwidth and number of bytes and then apply actions, such as transfer or discard, depending on whether the number of bytes in a packet is within the threshold or not.

## 7. Access Control List (ACL) Commands

---

```
create access_profile profile_id <value 1-6> profile_name <name 1-32> [ethernet {vlan {<hex 0x0-0x0fff>} | source_mac <macmask 000000000000-ffffffff> | destination_mac <macmask 000000000000-ffffffff> | 802.1p | ethernet_type}{1) | ip {vlan {<hex 0x0-0x0fff>} | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]] | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}}}(1) | packet_content_mask {offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>}(1) | ipv6 {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> | [tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | icmp {type | code}]]}(1)]

delete access_profile [profile_id <value 1-6> | profile_name <name 1-32> | all]

config access_profile [profile_id <value 1-6> | profile_name <name 1-32>] [add access_id [auto_assign | <value 1-256>] [ethernet {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_mac <macaddr> {mask <macmask>} | destination_mac <macaddr> {mask <macmask>} | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>}(1) | ip {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_ip <ipaddr> {mask <netmask>} | destination_ip <ipaddr> {mask <netmask>} | dscp <value 0-63> | [icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>} | flag [all | {urg | ack | psh | rst | syn | fin}]] | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}}}(1) | packet_content {offset_chunk_1 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_2 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_3 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_4 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}}}(1) | ipv6 {class <value 0-255> | flowlabel <hex 0x0-0xffff> | source_ipv6 <ipv6addr> {mask <ipv6mask>} | destination_ipv6 <ipv6addr> {mask <ipv6mask>} | [tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | icmp {type <value 0-255> | code <value 0-255>}}}(1)] [port [<portlist> | all] | vlan_based [vlan <vlan_name 32> | vlan_id <vlanid 1-4094>]] [permit {priority <value 0-7> {replace_priority} | [replace_dscp_with <value 0-63> | replace_tos_precedence_with <value 0-7>] | counter [enable | disable]} | mirror {group_id <value 1-4>} | deny] {time_range <range_name 32>} | delete access_id <value 1-256>]

show access_profile {[profile_id <value 1-6> | profile_name <name 1-32>]}

config time_range <range_name 32> [hours start_time <time hh:mm:ss> end_time <time hh:mm:ss> weekdays <daylist> | delete]

show time_range

show current_config access_profile

config flow_meter [profile_id <value 1-6> | profile_name <name 1-32>] access_id <value 1-256> [rate [<value 0-1048576>] {burst_size [<value 0-131072>]} rate_exceed [drop_packet | remark_dscp <value 0-63>] | tr_tcm cir <value 0-1048576> {cbs <value 0-131072>} pir <value 0-1048576> {pbs <value 0-131072>} {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | sr_tcm cir <value 0-1048576> cbs <value 0-131072> ebs <value 0-131072> {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | delete]
```

---

---

```
show flow_meter {[profile_id <value 1-6> | profile_name <name 1-32>] {access_id <value 1-256>}}
```

---

## 7.1. create access\_profile profile\_id

---

### ● Description

This command is used to create access list profiles.

### ● Format

```
create access_profile profile_id <value 1-6> profile_name <name 1-32> [ethernet {vlan
{<hex 0x0-0x0fff>} | source_mac <macmask 000000000000-ffffffffffff> |
destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type}{1) |
ip {vlan {<hex 0x0-0x0fff>} | source_ip_mask <netmask> | destination_ip_mask
<netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-
0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn |
fin}]] | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} |
protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}}](1) |
packet_content_mask {offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> |
offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_3 <value 0-31> <hex
0x0-0xffffffff> | offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>}(1) | ipv6 {class |
flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> | [tcp
{src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp
{src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | icmp {type |
code}}](1)]
```

### ● Parameters

---

**<value 1-6>**

Specify the profile ID between 1 and 6. The lower the profile ID, the higher the priority.

---

**profile\_name**

Specify a profile name.

**<name 1-32>**

The maximum length is 32 characters.

---

## 7. Access Control List (ACL) Commands

---

**ethernet** Specify an Ethernet access control list rule.

**vlan** Specify a VLAN mask. Only the last 12 bits of the mask will be considered.

**<hex 0x0-0x0fff>**

(Optional) Specify a VLAN mask.

**source\_mac**

Specify the source MAC mask.

**<macmask 000000000000-ffffffffffff>**

Specify the source MAC mask.

**destination\_mac**

Specify the destination MAC mask.

**<macmask 000000000000-ffffffffffff>**

Specify the destination MAC mask.

**802.1p**

Specify the 802.1p priority tag mask.

**ethernet\_type**

Specify the Ethernet type.

---

---

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ip</b>                  | Specify an IP access control list rule.                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>vlan</b>                | Specify a VLAN mask. Only the last 12 bits of the mask will be considered.<br><hex 0x0-0x0fff> - (Optional) Specify a VLAN mask.                                                                                                                                                                                                                                                                                                                                      |
| <b>source_ip_mask</b>      | Specify an IP source submask.<br><netmask><br>Specify an IP source submask.                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>destination_ip_mask</b> | Specify an IP destination submask.<br><netmask><br>Specify an IP destination submask.                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>dscp</b>                | Specify the DSCP mask.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>icmp</b>                | Specify that the rule applies to ICMP traffic.<br><b>type</b> (Optional) Specify the ICMP packet type.<br><b>code</b> (Optional) Specify the ICMP code.                                                                                                                                                                                                                                                                                                               |
| <b>igmp</b>                | Specify that the rule applies to IGMP traffic.<br><b>type</b> (Optional) Specify the IGMP packet type.<br><b>tcp</b> Specify that the rule applies to TCP traffic.                                                                                                                                                                                                                                                                                                    |
| <b>src_port_mask</b>       | (Optional) Specify the TCP source port mask.<br><hex 0x0-0xffff><br>Specify the TCP source port mask.                                                                                                                                                                                                                                                                                                                                                                 |
| <b>dst_port_mask</b>       | (Optional) Specify the TCP destination port mask.<br><hex 0x0-0xffff><br>Specify the TCP destination port mask.                                                                                                                                                                                                                                                                                                                                                       |
| <b>flag_mask</b>           | (Optional) Specify the TCP flag field mask.<br><b>all</b> Specify to check all parameters below.<br><b>urg</b> (Optional) Specify Urgent Pointer field significant.<br><b>ack</b> (Optional) Specify Acknowledgment field significant.<br><b>psh</b> (Optional) Specify Push Function.<br><b>rst</b> (Optional) Specify to reset the connection.<br><b>syn</b> (Optional) Specify to synchronize sequence numbers.<br><b>fin</b> (Optional) No more data from sender. |
| <b>udp</b>                 | Specify that the rule applies to UDP traffic.<br><b>src_port_mask</b><br>(Optional) Specify the TCP source port mask.<br><hex 0x0-0xffff><br>Specify the TCP source port mask.<br><b>dst_port_mask</b><br>(Optional) Specify the TCP destination port mask.<br><hex 0x0-0xffff><br>Specify the TCP destination port mask.                                                                                                                                             |
| <b>protocol_id_mask</b>    | Specify that the rule applies to the IP protocol ID traffic.<br><hex 0x0-0xff><br>Specify that the rule applies to the IP protocol ID traffic.                                                                                                                                                                                                                                                                                                                        |
| <b>user_define_mask</b>    | (Optional) Specify the L4 part mask.<br><hex 0x0-0xffffffff><br>Specify the L4 part mask.                                                                                                                                                                                                                                                                                                                                                                             |

---



## 7. Access Control List (ACL) Commands

---

### **packet\_content\_mask**

A maximum of four offsets can be specified. Each offset defines one byte of data which is identified as a single UDF field. The offset reference is also configurable. It can be defined to start at the end of the tag, the end of the Ethernet type, or the end of the IP header.

#### **offset\_chunk\_1**

Specifies the offset chunk 1 that allows users to examine the specified offset\_chunks within a packet at one time and specifies the frame content offset and mask.

**<value 0-31>**

Enter the offset chunk 1 value here. This value must be between 0 and 31.

**<hex 0x0-0xffffffff>**

Enter the offset chunk 1 mask value here.

#### **offset\_chunk\_2**

Specifies the offset chunk 2 that allows users to examine the specified offset\_chunks within a packet at one time and specifies the frame

**<value 0-31>**

Enter the offset chunk 2 value here. This value must be between 0 and 31.

**<hex 0x0-0xffffffff>**

Enter the offset chunk 2 mask value here.

#### **offset\_chunk\_3**

Specifies the offset chunk 3 that allows users to examine the specified offset\_chunks within a packet at one time and specifies the frame content offset and mask.

**<value 0-31>**

Enter the offset chunk 3 value here. This value must be between 0 and 31.

**<hex 0x0-0xffffffff>**

Enter the offset chunk 3 mask value here.

#### **offset\_chunk\_4**

Specifies the offset chunk 4 that allows users to examine the specified offset\_chunks within a packet at one time and specifies the frame content offset and mask.

**<value 0-31>**

Enter the offset chunk 4 value here. This value must be between 0 and 31.

**<hex 0x0-0xffffffff>**

Enter the offset chunk 4 mask value here.

---

---

|                              |                                                                                                                 |
|------------------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>ipv6</b>                  | <b>Specify the IPv6 filtering mask.</b>                                                                         |
| <b>class</b>                 | Specify the IPv6 class mask.                                                                                    |
| <b>flowlabel</b>             | Specify the IPv6 flow label mask.                                                                               |
| <b>source_ipv6_mask</b>      | Specify the IPv6 source IP mask.<br><ipv6mask><br>Specify the IPv6 source IP mask.                              |
| <b>destination_ipv6_mask</b> | Specify the IPv6 destination IP mask.<br><ipv6mask><br>Specify the IPv6 destination IP mask.                    |
| <b>tcp</b>                   | Specify that the rule applies to TCP traffic.                                                                   |
| <b>src_port_mask</b>         | (Optional) Specify the TCP source port mask.<br><hex 0x0-0xffff><br>Specify the TCP source port mask.           |
| <b>dst_port_mask</b>         | (Optional) Specify the TCP destination port mask.<br><hex 0x0-0xffff><br>Specify the TCP destination port mask. |
| <b>udp</b>                   | Specify that the rule applies to UDP traffic.                                                                   |
| <b>src_port_mask</b>         | (Optional) Specify the TCP source port mask.<br><hex 0x0-0xffff><br>Specify the TCP source port mask.           |
| <b>dst_port_mask</b>         | (Optional) Specify the TCP destination port mask.<br><hex 0x0-0xffff><br>Specify the TCP destination port mask. |
| <b>icmp</b>                  | Specify that the rule applies to ICMP traffic.                                                                  |
| <b>type</b>                  | (Optional) Specify the ICMP packet type.                                                                        |
| <b>code</b>                  | (Optional) Specify the ICMP code.                                                                               |

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## 7. Access Control List (ACL) Commands

### ● Example

To create access list profiles:

```
Zxxx0:admin#create access_profile profile_id 1 profile_name 1 ethernet vlan
source_mac FF-FF-FF-FF-FF-FF destination_mac 00-00-00-FF-FF-FF 802.1p
ethernet_type
Command: create access_profile profile_id 1 profile_name 1 ethernet vlan source_mac
FF-FF-FF-FF-FF-FF destination_mac 00-00-00-FF-FF-FF 802.1p ethernet_type

Success.

Zxxx0:admin#

Zxxx0:admin#create access_profile profile_id 2 profile_name 2 ip vlan
source_ip_mask 255.255.255.255 destination_ip_mask 255.255.255.0 dscp icmp
Command: create access_profile profile_id 2 profile_name 2 ip vlan source_ip_mask
255.255.255.255 destination_ip_mask 255.255.255.0 dscp icmp

Success.

Zxxx0:admin#
```

## 7.2. delete access\_profile

### ● Description

This command is used to delete access list profiles.

### ● Format

**delete access\_profile [profile\_id <value 1-6> | profile\_name <name 1-32> | all]**

### ● Parameters

---

**profile\_id**

Specify the index of the access list profile.

**<value 1-6>**

Specify the index of the access list profile. Enter a value between 1 and 6.

---

**profile\_name**

Specify the profile name.

**<name 1-32>**

Specify the profile name. The maximum length is 32 characters.

---

**all**

Specify the whole access list profile to delete.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To delete access list profiles:

```
Zxxx0:admin#delete access_profile profile_id 1
Command: delete access_profile profile_id 1

Success.

Zxxx0:admin#
```

## 7.3. config access\_profile

### ● Description

This command is used to configure access list entries.

### ● Format

```
config access_profile [profile_id <value 1-6> | profile_name <name 1-32>] [add
access_id [auto_assign | <value 1-256>] [ethernet {[vlan <vlan_name 32> | vlan_id
<vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_mac <macaddr> {mask
<macmask>} | destination_mac <macaddr> {mask <macmask>} | 802.1p <value 0-7> |
ethernet_type <hex 0x0-0xffff>}(1) | ip {[vlan <vlan_name 32> | vlan_id <vlanid 1-
4094>] {mask <hex 0x0-0x0fff>} | source_ip <ipaddr> {mask <netmask>} |
destination_ip <ipaddr> {mask <netmask>} | dscp <value 0-63> | [icmp {type <value 0-
255> | code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-
65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>} |
flag [all | {urg | ack | psh | rst | syn | fin}}] | udp {src_port <value 0-65535> {mask
<hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}}] | protocol_id
<value 0-255> {user_define <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}}](1) |
packet_content {offset_chunk_1 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} |
offset_chunk_2 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_3 <hex
0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_4 <hex 0x0-0xffffffff>
{mask <hex 0x0-0xffffffff>}}(1) | ipv6 {class <value 0-255> | flowlabel <hex 0x0-
0xffff> | source_ipv6 <ipv6addr> {mask <ipv6mask>} | destination_ipv6 <ipv6addr>
{mask <ipv6mask>} | [tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} |
dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | udp {src_port <value 0-65535>
{mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}}] | icmp
{type <value 0-255> | code <value 0-255>}}](1) [port [<portlist> | all] | vlan_based
[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>]] [permit {priority <value 0-7>
{replace_priority} | [replace_dscp_with <value 0-63> | replace_tos_precedence_with
<value 0-7>] | counter [enable | disable]] | mirror {group_id <value 1-4>} | deny]
{time_range <range_name 32>} | delete access_id <value 1-256>]
```

## 7. Access Control List (ACL) Commands

### ● Parameters

---

**profile\_id**

Specify the index of the access list profile.

**<value 1-6>**

Specify the value between 1 and 6.

---

**profile\_name**

Specify the profile name.

**<name 1-32>**

Specify the profile name. The maximum length is 32 characters.

---

**add access\_id**

Specify the index of the access list entry. The lower the access ID, the higher the priority.

**auto\_assign**

Specify to automatically assign the access ID.

**<value 1-256>**

Specify a value between 1 and 256.

---

**ethernet** Specify an Ethernet access control list rule.

**vlan** Specify the VLAN name.

**<vlan\_name 32>**

Specify the VLAN name. The maximum length is 32 characters.

**vlanid** Specify the VLAN ID.

**<vlanid 1-4094>**

**Specify the VLAN ID between 1 and 4094.**

**mask** (Optional) Specify the mask.

**<hex 0x0-0x0fff>**

Specify the mask.

**source\_mac**

Specify the source MAC address.

**<macaddr>**

**Specify the source MAC address.**

**mask** (Optional) Specify the mask.

**<macmask>**

Specify the mask.

**destination\_mac**

Specify the destination MAC address.

**<macaddr>**

Specify the destination MAC address.

**mask** (Optional) Specify the mask.

**<macmask>**

Specify the mask.

**802.1p**

Specify the value of the 802.1p priority tag.

**<value 0-7>**

Specify the value of the 802.1p priority tag. The priority tag ranges from 1 to 7.

**ethernet\_type**

Specify the Ethernet type.

**<hex 0x0-0xffff>**

Specify the Ethernet type.

---

---

|                       |                                                                                                                                                   |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ip</b>             | Specify an IP access control list rule.                                                                                                           |
| <b>vlan</b>           | Specify the VLAN name.<br><b>&lt;vlan_name 32&gt;</b><br>Specify the VLAN name. The maximum length is 32 characters.                              |
| <b>vlanid</b>         | Specify the VLAN ID.<br><b>&lt;vlanid 1-4094&gt;</b><br>Specify the VLAN ID between 1 and 4094.                                                   |
| <b>mask</b>           | (Optional) Specify the mask.<br><b>&lt;hex 0x0-0x0fff&gt;</b><br>Specify the mask.                                                                |
| <b>source_ip</b>      | Specify an IP source address.<br><b>&lt;ipaddr&gt;</b><br>Specify an IP source address.                                                           |
| <b>mask</b>           | (Optional) Specify the mask.<br><b>&lt;netmask&gt;</b><br>Specify the mask.                                                                       |
| <b>destination_ip</b> | Specify an IP destination address.<br><b>&lt;ipaddr&gt;</b><br>Specify an IP destination address.                                                 |
| <b>mask</b>           | (Optional) Specify the mask.<br><b>&lt;netmask&gt;</b><br>Specify the mask.                                                                       |
| <b>dscp</b>           | Specify the value of DSCP.<br><b>&lt;value 0-63&gt;</b><br>Specify the value of DSCP. The DSCP value ranges from 0 to 63.                         |
| <b>icmp</b>           | Specify the ICMP.                                                                                                                                 |
| <b>type</b>           | (Optional) Specify that the rule will apply to the ICMP Type traffic value.<br><b>&lt;value 0-255&gt;</b><br>Specify the value between 0 and 255. |
| <b>code</b>           | (Optional) Specify that the rule will apply to the ICMP Code traffic value.<br><b>&lt;value 0-255&gt;</b><br>Specify the value between 0 and 255. |
| <b>igmp</b>           | Specify the IGMP.                                                                                                                                 |
| <b>type</b>           | (Optional) Specify that the rule will apply to the IGMP Type traffic value.<br><b>&lt;value 0-255&gt;</b><br>Specify the value between 0 and 255. |
| <b>tcp</b>            | Specify TCP.                                                                                                                                      |

## 7. Access Control List (ACL) Commands

### **src\_port**

(Optional) Specify that the rule will apply to a range of TCP source ports.

**<value 0-65535>**

Specify the value between 0 and 65535.

**mask** (Optional) Specify the mask.

**<hex 0x0-0xffff>**

Specify the mask.

### **dst\_port**

(Optional) Specify that the rule will apply to a range of TCP destination ports.

**<value 0-65535>**

Specify the value between 0 and 65535.

**mask** (Optional) Specify the mask.

**<hex 0x0-0xffff>**

Specify the mask.

**flag** Specify the TCP flag field value.

**all** Specify to check all parameters below.

**urg** (Optional) Specify Urgent Pointer field significant.

**ack** (Optional) Specify Acknowledgment field significant.

**psh** (Optional) Specify Push Function.

**rst** (Optional) Specify to reset the connection.

**syn** (Optional) Specify to synchronize sequence numbers.

**fin** (Optional) No more data from sender.

**udp** Specify UDP.

### **src\_port**

(Optional) Specify the UDP source port range.

**<value 0-65535>**

Specify the value between 0 and 65535.

**mask** (Optional) Specify the mask.

**<hex 0x0-0xffff>**

Specify the mask.

### **dst\_port**

(Optional) Specify the UDP destination port range.

**<value 0-65535>**

Specify the value between 0 and 65535.

**mask** (Optional) Specify the mask.

**<hex 0x0-0xffff>**

Specify the mask.

### **protocol\_id**

Specify that the rule will apply to the value of IP protocol ID traffic.

**<value 0-255>**

Specify the value between 0 and 255.

### **user\_define**

(Optional) Specify that the rule will apply to the IP protocol ID and that the mask options behind the IP header, which has a length of 4 bytes.

**<hex 0x0-0xffffffff>**

Specify that the rule will apply to the IP protocol ID and that the mask options behind the IP header, which has a length of 4 bytes.

**mask** (Optional) Specify the mask.

**<hex 0x0-0xffffffff>**

Specify the mask.

---

**packet\_content**

Specify the packet content for the user defined mask.

**offset\_chunk\_1**

Specifies the contents of the offset trunk 1 to be monitored.

<hex 0x0-0xffffffff>

Enter the contents of the offset trunk 1 to be monitored here.

**mask** Specifies an additional mask for each field.

<hex 0x0-0xffffffff>

Enter the additional mask value used here.

**offset\_chunk\_2**

Specifies the contents of the offset trunk 2 to be monitored.

<hex 0x0-0xffffffff>

Enter the contents of the offset trunk 2 to be monitored here.

**mask** Specifies an additional mask for each field.

<hex 0x0-0xffffffff>

Enter the additional mask value used here.

**offset\_chunk\_3**

Specifies the contents of the offset trunk 3 to be monitored.

<hex 0x0-0xffffffff>

Enter the contents of the offset trunk 3 to be monitored here.

**mask** Specifies an additional mask for each field.

<hex 0x0-0xffffffff>

Enter the additional mask value used here.

**offset\_chunk\_4**

Specifies the contents of the offset trunk 4 to be monitored.

<hex 0x0-0xffffffff>

Enter the contents of the offset trunk 4 to be monitored here.

**mask** Specifies an additional mask for each field.

<hex 0x0-0xffffffff>

Enter the additional mask value used here.

---

**ipv6**

Specify that the rule applies to IPv6 fields.

**class** Specify the value of the IPv6 class.

<value 0-255>

Specify the value between 0 and 255.

**flowlabel**

Specify the value of the IPv6 flow label.

<hex 0x0-0xffff>

Specify the value of the IPv6 flow label.

**source\_ipv6**

Specify the value of the IPv6 source address.

<ipv6addr>

Specify the value of the IPv6 source address.

**mask** (Optional) Specify the mask.

<ipv6mask>

Specify the mask.

**destination\_ipv6**

Specify the value of the IPv6 destination address.

<ipv6addr>

Specify the value of the IPv6 destination address.

**mask** (Optional) Specify the mask.

<ipv6mask>

Specify the mask.



## 7. Access Control List (ACL) Commands

**tcp** Specify TCP.

**src\_port**

(Optional) Specify the TCP source port range.

**<value 0-65535>**

Specify the value between 0 and 65535.

**mask** (Optional) Specify the mask.

**<hex 0x0-0xffff>**

Specify the mask.

**dst\_port**

(Optional) Specify the TCP destination port range.

**<value 0-65535>**

Specify the value between 0 and 65535.

**mask** (Optional) Specify the mask.

**<hex 0x0-0xffff>**

Specify the mask.

**udp** Specify UDP.

**src\_port**

(Optional) Specify the UDP source port range.

**<value 0-65535>**

Specify the value between 0 and 65535.

**mask** (Optional) Specify the mask.

**<hex 0x0-0xffff>**

Specify the mask.

**dst\_port**

(Optional) Specify the UDP destination port range.

**<value 0-65535>**

Specify the value between 0 and 65535.

**mask** Specify the mask.

**<hex 0x0-0xffff>**

Specify the mask.

**icmp** Specifies that the rule applies to the value of ICMP traffic.

**type** Specifies that the rule applies to the value of ICMP type traffic.

**<value 0-255>**

Enter the ICMP type value used here. This value must be between 0 and 255.

**code** Specifies that the rule applies to the value of ICMP code traffic.

**<value 0-255>**

Enter the ICMP code value used here. This value must be between 0 and 255.

---

**port** The access profile rule may be defined for each port on the Switching Hub. The port list is specified by listing the lowest Switching Hub number and the beginning port number on that Switching Hub, separated by a colon.

**<portlist>**

Specify a list of ports.

**all** Specify that the access rule will apply to all ports.

---

## 7. Access Control List (ACL) Commands

---

### **vlan\_based**

Specify the VLAN-based ACL rule. There are two conditions: this rule will apply to all ports and packets must belong to the configured VLAN. It can be specified by VLAN name or VLAN ID.

**vlan** Specify the VLAN name.

**<vlan\_name 32>**

Specify the VLAN name. The maximum length is 32 characters.

**vlan\_id**

Specify the VLAN ID.

**<vlanid 1-4094>**

Specify the VLAN ID between 1 and 4094.

---

**permit** Specify the packets that match the access profile are permit by the Switching Hub.

---

**priority** (Optional) Specify the packets that match the access profile are remap the 802.1p priority tag field by the Switching Hub.

**<value 0-7>**

Specify the value between 0 and 7.

---

### **replace\_priority**

(Optional) Specify the packets that match the access profile remarking the 802.1p priority tag field by the Switching Hub.

---

### **replace\_dscp\_with**

(Optional) Specify the DSCP of the packets that match the access profile are modified according to the value.

**<value 0-63>**

Specify the value between 0 and 63.

---

### **replace\_tos\_precedence\_with**

(Optional) Specify that the IP precedence of the outgoing packet is changed with the new value. If used without an action priority, the packet is sent to the default TC.

**<value 0-7>**

Specify the value between 0 and 7.

---

**counter** (Optional) Specifies whether the ACL counter feature will be enabled or disabled.

#### **enable**

Specify whether the ACL counter feature is enabled. If the rule is not bound with the flow meter, all matching packets are counted. If the rule is bound with the flow meter, then the "counter" is overridden.

#### **disable**

Specify whether the ACL counter feature is disabled. The default option is disabled.

---

**mirror** Specify that packets matching the access profile are copied to the mirror port.

---

### **group\_id**

Specifies the group ID used.

**<value 1-4>**

Enter the group ID used here. This value must be between 1 and 4.

---

**deny** Specify the packets that match the access profile are filtered by the Switching Hub.

---

### **time\_range**

(Optional) Specify the name of this time range entry.

**<range\_name 32>**

Specify the name of this time range entry. The maximum length is 32 characters.

---

### **delete access\_id**

Specify to delete the access ID.

**<value 1-256>**

Specify the value between 1 and 256.

---

## 7. Access Control List (ACL) Commands

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure an access list entry:

```
Zxxx0:admin#config access_profile profile_id 1 add access_id 1 ip vlan default
source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp port 1 permit
Command: config access_profile profile_id 1 add access_id 1 ip vlan default
source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp port 1 permit
```

```
Success.
```

```
Zxxx0:admin#
```

## 7.4. show access\_profile

---

### ● Description

This command is used to display the current access list table.

### ● Format

show access\_profile {[profile\_id <value 1-6> | profile\_name <name 1-32>]}

### ● Parameters

---

#### profile\_id

(Optional) Specify the index of the access list profile.

<value 1-6>

Specify the profile ID between 1 and 6.

---

#### profile\_name

(Optional) Specify the name of the access list profile.

<name 1-32>

Specify the profile name between 1 and 32.

---

### ● Restrictions

None.

## ● Example

To display the current access list table:

```
Zxxx0:admin#show access_profile
Command: show access_profile

Access Profile Table

Total User Set Rule Entries : 3
Total Used HW Entries       : 19
Total Available HW Entries  : 1005
=====
Profile ID: 1      Profile Name: 1      Type: Ethernet
Mask on
  VLAN ID   : 0xFF
  Source MAC: FF-FF-FF-FF-FF-00
  802.1p
Available HW Entries: 254
-----
Rule ID : 1      Ports: 1-10
Match on:
  VLAN ID   : 2      Mask : 0xFFF
  Source MAC : 00-01-02-03-04-00
Action:
  Permit
  Replaced Priority to 2
  Replace DSCP to 33

Matched Count: 0 packets
-----
Rule ID : 256 (auto assign) Ports: -
Match on:
  VLAN ID   : 8
  Source MAC : 00-01-02-03-04-00
  802.1p
Action:
  Deny
=====
Profile ID: 3      Profile Name: 3      Type: IPv4
Mask on
  Source IP : 255.255.255.0
  TCP
  Source Port : 0x00FF
Available HW Entries: 254
-----
Rule ID : 4      Ports: 1-28
Match on:
  Source IP : 192.168.1.0
  TCP
Source Port: 210      Mask : 0x0FFF
Action:
  Mirror
=====
```

## 7. Access Control List (ACL) Commands

```
Profile ID: 2   Profile Name: IMPBv4

Mask
  Source MAC : FF-FF-FF-FF-FF-FF
  Source IP  : 255.255.255.255
Consumed HW Entries: 2
-----
Rule ID : 1      Ports: 1
Match on
  Source MAC : 00-05-04-03-02-01   Mask : FF-FF-FF-FF-FF-FF
  Source IP  : 10.10.10.1           Mask : 255.255.255.255
Action:
  Permit
-----
-
Rule ID : 2      Ports: 1
Match on
  Any
Action:
  Deny
=====
Profile ID: 3   Profile Name: VLAN Counter
Consumed HW Entries: 9

Profile ID: 4   Profile Name: System
Consumed HW Entries: 4

Zxxx0:admin#
```

### NOTE

"Total User Set Entries" indicates the total number of ACL rules created by the user. "Total Used HW Entries" indicates the total number of hardware entries used in the device. "Available HW Entries" indicates the total number of available hardware entries in the device.

## 7. Access Control List (ACL) Commands

To display an access profile that supports an entry mask for each rule:

```
Zxxx0:admin#show access_profile profile_id 2
Command: show access_profile profile_id 2

Access Profile Table

Profile ID: 2      Profile Name: 2      Type: Ethernet
Mask on
  VLAN           : 0xF
  Source MAC      : FF-FF-FF-00-00-00
  Destination MAC : 00-00-00-FF-FF-FF
Available HW Entries: 255
-----
Rule ID : 22      Ports: 1-7
Match on:
  VLAN ID         : 8                Mask : 0xFFFF
  Source MAC      : 00-01-02-03-04-05 Mask : FF-FF-FF-FF-FF-FF
  Destination MAC : 00-05-04-03-02-00 Mask : FF-FF-FF-FF-FF-00
Action:
  Deny

Zxxx0:admin#
```

To display the packet content mask profile for the profile with an ID of 5:

```
Zxxx0:admin#show access_profile profile_id 5
Command: show access_profile profile_id 5

Access Profile Table

=====
Profile ID: 5      Profile name: 5  Type: User Defined

MASK on
  offset_chunk_1 : 0      value : 0x0000FFFF

Available HW Entries : 256
=====

Zxxx0:admin#
```

### 7.5. **config time\_range**

---

#### ● Description

This command is used to define a specific range of time to activate a function on the Switch by specifying which time range in a day and which days in a week are covered in the time range. Note that the specified time range is based on SNTP time or configured time. If this time is not available, then the time range will not be met.

#### ● Format

**config time\_range** <range\_name 32> [ hours start\_time < hh:mm:ss> end\_time< hh:mm:ss> weekdays <daylist> | delete]

#### ● Parameters

---

**<range\_name 32>**

Specify the name of the time range settings.

---

**hours start\_time**

Specify the starting time in a day. (24-hr time). For example, 19:00 means 7PM. 19 is also acceptable. The start\_time must be smaller than the end\_time.

**< hh:mm:ss>**

Specify the time.

---

**end\_time**

Specify the ending time in a day. (24-hr time)

**< hh:mm:ss>**

Specify the time.

---

**weekdays**

Specify the list of days contained in the time range. Use a dash to define a period of days.

Use a comma to separate specific days. For example, mon-fri (Monday to Friday)

sun, mon, fri (Sunday, Monday, and Friday)

**<daylist>**

Specify a list of days.

---

**delete**

Delete a time range profile. When a time range profile has been associated with ACL entries, the deletion of this time range profile will fail.

---

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the range of time to activate a function on the Switching Hub:

```
Zxxx0:admin#config time_range testdaily hours start_time 12:0:0 end_time 13:0:0
weekdays mon,fri
Command: config time_range testdaily hours start_time 12:0:0 end_time 13:0:0
weekdays mon,fri

Success.

Zxxx0:admin#
```

## 7.6. show time\_range

---

### ● Description

This command is used to display current time range settings.

### ● Format

**show time\_range**

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display current time range setting:

```
Zxxx0:admin#show time_range
Command: show time_range

Time Range Information
-----
Range Name      : testdaily
Weekdays       : Mon,Fri
Start Time      : 12:00:00
End Time        : 13:00:00

Total Entries :1

Zxxx0:admin#
```



### 7.7. **show current\_config access\_profile**

---

#### ● Description

This command is used to display the ACL part of the current configuration, when logged in with user level privileges. The overall current configuration can be displayed by using the show config command, which is accessible with administrator level privileges.

#### ● Format

**show current\_config access\_profile**

#### ● Parameters

None.

#### ● Restrictions

None.

#### ● Example

To display the ACL part of the current configuration:

```
Zxxx0:admin#show current_config access_profile
Command: show current_config access_profile

#-----
# ACL
create access_profile Ethernet vlan profile_id 1
config access_profile profile_id 1 add access_id 1 ethernet vlan default port 1
permit

create access_profile ip source_ip_mask 255.255.255 profile_id 2
config access_profile profile_id 2 add access_id 1 ip source_ip 10.10.10.10 port 2
deny

#-----

Zxxx0:admin#
```

## 7.8. config flow\_meter

---

### ● Description

This command is used to configure the flow-based metering function. The metering function supports three modes: single rate two color, single rate three color, and two rate three color. The access rule must be created before the parameters of this function can be applied. For the single rate two color mode, users may set the preferred bandwidth for this rule, in Kbps, and once the bandwidth has been exceeded, overflowing packets will either be dropped or remarked DSCP, depending on the user configuration. For single rate three color mode, users need to specify the committed rate, in Kbps, the committed burst size, and the excess burst size. For the two rate three color mode, users need to specify the committed rate in Kbps, the committed burst size, the peak rate and the peak burst size. The green color packet will be treated as the conforming action, the yellow color packet will be treated as the exceeding action, and the red color packet will be treated as the violating action. The replace DSCP action can be performed on packets that conform (GREEN) and packets that do not conform (YELLOW and RED). If drop YELLOW/RED is selected, the action to replace the DSCP will not take effect. The color mapping for both "single rate three color" and "two rate three color" mode follow RFC 2697 and RFC 2698 in the color-blind situation.

### ● Format

```
config flow_meter [profile_id <value 1-6> | profile_name <name 1-32>] access_id
<value 1-256> [rate [<value 0-1048576>] {burst_size [<value 0-131072>]} rate_exceed
[drop_packet | remark_dscp <value 0-63>] | tr_tcm cir <value 0-1048576> {cbs <value
0-131072>} pir <value 0-1048576> {pbs <value 0-131072>} {[color_blind |
color_aware]}] {conform [permit | replace_dscp <value 0-63>] {counter [enable |
disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable |
disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable |
disable]} | sr_tcm cir <value 0-1048576> cbs <value 0-131072> ebs <value 0-131072>
{[color_blind | color_aware]}] {conform [permit | replace_dscp <value 0-63>] {counter
[enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter
[enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter
[enable | disable]} | delete]
```

## 7. Access Control List (ACL) Commands

### ● Parameters

|                     |                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>profile_id</b>   | Specify the index of the access list profile.<br><value 1-6><br>Specify the value between 1 and 6.                                                                                                                                                                                                                                                                                           |
| <b>profile_name</b> | Specify the name of the profile.<br><name 1-32><br>Specify the name of the profile. The maximum length is 32 characters.                                                                                                                                                                                                                                                                     |
| <b>access_id</b>    | Specify the index of the access list entry.<br><value 1-256><br>Specify the value between 1 and 256.                                                                                                                                                                                                                                                                                         |
| <b>rate</b>         | Specify the rate for single rate two color mode. Specify the committed bandwidth in Kbps for the flow.<br><value 0-1048576><br>Specify the value between 0 and 1048576.                                                                                                                                                                                                                      |
| <b>burst_size</b>   | (Optional) Specify the burst size for the single rate two color mode. The unit is Kbyte.<br><value 0-131072><br>Specify the value between 0 and 131072.                                                                                                                                                                                                                                      |
| <b>rate_exceed</b>  | Specify the action for packets that exceed the committed rate in single rate two color mode. The action can be specified as one of the following:<br><b>drop_packet</b><br>Drop the packet immediately.<br><b>remark_dscp</b><br>Mark the packet with a specified DSCP. The packet is set to drop for packets with a high precedence.<br><value 0-63><br>Specify the value between 0 and 63. |
| <b>tr_tcm</b>       | Specify the "two-rate three-color mode."                                                                                                                                                                                                                                                                                                                                                     |
| <b>cir</b>          | Specify the Committed Information Rate. The unit is Kbps. CIR should always be equal or less than PIR.<br><value 0-1048576><br>Specify the value between 0 and 1048576.                                                                                                                                                                                                                      |
| <b>cbs</b>          | (Optional) Specify the Committed Burst Size. The unit is Kbyte.<br><value 0-131072><br>Specify the value between 0 and 131072.                                                                                                                                                                                                                                                               |
| <b>pir</b>          | Specify the Peak information Rate. The unit is Kbps. PIR should always be equal to or greater than CIR.<br><value 0-1048576><br>Specify the value between 0 and 1048576.                                                                                                                                                                                                                     |
| <b>pbs</b>          | (Optional) Specify the Peak Burst Size. The unit is Kbyte.<br><value 0-131072><br>Specify the value between 0 and 131072.                                                                                                                                                                                                                                                                    |
| <b>color_blind</b>  | Specifies the meter mode as color-blind. The default is color-blind mode.                                                                                                                                                                                                                                                                                                                    |
| <b>color_aware</b>  | Specifies the meter mode as color-aware. The final color of the packet is determined by the initial color of the packet and the metering result.                                                                                                                                                                                                                                             |

---

**conform** (Optional) This field denotes the green packet flow. Green packet flows may have their DSCP field rewritten to a value stated in this field. Users may also choose to count green packets by using counter parameter.

**permit**

Enter this parameter to allow packet flows that are in the green flow.

**replace\_dscp**

Packets that are in the green flow may have their DSCP field rewritten using this parameter and entering the DSCP value to replace.

**<value 0-63>**

Specify the value between 0 and 63.

**counter**

(Optional) Use this parameter to enable or disable the packet counter for the specified ACL entry in the green flow.

**enable**

Enable the packet counter for the specified ACL entry in the green flow.

**disable**

Disable the packet counter for the specified ACL entry in the green flow.

---

**exceed** (Optional) This field denotes the yellow packet flow. Yellow packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field.

**permit**

Enter this parameter to allow packet flows that are in the yellow flow.

**replace\_dscp**

Specifies to change the DSCP of the packet.

**<value 0-63>**

Enter the replacement DSCP of the packet here. This value must be between 0 and 63.

**drop** Enter this parameter to drop packets that are in the yellow flow.

**counter**

(Optional) Use this parameter to enable or disable the packet counter for the specified ACL entry in the green flow.

**enable**

Enable the packet counter for the specified ACL entry in the green flow.

**disable**

Disable the packet counter for the specified ACL entry in the green flow.

---

**violate** This field denotes the red packet flow. Red packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field.

**permit**

Enter this parameter to allow packet flows that are in the red flow.

**replace\_dscp**

Specifies to change the DSCP of the packet.

**<value 0-63>**

Enter the replacement DSCP of the packet here. This value must be between 0 and 63.

**drop** Enter this parameter to drop packets that are in the red flow.

**counter**

(Optional) Use this parameter to enable or disable the packet counter for the specified ACL entry in the green flow.

**enable**

Enable the packet counter for the specified ACL entry in the green flow.

**disable**

Disable the packet counter for the specified ACL entry in the green flow.

---

## 7. Access Control List (ACL) Commands

---

|               |                                                                                                                               |
|---------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>sr_tcm</b> | Specify the "single-rate three-color mode".                                                                                   |
| <b>cir</b>    | Specify the Committed Information Rate. The unit is in Kbps.<br><value 0-1048576><br>Specify the value between 0 and 1048576. |
| <b>cbs</b>    | Specify the Committed Burst Size. The unit is in Kbyte.<br><value 0-131072><br>Specify the value between 0 and 131072.        |
| <b>ebs</b>    | Specify the Excess Burst Size. The unit is Kbyte.<br><value 0-131072><br>Specify the value between 0 and 131072.              |

---

|                    |                                                                           |
|--------------------|---------------------------------------------------------------------------|
| <b>color_blind</b> | Specifies the meter mode as color-blind. The default is color-blind mode. |
|--------------------|---------------------------------------------------------------------------|

---

|                    |                                                                                                                                                  |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>color_aware</b> | Specifies the meter mode as color-aware. The final color of the packet is determined by the initial color of the packet and the metering result. |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|

---

|                     |                                                                                                                                                                                                                       |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>conform</b>      | (Optional) This field denotes the green packet flow. Green packet flows may have their DSCP field rewritten to a value stated in this field. Users may also choose to count green packets by using counter parameter. |
| <b>permit</b>       | Enter this parameter to allow packet flows that are in the green flow.                                                                                                                                                |
| <b>replace_dscp</b> | Packets that are in the green flow may have their DSCP field rewritten using this parameter and entering the DSCP value to replace.<br><value 0-63><br>Specify the value between 0 and 63.                            |
| <b>counter</b>      | (Optional) Use this parameter to enable or disable the packet counter for the specified ACL entry in the green flow.                                                                                                  |
| <b>enable</b>       | Enable the packet counter for the specified ACL entry in the green flow.                                                                                                                                              |
| <b>disable</b>      | Disable the packet counter for the specified ACL entry in the green flow.                                                                                                                                             |

---

|                     |                                                                                                                                                                                                                                                                     |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>exceed</b>       | (Optional) This field denotes the yellow packet flow. Yellow packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field. |
| <b>permit</b>       | Enter this parameter to allow packet flows that are in the yellow flow.                                                                                                                                                                                             |
| <b>replace_dscp</b> | Specifies to change the DSCP of the packet.<br><value 0-63><br>Enter the replacement DSCP of the packet here. This value must be between 0 and 63.                                                                                                                  |
| <b>drop</b>         | Enter this parameter to drop packets that are in the yellow flow.                                                                                                                                                                                                   |
| <b>counter</b>      | (Optional) Use this parameter to enable or disable the packet counter for the specified ACL entry in the green flow.                                                                                                                                                |
| <b>enable</b>       | Enable the packet counter for the specified ACL entry in the green flow.                                                                                                                                                                                            |
| <b>disable</b>      | Disable the packet counter for the specified ACL entry in the green flow.                                                                                                                                                                                           |

---

---

|                           |                                                                                                                                                                                                                                                    |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>violate</b>            | This field denotes the red packet flow. Red packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field. |
| <b>permit</b>             | Enter this parameter to allow packet flows that are in the red flow.                                                                                                                                                                               |
| <b>replace_dscp</b>       | Specifies to change the DSCP of the packet.                                                                                                                                                                                                        |
| <b>&lt;value 0-63&gt;</b> | Enter the replacement DSCP of the packet here. This value must be between 0 and 63.                                                                                                                                                                |
| <b>drop</b>               | Enter this parameter to drop packets that are in the red flow.                                                                                                                                                                                     |
| <b>counter</b>            | (Optional) Use this parameter to enable or disable the packet counter for the specified ACL entry in the green flow.                                                                                                                               |
| <b>enable</b>             | Enable the packet counter for the specified ACL entry in the green flow.                                                                                                                                                                           |
| <b>disable</b>            | Disable the packet counter for the specified ACL entry in the green flow.                                                                                                                                                                          |
| <b>delete</b>             | Use this parameter to delete the specified flow meter.                                                                                                                                                                                             |

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure a two rate, three color flow meter:

```
Zxxx0:admin#config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 200 pir
2000 pbs 200 conform replace_dscp 21 exceed drop violate permit
Command: config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 200 pir
2000 pbs 200 conform replace_dscp 21 exceed drop violate permit

Success.

Zxxx0:admin#
```

To replace DSCP action changed to perform on conform (green) and unconform (yellow and red) packets:

```
Zxxx0:admin# config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 200 pir
2000 pbs 200 exceed permit replace_dscp 21 violate permit replace_dscp 21
Command: config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 200 pir
2000 pbs 200 exceed permit replace_dscp 21 violate permit replace_dscp 21

Success.

Zxxx0:admin#
```

# 7.9. show flow\_meter

### ● Description

This command is used to display the flow meter table.

### ● Format

**show flow\_meter** {[profile\_id <value 1-6> | profile\_name <name 1-32>] {access\_id <value 1-256>}}

### ● Parameters

---

**profile\_id**(Optional) Specify the profile ID.  
    <value 1-6>

Specify the profile ID. Enter a value between 1 and 6.

---

**profile\_name**  
(Optional) Specify the name of the profile.  
    <name 1-32>

Specify the name of the profile. The maximum length is 32 characters.

---

**access\_id** (Optional) Specify the access ID.  
    <value 1-256>

Specify the access ID. Enter a value between 1 and 256.

---

### ● Restrictions

None.

### ● Example

To display the flow meter configuration:

```
Zxxx0:admin#show flow_meter
Command: show flow_meter

Flow Meter Information
-----
Profile ID:1      Access ID:1      Mode : trTCM / ColorBlind
CIR(Kbps):1000    CBS(Kbyte):200    PIR(Kbps):2000    PBS(Kbyte):200
Action:
    Conform : Permit          Counter: Disabled
    Exceed  : Permit          Counter: Disabled
    Violate  : Permit          Counter: Disabled
-----

Total Entries: 1

Zxxx0:admin#
```

## 8. Access Control List (ACL) Egress Command List

While "Access Control List (ACL) Commands" filter packets reaching the Switching Hub, these commands filter packets output from the Switching Hub.

For overview on filtering, refer to "Access Control List (ACL) Commands."

**NOTE** Up to 4 profiles and 128 rules per profile can be created.

You can create a port group and specify an ACL target with the group name and group ID.

```
create egress_access_profile profile_id <value 1-4> profile_name <name 1-32> [ethernet {vlan
  {<hex 0x0-0x0fff>} | source_mac <macmask 000000000000-ffffffff>} | destination_mac
  <macmask 000000000000-ffffffff>} | 802.1p | ethernet_type} | ip {vlan {<hex 0x0-
  0x0fff>} | source_ip_mask <netmask>} | destination_ip_mask <netmask>} | dscp | [icmp {type
  | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff>} | dst_port_mask <hex 0x0-
  0xffff>} | flag_mask [all | {urg | ack | psh | rst | syn | fin}]] | udp {src_port_mask <hex 0x0-
  0xffff>} | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff>
  {user_define_mask <hex 0x0-0xffffffff>}}] | ipv6 {class | source_ipv6_mask <ipv6mask>} |
  destination_ipv6_mask <ipv6mask>} | [tcp {src_port_mask <hex 0x0-0xffff>} | dst_port_mask
  <hex 0x0-0xffff>} | udp {src_port_mask <hex 0x0-0xffff>} | dst_port_mask <hex 0x0-0xffff>} |
  icmp {type | code}]]]
```

```
delete egress_access_profile [profile_id <value 1-4> | profile_name <name 1-32> | all]
```

```
config egress_access_profile [profile_id <value 1-4> | profile_name <name 1-32>] [add access_id
  [auto_assign | <value 1-128>] [ethernet { [vlan <vlan_name 32> | vlan_id <vlanid 1-4094>]
  {mask <hex 0x0-0x0fff>} | source_mac <macaddr> {mask <macmask>} | destination_mac
  <macaddr> {mask <macmask>} | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ip
  {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_ip
  <ipaddr> {mask <netmask>} | destination_ip <ipaddr> {mask <netmask>} | dscp <value 0-
  63> | [icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>} | tcp
  {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex
  0x0-0xffff>} | flag [all | {urg | ack | psh | rst | syn | fin}]] | udp {src_port <value 0-65535>
  {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | protocol_id
  <value 0-255> {user_define <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}}]]] | ipv6 {class
  <value 0-255> | source_ipv6 <ipv6addr> {mask <ipv6mask>} | destination_ipv6 <ipv6addr>
  {mask <ipv6mask>} | [tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port
  <value 0-65535> {mask <hex 0x0-0xffff>}} | udp {src_port <value 0-65535> {mask <hex 0x0-
  0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | icmp {type <value 0-255> |
  code <value 0-255>}}]]] [vlan_based [vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] |
  port_group [id <value 1-64> | name <name 16>] | port <port>] [permit {replace_priority_with
  <value 0-7> | replace_dscp_with <value 0-63> | counter [enable | disable]} | deny]
  {time_range <range_name 32>} | delete access_id <value 1-128>]
```

```
show egress_access_profile [[profile_id <value 1-4> | profile_name <name 1-32>]]
```

```
show current_config egress_access_profile
```



## 8. Access Control List (ACL) Egress Command List

---

```
config egress_flow_meter [profile_id <value 1-4> | profile_name <name 1-32>] access_id <value 1-128> [rate <value 0-1048576> {burst_size <value 0-131072>} rate_exceed [drop_packet | remark_dscp <value 0-63>] | tr_tcm cir <value 0-1048576> {cbs <value 0-131072>} pir <value 0-1048576> {pbs <value 0-131072>} {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63> | drop} {counter [enable | disable]} violate [permit {replace_dscp <value 0-63> | drop} {counter [enable | disable]} | sr_tcm cir <value 0-1048576> cbs <value 0-131072> ebs <value 0-131072> {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63> | drop} {counter [enable | disable]} violate [permit {replace_dscp <value 0-63> | drop} {counter [enable | disable]} | delete]
show egress_flow_meter {[profile_id <value 1-4> | profile_name <name 1-32>] {access_id <value 1-128>}}
create port_group id <value 1-64> name <name 16>
config port_group [id <value 1-64> | name <name 16>] [add | delete] [<portlist> | all]
delete port_group [id <value 1-64> | name <name 16>]
show port_group {id <value 1-64> | name <name 16>}
```

---

### 8.1. create egress\_access\_profile

---

#### ● Description

This command is used to create an egress access list profile. For example, for some hardware, it may be invalid to specify destination IPv6 address and source IPv6 address at the same time. The user will be prompted for these limitations.

#### ● Format

```
create egress_access_profile profile_id <value 1-4> profile_name <name 1-32>
[ethernet {vlan {<hex 0x0-0x0fff>} | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type} |
ip {vlan {<hex 0x0-0x0fff>} | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]] | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}}] | ipv6 {class | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> | [tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | icmp {type | code}}]]]
```

## ● Parameters

---

### **profile\_id**

Specifies the index of the egress access list profile. The lower the profile ID, the higher the priority.

**<value 1-4>**

Enter the profile ID used here. This value must be between 1 and 4.

---

### **profile\_name**

The name of the profile must be specified. The maximum length is 32 characters.

**<name 1-32>**

Enter the profile name used here. This name can be up to 32 characters long.

---

### **ethernet** Specifies this is an Ethernet mask.

**vlan** (Optional) Specifies a VLAN mask.

**<hex 0x0-0x0fff>**

Enter the VLAN mask used here.

### **source\_mac**

(Optional) Specifies the source MAC mask.

**<macmask 000000000000-ffffffffffff>**

Enter the source MAC mask used here.

### **destination\_mac**

(Optional) Specifies the destination MAC mask.

**<macmask 000000000000-ffffffffffff>**

Enter the destination MAC mask used here.

### **802.1p**

(Optional) Specifies 802.1p priority tag mask.

### **ethernet\_type**

(Optional) Specifies the Ethernet type mask.

---

## 8. Access Control List (ACL) Egress Command List

---

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ip</b>                  | Specifies this is an IPv4 mask.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>vlan</b>                | (Optional) Specifies a VLAN mask.<br><hex 0x0-0x0fff><br>Enter the VLAN mask used here.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>source_ip_mask</b>      | (Optional) Specifies a source IP address mask.<br><netmask><br>Enter the source network mask used here.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>destination_ip_mask</b> | (Optional) Enter the source network mask used here.<br><netmask><br>Enter the destination network mask used here.                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>dscp</b>                | (Optional) Specifies the DSCP mask.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>icmp</b>                | (Optional) Specifies that the rule applies to ICMP traffic.<br>type Specifies the type of ICMP traffic.<br>code Specifies the code of ICMP traffic.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>igmp</b>                | (Optional) Specifies that the rule applies to IGMP traffic.<br>type Specifies the type of IGMP traffic.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>tcp</b>                 | (Optional) Specifies that the rule applies to TCP traffic.<br><b>src_port_mask</b><br>Specifies the TCP source port mask.<br><hex 0x0-0xffff><br>Enter the TCP source port mask value here.<br><b>dst_port_mask</b><br>Specifies the TCP destination port mask.<br><hex 0x0-0xffff><br>Enter the TCP source port mask value here.                                                                                                                                                                                                                                                          |
| <b>flag_mask</b>           | (Optional) Specifies the TCP flag field mask.<br><b>all</b> Specifies that the TCP flag field mask will be set to 'all'.<br><b>urg</b> Specifies that the TCP flag field mask will be set to 'urg'.<br><b>ack</b> Specifies that the TCP flag field mask will be set to 'ack'.<br><b>psh</b> Specifies that the TCP flag field mask will be set to 'psh'.<br><b>rst</b> Specifies that the TCP flag field mask will be set to 'rst'.<br><b>syn</b> Specifies that the TCP flag field mask will be set to 'syn'.<br><b>fin</b> Specifies that the TCP flag field mask will be set to 'fin'. |
| <b>udp</b>                 | (Optional) Specifies that the rule applies to UDP traffic.<br><b>src_port_mask</b><br>Specifies the UDP source port mask.<br><hex 0x0-0xffff><br>Enter the UDP source port mask value here.<br><b>dst_port_mask</b><br>Specifies the UDP destination port mask.<br><hex 0x0-0xffff><br>Enter the UDP destination port mask value here.                                                                                                                                                                                                                                                     |
| <b>protocod_id_mask</b>    | (Optional) Specifies that the rule applies to IP protocol ID traffic.<br><hex 0x0-0xff><br>Enter the protocol ID mask value here.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>user_define_mask</b>    | (Optional) Specifies that the rule applies to the IP protocol ID, and that the mask option behind the IP header length is 20 bytes.<br><hex 0x0-0xffffffff><br>Enter the user-defined mask value here.                                                                                                                                                                                                                                                                                                                                                                                     |

---

---

|                              |                                                                                                                                  |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6</b>                  | (Optional) Specifies this is an IPv6 mask.                                                                                       |
| <b>class</b>                 | (Optional) Specifies the IPv6 class.                                                                                             |
| <b>source_ipv6_mask</b>      | (Optional) Specifies an IPv6 source sub-mask.<br><ipv6mask><br>Enter the IPv6 source sub-mask value here.                        |
| <b>destination_ipv6_mask</b> | Specifies an IPv6 destination sub-mask.<br><ipv6mask><br>Enter the IPv6 destination sub-mask value here.                         |
| <b>tcp</b>                   | (Optional) Specifies that the following parameter are application to the TCP configuration.                                      |
| <b>src_port_mask</b>         | Specifies an IPv6 Layer 4 TCP source port mask.<br><hex 0x0-0xffff><br>Enter the Ipv6 TCP source port mask value here.           |
| <b>dst_port_mask</b>         | Specifies an IPv6 Layer 4 TCP destination port mask.<br><hex 0x0-0xffff><br>Enter the Ipv6 TCP destination port mask value here. |
| <b>udp</b>                   | (Optional) Specifies that the following parameter are application to the UDP configuration.                                      |
| <b>src_port_mask</b>         | Specifies an IPv6 Layer 4 UDP source port mask.<br><hex 0x0-0xffff><br>Enter the Ipv6 UDP source port mask value here.           |
| <b>dst_port_mask</b>         | Specifies an IPv6 Layer 4 UDP destination port mask.<br><hex 0x0-0xffff><br>Enter the Ipv6 UDP destination port mask value here. |
| <b>icmp</b>                  | (Optional) Specifies that the rule applies to ICMP traffic.                                                                      |
| <b>type</b>                  | Specifies the type of ICMP traffic.                                                                                              |
| <b>code</b>                  | Specifies the code of ICMP traffic.                                                                                              |

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To create an egress access list profile with the name "eap-eth-bc" and assign the profile ID to be 1:

```
Zxxx0:admin# create egress_access_profile profile_id 1 profile_name eap-eth-bc
ethernet source_mac FF-FF-FF-FF-FF-FF
Command: create egress_access_profile profile_id 1 profile_name eap-eth-bc
ethernet source_mac FF-FF-FF-FF-FF-FF

Zxxx0:admin#
```

## 8.2. delete egress\_access\_profile

---

### ● Description

Delete egress access profile command can only delete the profile which is created by egress ACL module.

### ● Format

**delete egress\_access\_profile [profile\_id <value 1-4> | profile\_name <name 1-32> | all]**

### ● Parameters

---

**profile\_id**

Specifies the index of the egress access list profile.

**<value 1-4>**

Enter the profile ID used here. This value must be between 1 and 4.

---

**profile\_name**

Specifies the name of the profile. The maximum length is 32 characters.

**<name 1-32>**

Enter the profile name used here. This name can be up to 32 characters long.

**all** Specifies that the whole egress access list profile will be deleted.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete egress access list profile ID 1:

```
Zxxx0:admin# delete egress_access_profile profile_id 1
Command: delete egress_access_profile profile_id 1

Success.

Zxxx0:admin#
```

## 8.3. config egress\_access\_profile

### ● Description

This command is used to configure egress access list entries.

### ● Format

```
config egress_access_profile [profile_id <value 1-4> | profile_name <name 1-32>] [add
access_id [auto_assign | <value 1-128>] [ethernet {[vlan <vlan_name 32> | vlan_id
<vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_mac <macaddr> {mask
<macmask>} | destination_mac <macaddr> {mask <macmask>} | 802.1p <value 0-7> |
ethernet_type <hex 0x0-0xffff>} | ip {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>]
{mask <hex 0x0-0x0fff>} | source_ip <ipaddr> {mask <netmask>} | destination_ip
<ipaddr> {mask <netmask>} | dscp <value 0-63> | [icmp {type <value 0-255> | code
<value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> {mask
<hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>} | flag [all | {urg
| ack | psh | rst | syn | fin}}] | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>}
| dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | protocol_id <value 0-255>
{user_define <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}}}] | ipv6 {class <value 0-
255> | source_ipv6 <ipv6addr> {mask <ipv6mask>} | destination_ipv6 <ipv6addr>
{mask <ipv6mask>} | [tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} |
dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | udp {src_port <value 0-65535>
{mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | icmp
{type <value 0-255> | code <value 0-255>}}}] [vlan_based [vlan <vlan_name 32> |
vlan_id <vlanid 1-4094>] | port_group [id <value 1-64> | name <name 16>] | port
<port>] [permit {replace_priority_with <value 0-7> | replace_dscp_with <value 0-63> |
counter [enable | disable]} | deny] {time_range <range_name 32>} | delete access_id
<value 1-128>]
```

### ● Parameters

#### profile\_id

Specifies the index of the egress access list profile.

<value 1-4>

Enter the profile ID used here. This value must be between 1 and 4.

#### profile\_name

Specifies the name of the profile.

<name 1-32>

Enter the profile name here. This name can be up to 32 characters long.

#### add

Specifies to add a profile or rule.

#### access\_id

Specifies the index of the access list entry. If the auto\_assign option is selected, the access ID is automatically assigned. The lower the access ID, the higher the priority.

#### auto assign

Specifies that the access ID will be configured automatically.

<value 1-128>

Enter the access ID used here. This value must be between 1 and 128.

## 8. Access Control List (ACL) Egress Command List

---

### ethernet

Specifies an Ethernet egress ACL rule.

**vlan** (Optional) Specifies the VLAN name.

**<vlan\_name 32>**

Enter the VLAN name used for this configuration here. This name can be up to 32 characters long.

**vlanid** Specifies a VLAN ID.

**<vlanid 1-4094>**

Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.

**mask** (Optional) Specifies the mask used.

**<hex 0x0-x0fff>**

Enter the mask value used here.

**source\_mac**

(Optional) Specifies the source MAC address.

**<macaddr>**

Enter the source MAC address used here.

**mask** Specifies that source MAC mask used.

**<macmask>**

Enter the source MAC mask value here.

**destination\_mac**

Specifies the destination MAC address.

**<macaddr>**

Enter the destination MAC address used here.

**mask** Specifies that destination MAC mask used.

**<macmask>**

Enter the destination MAC mask value here.

**802.1p**

(Optional) Specifies the value of the 802.1p priority tag. The priority tag ranges from 1 to 7.

**<value 0-7>**

Enter the 802.1p priority tag used here.

**ethernet\_type**

(Optional) Specifies the Ethernet type.

**<hex 0x0-0xffff>**

Enter the Ethernet type mask used here.

---

### ip

Specifies an IP egress ACL rule.

**vlan** (Optional) Specifies the VLAN name.

**<vlan\_name 32>**

Enter the VLAN name used for this configuration here. This name can be up to 32 characters long.

**vlanid** Specifies a VLAN ID.

**<vlanid 1-4094>**

Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.

## 8. Access Control List (ACL) Egress Command List

### **mask**

(Optional) Specifies the mask used.

**<hex 0x0-x0fff>**

Enter the mask value used here.

### **source\_ip**

(Optional) Specifies an IP source address.

**<ipaddr>**

Enter the source IP address used here.

**mask** Specifies the source IP address used here.

**<netmask>**

Enter the source network mask here.

### **destination\_ip**

(Optional) Specifies an IP destination address.

**<ipaddr>**

Enter the destination IP address used here.

**mask** Specifies the destination IP address used here.

**<netmask>**

Enter the destination network mask here.

**dscp** (Optional) Specifies the value of DSCP. The DSCP value ranges from 0 to 63.

**<value 0-63>**

Enter the DSCP value used here. This value must be between 0 and 63.

**icmp** (Optional) Specifies that the following parameters configured will apply to the ICMP configuration.

**type** Specifies that the rule will apply to the ICMP type traffic value.

**<value 0-255>**

Enter the ICMP traffic type value here. This value must be between 0 and 255.

**code** Specifies that the rule will apply to the ICMP code traffic value.

**<value 0-255>**

Enter the ICMP code traffic value here. This value must be between 0 and 255.

**igmp** (Optional) Specifies that the following parameters configured will apply to the IGMP configuration.

**type** Specifies that the rule will apply to the IGMP type traffic value.

**<value 0-255>**

Enter the IGMP type traffic value here. This value must be between 0 and 255.

**tcp** (Optional) Specifies that the following parameters configured will apply to the TCP configuration.

### **src\_port**

Specifies that the rule will apply to a range of TCP source ports.

**<value 0-65535>**

Enter the source port value here. This value must be between 0 and 65535.

**mask** Specifies the TCP source port mask here.

**<hex 0x0-0xffff>**

Enter the TCP source port mask value here.

### **dst\_port**

Specifies that the rule will apply to a range of TCP destination ports.

**<value 0-65535>**

Enter the destination port value here. This value must be between 0 and 65535.

**mask** Specifies the TCP destination port mask here.

**<hex 0x0-0xffff>**

Enter the TCP destination port mask value here.



## 8. Access Control List (ACL) Egress Command List

**flag** (Optional) Specifies the TCP flag fields.

- all** Specifies that the TCP flag field will be set to 'all'.
- urg** Specifies that the TCP flag field will be set to 'urg'.
- ack** Specifies that the TCP flag field will be set to 'ack'.
- psh** Specifies that the TCP flag field will be set to 'psh'.
- rst** Specifies that the TCP flag field will be set to 'rst'.
- syn** Specifies that the TCP flag field will be set to 'syn'.
- fin** Specifies that the TCP flag field will be set to 'fin'.

**udp** (Optional) Specifies that the following parameters configured will apply to the UDP configuration.

**src\_port**  
Specifies the UDP source port range.  
<value 0-65535>  
Enter the UDP source port range value here.

**mask** Specifies the UDP source port mask here.  
<hex 0x0-0xffff>  
Enter the UDP source port mask value here.

**dst\_port**  
Specifies the UDP destination port range.  
<value 0-65535>  
Enter the UDP destination port range value here.

**mask** Specifies the UDP destination port mask here.  
<hex 0x0-0xffff>  
Enter the UDP destination port mask value here.

**protocol\_id**  
(Optional) Specifies that the rule will apply to the value of IP protocol ID traffic.  
<value 0-255>  
Enter the protocol ID used here. This value must be between 0 and 255.

**user\_define**  
(Optional) Specifies that the rule will apply to the IP protocol ID and that the mask options behind the IP header, which has a length of 20 bytes.  
<hex 0x0-0xffffffff>  
Enter the user-defined mask value here.

**mask** Specifies the user-defined mask here.  
<hex 0x0-0xffffffff>  
Enter the user-defined mask value here.

---

---

|                         |                                                                                                                                                                                                                                  |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv6</b>             | Specifies the rule applies to IPv6 fields.                                                                                                                                                                                       |
| <b>class</b>            | (Optional) Specifies the value of IPv6 class.<br><div style="margin-left: 20px;"><b>&lt;value 0-255&gt;</b><br/> Enter the IPv6 class value here. This value must be between 0 and 255.</div>                                    |
| <b>source_ipv6</b>      | (Optional) Specifies the value of IPv6 source address.<br><div style="margin-left: 20px;"><b>&lt;ipv6addr&gt;</b><br/> Enter the source IPv6 source address here.</div>                                                          |
| <b>mask</b>             | Specifies the IPv6 source address mask here.<br><div style="margin-left: 20px;"><b>&lt;ipv6mask&gt;</b><br/> Enter the IPv6 source address mask value here.</div>                                                                |
| <b>destination_ipv6</b> | (Optional) Specifies the value of IPv6 destination address.<br><div style="margin-left: 20px;"><b>&lt;ipv6addr&gt;</b><br/> Enter the source IPv6 destination address here.</div>                                                |
| <b>mask</b>             | Specifies the IPv6 destination address mask here.<br><div style="margin-left: 20px;"><b>&lt;ipv6mask&gt;</b><br/> Enter the IPv6 destination address mask value here.</div>                                                      |
| <b>tcp</b>              | (Optional) Specifies the TCP protocol                                                                                                                                                                                            |
| <b>src_port</b>         | Specifies the value of the IPv6 layer 4 TCP source port.<br><div style="margin-left: 20px;"><b>&lt;value 0-65535&gt;</b><br/> Enter the IPv6 TCP source port value here. This value must be between 0 and 65535.</div>           |
| <b>mask</b>             | Specifies the IPv6 TCP source port mask here.<br><div style="margin-left: 20px;"><b>&lt;hex 0x0-0xffff&gt;</b><br/> Enter the IPv6 TCP source port mask value here.</div>                                                        |
| <b>dst_port</b>         | Specifies the value of the IPv6 layer 4 TCP destination port.<br><div style="margin-left: 20px;"><b>&lt;value 0-65535&gt;</b><br/> Enter the IPv6 TCP destination port value here. This value must be between 0 and 65535.</div> |
| <b>mask</b>             | Specifies the IPv6 TCP destination port mask here.<br><div style="margin-left: 20px;"><b>&lt;hex 0x0-0xffff&gt;</b><br/> Enter the IPv6 TCP destination port mask value here.</div>                                              |
| <b>udp</b>              | (Optional) Specifies the UDP protocol.                                                                                                                                                                                           |
| <b>src_port</b>         | Specifies the value of the IPv6 layer 4 UDP source port.<br><div style="margin-left: 20px;"><b>&lt;value 0-65535&gt;</b><br/> Enter the IPv6 UDP source port value here. This value must be between 0 and 65535.</div>           |
| <b>mask</b>             | Specifies the IPv6 UDP source port mask here.<br><div style="margin-left: 20px;"><b>&lt;hex 0x0-0xffff&gt;</b><br/> Enter the IPv6 UDP source port mask value here.</div>                                                        |
| <b>dst_port</b>         | Specifies the value of the IPv6 layer 4 UDP destination port.<br><div style="margin-left: 20px;"><b>&lt;value 0-65535&gt;</b><br/> Enter the IPv6 UDP destination port value here. This value must be between 0 and 65535.</div> |
| <b>mask</b>             | Specifies the IPv6 UDP destination port mask here.<br><div style="margin-left: 20px;"><b>&lt;hex 0x0-0xffff&gt;</b><br/> Enter the IPv6 UDP destination port mask value here.</div>                                              |
| <b>icmp</b>             | (Optional) Specifies that the following parameters configured will apply to the ICMP configuration.                                                                                                                              |

## 8. Access Control List (ACL) Egress Command List

|                              |                                                                                                                                                                                                                                                                                                      |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>type</b>                  | Specifies that the rule will apply to the ICMP type traffic value.<br><b>&lt;value 0-255&gt;</b><br>Enter the ICMP traffic type value here. This value must be between 0 and 255.                                                                                                                    |
| <b>code</b>                  | Specifies that the rule will apply to the ICMP code traffic value.<br><b>&lt;value 0-255&gt;</b> - Enter the ICMP code traffic value here. This value must be between 0 and 255.                                                                                                                     |
| <b>vlan_based</b>            | The rule applies on the specified VLAN.                                                                                                                                                                                                                                                              |
| <b>vlan</b>                  | Specifies the VLAN name.<br><b>&lt;vlan_name 32&gt;</b><br>Enter the VLAN name used for this configuration here. This name can be up to 32 characters long.                                                                                                                                          |
| <b>vlanid</b>                | Specifies a VLAN ID.<br><b>&lt;vlanid 1-4094&gt;</b><br>Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.                                                                                                                                                   |
| <b>port_group</b>            | Specifies the port group value here.                                                                                                                                                                                                                                                                 |
| <b>id</b>                    | Specifies the ID of the port group which the rule applies.<br><b>&lt;value 1-64&gt;</b><br>Enter the group ID value here. This value must be between 1 and 64.                                                                                                                                       |
| <b>name</b>                  | Specifies the name of the port group which the rule applies.<br><b>&lt;name 16&gt;</b><br>Enter the port group name here. This name can be up to 16 characters long.                                                                                                                                 |
| <b>port</b>                  | Specifies the port in the port group used.<br><b>&lt;port&gt;</b><br>Enter the port number used here.                                                                                                                                                                                                |
| <b>permit</b>                | Specifies that packets matching the egress access rule are permitted by the Switching Hub.                                                                                                                                                                                                           |
| <b>replace_priority_with</b> | (Optional) Specifies the packets that match the egress access rule are changed the 802.1p priority tag field by the Switching Hub.<br><b>&lt;value 0-7&gt;</b><br>Enter the replace priority with value here. This value must be between 0 and 7.                                                    |
| <b>replace_dscp_with</b>     | (Optional) Specifies the packets that match the egress access rule are changed the DSCP value by the Switching Hub.<br><b>&lt;value 0-63&gt;</b><br>Enter the replace DSCP with value here. This value must be between 0 and 63.                                                                     |
| <b>counter</b>               | (Optional) Specifies whether the ACL counter feature is enabled or disabled. This parameter is optional. The default option is disabled. If the rule is not bound with the flow_meter, all matching packets are counted. If the rule is bound with the flow_meter, then the "counter" is overridden. |
| <b>enable</b>                | Specifies that the ACL counter feature will be enabled.                                                                                                                                                                                                                                              |
| <b>disable</b>               | Specifies that the ACL counter feature will be disabled.                                                                                                                                                                                                                                             |
| <b>deny</b>                  | Specifies the packets that match the egress access rule are filtered by the Switching Hub.                                                                                                                                                                                                           |

## 8. Access Control List (ACL) Egress Command List

---

### **time\_range**

(Optional) Specifies the name of the time range entry.

**<range\_name 32>**

Enter the time range value here. This name can be up to 32 characters long.

---

**delete** Specifies to delete a profile or rule.

---

### **access\_id**

Specifies the index of the access list entry. If the auto\_assign option is selected, the access ID is automatically assigned.

**<value 1-128>**

Enter the access ID used here. This value must be between 1 and 128.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure a port-base egress access rule that when the packet go out Switching Hub which match the specified source IP, DSCP and destination IP field, it will not be dropped:

```
Zxxx0:admin# config egress_access_profile profile_id 2 add access_id auto_assign  
ip source_ip 10.0.0.1 dscp 25 destination_ip 10.90.90.90 port_group id 1 permit  
Command: config egress_access_profile profile_id 2 add access_id auto_assign ip  
source_ip 10.0.0.1 dscp 25 destination_ip 10.90.90.90 port_group id 1 permit
```

Success.

Zxxx0:admin#

To configure a vlan-base egress access rule that when the packet go out Switching Hub which match the specified source MAC field, it will be dropped:

```
Zxxx0:admin# config egress_access_profile profile_id 2 add access_id 1 ethernet  
source_mac 11-22-33-44-55-66 vlan_based vlan_id 1 deny  
Command: config egress_access_profile profile_id 2 add access_id 1 ethernet  
source_mac 11-22-33-44-55-66 vlan_based vlan_id 1 deny
```

Success.

Zxxx0:admin#

## 8.4. **show egress\_access\_profile**

---

### ● Description

This command is used to display current egress access list table.

### ● Format

**show egress\_access\_profile** {[profile\_id <value 1-4> | profile\_name <name 1-32>]}

### ● Parameters

---

**profile\_id**

(Optional) Specifies the index of the egress access list profile.

**<value 1-4>**

Enter the profile ID here. This value must be between 1 and 4.

---

**profile\_name**

(Optional) Specifies the name of the profile. The maximum length is 32 characters.

**<name 1-32>**

Enter the profile name here. This name can be up to 32 characters long.

---

If no parameter is specified, will show the all egress access profile.

### ● Restrictions

None.

### ● Example

To display current egress access list table:

## 8. Access Control List (ACL) Egress Command List

```
Zxxx0:admin# show egress_access_profile
Command: show access_profile
```

### Egress Access Profile Table

```
Total User Set Rule Entries      : 3
Total Used Hardware Entries       : 3
Total Available Hardware Entries  : 253
```

```
=====
Profile ID: 1      Profile name: 1  Type: Ethernet
```

```
Mask on
  Source MAC       : FF-FF-FF-FF-FF-FF
```

```
Available Hardware Entries : 127
-----
```

```
Rule ID : 1      Port group: -
```

```
Match on
  VLAN ID          : 1
  Source MAC       : 00-00-00-00-00-01
```

```
Action:
  Permit
```

```
=====
Profile ID: 2      Profile name: 2  Type: IPv4
```

```
Mask on
  Source IP        : 255.255.255.255
  Destination IP   : 255.255.255.255
  DSCP
```

```
Available Hardware Entries : 126
-----
```

## 8. Access Control List (ACL) Egress Command List

```
Rule ID : 1      (auto assign)      Port group: 1
```

```
Match on
```

```
Source IP      : 10.0.0.2
Destination IP  : 10.90.90.90
DSCP           : 25
```

```
Action:
```

```
Permit
```

```
-----
Rule ID : 2      (auto assign)      Port group: 1
```

```
Match on
```

```
Source IP      : 10.0.0.1
Destination IP  : 10.90.90.90
DSCP           : 25
```

```
Action:
```

```
Permit
```

```
Matched Count : 0 packets
```

```
=====
Zxxx0:admin#
```

The following example displays an egress access profile that supports an entry mask for each rule:

```
Zxxx0:admin# show egress_access_profile profile_id 1
```

```
Command: show egress_access_profile profile_id 1
```

```
Egress Access Profile Table
```

```
=====
Profile ID: 1      Profile name: 1  Type: Ethernet
```

```
Mask on
```

```
Source MAC      : FF-FF-FF-FF-FF-FF
```

```
Available Hardware Entries : 127
```

```
-----
Rule ID : 1      Port group: -
```

```
Match on
```

```
VLAN ID        : 1
Source MAC      : 00-00-00-00-00-01
```

```
Action:
```

```
Permit
```

```
=====
Zxxx0:admin#
```

## 8.5. show current\_config egress\_access\_profile

---

### ● Description

This command is used to display the egress ACL part of current configuration in user level of privilege.

The overall current configuration can be displayed by "show config" command which is accessible in administrator level of privilege.

### ● Format

**show current\_config egress\_access\_profile**

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display current configuration of egress access list table:

```
Zxxx0:admin# show current_config egress_access_profile
Command: show current_config egress_access_profile

#-----

# Egress ACL

create egress_access_profile profile_id 1 profile_name 1 ethernet source_mac FF-
FF-FF-FF-FF-FF
config egress_access_profile profile_id 1 add access_id 1 ethernet source_mac 00
-00-00-00-00-01 vlan_based vlan_id 1 permit
create egress_access_profile profile_id 2 profile_name 2 ip source_ip_mask 255.2
55.255.255 destination_ip_mask 255.255.255.255 dscp
config egress_access_profile profile_id 2 add access_id auto_assign ip source_ip
10.0.0.2 destination_ip 10.90.90.90 dscp 25 port_group id 1 permit counter enable
config egress_access_profile profile_id 2 add access_id auto_assign ip source_ip
10.0.0.1 destination_ip 10.90.90.90 dscp 25 port_group id 1 permit

#-----

Zxxx0:admin#
```



## 8.6. config egress\_flow\_meter

---

### ● Description

This command is used to configure the packet flow-based metering based on an egress access profile and rule.

### ● Format

```
config egress_flow_meter [profile_id <value 1-4> | profile_name <name 1-32>]
access_id <value 1-128> [rate <value 0-1048576> {burst_size <value 0-131072>}
rate_exceed [drop_packet | remark_dscp <value 0-63>] | tr_tcm cir <value 0-1048576>
{cbs <value 0-131072>} pir <value 0-1048576> {pbs <value 0-131072>} {[color_blind |
color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable |
disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable |
disable]}} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable |
disable]}} | sr_tcm cir <value 0-1048576> cbs <value 0-131072> ebs <value 0-131072>
{[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter
[enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter
[enable | disable]}} violate [permit {replace_dscp <value 0-63>} | drop] {counter
[enable | disable]}} | delete]
```

### ● Parameters

---

#### profile\_id

Specify the profile ID.

**<value 1-4>**

Enter the profile ID used here. This value must be between 1 and 4.

---

#### profile\_name

Specifies the name of the profile.

**<name 1-32>**

Enter the profile name used here. This name can be up to 32 characters long.

---

#### access\_id

Specifies the access ID.

**<value 1-128>**

Enter the access ID used here. This value must be between 1 and 128.

---

#### rate

This specifies the rate for single rate two-color mode. Specify the committed bandwidth in Kbps for the flow. The value m and n are determined by the project.

**<value 0-1048576>**

Enter the rate for single rate two-color mode here. This value must be between 0 and 1048576.

---

#### burst\_size

(Optional) This specifies the burst size for the single rate "two color" mode. The unit is Kbytes.

**<value 0-131072>**

Enter the burst size value here. This value must be between 0 and 131072.

---

## 8. Access Control List (ACL) Egress Command List

---

### **rate\_exceed**

This specifies the action for packets that exceed the committed rate in single rate "two color" mode. The action can be specified as one of the following:

#### **drop\_packet**

Drop the packet immediately.

#### **remark\_dscp**

Mark the packet with a specified DSCP. The packet is set to have the higher drop precedence.

**<value 0-63>**

Enter the remark DSCP value here. This value must be between 0 and 63.

---

**tr\_tcm** Specify the "two rate three color mode".

**cir** Specifies the two rate three color mode used.

**<value 0-1048576>**

Enter the two rate three color mode value here. This value must be between 0 and 1048576.

**cbs** (Optional) Specifies the "Committed Burst Size". The unit is Kbytes. That is to say, 1 means 1Kbytes. This parameter is an optional parameter. The default value is 4\*1024.

**<value 0-131072>**

Enter the committed burst size value here. This value must be between 0 and 131072.

**pir** Specifies the "Peak Information Rate". The unit is in Kbps. PIR should always be equal to or greater than CIR.

**<value 0-1048576>**

Enter the peak information rate value here. This value must be between 0 and 1048576.

**pbs** (Optional) Specifies the "Peak Burst Size". The unit is in Kbytes.

**<value 0-131072>**

Enter the peak burst size value here. This value must be between 0 and 131072.

#### **color\_blind**

(Optional) Specify the meter mode to be color-blind. The default is color-blind mode.

#### **color\_aware**

(Optional) Specify the meter mode to be color-aware. When this code is specified, user could set the "in-coming packet color" by using command "config color\_aware". The final color of packet is determined by the initial color of packet and the metering result.

---

**conform** (Optional) Specify the action when packet is in "green color".

#### **permit**

Permit the packet.

#### **replace\_dscp**

Changes the DSCP of the packet.

**<value 0-63>**

Enter the replace DSCP value here. This value must be between 0 and 63.

#### **counter**

(Optional) Specifies the ACL counter. This is optional. The default is "disable". The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.

#### **enable**

Specifies that the ACL counter parameter will be enabled.

#### **disable**

Specifies that the ACL counter parameter will be disabled.

---

## 8. Access Control List (ACL) Egress Command List

---

|                     |                                                                                                                                                                                                              |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>exceed</b>       | Specify the action when packet is in "yellow color".                                                                                                                                                         |
| <b>permit</b>       | (Optional) Permit the packet.                                                                                                                                                                                |
| <b>replace_dscp</b> | Changes the DSCP of the packet.<br><value 0-63><br>Enter the DSCP replace value here. This value must be between 0 and 63.                                                                                   |
| <b>drop</b>         | Drops the packet.                                                                                                                                                                                            |
| <b>counter</b>      | (Optional) Specifies the ACL counter. This is optional. The default is "disable". The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled. |
| <b>enable</b>       | Specifies that the ACL counter parameter will be enabled.                                                                                                                                                    |
| <b>disable</b>      | Specifies that the ACL counter parameter will be disabled.                                                                                                                                                   |

---

|                     |                                                                                                                                                                                                              |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>violate</b>      | Specify the action when packet is in "red color".                                                                                                                                                            |
| <b>permit</b>       | Permit the packet.                                                                                                                                                                                           |
| <b>replace_dscp</b> | (Optional) Changes the DSCP of the packet.<br><value 0-63><br>Enter the DSCP replace value here. This value must be between 0 and 63.                                                                        |
| <b>drop</b>         | Drops the packet.                                                                                                                                                                                            |
| <b>counter</b>      | (Optional) Specifies the ACL counter. This is optional. The default is "disable". The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled. |
| <b>enable</b>       | Specifies that the ACL counter parameter will be enabled.                                                                                                                                                    |
| <b>disable</b>      | Specifies that the ACL counter parameter will be disabled.                                                                                                                                                   |

---

|                    |                                                                                                                                                                                                                                                                      |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>sr_tcm</b>      | Specify the "single rate three color mode".                                                                                                                                                                                                                          |
| <b>cir</b>         | Specifies the single rate three color mode used.<br><value 0-1048576><br>Enter the single rate three color mode value here. This value must be between 0 and 1048576.                                                                                                |
| <b>cbs</b>         | Specify the "committed burst size". The unit is Kbytes.<br><value 0-131072><br>Enter the committed burst size value here. This value must be between 0 and 131072.                                                                                                   |
| <b>ebs</b>         | Specify the "Excess Burst Size". The unit is Kbytes.<br><value 0-131072><br>Enter the excess burst size value here. This value must be between 0 and 131072.                                                                                                         |
| <b>color_blind</b> | (Optional) Specify the meter mode to be color-blind. The default is color-blind mode.                                                                                                                                                                                |
| <b>color_aware</b> | (Optional) Specify the meter mode to be color-aware. When this code is specified, user could set the "in-coming packet color" by using command "config color_aware". The final color of packet is determined by the initial color of packet and the metering result. |

---

## 8. Access Control List (ACL) Egress Command List

---

**conform** (Optional) Specify the action when packet is in "green color".

**permit**

(Optional) Permit the packet.

**replace\_dscp**

Changes the DSCP of the packet.

**<value 0-63>**

Enter the replace DSCP value here. This value must be between 0 and 63.

**counter**

(Optional) Specifies the ACL counter. This is optional. The default is "disable". The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.

**enable**

Specifies that the ACL counter parameter will be enabled.

**disable**

Specifies that the ACL counter parameter will be disabled.

---

**exceed** Specify the action when packet is in "yellow color".

**permit**

Permit the packet.

**replace\_dscp**

(Optional) Changes the DSCP of the packet.

**<value 0-63>**

Enter the DSCP replace value here. This value must be between 0 and 63.

**drop** Drops the packet.

**counter**

(Optional) Specifies the ACL counter. This is optional. The default is "disable". The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.

**enable**

Specifies that the ACL counter parameter will be enabled.

**disable**

Specifies that the ACL counter parameter will be disabled.

---

**violate** Specify the action when packet is in "red color".

**permit**

Permit the packet.

**replace\_dscp**

(Optional) Changes the DSCP of the packet.

**<value 0-63>**

Enter the DSCP replace value here. This value must be between 0 and 63.

**drop** Drops the packet.

**counter**

(Optional) Specifies the ACL counter. This is optional. The default is "disable". The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.

**enable**

Specifies that the ACL counter parameter will be enabled.

**disable**

Specifies that the ACL counter parameter will be disabled.

---

**delete** Delete the specified "flow\_meter".

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## 8. Access Control List (ACL) Egress Command List

### ● Example

To configure a "two rates three color" flow meter:

```
Zxxx0:admin# config egress_flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 200 pir 2000 pbs 200 exceed replace_dscp 21 violate drop
command: config egress_flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 200 pir 2000 pbs 200 exceed replace_dscp 21 violate drop

Success.

Zxxx0:admin#
```

## 8.7. show egress\_flow\_meter

### ● Description

This command is used to display the egress flow-based metering configuration.

### ● Format

**show egress\_flow\_meter** {[profile\_id <value 1-4> | profile\_name <name 1-32>]  
{access\_id <value 1-128>}}

### ● Parameters

---

**profile\_id**

(Optional) Specifies the index of access list profile.

**<value 1-4>**

Enter the profile ID used here. This value must be between 1 and 4.

---

**profile\_name**

(Optional) Specifies the name of the profile.

**<name 1-32>**

Enter the profile name used here. This name can be up to 32 characters long.

---

**access\_id**

(Optional) Specifies the access ID.

**<value 1-128>**

Enter the access ID used here. This value must be between 1 and 128.

---

### ● Restrictions

None.

### ● Example

To display current egress flow meter table:

```
Zxxx0:admin# show egress_flow_meter
Command: show egress_flow_meter

Flow Meter Information:
-----
Profile ID : 1      Access ID : 1      Mode : trTcm / color-blind
CIR:1000 (Kbps)    CBS:2000 (Kbyte)    PIR:2000 (Kbps)    PBS:2000 (Kbyte)
Actions:
Conform : Permit    Replace DSCP : 11    Counter : enable
Exceed  : Permit    Replace DSCP : 22    Counter : enable
Violate  : Drop

Profile ID : 1      Access ID : 1      Mode : srTcm / color-blind
CIR:2500 (Kbps)    CBS:2000 (Kbyte)    EBS:3500 (Kbyte)
Actions:
Conform : Permit                                Counter : enable
Exceed  : Permit    Replace DSCP: 33    Counter : enable
Violate  : Drop

Total Entries: 2

Zxxx0:admin#
```

### 8.8. create port\_group id

---

#### ● Description

This command is used to create a port group.

#### ● Format

**create port\_group id <value 1-64> name <name 16>**

#### ● Parameters

|             |                                                                                                                                        |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>id</b>   | Specifies the port group ID.<br><b>&lt;value 1-64&gt;</b><br>Enter the port group ID here. This value must be between 1 and 64.        |
| <b>name</b> | Specifies the port group name.<br><b>&lt;name 16&gt;</b><br>Enter the port group name here. This name can be up to 16 characters long. |

#### ● Restrictions

Only Administrator and Operator-level users can issue this command.

#### ● Example

Only Administrator and Operator-level users can issue this command.

## 8. Access Control List (ACL) Egress Command List

```
Zxxx0:admin# create port_group id 2 name group2
Command: create port_group id 2 name group2

Success.

Zxxx0:admin#
```

### 8.9. config port\_group

#### ● Description

This command is used to add or delete a port list to a port group.

#### ● Format

**config port\_group [id <value 1-64> | name <name 16>] [add | delete] [<portlist> | all]**

#### ● Parameters

|                         |                                                                                                                                        |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>id</b>               | Specifies the port group ID.<br><b>&lt;value 1-64&gt;</b><br>Enter the port group ID used here. This value must be between 1 and 64.   |
| <b>name</b>             | Specifies the port group name.<br><b>&lt;name 16&gt;</b><br>Enter the port group name here. This name can be up to 16 characters long. |
| <b>add</b>              | Add a port list to this port group.                                                                                                    |
| <b>delete</b>           | Delete a port list from this port group.                                                                                               |
| <b>&lt;portlist&gt;</b> | Enter a list of ports used for the configuration here.                                                                                 |
| <b>all</b>              | Specifies that all the ports will be used for this configuration.                                                                      |

#### ● Restrictions

Only Administrator and Operator-level users can issue this command.

#### ● Example

Add port list "1-3" to the port group which ID is "2":

```
Zxxx0:admin# config port_group id 2 add 1-3
Command: config port_group id 2 add 1-3

Success.

Zxxx0:admin#
```

## 8.10. delete port\_group

---

### ● Description

This command is used to delete port group.

### ● Format

**delete port\_group** [id <value 1-64> | name <name 16>]

### ● Parameters

|             |                                                                                                                           |
|-------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>id</b>   | Specifies the port group ID.<br><value 1-64><br>Enter the port group ID used here. This value must be between 1 and 64.   |
| <b>name</b> | Specifies the port group name.<br><name 16><br>Enter the port group name here. This name can be up to 16 characters long. |

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To delete the port group which ID is "2":

```
Zxxx0:admin# delete port_group id 2
Command: delete port_group id 2

Success.

Zxxx0:admin#
```



## 8.11. show port\_group

---

### ● Description

This command is used to display the port group information.

### ● Format

**show port\_group {id <value 1-64> | name <name 16>}**

### ● Parameters

---

|             |                                                                                                                                                   |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>id</b>   | (Optional) Specifies the port group ID.<br><b>&lt;value 1-64&gt;</b><br>Enter the port group ID used here. This value must be between 1 and 64.   |
| <b>name</b> | (Optional) Specifies the port group name.<br><b>&lt;name 16&gt;</b><br>Enter the port group name here. This name can be up to 16 characters long. |

---

If not specified parameter, will show all the port group.

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To show all the port group information:

```
Zxxx0:admin# show port_group
Command: show port_group

Port Group Table
Group ID      Group Name      Ports
1             group1          1-2, 5
2             group2          4, 5, 7, 9, 11, 13
               15, 17, 19-25
4             group3          5-7

Total Entries :3

Zxxx0:admin#
```

## 9. ARP Commands

ARP (Address Resolution Protocol) is a protocol to calculate a MAC address from an IP address.

The Switching Hub sends an ARP request to devices on the same network and manages a mapping between IP addresses and MAC addresses in table data called an ARP table based on responses from the devices.

```
Interface-----IP Address-----MAC Address-----Type,
-----
System-----10.0.0.0-----FF-FF-FF-FF-FF-FF Local/Broadcast,
System-----10.90.90.90-----00-01-02-03-04-00 Local,
System-----10.255.255.255-----FF-FF-FF-FF-FF-FF Local/Broadcast,
```

An ARP table is usually created automatically (dynamic entry) but can also be written manually (static entry). Dynamic entries are removed after a specified time (aging time) without any access while static entries are retained until they are intentionally removed.

```
create arpentry <ipaddr> <macaddr>
delete arpentry [<ipaddr> | all]
config arpentry <ipaddr> <macaddr>
config arp refresh time_out state [enable | disable]
config arp_aging time <min 0-65535>
show arpentry {ipif <ipif_name 12> | ipaddress <ipaddr> | static | mac_address <macaddr>}
clear arptable
show ipfdb {[ip_address <ipaddr> | interface <ipif_name 12> | port <port>]}
```

### 9.1. create arpentry

#### ● Description

This command is used to enter an IP address and the corresponding MAC address into the Switching Hub's ARP table.

#### ● Format

```
create arpentry <ipaddr> <macaddr>
```

#### ● Parameters

```
<ipaddr> The IP address of the end node or station.
```

## 9. ARP Commands

---

**<macaddr>**

The MAC address corresponding to the IP address above.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create a static ARP entry for the IP address 10.48.74.121 and MAC address 00:50:BA:00:07:36:

```
Zxxx0:admin#create arpentry 10.48.74.121 00-50-BA-00-07-36
Command: create arpentry 10.48.74.121 00-50-BA-00-07-36

Success.

Zxxx0:admin#
```

## 9.2. delete arpentry

---

### ● Description

This command is used to delete a static ARP entry, made using the **create arpentry** command above, by specifying either the IP address of the entry or **all**. Specifying **all** deletes the Switching Hub's ARP table.

### ● Format

**delete arpentry** [<ipaddr> | all]

### ● Parameters

---

**<ipaddr>** The IP address of the end node or station.

---

**all** Delete all ARP entries

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete an entry of IP address 10.48.74.121 from the ARP table:

```
Zxxx0:admin#delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

Zxxx0:admin#
```

## 9.3. config arpentry

---

### ● Description

This command is used to configure a static entry in the ARP table. Specify the IP address and MAC address of the entry.

### ● Format

**config arpentry <ipaddr> <macaddr>**

### ● Parameters

---

**<ipaddr>** The IP address of the end node or station.

---

**<macaddr>**

The MAC address corresponding to the IP address above.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure a static ARP entry for the IP address 10.48.74.121 and MAC address 00:50:BA:00:07:36:

```
Zxxx0:admin#config arpentry 10.48.74.121 00-50-BA-00-07-36
Command: config arpentry 10.48.74.121 00-50-BA-00-07-36

Success.

Zxxx0:admin#
```

## 9.4. config arp refresh time\_out state

---

### ● Description

This command is used to set the ARP refresh function.

This function checks the learnt ARP entry if it is still existed or not before aging out to prevent the packet loss while learning the ARP entry again.

### ● Format

**config arp refresh time\_out state [enable | disable]**

## 9. ARP Commands

### ● Parameters

---

|                |                                                           |
|----------------|-----------------------------------------------------------|
| <b>state</b>   | Enable or disable the ARP refresh. The default is enable. |
| <b>enable</b>  | Enable the ARP refresh.                                   |
| <b>disable</b> | Disable the ARP refresh.                                  |

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To disable the ARP refresh state:

```
Zxxx0:admin#config arp refresh time_out state disable
Command: config arp refresh time_out state disable

Success.

Zxxx0:admin#
```

## 9.5. **config arp\_aging time**

---

### ● Description

This command is used to set the maximum amount of time, in minutes, that an ARP entry can remain in the Switching Hub's ARP table, without being accessed, before it is dropped from the table.

### ● Format

**config arp\_aging time <min 0-65535>**

### ● Parameters

---

|                            |                                                                                               |
|----------------------------|-----------------------------------------------------------------------------------------------|
| <b>&lt;min 0-65535&gt;</b> | The ARP age-out time, in minutes. The default is 20 minutes. The range is 0 to 65535 minutes. |
|----------------------------|-----------------------------------------------------------------------------------------------|

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure the ARP aging time:

```
Zxxx0:admin#config arp_aging time 30
Command: config arp_aging time 30

Success.

Zxxx0:admin#
```

## 9.6. show arpentry

### ● Description

This command is used to display the Address Resolution Protocol (ARP) table. Filter the display by IP address, interface name, or static entries.

### ● Format

**show arpentry { ipif <ipif\_name 12> | ipaddress <ipaddr> | static | mac\_address <macaddr> }**

### ● Parameters

|                    |                                                                                                                                                                                                                |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b>        | The name of the IP interface the end node or station for which the ARP table entry was made, resides on.<br><b>&lt;ipif_name 12&gt;</b><br>Specify the IP interface name. The maximum length is 12 characters. |
| <b>ipaddress</b>   | The IP address of the end node or station.<br><b>&lt;ipaddr&gt;</b><br>Specify the IP address.                                                                                                                 |
| <b>static</b>      | Displays the static entries to the ARP table.                                                                                                                                                                  |
| <b>mac_address</b> | Displays the ARP entry by MAC address.<br><b>&lt;macaddr&gt;</b><br>Specify the MAC address.                                                                                                                   |

**NOTE** If no parameter is specified, all ARP entries will be displayed.

### ● Restrictions

None.

## 9. ARP Commands

### ● Example

To display the ARP table:

```
Zxxx0:admin# show arprentry
Command: show arprentry

ARP Aging Time : 20

Interface      IP Address      MAC Address      Type
-----
System         10.0.0.0        FF-FF-FF-FF-FF-FF Local/Broadcast
System         10.90.90.90     00-01-02-03-04-00 Local
System         10.255.255.255  FF-FF-FF-FF-FF-FF Local/Broadcast

Total Entries: 3

Zxxx0:admin#
```

## 9.7. clear arptable

---

### ● Description

This command is used to remove dynamic entries from the ARP table. Static ARP entries are not affected.

### ● Format

**clear arptable**

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To remove the dynamic entries from the ARP table:

```
Zxxx0:admin#clear arptable
Command: clear arptable

Success.

Zxxx0:admin#
```

## 9.8. show ipfdb

---

### ● Description

This command is used to display the IP address forwarding table on the Switch.

### ● Format

**show ipfdb** {[ip\_address <ipaddr> | interface <ipif\_name 12> | port <port>]}

### ● Parameters

---

#### ip\_address

(Optional) Specifies the IP address of the forwarding table.

**<ipaddr>**

Enter the IP address to be displayed.

---

**interface**(Optional) Specifies the interface name of the forwarding table.

**<ipif\_name 12>**

Enter the interface name here. This name can be up to 12 characters long.

---

**port** (Optional) Specifies the port to be displayed.

**<port>**

Enter the port number to be displayed.

---

### ● Restrictions

None.

### ● Example

To display the IP address forwarding table on the Switch:

```
Zxxx0:admin# show ipfdb
Command: show ipfdb

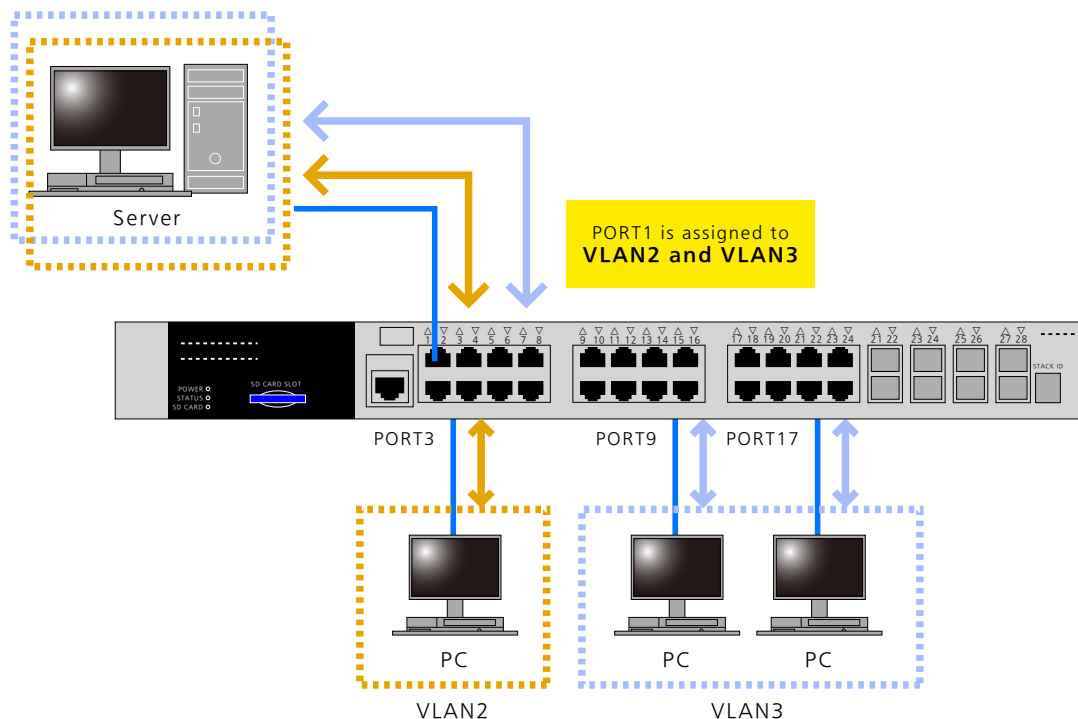
Interface      IP Address      Port      Learned
-----
Total Entries: 0

Zxxx0:admin#
```



# 10. Asymmetric VLAN Commands

Asymmetric VLAN is one of functions used to access shared resources, such as the Internet or corporate server, from multiple VLANs while blocking communications between VLANs. It assigns a specific port to multiple VLANs. This is used when tagged VLANs are not available.



Port 1: Assigned to VLAN2, VLAN3

Port 3: Assigned to VLAN2

Port 9, 17: Assigned to VLAN3

Figure 10-1 Asymmetric VLAN overview

In the above example, communications between VLAN2 and VLAN3 except for the server are blocked but VLAN2 and VLAN3 terminals can access the server.

```
enable asymmetric_vlan
disable asymmetric_vlan
show asymmetric_vlan
```

## 10.1. enable asymmetric\_vlan

---

### ● Description

This command is used to enable the asymmetric VLAN function..

### ● Format

enable asymmetric\_vlan

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable asymmetric VLAN setting:

```
Zxxx0:admin# enable asymmetric_vlan
Command: enable asymmetric_vlan

Success.

Zxxx0:admin#
```

## 10.2. disable asymmetric\_vlan

---

### ● Description

This command is used to disable the asymmetric VLAN function.

### ● Format

disable asymmetric\_vlan

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## 10. Asymmetric VLAN Commands

### ● Example

To disable asymmetric VLAN setting:

```
Zxxx0:admin# disable asymmetric_vlan
Command: disable asymmetric_vlan

Success.

Zxxx0:admin#
```

## 10.3. show asymmetric\_vlan

---

### ● Description

This command is used to display the asymmetric VLAN function.

### ● Format

**show asymmetric\_vlan**

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display asymmetric VLAN:

```
Zxxx0:admin# show asymmetric_vlan
Command: show asymmetric_vlan

Asymmetric Vlan : Disabled

Zxxx0:admin#
```

---

# 11.Auto Configuration Commands

---

When the Auto Configuration function is enabled, the Switching Hub loads the configuration file from a previously installed TFTP server during a boot via BOOTP parameters.

---

```
show autoconfig
enable autoconfig
disable autoconfig
```

---

## 11.1. show autoconfig

---

### ● Description

This command is used to display the status of automatically getting configuration from a TFTP server.

### ● Format

`show autoconfig`

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display the DHCP auto configuration status:

```
Zxxx0:admin#show autoconfig
Command: show autoconfig

Autoconfig State: Disabled

Zxxx0:admin#
```

### 11.2. enable autoconfig

---

#### ● Description

This command is used to enable automatically to get configuration from a TFTP server according to the options in the DHCP reply packet. To employ this method, the DHCP server must be set up to deliver the TFTP server IP address and configuration file name information first.

#### ● Format

**enable autoconfig**

#### ● Parameters

None.

#### ● Restrictions

Only Administrator and Operator-level users can issue this command.

#### ● Example

To enable DHCP auto configuration status:

```
Zxxx0:admin#enable autoconfig
Command: enable autoconfig

Success.

Zxxx0:admin#
```

### 11.3. disable autoconfig

---

#### ● Description

This command is used to disable automatically to get configuration from a TFTP server.

#### ● Format

**disable autoconfig**

#### ● Parameters

None.

- **Restrictions**

Only Administrator and Operator-level users can issue this command.

- **Example**

To disable the DHCP auto configuration status:

```
Zxxx0:admin#disable autoconfig
Command: disable autoconfig

Success.

Zxxx0:admin#
```

## 12. Basic IP Commands

In this chapter, you will configure the following basic IP network settings for each interface.

- IP address (IPv4, IPv6), net mask, enable/disable
- Proxy ARP, which responds to an ARP request to other devices
- MTU (Maximum Transmission Unit) value, which specifies the maximum data size to send (Default: 1500 bytes)
- IPv4 secondary interface

The following setting is also available.

### • IPv6 Link-Local address

In general, if an IPv6 address is not configured, the link-local address is also not configured. When the automatic configuration of link-local address is enabled, the link-local address is automatically configured even though an IPv6 address is not configured, allowing for communications in the local network.

### • IP Setup Interface

Our free application “ZEQUO assist Plus” provides an easy-to-use user interface to change the IP address.

---

```

config ipif <ipif_name 12> [{ipaddress <network_address> | vlan <vlan_name 32> | state [enable
| disable]}] | bootp | dhcp | proxy_arp [enable | disable] {local [enable | disable]} | ipv6
[ipv6address <ipv6networkaddr> | state [enable | disable]] | ip_mtu <value 512-1712> | ipv4
state [enable | disable] | dhcpv6_client [enable | disable] | ip_directed_broadcast [enable |
disable]]
create ipif <ipif_name 12> {<network_address>} <vlan_name 32> {secondary | state [enable |
disable] | proxy_arp [enable | disable] {local [enable | disable]}}
delete ipif [<ipif_name 12> {ipv6address <ipv6networkaddr>} | all]
enable ipif [<ipif_name 12> | all]
disable ipif [<ipif_name 12> | all]
show ipif {<ipif_name 12>}
enable ipif_ipv6_link_local_auto [<ipif_name 12> | all]
disable ipif_ipv6_link_local_auto [<ipif_name 12> | all]
show ipif_ipv6_link_local_auto {<ipif_name 12>}
enable ip_setup_interface
disable ip_setup_interface
show ip_setup_interface

```

---

## 12.1. config ipif

---

### ● Description

Configure the parameters for an L3 interface. For IPv4, only the system interface can be specified for the way to get the IP address. If the mode is set to BOOTP or DHCP, then the IPv4 address will be obtained through the operation of protocols. The manual configuration of the IP address will be of no use. If the mode is configured to BOOTP or DHCP first, and then the user configures IP address later, the mode will be changed to manual configured mode. For IPv6, multiple addresses can be defined on the same L3 interface. For IPv4, multi-netting must be done by creation of a secondary interface. Note that an IPv6 address is not allowed to be configured on a secondary interface.

### ● Format

```
config ipif <ipif_name 12> [{ipaddress <network_address> | vlan <vlan_name 32> |
state [enable | disable]} | bootp | dhcp | proxy_arp [enable | disable] {local [enable |
disable]} | ipv6 [ipv6address <ipv6networkaddr> | state [enable | disable]] | ip_mtu
<value 512-1712> | ipv4 state [enable | disable] | dhcpv6_client [enable | disable] |
ip_directed_broadcast [enable | disable]]
```

### ● Parameters

|                             |                                                                                                                                                                                                                                           |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b>                 | Specifies the IP interface configured.<br><b>&lt;ipif_name 12&gt;</b><br>Enter the name of the IP interface used here. This name can be up to 12 characters long. The default interface is 'System'.                                      |
| <b>ipaddress</b> (Optional) | The IP address and netmask of the IP interface to be created.<br><b>&lt;network_address&gt;</b><br>Specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8). |
| <b>vlan</b>                 | (Optional) The name of the VLAN corresponding to the IP interface.<br><b>&lt;vlan_name 32&gt;</b><br>Specify the VLAN name. The maximum length is 32 characters.                                                                          |
| <b>state</b>                | Enable or disable the IP interface.<br><b>enable</b><br>Enable the IP interface.<br><b>disable</b><br>Disable the IP interface.                                                                                                           |
| <b>bootp</b>                | Enable or disable the BOOTP client to get the IP address.                                                                                                                                                                                 |
| <b>dhcp</b>                 | Enable or disable the DHCP client to get the IP address.                                                                                                                                                                                  |
| <b>proxy_arp</b>            | (Optional) Enable or disable the proxy ARP. This is for the IPv4 function. The default is disabled.<br><b>enable</b><br>Enable the proxy ARP.<br><b>disable</b><br>Disable the proxy ARP.                                                 |



## 12. Basic IP Commands

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>local</b>                 | (Optional) This setting controls whether the system provides the proxy reply for the ARP packets destined for IP addresses located in the same interface as the received interface. When proxy ARP is enabled for an interface, the system will do the proxy reply for the ARP packets destined for IP addresses located on a different interface. For ARP packets destined for IP address located on the same interface, the system will check this setting to determine whether to reply. The default is disabled.<br><b>enable</b><br>Enable the local proxy ARP function.<br><b>disable</b><br>Disable the local proxy ARP function. |
| <b>ipv6</b>                  | The following are IPv6-related parameters.<br><b>ipv6address</b><br>The IPv6 address and subnet prefix of the IPV6 address to be created.<br><ipv6networkaddr><br>The IPv6 address and subnet prefix of the IPV6 address to be created.<br><b>state</b> Enable or disable the IPv6 state of the IP interface.<br><b>enable</b><br>Enable the IPv6 state of the IP interface.<br><b>disable</b><br>Disable the IPv6 state of the IP interface.                                                                                                                                                                                            |
| <b>ip_mtu</b>                | Specifies the IP Layer MTU value used.<br><value 512-1712><br>Enter the IP Layer MTU value used here. The value must be between 512 and 1712.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>dhcpcv6_client</b>        | Specifies the DHCPv6 client state.<br><b>enable</b><br>Enable the DHCPv6 client.<br><b>disable</b><br>Disable the DHCPv6 client.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>ipv4 state</b>            | The state of the IPv4 interface.<br><b>enable</b><br>Enable the IPv4 state of the IP interface.<br><b>disable</b><br>Disable the IPv4 state of the IP interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>ip_directed_broadcast</b> | Specifies the IP directed-broadcast state of the interface.<br><b>enable</b><br>Specifies that the IP directed-broadcast state of the interface will be enabled.<br><b>disable</b><br>Specifies that the IP directed-broadcast state of the interface will be disabled.                                                                                                                                                                                                                                                                                                                                                                  |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the System IP interface:

```
Zxxx0:admin#config ipif System vlan v1
Command: config ipif System vlan v1

Success.

Zxxx0:admin#
```

## 12.2. create ipif

---

### ● Description

This command is used to create an L3 interface. This interface can be configured with IPv4 or IPv6 addresses. Currently, it has a restriction: an interface can have only one IPv4 address defined. But it can have multiple IPv6 addresses defined. Thus, the multinetting configuration of IPv4 must be done through creation of a secondary interface on the same VLAN, instead of directly configuring multiple IPv4 addresses on the same interface. Configuration of IPv6 addresses must be done through the command **config ipif**.

### ● Format

**create ipif** <ipif\_name 12> {<network\_address>} <vlan\_name 32> {secondary | state [enable | disable] | proxy\_arp [enable | disable] {local [enable | disable]}}

### ● Parameters

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;ipif_name 12&gt;</b>    | Specify the name of the interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>&lt;network_address&gt;</b> | (Optional) Specify a host address and length of network mask.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>&lt;vlan_name 32&gt;</b>    | Specify the name of the VLAN corresponding to the IP interface. The maximum length is 32 characters.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>secondary</b>               | The IPv4 secondary interface to be created.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>state</b>                   | The state of the IP interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>enable</b>                  | Enable the state setting.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>disable</b>                 | Disable the state setting.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>proxy_arp</b>               | Enable or disable the proxy ARP function. It is for IPv4 function. The default is disabled.                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>enable</b>                  | Enable the proxy ARP function.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>disable</b>                 | Disable the proxy ARP function.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>local</b>                   | (Optional) This setting controls whether the system provides the proxy reply for the ARP packets destined for IP address located on the same interface as the received interface. When proxy ARP is enabled for an interface, the system will do the proxy reply for the ARP packets destined for an IP address located on a different interface. For ARP packets destined for an IP address located on the same interface, the system will check this setting to determine whether to reply. The default is disabled. |
| <b>enable</b>                  | Enable the local setting.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>disable</b>                 | Disable the local setting.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |



## 12. Basic IP Commands

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create an IP interface petrovic1:

```
Zxxx0:admin#create ipif petrovic1 100.1.1.2/16 VLAN598
Command: create ipif petrovic1 100.1.1.2/16 VLAN598

Success.

Zxxx0:admin#
```

## 12.3. delete ipif

---

### ● Description

This command is used to delete an interface or an IPv6 address.

### ● Format

**delete ipif** [<ipif\_name 12> {ipv6address <ipv6networkaddr>} | all]

### ● Parameters

---

**<ipif\_name 12>**

The name of the interface.

**ipv6address**

(Optional) The IPv6 network address to be deleted.

**<ipv6networkaddr>**

The IPv6 network address to be deleted.

---

**all** All IP interfaces except the System IP interface will be deleted.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete interface petrovic1:

```
Zxxx0:admin#delete ipif petrovic1
Command: delete ipif petrovic1

Success.

Zxxx0:admin#
```

## 12.4. enable ipif

---

### ● Description

This command is used to enable the state for an IPIF. When the state is enabled, the IPv4 processing will be started when an IPv4 address is configured on the IPIF. The IPv6 processing will be started when an IPv6 address is explicitly configured on the IPIF.

### ● Format

**enable ipif** [<ipif\_name 12> | all]

### ● Parameters

|                |                            |
|----------------|----------------------------|
| <ipif_name 12> | The name of the interface. |
| all            | All of the IP interfaces.  |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable the state for interface petrovic1:

```
Zxxx0:admin#enable ipif petrovic1
Command: enable ipif petrovic1

Success.

Zxxx0:admin#
```

## 12.5. disable ipif

---

### ● Description

This command is used to disable the state of an interface.

### ● Format

**disable ipif** [<ipif\_name 12> | all]

### ● Parameters

|                |                            |
|----------------|----------------------------|
| <ipif_name 12> | The name of the interface. |
|----------------|----------------------------|

## 12. Basic IP Commands

---

|            |                           |
|------------|---------------------------|
| <b>all</b> | All of the IP interfaces. |
|------------|---------------------------|

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To disable the state for an interface:

```
Zxxx0:admin#disable ipif petrovic1
Command: disable ipif petrovic1

Success.

Zxxx0:admin#
```

## 12.6. show ipif

---

### ● Description

This command is used to display IP interface settings.

### ● Format

show ipif {<ipif\_name 12>}

### ● Parameters

---

|                                       |
|---------------------------------------|
| <ipif_name 12>                        |
| (Optional) The name of the interface. |

---

### ● Restrictions

None.

### ● Example

To display IP interface settings:

```

Zxxx0:admin#show ipif
Command: show ipif

IP Interface           : System
VLAN Name              : default
Interface Admin State  : Enabled
IPv4 Address           : 10.90.90.90/8 (Manual) Primary
Proxy ARP              : Disabled (Local : Disabled)
IP Directed Broadcast  : Disabled
IPv4 State             : Enabled
IPv6 State             : Enabled
IP MTU                 : 1500

IP Interface           : mgmt_ipif
Status                 : Enabled
IP Address              : 192.168.0.1
Subnet Mask             : 255.255.255.0
Gateway                : 0.0.0.0
Link Status             : Link Down

Total Entries: 2

Zxxx0:admin#

```

## 12.7. enable ipif\_ipv6\_link\_local\_auto

### ● Description

This command is used to enable the auto configuration of link local address when there are no IPv6 addresses explicitly configured. When an IPv6 address is explicitly configured, the link local address will be automatically configured, and the IPv6 processing will be started. When there is no IPv6 address explicitly configured, by default, link local address is not configured and the IPv6 processing will be disabled. By enabling this automatic configuration, the link local address will be automatically configured and IPv6 processing will be started.

### ● Format

**enable ipif\_ipv6\_link\_local\_auto** [<ipif\_name 12> | all]

### ● Parameters

|                |                            |
|----------------|----------------------------|
| <ipif_name 12> | The name of the interface. |
| all            | All of the IP interfaces.  |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.



## 12. Basic IP Commands

### ● Example

To enable the automatic configuration of link local address for an interface:

```
Zxxx0:admin#enable ipif_ipv6_link_local_auto interface1
Command: enable ipif_ipv6_link_local_auto interface1

Success.

Zxxx0:admin#
```

## 12.8. disable ipif\_ipv6\_link\_local\_auto

### ● Description

This command is used to disable the auto configuration of link local address when no IPv6 address is explicitly configured.

### ● Format

disable ipif\_ipv6\_link\_local\_auto [<ipif\_name 12> | all]

### ● Parameters

---

<ipif\_name 12>

The name of the interface.

---

all

All of the IP interfaces.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To disable the automatic configuration of link local address for an interface:

```
Zxxx0:admin#disable ipif_ipv6_link_local_auto interface1
Command: disable ipif_ipv6_link_local_auto interface1

Success.

Zxxx0:admin#
```

## 12.9. show ipif\_ipv6\_link\_local\_auto

### ● Description

This command is used to display the link local address automatic configuration state.

### ● Format

show ipif\_ipv6\_link\_local\_auto {<ipif\_name 12>}

### ● Parameters

---

<ipif\_name 12>

(Optional) The name of the interface.

---

## 12. Basic IP Commands

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To display the link local address automatic configuration state:

```
Zxxx0:admin#show ipif_ipv6_link_local_auto
Command: show ipif_ipv6_link_local_auto

  IPIF: System           Automatic Link Local Address: Disabled

Zxxx0:admin#
```

## **12.10. enable ip\_setup\_interface**

### ● Description

This command is used to enable the IP setup interface function. The factory default status is enabled.

This function provides easy-to-use IP address setting via our application “ZEQUO assist” . If this function is enabled, ZEQUO assist can find this Switching Hubs in the same network segment and can configure each IP address. For security reason, the IP address setting is allowed for 20 minutes from boot-up except factory default setting.

### ● Format

**enable ip\_setup\_interface**

### ● Parameters

None

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable the IP setup interface function:

```
Zxxx0:admin#enable ip_setup_interface
Command: enable ip_setup_interface

Success.

Zxxx0:admin#
```

## 12.11. disable ip\_setup\_interface

---

### ● Description

This command is used to disable the IP setup interface.

### ● Format

disable ip\_setup\_interface

### ● Parameters

None

### ● Restrictions

disable ip\_setup\_interface Only Administrator and Power-User level users can issue this command.

### ● Example

To enable the IP setup interface function:

```
Zxxx0:admin#disable ip_setup_interface
Command: disable ip_setup_interface

Success.

Zxxx0:admin#
```

## 12.12. show ip\_setup\_interface

---

### ● Description

This command is used to display the IP setup interface status.

### ● Format

show ip\_setup\_interface

### ● Parameters

None

### ● Restrictions

None

## 12. Basic IP Commands

### ● Example

To display the IP setup interface status:

```
Zxxx0:admin#show ip_setup_interface
Command: show ip_setup_interface

IP Setup Interface: Enabled

Zxxx0:admin#
```

---

## 13. Bootup Function Commands

---

---

show boot\_file  
config boot\_up command

---

---

### 13.1. show boot\_file

---

#### ● Description

Use this command to show the boot file.

1. 1<sup>st</sup> Bootup Firmware/Configuration cannot be changed forever.
2. The 2<sup>nd</sup> Bootup Firmware can be set by command "**config firmware image <pathname> boot\_up**". The 2<sup>nd</sup> Bootup Configuration can be set by command "**config configuration <pathname> boot\_up**".
3. Actual Bootup Firmware/Configuration is shown the current actual boot up firmware and configuration.
4. If don't input <pathname> for **save** command, the configuration will be saved to the 2<sup>nd</sup> Bootup Configuration path and if this path is not exist, the **save** command will be fail and print prompt message.

#### ● Format

show boot\_file

#### ● Parameters

None.

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## 13. Bootup Function Commands

### ● Example

To show boot\_file

```
Zxxx0:admin#show boot_file
Command: show boot_file

*1st Bootup Firmware      : /d:/sd_runtime.rom
*1st Bootup Configuration : /d:/sd_config.cfg
  *Can not change 1st Bootup File

2nd Bootup Firmware      : /c:/runtime.rom
2nd Bootup Configuration : /c:/config.cfg

Actual Bootup Firmware   : /c:/runtime.rom
Actual Bootup Configuration : /c:/config.cfg

SD card: d drive, FLASH: c drive
Zxxx0:admin#
```

## 13.2. config boot\_up command

---

### ● Description

This command is used to config the boot\_up command.

1. The parameter "<pathname>" can specifies file on either SD card or flash. Pathname of the boot up file will be recorded in the system after issue the commands above. And the 2nd boot up files can be shown by command "show boot\_file".
2. When use "config firmware image <pathname> boot\_up" or "config configuration <pathname> boot\_up" commands, will check the file indicated by <pathname> is existed or valid for boot up. If the file is not existed or not valid for boot up, executing command will be failed.
3. The 2<sup>nd</sup> Bootup Firmware/Configuration will not be changed until using command to configure it. That means it will not clear the 2<sup>nd</sup> Bootup Firmware/Configuration pathname when it is saved in SD card even though the SD card is pushed out or insert SD card no this boot file or system is rebooted.
4. For 2<sup>nd</sup> Bootup Firmware or 2<sup>nd</sup> Bootup Configuration, the factory default boot up file should be: /c:/runtime.rom, /c:/config.cfg.

### ● Format

```
config firmware image <pathname> boot_up
config configuration <pathname> boot_up
```

### ● Parameters

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

None.



## 14. BPDU Attack Protection Commands

BPDU (Bridge Protocol Data Unit) is a spanning tree protocol and a packet to detect loops. In general, it is not received by any other than specific ports. If BPDU packets were received by an unexpected port, a loop failure may have occurred or an unauthorized Switching Hub may have been added, resulting in the path change.

BPDU Attack Protection is a function to protect network by setting actions, such as discarding packets or shutting down ports, when receiving unexpected BPDU packets.

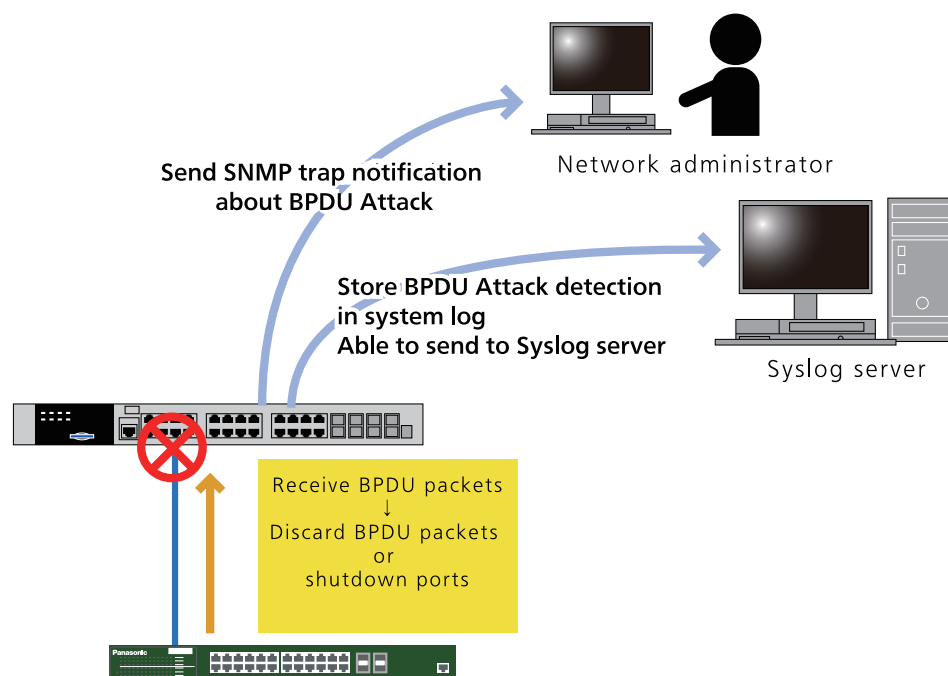


Figure 14-1 BPDU Attack Protection overview

The commands are used to configure the Switching Hub to send SNMP trap notification or log when packets are discarded or ports are shut down because of the protection function. You can also configure to recover the state automatically after a specified time or manually by a network administrator.

```
config bpdu_protection ports [<portlist> | all] {state [enable | disable] | mode [drop | block | shutdown]}}(1)
config bpdu_protection recovery_timer [<sec 60-1000000> | infinite]
config bpdu_protection [trap | log] [none | attack_detected | attack_cleared | both]
enable bpdu_protection
disable bpdu_protection
show bpdu_protection {ports {<portlist>}}
```

## 14.1. config bpdu\_protection ports

### ● Description

This command is used to configure port state and mode for BPDU protection.

### ● Format

config bpdu\_protection ports [<portlist> | all] {state [enable | disable] | mode [drop | block | shutdown]} (1)

### ● Parameters

|                 |                                                                                                            |
|-----------------|------------------------------------------------------------------------------------------------------------|
| <portlist>      | Specify a range of ports to be configured.                                                                 |
| <b>all</b>      | Specify to set all ports in the system.                                                                    |
| <b>state</b>    | Specify the BPDU protection state. The default state is disabled.                                          |
| <b>enable</b>   | Enable the BPDU protection state.                                                                          |
| <b>disable</b>  | Disable the BPDU protection state.                                                                         |
| <b>mode</b>     | Specify the BPDU protection mode. The default mode is shutdown.                                            |
| <b>drop</b>     | Specify to drop all received BPDU packets when the port enters the under attack state.                     |
| <b>block</b>    | Specify to drop all packets (include BPDU and normal packets) when the port enters the under attack state. |
| <b>shutdown</b> | Specify to shut down the port when the port enters the under attack state.                                 |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure port state to enable and drop mode:

```
Zxxx0:admin#config bpdu_protection ports 1 state enable mode drop
Command: config bpdu_protection ports 1 state enable mode drop

Success.
Zxxx0:admin#
```

### **14.2. config bpdu\_protection recovery\_timer**

#### ● Description

When a port enters the under attack state, it can be disabled or blocked based on the configuration. The state can be recovered manually or by the auto recovery mechanism. This command is used to configure the auto-recovery timer. To manually recover the port, the user needs to disable and re-enable the port.

#### ● Format

**config bpdu\_protection recovery\_timer [<sec 60-1000000> | infinite]**

#### ● Parameters

---

**<sec 60-1000000>**

Specify the timer (in seconds) used by the Auto-recovery mechanism to recover the port.  
The valid range is 60 to 1000000. Auto-recovery time is 60 seconds by default.

---

**infinite** Specify the port will not be auto recovered.

---

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To configure the BPDU protection recovery timer to 120 seconds for the entire Switching Hub:

```
Zxxx0:admin#config bpdu_protection recovery_timer 120
Command: config bpdu_protection recovery_timer 120

Success.

Zxxx0:admin#
```

## 14.3. config bpdu\_protection

### ● Description

This command is used to configure the BPDU protection trap state or log state.

### ● Format

**config bpdu\_protection** [trap | log] [none | attack\_detected | attack\_cleared | both]

### ● Parameters

|                        |                                                                                      |
|------------------------|--------------------------------------------------------------------------------------|
| <b>trap</b>            | Specify the trap state.                                                              |
| <b>log</b>             | Specify the log state.                                                               |
| <b>none</b>            | Specify neither attack_detected nor attack_cleared is trapped or logged.             |
| <b>attack_detected</b> | Specify events will be logged or trapped when the BPDU attacks is detected.          |
| <b>attack_cleared</b>  | Specify events will be logged or trapped when the BPDU attacks is cleared.           |
| <b>both</b>            | Specify the events of attack_detected and attack_cleared shall be trapped or logged. |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the BPDU protection trap state as both for the entire Switching Hub:

```
Zxxx0:admin#config bpdu_protection trap both
Command: config bpdu_protection trap both

Success.

Zxxx0:admin#
```

## 14.4. enable bpdu\_protection

### ● Description

This command is used to enable BPDU protection globally for the entire Switching Hub.

### ● Format

**enable bpdu\_protection**

### ● Parameters

None.

## 14. BPDU Attack Protection Commands

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable BPDU protection for the entire Switching Hub:

```
Zxxx0:admin#enable bpdu_protection
Command: enable bpdu_protection

Success.

Zxxx0:admin#
```

## 14.5. disable bpdu\_protection

---

### ● Description

This command is used to disable BPDU protection globally for the entire Switching Hub.

### ● Format

**disable bpdu\_protection**

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To disable BPDU protection:

```
Zxxx0:admin#disable bpdu_protection
Command: disable bpdu_protection

Success.

Zxxx0:admin#
```

## 14.6. show bpdu\_protection

### ● Description

This command is used to display BPDU protection global configuration or per port configuration and current status.

### ● Format

**show bpdu\_protection {ports {<portlist>}}**

### ● Parameters

|                         |                                                      |
|-------------------------|------------------------------------------------------|
| <b>ports</b>            | (Optional) Specify all ports to be displayed.        |
| <b>&lt;portlist&gt;</b> | (Optional) Specify a range of ports to be displayed. |

### ● Restrictions

- None.

### ● Example

To display BPDU protection information for the entire Switching Hub:

```
Zxxx0:admin#show bpdu_protection
Command: show bpdu_protection

BPDU Protection Global Settings
-----
BPDU Protection Status      : Disabled
BPDU Protection Recover Time : 60 seconds
BPDU Protection Trap State   : None
BPDU Protection Log State    : Both

Zxxx0:admin#
```

To display BPDU protection status for ports 1 to 3:

```
Zxxx0:admin#show bpdu_protection ports 1-3
Command: show bpdu_protection ports 1-3

Port  State      Mode      Status
-----
1     Disabled     Shutdown  Normal
2     Disabled     Shutdown  Normal
3     Disabled     Shutdown  Normal

Zxxx0:admin#
```

---

## 15. Cable Diagnostics Commands

---

The commands are used to diagnose the link status, failure status, and possible failure position of copper cabling connected to ports of this Switching Hub. After diagnosing open, short, and crosstalk of the cable, the cable length can be measured if there is no open or short.

---

**NOTE** Optical fiber cables are not diagnosed.

---

---

**cable\_diag ports** [<portlist> | all]

---

### 15.1. cable\_diag ports

---

#### ● Description

This command is used to test copper cabling.

For 10/100Based-TX link speed RJ45 cables, two pairs of cables will be diagnosed.

For 1000Base-T link speed RJ45 cables, four pairs of cables will be diagnosed.

The type of cable errors can be open, short, or crosstalk.

- **Open** means that the cable in the error pair does not have a connection at the specified position.
- **Short** means that the cables in the error pair has a short problem at the specified position.
- **Crosstalk** means that the cable in the error pair has a crosstalk problem at the specified position.

#### For Fast Ethernet ports:

- Where the **link partner** is **powered on with no errors** and the **link is up**, this command cannot detect the cable length.
- Where the **link partner** is **powered on with errors**, this command can detect whether the error is open, short, or crosstalk. In this case this command can also detect the distance of the error.
- Where the **link partner** is **powered down with no errors** and the **link is down**, this command cannot detect the cable length.
- When the **link partner** is **powered down with errors**, this command can detect whether the error is open, short, or crosstalk. In this case this command can also detect the distance of the error.
- When there is **no link partner** with **no errors** and the **link is up**, this command can detect the cable length.
- When there is **no link partner** with errors, this command can detect whether the error is open, short, or crosstalk. In this case this command can also detect the distance of the error.

**For Gigabit Ethernet ports:**

- Where the **link partner** is **powered on with no errors** and the **link is up**, this command cannot detect the cable length.
- Where the **link partner** is **powered on with errors**, this command can detect whether the error is open, short, or crosstalk. In this case this command can also detect the distance of the error.
- Where the **link partner** is **powered down with no errors** and the **link is down**, this command cannot detect the cable length.
- When the **link partner** is **powered down with errors**, this command can detect whether the error is open, short, or crosstalk. In this case this command can also detect the distance of the error.
- When there is no **link partner** with **no errors** and the **link is up**, this command can detect the cable length.
- When there is **no link partner with errors**, this command can detect whether the error is open, short, or crosstalk. In this case this command can also detect the distance of the error.

The Cable length range that can be detected is as follows:

- Smaller than 50m (<50m)
- Between 50m and 80m (50m~80m)
- Between 80m and 100m (80m~100m)
- Greater than 100m (>100m)

The cable length deviation value is 5m, therefore if the cable length is less than 5m, 'No Cable' may be displayed under the 'Test Result' column.

---

**NOTE** This test will consume a low number of packets. Since this test is for copper cable, the port with fiber cable will be skipped from the test.

---

## ● Format

`cable_diag ports [<portlist> | all]`

## ● Parameters

---

`<portlist>` Specify a range of ports to be configured.

---

`<portlist>` Specify to set all ports in the system.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To test the cable on ports 1 to 4, and 8:



## 15. Cable Diagnostics Commands

```
Zxxx0:admin# cable_diag ports 1:1-1:10,1:21
```

```
Command: cable_diag ports 1:1-1:10,1:21
```

```
Perform Cable Diagnostics ...
```

| Port  | Type       | Link Status | Test Result                                                                                  | Cable Length (M) |
|-------|------------|-------------|----------------------------------------------------------------------------------------------|------------------|
| ----- | -----      | -----       | -----                                                                                        | -----            |
| 1:1   | 1000BASE-T | Link Up     | OK                                                                                           | 65               |
| 1:2   | 1000BASE-T | Link Up     | OK                                                                                           | -                |
| 1:3   | 1000BASE-T | Link Down   | Shutdown                                                                                     | 25               |
| 1:4   | 1000BASE-T | Link Down   | Shutdown                                                                                     | -                |
| 1:5   | 1000BASE-T | Link Down   | Unknown                                                                                      | -                |
| 1:6   | 1000BASE-T | Link Down   | Pair 1 Crosstalk at 30M<br>Pair 2 Crosstalk at 30M<br>Pair 3 OK at 110M<br>Pair 4 OK at 110M | -                |
| 1:7   | 1000BASE-T | Link Down   | NO Cable                                                                                     | -                |
| 1:8   | 1000BASE-T | Link Down   | Pair 1 Open at 16M<br>Pair 2 Open at 16M<br>Pair 3 OK at 50M<br>Pair 4 OK at 50M             | -                |
| 1:9   | 1000BASE-T | Link Down   | Pair 1 Short at 5M<br>Pair 2 Short at 5M<br>Pair 3 OK at 110M<br>Pair 4 OK at 110M           | -                |
| 1:10  | 1000BASE-T | Link Down   | Pair 1 Unknown<br>Pair 2 Short at 5M<br>Pair 3 OK at 110M<br>Pair 4 OK at 110M               | -                |
| 1:21  | 1000BASE-X | Link Up     | Unknown                                                                                      | -                |

```
Zxxx0:admin#
```

## 16. Command List History Commands

The "?" command is used to display available commands and options in this Switching Hub.

Previously entered commands are stored in the command history and can be recalled with the up-arrow key for entry. The default number of commands stored in the history is 25. You can set it between 1 and 40.

---

```
?{<Command>}
show command_history
config command_history <value 1-40>
```

---

### 16.1. ?

---

#### ● Description

This command is used to display all of the commands available, on the current login account level, through the Command Line Interface (CLI).

#### ● Format

? {<Command>}

#### ● Parameters

---

```
<Command>
(Optional) Specify a command.
```

---



---

**NOTE** If no command is specified, the system will display all commands of the corresponding user level.

---

#### ● Restrictions

None.

#### ● Example

To display all commands:

## 16. Command List History Commands

```
Zxxx0:admin#?  
Command: ?  
  
..  
?  
cable_diag ports  
cd  
clear  
clear address_binding dhcp_snoop binding_entry ports  
clear arptable  
clear attack_log  
clear counters  
clear dhcp binding  
clear dhcp conflict_ip  
clear fdb  
clear historical_counters ports  
clear igmp_snooping data_driven_group  
clear igmp_snooping statistic counter  
clear log  
clear mac_based_access_control auth_state  
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

To display the syntax for "config account":

```
Zxxx0:admin#? config account  
Command: ? config account  
  
Command: config account  
Usage: <username> {encrypt [plain_text| sha_1] <password>}  
Description: Used to configure user accounts.  
  
Zxxx0:admin#
```

## 16.2. show command\_history

---

### ● Description

This command is used to display the command history.

### ● Format

**show command\_history**

### ● Parameters

None.

### ● Restrictions

None.

## ● Example

To display the command history:

```
Zxxx0:admin# show command_history
Command: show command_history

?
?
show traffic_segmentation 1-6
config traffic_segmentation 1-6 forward_list 7-8
config radius delete 1
config radius add 1 10.48.74.121 key manager default
config 802.1x reauth port_based ports all
config 802.1x init port_based ports all
config 802.1x auth_mode port_based
config 802.1x auth_parameter ports 1-50 direction both
config 802.1x capability ports 1-5 authenticator
show 802.1x auth_configuration ports 1
show 802.1x auth_state ports 1-5
enable 802.1x
show 802.1x auth_state ports 1-5
show igmp_snooping
enable igmp_snooping

Zxxx0:admin#
```

## 16.3. config command\_history

---

### ● Description

This command is used to configure the number of commands that the Switching Hub can record. The Switching Hub can keep records for the last 40 (maximum) commands you entered.

### ● Format

**config command\_history <value 1-40>**

### ● Parameters

---

**<value 1-40>**

Specify the number of commands (1 to 40) that the Switching Hub can record. The default value is 25.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

## 16. Command List History Commands

To configure the number of commands the Switching Hub can record to the last 20 commands:

```
Zxxx0:admin#config command_history 20
Command: config command_history 20

Success.

Zxxx0:admin#
```

---

## 17. Command Logging Command List

---

The commands are used to log the execution history of commands that change this Switching Hub's settings.

---

**NOTE** The history of commands that do not affect the setting changes (e.g. show) is not stored.

---

---

enable command logging  
disable command logging  
show command logging

---

### 17.1. enable command logging

---

#### ● Description

The enable command logging command is used to enable the command logging function.

---

**NOTE** When the Switching Hub is under the booting procedure and the procedure of downloading the configuration to execute immediately, all configuration commands should not be logged. When the user is under AAA authentication, the user name should not be changed if the user uses "enable admin" command to replace its privilege.

---

#### ● Format

enable command logging

#### ● Parameters

None.

#### ● Restrictions

Only Administrator-level users can issue this command.

#### ● Example

To enable the command logging function:

## 17. Command Logging Command List

```
Zxxx0:admin# enable command logging
Command: enable command logging

Success.

Zxxx0:admin#
```

### 17.2. disable command logging

---

#### ● Description

The disable command logging command is used to disable the command logging function.

#### ● Format

disable command logging

#### ● Parameters

None.

#### ● Restrictions

Only Administrator-level users can issue this command.

#### ● Example

To disable the command logging:

```
Zxxx0:admin# disable command logging
Command: disable command logging

Success.

Zxxx0:admin#
```

### 17.3. show command logging

---

#### ● Description

This command displays the Switching Hub's general command logging configuration status.

#### ● Format

show command logging

- **Parameters**

None.

- **Restrictions**

Only Administrator and Operator-level users can issue this command.

- **Example**

To show the command logging configuration status:

```
Zxxx0:admin# show command logging
Command: show command logging

Command Logging State : Disabled

Zxxx0:admin#
```



## 17. Command Logging Command List

## 18. Network Access Authentication Command List

The commands are used to configure the authentication server settings for network access authentication.

---

```

config authentication ports [<portlist> | all] {auth_mode [port_based | host_based {vlanid
    <vidlist> state [enable | disable]}(1)
config authentication mac_format {case [lowercase | uppercase] | delimiter {[hyphen | colon |
    dot | none] | number [1 | 2 | 5]}(1)}(1)
show authentication ports {<portlist>}
enable authorization network attributes
disable authorization network attributes
show authorization
config authentication server failover [local | permit | block]
show authentication
show authentication mac_format
  
```

---

### 18.1. config authentication ports

#### ● Description

This command is used to configure security port(s).

#### ● Format

```

config authentication ports [<portlist> | all] {auth_mode [port_based | host_based {vlanid
    <vid_list> state [enable | disable]}]}(1)
  
```

## 18. Network Access Authentication Command List

### ● Parameters

---

**<portlist>** Enter the list of ports to be configured here.

---

**all** Specify all ports on the Switch.

---

**auth\_mode**

(Optional) Specify the authentication mode used.

**port\_based**

If one of the attached hosts passes the authentication, all hosts on the same port will be granted to access network. If the user fails to authorize, this port will keep trying the next authentication

**host\_based**

Every user can be authenticated individually. v2.01 and later, can authenticate client on specific authentication VLAN(s) only for WAC.

**vlanid**

(Optional) Specific authentication VLAN(s). This is useful when different VLANs on the Switch have different authentication requirements.

**<vidlist>**

Enter the VLAN ID list here.

**state**

(Optional) Specify the VID list's authentication state.

**enable**

Assign the specified VID list as authentication VLAN(s).

**disable**

Remove the specified VID list from authentication VLAN(s). If "vlanid" is not specified, or all VLANs is disabled, means do not care which VLAN the client comes from, the client will be authenticated if the client's MAC(not care the VLAN) is not authenticated. After the client is authenticated, the client will not be re-authenticated when received from other VLANs. All VLANs are disabled by default.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

The following example sets the authorization mode and authentication VLAN for all ports.

```
Zxxx0:admin# config authentication ports all auth_mode host_based vlanid 1 state enable
Command: config authentication ports all auth_mode host_based vlanid 1 state enable

Success.

Zxxx0:admin#
```

## 18.2. config authentication mac\_format

### ● Description

This command is used to configure the MAC address format of the RADIUS authentication user name for MAC-based Access Control.

### ● Format

**config authentication mac\_format {case [lowercase | uppercase] | delimiter {[hyphen | colon | dot | none] | number [1 | 2 | 5]}(1)}(1)**

### ● Parameters

|                  |                                                                                       |
|------------------|---------------------------------------------------------------------------------------|
| <b>case</b>      | (Optional) Specify the letter format.                                                 |
| <b>lowercase</b> | User lowercase letters, e.g. aabbccddeeff.                                            |
| <b>uppercase</b> | User uppercase letters, e.g. AABBCCDDEEFF.                                            |
| <b>delimiter</b> | (Optional) Specify whether to use delimiter and number of delimiters for MAC address. |
| <b>hyphen</b>    | (Optional) Use "-" when specifying MAC address, e.g. aa-bb-cc-dd-ee-ff.               |
| <b>colon</b>     | (Optional) Use ":" when specifying MAC address, e.g. aa:bb:cc:dd:ee:ff.               |
| <b>dot</b>       | (Optional) Use "." when specifying MAC address, e.g. aa.bb.cc.dd.ee.ff.               |
| <b>none</b>      | (Optional) Do not use any delimiter when specifying MAC address, e.g. aabbccddeeff.   |
| <b>number</b>    | (Optional) Specify the number of delimiters.                                          |
| <b>1</b>         | Use one delimiter, e.g. aabbcc-ddeeff.                                                |
| <b>2</b>         | Use two delimiters, e.g. aabb-ccdd-eeff.                                              |
| <b>5</b>         | Use five delimiters, e.g. aa-bb-cc-dd-ee-ff.                                          |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the MAC address format to IEFT style:

```
Zxxx0:admin# config authentication mac_format case uppercase delimiter hyphen
number 5
Command: config authentication mac_format case uppercase delimiter hyphen number 5

Success.

Zxxx0:admin#
```

## 18.3. show authentication ports

---

- **Description**

This command is used to display authentication setting on port(s).

- **Format**

show authentication ports {<portlist>}

- **Parameters**

---

<portlist>Enter a list of ports to be displayed.

---

- **Restrictions**

None.

## ● Example

This example displays authentication setting for all ports:

```
Zxxx0:admin# show authentication ports
Command: show authentication ports

Port   Auth Mode   Authentication VLAN(s)
-----
1      Host-based
2      Host-based
3      Host-based
4      Host-based
5      Host-based
6      Host-based
7      Host-based
8      Host-based
9      Host-based
10     Host-based
11     Host-based
12     Host-based
13     Host-based
14     Host-based
15     Host-based
16     Host-based
17     Host-based
18     Host-based
19     Host-based
20     Host-based
21     Host-based
22     Host-based
23     Host-based
24     Host-based
25     Host-based
26     Host-based
27     Host-based
28     Host-based

Zxxx0:admin#
```

## 18.4. enable authorization attributes

---

### ● Description

This command is used to enable authorization.

### ● Format

enable authorization attributes

### ● Parameters

None.

## 18. Network Access Authentication Command List

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

This example sets authorization global state enabled:

```
Zxxx0:admin# enable authorization attributes
Command: enable authorization attributes

Success.

Zxxx0:admin#
```

## **18.5. disable authorization attributes**

---

### ● Description

This command is used to disable authorization.

### ● Format

**disable authorization attributes**

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

This example sets authorization global state disabled:

```
Zxxx0:admin# disable authorization attributes
Command: disable authorization attributes

Success.

Zxxx0:admin#
```

## 18.6. show authorization

---

### ● Description

This command is used to display authorization status.

### ● Format

show authorization

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

This example displays authorization status:

```
Zxxx0:admin# show authorization
Command: show authorization

Authorization for Attributes: Disabled

Zxxx0:admin#
```

## 18.7. config authentication server failover

---

### ● Description

This command is used to configure authentication server failover function.

### ● Format

config authentication server failover [local | permit | block]

### ● Parameters

|               |                                                 |
|---------------|-------------------------------------------------|
| <b>local</b>  | Use local DB to authenticate the client.        |
| <b>permit</b> | The client is always regarded as authenticated. |
| <b>block</b>  | Block the client (Default setting).             |



## 18. Network Access Authentication Command List

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

Set authentication server auth fail over state:

```
Zxxx0:admin# config authentication server failover local
Command: config authentication server failover local

Success.

Zxxx0:admin#
```

## 18.8. show authentication

---

### ● Description

This command is used to display authentication global configuration.

### ● Format

**show authentication**

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To show authentication global configuration:

```
Zxxx0:admin# show authentication
Command: show authentication

Authentication Server Failover: Block.

Zxxx0:admin#
```

## 18.9. **show authentication mac\_format**

---

- **Description**

This command is used to display the authentication MAC format settings.

- **Format**

**show authentication mac\_format**

- **Parameters**

None.

- **Restrictions**

None.

- **Example**

To display the authentication MAC format settings:

```
Zxxx0:admin# show authentication mac_format
Command: show authentication mac_format

Case           : Uppercase
Delimiter       : None
Delimiter Number : 5

Zxxx0:admin#
```

## 19. Digital Diagnostic Monitoring (DDM) Commands

---

```

config ddm ports [ <portlist> | all ] [[temperature_threshold { high_alarm <degrees> | low_alarm
<degrees> | high_warning <degrees> | low_warning <degrees> } | voltage_threshold {
high_alarm <voltage> | low_alarm <voltage> | high_warning <voltage> |
low_warning<voltage> } | bias_current_threshold { high_alarm <milliampere> | low_alarm
<milliampere> | high_warning <milliampere> | low_warning<milliampere> } |
tx_power_threshold { high_alarm <mw_or_dbm> | low_alarm <mw_or_dbm> |
high_warning <mw_or_dbm> | low_warning<mw_or_dbm> } | rx_power_threshold {
high_alarm <mw_or_dbm> | low_alarm <mw_or_dbm> | high_warning <mw_or_dbm> |
low_warning <mw_or_dbm> } ] | {state [enable|disable] | shutdown [alarm | warning |
none]]]
config ddm [trap | log] [enable|disable]
config ddm power_unit [mw|dbm]
show ddm
show ddm ports {<portlist>} [status|configuration]

```

---

### 19.1. config ddm ports temperature\_threshold

#### ● Description

This command is used to configure the thresholds of temperature of the specified ports. The command configures the temperature thresholds of the specified ports. The precision of the effective threshold is dependent on the hardware.

#### ● Format

```

config ddm ports [<portlist> | all] temperature_threshold { high_alarm <degrees> |
low_alarm <degrees> | high_warning <degrees> | low_warning <degrees> } (1)

```

#### ● Parameters

---

**ports**

**<portlist>**

Specifies a range of ports to be configured. (The portlist format: UnitID: port number).

**all**

If 'all' parameter is chosen, all optic ports' operating parameters will be configured.

---

**temperature\_threshold**

Specifies the threshold of the optic module's temperature in centigrade. At least one parameter shall be specified for this threshold.

---

---

### high\_alarm

<degrees>

Specifies the high threshold value for the temperature alarm.

When the operating parameter rises above this value, the action associated with the alarm is taken. The range of this parameter is from -128 to 127.996 degrees Celsius.

---

### low\_alarm

<degrees>

Specifies the low threshold value for the temperature alarm.

When the operating parameter falls below this value, the action associated with the alarm is taken. The range of this parameter is from -128 to 127.996 degrees Celsius.

---

### high\_warning

<degrees>

Specifies the high threshold value for temperature warning.

When the operating parameter rises above this value, the action associated with the warning is taken. The range of this parameter is from -128 to 127.996 degrees Celsius.

---

### low\_warning

<degrees>

Specifies the low threshold value for temperature warning.

When the operating parameter falls below this value, the action associated with the warning is taken. The range of this parameter is from -128 to 127.996 degrees Celsius.

---

## ● Restrictions

Only Administrator and Operator-level users can issue this command.

## ● Example

To configure the port 21's temperature threshold:

```
Zxxx0:admin# config ddm ports 21 temperature threshold high_alarm 84.9555
low_alarm -10 high_warning 70 low_warning 2.2525
Command: config ddm ports 21 temperature_threshold high_alarm 84.9555 low_alarm -10
high_warning 70 low_warning 2.2525
```

According to the DDM precision definition, closest value 84.9531 and 2.25 are chosen.

Success.

```
Zxxx0:admin#
```

## 19.2. config ddm ports voltage\_threshold

### ● Description

The command configures the voltage thresholds of the specified ports. The precision of the effective threshold is dependent on the hardware.

### ● Format

```
config ddm ports [<portlist> | all] voltage_threshold { high_alarm < voltage > |
low_alarm < voltage > igh_warning < voltage >
| low_warning < voltage > } (1)
```

### ● Parameters

---

#### ports

##### <portlist>

Specifies a range of ports to be configured. (The portlist format: UnitID: port number).

##### all

If 'all' parameter is chosen, all optic ports' operating parameters will be configured.

---

#### voltage\_threshold

Specifies the threshold of optic module's voltage.

---

#### high\_alarm

##### <voltage>

Specifies the high threshold for the voltage alarm.

When the operating parameter rises above this value, the action associated with the alarm is taken. The range of this parameter is from 0 to 6.5535 voltages.

---

#### low\_alarm

##### <voltage>

Specifies the low threshold for the voltage alarm.

When the operating parameter falls below this value, the action associated with the alarm is taken. The range of this parameter is from 0 to 6.5535 voltages.

---

#### high\_warning

##### <voltage>

Specifies the high threshold for the voltage warning.

When the operating parameter rises above this value, the action associated with the warning is taken. The range of this parameter is from 0 to 6.5535 voltages.

---

#### low\_warning

##### <voltage>

Specifies the low threshold for the voltage warning.

When the operating parameter falls below this value, the action associated with the warning is taken. The range of this parameter is from 0 to 6.5535 voltages.

---

**NOTE**

The parameter type voltage allows the user to input the decimal in the CLI command. The CLI does not restrict the number of input digits, the only limitation of the inputted digits are the size of the command buffer and the float-point precision. The user inputted digits will be converted to the floating-point number and applied to the configuration database. The default precision of a floating-point number is 6 digits. For example, input "12.3456", will get a float value 12.3456, input "12.3456789", will get a float value 12.3457.

### ● Restrictions

Administrators and operators.

### ● Example

To configure the port 21's voltage threshold

```
Zxxx0:admin# config ddm ports 21 voltage_threshold high_alarm 4.25 low_alarm 2.5
high_warning 3.5 low_warning 3
Command: config ddm ports 21 voltage_threshold high_alarm 4.25 low_alarm 2.5 high_w
arning 3.5 low_warning 3
```

```
Success.
```

```
Zxxx0:admin#
```

## 19.3. config ddm ports bias\_current\_threshold

---

### ● Description

This command is used to configure the thresholds of bias current of the specified ports. The command configures the bias current thresholds of the specified ports. The precision of the effective threshold is dependent on the hardware.

### ● Format

```
config ddm ports [<portlist> | all] bias_current_threshold { high_alarm < milliampere > |
low_alarm < milliampere > | high_warning < milliampere > |
low_warning < milliampere > } (1)
```

### ● Parameters

---

#### ports

##### <portlist>

Specifies a range of ports to be configured. (The portlist format: UnitID: port number).

##### all

If 'all' parameter is chosen, all optic ports' operating parameters will be configured.

---

#### bias\_current\_threshold

Specifies the threshold of the optic module's bias current.

---

#### high\_alarm

##### <milliampere>

Specifies the high threshold for the bias current alarm.

When the operating parameter rises above this value, the action associated with the alarm is taken. The range of this parameter is from 0 to 131mA.

---

#### low\_alarm

##### <milliampere>

Specifies the low threshold for the bias current alarm.

When the operating parameter falls below this value, the action associated with the alarm is taken. The range of this parameter is from 0 to 131mA

---

#### high\_warning

##### <milliampere>

Specifies the high threshold for the bias current warning.

When the operating parameter rises above this value, the action associated with the warning is taken. The range of this parameter is from 0 to 131mA

---

#### low\_warning

##### <milliampere>

Specifies the low threshold for the bias current warning.

When the operating parameter falls below this value, the action associated with the warning is taken. The range of this parameter is from 0 to 131mA

---

**NOTE**

The parameter type milliampere allows the user to input the decimal in the CLI command. The CLI does not restrict the number of input digits, the only limitation of the inputted digits are the size of the command buffer and the float-point precision. The user inputted digits will be converted to the floating-point number and applied to the configuration database. The default precision of a floating-point number is 6 digits. For example, input "12.3456", will get a float value 12.3456, input "12.3456789", will get a float value 12.3457.

## ● Restrictions

Administrators and operators.

## ● Example

To configure the port 21's voltage threshold

```
Zxxx0:admin# config ddm ports 21 bias_current_threshold high_alarm 7.25 low_alarm
0.004 high_warning 0.5 low_warning 0.008
Command: config ddm ports 21 bias_current_threshold high_alarm 7.25 low_alarm 0.004
high_warning 0.5 low_warning 0.008

Success

Zxxx0:admin#
```

## 19.4. config ddm ports tx\_power\_threshold

### ● Description

This command is used to configure the thresholds of the output power of the specified ports. The command configures the bias current thresholds of the specified ports. The precision of the effective threshold is dependent on the hardware.

### ● Format

```
config ddm ports [<portlist> | all] tx_power_threshold { high_alarm < milliwatts > |
low_alarm < milliwatts > | high_warning < milliwatts > | low_warning < milliwatts > } (1))
```

### ● Parameters

#### ports

##### <portlist>

Specifies a range of ports to be configured. (The portlist format: UnitID: port number).

**all** If 'all' parameter is chosen, all optic ports' operating parameters will be configured.

#### tx\_power\_threshold

Specifies the threshold of the optic module's output power.



## 19. Didital Diagnostic Monitoring (DDM) Commands

---

### high\_alarm

#### <mw\_or\_dbm>

Specifies the high threshold for the transmit power alarm.

When the operating parameter rises above this value, the action associated with alarm is taken.

If the unit is mW, the range of this parameter is from 0 to 6.5535mW. If the unit is dBm, the range of this parameter is form -40 to 8.1647dBm.

---

### low\_alarm

#### <mw\_or\_dbm>

Specifies the low threshold for the transmit power alarm.

When the operating parameter falls below this value, the action associated with the alarm is taken.

If the unit is mW, the range of this parameter is from 0 to 6.5535mW. If the unit is dBm, the range of this parameter is form -40 to 8.1647dBm.

---

### high\_warning

#### <mw\_or\_dbm>

Specifies the high threshold for the transmit power warning.

When the operating parameter rises above this value, the action associated with the warning is taken.

If the unit is mW, the range of this parameter is from 0 to 6.5535mW. If the unit is dBm, the range of this parameter is form -40 to 8.1647dBm.

---

### low\_warning

#### <mw\_or\_dbm>

Specifies the low threshold for the transmit power warning.

When the operating parameter falls below this value, the action associated with the warning is taken.

If the unit is mW, the range of this parameter is from 0 to 6.5535mW. If the unit is dBm, the range of this parameter is form -40 to 8.1647dBm.

---

### NOTE

The threshold unit **mW** or **dBm** allows the user to input the decimal in the CLI command. The CLI does not restrict the number of input digits, the only limitation of the inputted digits are the size of the command buffer and the float-point precision. The user inputted digits will be converted to the floating-point number and applied to the configuration database.

The default precision of a floating-point number is 6 digits.

For example, input "12.3456", will get a float value 12.3456, input "12.3456789", will get a float value 12.3457.

---

## ● Restrictions

Administrators and operators.

## ● Example

To configure the port 21's transmit power threshold

## 19. Digital Diagnostic Monitoring (DDM) Commands

```
Zxxx0:admin# config ddm ports 21 tx_power_threshold high_alarm 0.625 low_alarm  
0.006 high_warning 0.55 low_warning 0.008  
Command: config ddm ports 21 tx_power_threshold high_alarm 0.625 low_alarm 0.006  
high_warning 0.55 low_warning 0.008
```

Success.

```
Zxxx0:admin#
```

## 19.5. config ddm ports rx\_power\_threshold

### ● Description

This command is used to configure the thresholds of the output power of the specified ports. The command configures the bias current thresholds of the specified ports. The precision of the effective threshold is dependent on the hardware.

### ● Format

```
config ddm ports [<portlist> | all] tx_power_threshold { high_alarm < mw_or_dbm > |
low_alarm < mw_or_dbm > | high_warning < mw_or_dbm > |
low_warning < mw_or_dbm > } (1))
```

### ● Parameters

#### ports

##### <portlist>

Specifies a range of ports to be configured. (The portlist format: UnitID: port number).

##### all

If 'all' parameter is chosen, all optic ports' operating parameters will be configured.

#### tx\_power\_threshold

Specifies the threshold of the optic module's output power.

#### high\_alarm

##### <mw\_or\_dbm>

Specifies the high threshold for the transmit power alarm.

When the operating parameter rises above this value, the action associated with alarm is taken.

If the unit is mW, the range of this parameter is from 0 to 6.5535mW. If the unit is dBm, the range of this parameter is from -40 to 8.1647dBm.

#### low\_alarm

##### <mw\_or\_dbm>

Specifies the low threshold for the transmit power alarm.

When the operating parameter falls below this value, the action associated with the alarm is taken.

If the unit is mW, the range of this parameter is from 0 to 6.5535mW. If the unit is dBm, the range of this parameter is from -40 to 8.1647dBm.

#### high\_warning

##### <mw\_or\_dbm>

Specifies the high threshold for the transmit power warning.

When the operating parameter rises above this value, the action associated with the warning is taken.

If the unit is mW, the range of this parameter is from 0 to 6.5535mW. If the unit is dBm, the range of this parameter is from -40 to 8.1647dBm.

---

### low\_warning

<mw\_or\_dbm>

Specifies the low threshold for the transmit power warning.

When the operating parameter falls below this value, the action associated with the warning is taken.

If the unit is mW, the range of this parameter is from 0 to 6.5535mW. If the unit is dBm, the range of this parameter is from -40 to 8.1647dBm.

---

#### NOTE

The threshold unit **mW** or **dBm** allows the user to input the decimal in the CLI command. The CLI does not restrict the number of input digits, the only limitation of the inputted digits are the size of the command buffer and the float-point precision. The user inputted digits will be converted to the floating-point number and applied to the configuration database.

The default precision of a floating-point number is 6 digits.

For example, input "12.3456", will get a float value 12.3456, input "12.3456789", will get a float value 12.3457.

---

### ● Restrictions

Administrators and operators.

### ● Example

To configure the port 21's transmit power threshold

```
Zxxx0:admin# config ddm ports 21 rx_power_threshold high_alarm 4.55 low_alarm 0.01
high_warning 3.5 low_warning 0.03
Command: config ddm ports 21 rx_power_threshold high_alarm 4.55 low_alarm 0.01
high_warning 3.5 low_warning 0.03
```

Success.

```
Zxxx0:admin#
```

## 19.6. config ddm ports reload threshold

---

### ● Description

This command is used to reload the DDM threshold configuration. The command reloads default threshold configuration of special ports. If the ports are link up with optic modules, all thresholds of those ports will be set to hardware default. If the ports are not optic ports, or the ports are link down, all thresholds configuration will be clear.

### ● Format

`config ddm ports [<portlist> | all] reload_threshold`

### ● Parameters

---

**ports**

**<portlist>**

Specifies a range of ports to be configured. (The portlist format: UnitID: port number).

**all** If 'all' parameter is chosen, all optic ports' operating parameters will be configured.

---

### ● Restrictions

Administrators and operators.

### ● Example

To reload port 21's threshold configuration:

```
Zxxx0:admin# config ddm ports 21 reload_threshold
Command: config ddm ports 21 reload_threshold

Success.

Zxxx0:admin#
```

## 19.7. config ddm ports state

---

### ● Description

This command is used to configure the DDM state and/or the DDM shutdown action when it encounters an exceeding alarm or warning threshold event. The command configures the DDM state and/or the DDM shutdown action when it encounters an exceeding alarm or warning threshold event.

### ● Format

**config ddm ports** [<portlist> | all] { **state** [enable | disable] | **shutdown** [alarm | warning | none] } (1)

### ● Parameters

---

|                         |                                                                                                                                            |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ports</b>            |                                                                                                                                            |
| <b>&lt;portlist&gt;</b> | Specifies a range of ports to be configured. (The portlist format: UnitID: port number).                                                   |
| <b>all</b>              | If 'all' parameter is chosen, all optic ports' operating parameters will be configured.                                                    |
| <b>state</b>            | Specifies the DDM state to enabled or disabled. If the state is disabled, no DDM action will take effect.                                  |
| <b>shutdown</b>         | Specifies whether or not to shutdown the port when the operating parameter exceeds the corresponding alarm threshold or warning threshold. |
| <b>alarm</b>            | Shutdown the port when the configured alarm threshold range is exceeded.                                                                   |
| <b>warning</b>          | Shutdown the port when the configured warning threshold range is exceeded.                                                                 |
| <b>none</b>             | The port will never shutdown regardless if the threshold ranges are exceeded or not.                                                       |

---



---

**NOTE** The port being shutdown, cannot be recovered to normal operation automatically, and needs to use the "**config ports <portlist> state enable**" command to manually recover the port.  
The shutdown action is none by default.

---

### ● Restrictions

Administrators and operators.

### ● Example

To configure port 21's actions associate with the alarm:

## 19. Digital Diagnostic Monitoring (DDM) Commands

```
Zxxx0:admin# config ddm ports 11 state enable shutdown alarm
Command: config ddm ports 11 state enable shutdown alarm

Success.

Zxxx0:admin#
```

### 19.8. config ddm log

---

#### ● Description

Enable or disable the log when parameters of the optic module exceed its DDM threshold. The command configures the DDM log action when encountering an exceeding alarm or warning thresholds event.

#### ● Format

`config ddm log [enable | disable]`

#### ● Parameters

|            |                                                                                                                                          |
|------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <b>log</b> | Specifies whether to send a log, when the operating parameter exceeds the corresponding threshold.<br>The DDM log is enabled by default. |
|------------|------------------------------------------------------------------------------------------------------------------------------------------|

---

#### ● Restrictions

Administrators and operators.

#### ● Example

To configure DDM log state to enable:

```
Zxxx0:admin# config ddm log enable
Command: config ddm log enable

Success.

Zxxx0:admin#
```

## 19.9. config ddm trap

---

### ● Description

This command is used to enable or disable the trap when parameters of the optic module exceed its DDM threshold. The command configures the DDM trap action when encountering an exceeding alarm or warning thresholds event.

### ● Format

`config ddm trap [enable | disable]`

### ● Parameters

---

|             |                                                                                                                                            |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>trap</b> | Specifies whether to send traps, when the operating parameter exceeds the corresponding threshold.<br>The DDM trap is disabled by default. |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------|

---

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To configure DDM trap state to enabled:

```
Zxxx0:admin# config ddm trap enable
Command: config ddm trap enable

Success.

Zxxx0:admin#
```



## 19.10. config ddm power\_unit

---

### ● Description

This command is used to configure the unit of DDM TX/RX power. The command configures the global unit of DDM TX/RX power.

### ● Format

config ddm power\_unit [mw | dbm]

### ● Parameters

---

#### power\_unit

Specifies the unit of DDM TX/RX power. If the unit has been set, the display message and configure value of TX/RX power use the same unit.

The default unit is mW.

---

### ● Restrictions

Administrators and operators.

### ● Example

To configure the unit of DDM TX/RX power:

```
Zxxx0:admin# config ddm power_unit dbm
Command: config ddm power_unit dbm

Success.

Zxxx0:admin#
```

## 19.11. show ddm ports status

### ● Description

This command is used to show the current operating DDM parameters values of the optic module of the specified ports. This command displays the current operating parameters of the optic modules.

### ● Format

**show ddm ports {<portlist> } status**

### ● Parameters

**ports**

**<portlist>**

Specifies a range of ports to be displayed.

If the port parameter is not specified, all optic ports' operating parameters will be displayed.

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To show port 21-23's operating parameters:

```
Zxxx0:admin# show ddm ports 21-23 status
```

```
Command: show ddm ports 21-23 status
```

| Port | Temperature<br>(in Celsius) | Voltage<br>(V) | Bias-Current<br>(mA) | TX-Power<br>(dBm) | RX-Power<br>(dBm) |
|------|-----------------------------|----------------|----------------------|-------------------|-------------------|
| 21   | -                           | -              | -                    | -                 | -                 |
| 22   | 25.0625                     | 3.5036         | 12.6473              | -9.9097           | -5.4166           |
| 23   | -                           | -              | -                    | -                 | -                 |

```
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

## 19.12. show ddm ports configuration

### ● Description

This command is used to display the current configurations of the optic modules. There are two types of thresholds: the administrative configuration and the operation configuration threshold.

For the optic port, when a particular threshold was configured by the user, it will be shown in this command with a tag indicating that it is a threshold that the user configured, else it would be the threshold read from the optic module that is being inserted.

### ● Format

show ddm ports {<portlist>} configuration

### ● Parameters

ports

<portlist>

Specifies a range of ports to be displayed.

If the port parameter is not specified, all optic ports' operating parameters will be displayed.

### ● Restrictions

None.

### ● Example

To show port 21's configuration:

```
Zxxx0:admin# show ddm ports 21 configuration
Command: show ddm ports 21 configuration

Port 21
-----
DDM State : Enabled
Shutdown  : Alarm

Threshold      Temperature      Voltage      Bias-Current      TX-Power      RX-Power
              (in Celsius)      (V)          (mA)              (dBm)         (dBm)
-----
High Alarm     85.0000 (A)      3.5000       100.0540          -8.9997       -2.9904
Low Alarm      -5.0000          3.1000       6.0040            -11.8977      -23.9794
High Warning   80.0000 (A)      3.4500       90.0480           -9.5001       -3.4901
Low Warning     0.0000          3.1500       7.0040            -11.4026      -23.0103
```

A means that the threshold is administratively configured.

```
Zxxx0:admin#
```

## 19.13. show ddm

---

- **Description**

This command is used to display the DDM global settings.

- **Format**

show ddm

- **Parameters**

None.

- **Restrictions**

None.

- **Example**

To display the DDM global settings:

```
Zxxx0:admin# show ddm

Command: show ddm

DDM Log           : Enabled
DDM Trap          : Enabled
DDM TX/RX Power Unit : dBm

Zxxx0:admin#
```

## 20. Debug Software Command List

The commands are used to configure the monitoring and logging of protocol communication status and how to handle when an error occurs. The following protocols are supported, as well as general protocols.

- VRRP (Virtual Router Redundancy Protocol), which multiplexes a router or L3 Switching Hub
- STP (Spanning Tree Protocol), which prevents loops and provides redundancy
- OSPF (Open Shortest Path First), which provides routing
- DHCPv6 relay and server
- PIM-SSM, which provides multicast routing

---

```

debug error_log [dump | clear | upload_toTFTP <ipaddr> <path_filename 64>]
debug buffer [utilization | dump | clear | upload_toTFTP <ipaddr> <path_filename 64>]
debug output [module <module_list> | all] [buffer | console]
debug config error_reboot [enable | disable]
debug config state [enable | disable]
debug show error_reboot state
debug stp clear counter {ports [<portlist> | all]}
debug stp config ports [<portlist> | all] [event | bpdu | state_machine | all] state [disable | brief |
    detail]
debug stp show counter {ports [<portlist> | all]}
debug stp show flag {ports <portlist>}
debug stp show information
debug stp state [disable | enable]
debug ospf [neighbor_state_change | interface_state_change {dr_bdr_selection} | lsa {all |
    originating | installing | receiving | flooding} (1) | packet {all | receiving | sending} (1) |
    retransmission | spf {all | intra | inter | extern} (1) | timer | virtual_link | route |
    redistribution] state [enable | disable]
debug ospf clear counter {packet | neighbor | spf}
debug ospf log state [enable | disable]
debug ospf show counter {packet | neighbor | spf}
debug ospf show detail external_link
debug ospf show detail net_link
debug ospf show detail rt_link
debug ospf show detail summary_link
debug ospf show detail type7_link
debug ospf show flag
debug ospf show log state
debug ospf show redistribution
debug ospf show request_list
debug ospf show summary_list
debug ospf state [enable | disable]
debug vrrp [vr_state_change | packet [all | {receiving | sending}(1)] | mac_addr_update |
    interface_change | timers] state [enable | disable]
debug vrrp clear counter
debug vrrp log state [enable | disable]
debug vrrp show counter
  
```

---

---

```
debug vrrp show flag
debug vrrp show log state
debug vrrp state [enable | disable]
debug dhcpv6_relay state enable
debug dhcpv6_relay state disable
debug dhcpv6_relay hop_count state [enable | disable]
debug dhcpv6_relay output [buffer | console]
debug dhcpv6_relay packet {all | receiving | sending} state [enable | disable]
debug dhcpv6_server packet [all | receiving | sending] state [enable | disable]
debug dhcpv6_server state disable
debug dhcpv6_server state enable
debug pim ssm
no debug pim ssm
debug show status {module <module_list>}
```

---

## 20.1. debug error\_log

---

### ● Description

Use this command to dump, clear or upload the software error log to a TFTP server.

### ● Format

**debug error\_log** [dump | clear | upload\_toTFTP <ipaddr> <path\_filename 64>]

### ● Parameters

|                                 |                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dump</b>                     | Display the debug message of the debug log.                                                                                                                    |
| <b>clear</b>                    | Clear the debug log.                                                                                                                                           |
| <b>upload_toTFTP</b>            | Upload the debug log to a TFTP server specified by IP address.                                                                                                 |
| <b>&lt;ipaddr&gt;</b>           | Specifies the IPv4 address of the TFTP server.                                                                                                                 |
| <b>&lt;path_filename 64&gt;</b> | The pathname specifies the DOS pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This value can be up to 64 characters long. |

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To dump the error log:

```

Zxxx0:admin# debug error_log dump
Command: debug error_log dump

*****
# debug log: 1
# firmware version: 1.0.0.xx
# level: CPU exception
# clock: 437453880 ms
# time : 2000-01-08 05:55:40

===== CPU EXCEPTION =====
Current Task = IP-Tic Stack Pointer = 4CFEA7A0
-----CP0 Registers-----
Status : 1000FC01  Interrupt enable  Normal level
Cause  : 00000008  TLB exception (load or instruction fetch)
EPC    : 80A0297C      Addr   : 00000008
Stack  : 4CFEA7A0      Return : 80A02938
-----normal registers-----
$0($0) : 00000000  at($1) : FFFFFFFE  v0($2) : 00000000  v1($3) : 00000001
a0($4) : 00000000  a1($5) : 4825B4A8  a2($6) : 00000001  a3($7) : 00000001
t0($8) : 814D7FCC  t1($9) : 0000FC00  t2($10) : 828100C4  t3($11) : 00000017
t4($12) : 828100BC  t5($13) : 4CFEA430  t6($14) : 82810048  t7($15) : 00000000
s0($16) : 4825D94A  s1($17) : 4825D890  s2($18) : 4825D949  s3($19) : 4825D946
s4($20) : 00000000  s5($21) : 00000008  s6($22) : 81800000  s7($23) : 00090000
t8($24) : 00000000  t9($25) : FFFFFFFC0  k0($26) : 00000000  k1($27) : 00000000
gp($28) : 8180ADA0  sp($29) : 4CFEA7A0  fp($30) : 00000001  ra($31) : 80A02938

----- TASK STACKTRACE -----
->81150A58
->809B346C
->809E1DEC
->809D7E6C
->80A038CC
->80A033B0
->80A0297C

```

### To clear the error log:

```

Zxxx0:admin# debug error_log clear
Command: debug error_log clear

Success.

Zxxx0:admin#

```

### To upload the error log to TFTP server:

```

Zxxx0:admin# debug error_log upload_toTFTP 10.0.0.90 debug-log.txt
Command: debug error_log upload_toTFTP 10.0.0.90 debug-log.txt

Connecting to server..... Done.
Upload configuration..... Done.

Zxxx0:admin#

```



## 20.2. debug buffer

### ● Description

Use this command to show the debug buffer's state, or dump, clear, or upload the debug buffer to a TFTP server.

#### NOTE

When selecting to output to the debug buffer and there are debug messages being outputted, the system memory pool will be used as the debug buffer. The functions which will use the system memory pool resource may fail to execute command such as download and upload firmware, or save configuration. If you want to execute these commands successfully, please use the command "debug buffer clear" to release the system's memory pool resources manually first.

### ● Format

**debug buffer** [utilization | dump | clear | upload\_toTFTP <ipaddr> <path\_filename 64>]

### ● Parameters

#### utilization

Display the debug buffer's state.

#### dump

Display the debug message in the debug buffer.

#### clear

Clear the debug buffer.

#### upload\_toTFTP

Upload the debug buffer to a TFTP server specified by IP address.

#### <ipaddr>

Specifies the IPv4 address of the TFTP server.

#### <path\_filename 64>

The pathname specifies the DOS pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This value can be up to 64 characters long.

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To show the debug buffer's state:

```
Zxxx0:admin# debug buffer utilization
Command: debug buffer utilization

Allocate from      :      System memory
Total size         :      2 MB
Utilization rate   :      30%

Zxxx0:admin#
```

To clear the debug buffer:

```
Zxxx0:admin# debug buffer clear
Command: debug buffer clear

Success.

Zxxx0:admin#
```

To upload the messages stored in debug buffer to TFTP server:

```
Zxxx0:admin# debug buffer upload_toTFTP 10.0.0.90 debugcontent.txt
Command: debug buffer upload_toTFTP 10.0.0.90 debugcontent.txt

Connecting to server..... Done.
Upload configuration..... Done.

Zxxx0:admin#
```

## 20.3. debug output

### ● Description

Use the command to set a specified module's debug message output to debug buffer or local console. If the user uses the command in a Telnet session, the error message also is output to the local console.

**NOTE** When selecting to output to the debug buffer and there are debug messages being outputted, the system memory pool will be used as the debug buffer. The functions which will use the system memory pool resource may fail to execute command such as download and upload firmware, or save configuration. If you want to execute these commands successfully, please use the command "debug buffer clear" to release the system's memory pool resources manually first.

### ● Format

**debug output** [module <module\_list> | all] [buffer | console]

### ● Parameters

|                |                                                                            |
|----------------|----------------------------------------------------------------------------|
| <b>module</b>  | Specifies the module list.<br><module_list><br>Enter the module list here. |
| <b>all</b>     | Control output method of all modules.                                      |
| <b>buffer</b>  | Direct the debug message of the module output to debug buffer(default).    |
| <b>console</b> | Direct the debug message of the module output to local console.            |

## 20. Debug Software Command List

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To set all module debug message outputs to local console:

```
Zxxx0:admin# debug output all console
Command: debug output all console

Success.

Zxxx0:admin#
```

## 20.4. debug config error\_reboot

---

### ● Description

This command is used to set if the Switching Hub needs to be rebooted when a fatal error occurs. When the error occurs, the watchdog timer will be disabled by the system first, and then all debug information will be saved in NVRAM. If the error\_reboot is enabled, the watchdog shall be enabled after all information is stored into NVRAM.

### ● Format

**debug config error\_reboot [enable | disable]**

### ● Parameters

|                |                                                                                                                                    |
|----------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>enable</b>  | Need reboot Switching Hub when fatal error happens.(if the project do not define the default setting, enable for default).         |
| <b>disable</b> | Do not need reboot Switching Hub when fatal error happens, system will hang-up for debug and enter the debug shell mode for debug. |

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To set the Switching Hub to not need a reboot when a fatal error occurs:

```
Zxxx0:admin# debug config error_reboot disable
Command: debug config error_reboot disable

Success.

Zxxx0:admin#
```

## 20.5. debug config state

---

### ● Description

Use the command to set the state of the debug.

### ● Format

debug config state [enable | disable]

### ● Parameters

|                |                          |
|----------------|--------------------------|
| <b>enable</b>  | Enable the debug state.  |
| <b>disable</b> | Disable the debug state. |

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To set the debug state to disabled:

```
Zxxx0:admin# debug config state disable
Command: debug config state disable

Success.

Zxxx0:admin#
```

## 20.6. debug show error\_reboot state

---

### ● Description

Use the command to show the error reboot status.

### ● Format

debug show error\_reboot state

### ● Parameters

None.

### ● Restrictions

Only Administrator-level users can issue this command.

## 20. Debug Software Command List

### ● Example

To show the error reboot status:

```
Zxxx0:admin#debug show error_reboot state
Command: debug show error_reboot state

Error Reboot: Enabled

Zxxx0:admin#
```

## 20.7. debug stp clear counter

---

### ● Description

This command used to clear the STP counters.

### ● Format

**debug stp clear counter {ports [<portlist> | all]}**

### ● Parameters

|              |                                                                                                                  |
|--------------|------------------------------------------------------------------------------------------------------------------|
| <b>ports</b> | Specifies the port range.<br><b>&lt;portlist&gt;</b><br>Enter the list of port used for this configuration here. |
| <b>all</b>   | Clears all port counters.                                                                                        |

---

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To clear all STP counters on the Switching Hub:

```
Zxxx0:admin# debug stp clear counter ports all
Command : debug stp clear counter ports all

Success.

Zxxx0:admin#
```

## 20.8. debug stp config ports

---

### ● Description

This command used to configure per-port STP debug level on the specified ports.

### ● Format

**debug stp config ports** [<portlist> | all] [event | bpdu | state\_machine | all] state [disable | brief | detail]

### ● Parameters

|                      |                                                                                                                               |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>ports</b>         | Specifies the STP port range to debug.<br><b>&lt;portlist&gt;</b><br>Enter the list of port used for this configuration here. |
| <b>all</b>           | Specifies to debug all ports on the Switching Hub.                                                                            |
| <b>event</b>         | Debug the external operation and event processing.                                                                            |
| <b>bpdu</b>          | Debug the BPDU's that have been received and transmitted.                                                                     |
| <b>state_machine</b> | Debug the state change of the STP state machine.                                                                              |
| <b>all</b>           | Debug all of the above.                                                                                                       |
| <b>state</b>         | Specifies the state of the debug mechanism.                                                                                   |
| <b>disable</b>       | Disables the debug mechanism.                                                                                                 |
| <b>brief</b>         | Sets the debug level to brief.                                                                                                |
| <b>detail</b>        | Sets the debug level to detail.                                                                                               |

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To configure all STP debug flags to brief level on all ports:

```
Zxxx0:admin# debug stp config ports all all state brief
Command: debug stp config ports all all state brief

Success.

Zxxx0:admin#
```

## 20.9. debug stp show counter

### ● Description

This command used to display the STP counters.

### ● Format

**debug stp show counter {ports [<portlist> | all]}**

### ● Parameters

---

|              |                                                                            |
|--------------|----------------------------------------------------------------------------|
| <b>ports</b> | (Optional) Specifies the STP ports for display.<br><b>&lt;portlist&gt;</b> |
|              | Enter the list of port used for this configuration here.                   |
| <b>all</b>   | Display all port's counters.                                               |

---

If no parameter is specified, display the global counters.

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To show the STP counters for port 9:

```
Zxxx0:admin# debug stp show counter ports 9
Command: debug stp show counter ports 9

STP Counters
-----
Port 9 :
Receive:
Total STP Packets      :32
Configuration BPDU     :0
TCN BPDU               :0
RSTP TC-Flag           :15
RST BPDU               :32
Transmit:
Total STP Packets      :32
Configuration BPDU     :0
TCN BPDU               :0
RSTP TC-Flag           :7
RST BPDU               :32

Discard:
Total Discarded BPDU   :0
Global STP Disabled    :0
Port STP Disabled      :0
Invalid Packet Format   :0
Invalid Protocol        :0
Configuration BPDU Length :0
TCN BPDU Length        :0
RST BPDU Length        :0
Invalid Type            :0
Invalid Timers          :0

Zxxx0:admin#
```

## 20.10. debug stp show flag

### ● Description

This command used to display the STP debug level on specified ports.

### ● Format

**debug stp show flag {ports <portlist>}**

### ● Parameters

---

**ports** (Optional) Specifies the STP ports to display.  
**<portlist>**

(Optional) Enter the list of port used for this configuration here.

---

If no parameter is specified, all ports on the Switching Hub will be displayed.

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To display the debug STP levels on all ports:

```
Zxxx0:admin# debug stp show flag
Command: debug stp show flag
```

```
Global State: Enabled
```

| Port Index | Event flag | BPDU Flag | State Machine Flag |
|------------|------------|-----------|--------------------|
| -----      | -----      | -----     | -----              |
| 1          | Detail     | Brief     | Disable            |
| 2          | Detail     | Brief     | Disable            |
| 3          | Detail     | Brief     | Disable            |
| 4          | Detail     | Brief     | Disable            |
| 5          | Detail     | Brief     | Disable            |
| 6          | Detail     | Brief     | Disable            |
| 7          | Detail     | Brief     | Disable            |
| 8          | Detail     | Brief     | Disable            |
| 9          | Detail     | Brief     | Disable            |
| 10         | Detail     | Brief     | Disable            |
| 11         | Detail     | Brief     | Disable            |
| 12         | Detail     | Brief     | Disable            |

```
Zxxx0:admin#
```



## 20.11. debug stp show information

---

- **Description**

This command used to display STP detailed information, such as the hardware tables, the STP state machine, etc.

- **Format**

`debug stp show information`

- **Parameters**

None.

- **Restrictions**

Only Administrator-level users can issue this command.

- **Example**

To show STP debug information:

```

Zxxx0:admin# debug stp show information
Command: debug stp show information

Spanning Tree Debug Information:
-----

Port Status In Hardware Table:
Instance 0:
Port 1 :BLK  Port 2 :BLK  Port 3 :BLK  Port 4 :BLK  Port 5 :BLK  Port 6 :BLK
Port 7 :FOR  Port 8 :BLK  Port 9 :BLK  Port 10:BLK  Port 11:BLK  Port 12:BLK
Instance 1:
Port 1 :BLK  Port 2 :BLK  Port 3 :BLK  Port 4 :BLK  Port 5 :BLK  Port 6 :BLK
Port 7 :FOR  Port 8 :BLK  Port 9 :BLK  Port 10:BLK  Port 11:BLK  Port 12:BLK
-----

Root Priority And Times :
Instance 0:
  Designated Root Bridge      : 32768/00-01-02-03-04-00
  External Root Cost          : 0
  Regional Root Bridge        : 32768/00-01-02-03-04-00
  Internal Root Cost          : 0
  Designated Bridge           : 32768/00-01-02-03-04-00
  Designated Port             : 0
  Message Age                 : 0
  Max Age                     : 20
  Forward Delay               : 15
  Hello Time                  : 2
Instance 1:
  Regional Root Bridge        : 32769/00-01-02-03-04-00
  Internal Root Cost          : 0
  Designated Bridge           : 32769/00-01-02-03-04-00
  Designated Port             : 0
  Remaining Hops              : 20
-----

Designated Priority And Times:
Instance 0:
Port 1 :
  Designated Root Bridge      : 0      /00-00-00-00-00-00
  External Root Cost          : 0
  Regional Root Bridge        : 0      /00-00-00-00-00-00
  Internal Root Cost          : 0
  Designated Bridge           : 0      /00-00-00-00-00-00
  Designated Port             : 0
  Message Age                 : 0
  Max Age                     : 20
  Forward Delay               : 15
  Hello Time                  : 2

Instance 1:
Port 1 :
  Regional Root Bridge        : 0      /00-00-00-00-00-00
  Internal Root Cost          : 0
  Designated Bridge           : 0      /00-00-00-00-00-00
  Designated Port             : 0
  Remaining Hops              : 20

Zxxx0:admin#

```

## 20.12. debug stp state

---

### ● Description

This command is used to enable or disable the STP debug state.

### ● Format

**debug stp state [enable | disable]**

### ● Parameters

---

|                |                                |
|----------------|--------------------------------|
| <b>state</b>   | Specifies the STP debug state. |
| <b>enable</b>  | Enable the STP debug state.    |
| <b>disable</b> | Disable the STP debug state.   |

---

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To configure the STP debug state to enable, and then disable the STP debug state:

```
Zxxx0:admin# debug stp state enable
Command: debug stp state enable

Success.

Zxxx0:admin# debug stp state disable
Command: debug stp state disable

Success.

Zxxx0:admin#
```

## 20.13. debug ospf

---

### ● Description

This command is used to enable or disable OSPF debug flags.

### ● Format

**debug ospf** [**neighbor\_state\_change** | **interface\_state\_change** {**dr\_bdr\_selection**} | **lsa** {**all** | **originating** | **installing** | **receiving** | **flooding**} (1) | **packet** {**all** | **receiving** | **sending**} (1) | **retransmission** | **spf** {**all** | **intra** | **inter** | **extern**} (1) | **timer** | **virtual\_link** | **route** | **redistribution**] **state** [**enable** | **disable**]

### ● Parameters

|                               |                                                                               |
|-------------------------------|-------------------------------------------------------------------------------|
| <b>neighbor_state_change</b>  | The state of the OSPF neighbor state change debug.                            |
| <b>interface_state_change</b> | The state of the OSPF interface state change debug.                           |
| <b>dr_bdr_selection</b>       | (Optional) Used to include or exclude debug information for DR/BDR selection. |
| <b>lsa</b>                    | The state of the designated debug flag.                                       |
| <b>all</b>                    | (Optional) Set all LSA debug flags.                                           |
| <b>originating</b>            | (Optional) Set LSA originating debug flag.                                    |
| <b>installing</b>             | (Optional) Set LSA installing debug flag.                                     |
| <b>receiving</b>              | (Optional) Set LSA receiving debug flag.                                      |
| <b>flooding</b>               | (Optional) Set LSA flooding debug flag.                                       |
| <b>packet</b>                 | The state of the designated debug flag.                                       |
| <b>all</b>                    | (Optional) Set all packet debug flags.                                        |
| <b>receiving</b>              | (Optional) Set packet receiving debug flag.                                   |
| <b>sending</b>                | (Optional) Set packet sending debug flag.                                     |
| <b>retransmission</b>         | The state of the OSPF retransmission debug flag.                              |
| <b>spf</b>                    | The state of the designated debug flag.                                       |
| <b>all</b>                    | (Optional) Set all SPF debug flags.                                           |
| <b>intra</b>                  | (Optional) Set intra-area SPF debug flag.                                     |
| <b>inter</b>                  | (Optional) Set inter-area SPF debug flag.                                     |
| <b>extern</b>                 | (Optional) Set AS external SPF debug flag.                                    |
| <b>timer</b>                  | The state of the OSPF timer debug flag.                                       |
| <b>virtual_link</b>           | The state of the OSPF virtual link debug flag.                                |
| <b>route</b>                  | The state of OSPF route debug flag.                                           |

## 20. Debug Software Command List

---

### redistribution

The state of OSPF redistribution debug.

---

**state** Specifies to set the OSPF debug global state.

**enable**

Specifies that the OSPF debug global state will be enabled.

**disable**

Specifies that the OSPF debug global state will be disabled.

---

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To enable OSPF neighbor state change debug:

```
Zxxx0:admin# debug ospf neighbor_state_change state enable
Command: debug ospf neighbor_state_change state enable

Success.

Zxxx0:admin#
```

To enable OSPF interface state change debug:

```
Zxxx0:admin# debug ospf interface_state_change state enable
Command: debug ospf interface_state_change state enable

Success.

Zxxx0:admin#
```

To enable all OSPF LSA debug flags:

```
Zxxx0:admin# debug ospf lsa all state enable
Command: debug ospf lsa all state enable

Success.

Zxxx0:admin#
```

To enable all OSPF packet debug flags:

```
Zxxx0:admin# debug ospf packet all state enable
Command: debug ospf packet all state enable

Success.

Zxxx0:admin#
```

To enable all OSPF retransmission debug flags:

```
Zxxx0:admin# debug ospf retransmission state enable
Command: debug ospf retransmission state enable

Success.

Zxxx0:admin#
```

To enable all OSPF SPF debug flags:

```
Zxxx0:admin# debug ospf spf all state enable
Command: debug ospf spf all state enable

Success.

Zxxx0:admin#
```

## 20.14. debug ospf clear counter

### ● Description

This command is used to reset the OSPF statistic counters.

### ● Format

**debug ospf clear counter {packet | neighbor | spf}**

### ● Parameters

---

**packet** (Optional) Specifies to reset the OSPF packet counter.

---

**neighbor** (Optional) Specifies to reset the OSPF neighbor event counter.

---

**spf** (Optional) Specifies to reset the OSPF SPF event counter.

---

If the parameter is not specified, all OSPF counters will be cleared.

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To clear all OSPF statistic counters:

```
Zxxx0:admin# debug ospf clear counter
Command: debug ospf clear counter

Success.

Zxxx0:admin#
```

## 20.15. debug ospf log state

---

### ● Description

This command is used to enable or disable the debug OSPF log.

### ● Format

**debug ospf log state** [enable | disable]

### ● Parameters

---

|                |                                                           |
|----------------|-----------------------------------------------------------|
| <b>state</b>   | Specifies the state of the OSPF debug log.                |
| <b>enable</b>  | Specifies that the OSPF debug log state will be enabled.  |
| <b>disable</b> | Specifies that the OSPF debug log state will be disabled. |

---

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To enable the OSPF debug log:

```
Zxxx0:admin# debug ospf log state enable
Command: debug ospf log state enable

Success.

Zxxx0:admin#
```

## 20.16. debug ospf show counter

---

### ● Description

This command is used to display OSPF statistic counters.

### ● Format

**debug ospf show counter** {packet | neighbor | spf}

### ● Parameters

---

|                 |                                                                  |
|-----------------|------------------------------------------------------------------|
| <b>packet</b>   | (Optional) Specifies to display the OSPF packet counter.         |
| <b>neighbor</b> | (Optional) Specifies to display the OSPF neighbor event counter. |
| <b>spf</b>      | (Optional) Specifies to display the OSPF SPF event counter.      |

---

If the parameter is not specified, all OSPF counters will be displayed.

- **Restrictions**

Only Administrator-level users can issue this command.

- **Example**

To show all OSPF statistic counters:

```
Zxxx0:admin# debug ospf show counter
Command: debug ospf show counter

OSPF Debug Statistic Counters
Packet Receiving:
  Total   : 30
  Hello   : 30
  DD      : 0
  LSR     : 0
  LSU     : 0
  LSAck   : 0
  Drop    : 0
  Auth Fail : 0

Packet Sending:
  Total   : 59
  Hello   : 59
  DD      : 0
  LSR     : 0
  LSU     : 0
  LSAck   : 0

Neighbor State:
  Change  : 0
  SeqMismatch : 0

SPF Calculation:
  Intra   : 0
  Inter   : 0
  Extern  : 0

Zxxx0:admin#
```

## **20.17. debug ospf show detail external\_link**

- **Description**

This command is used to display all AS external LSAs with detail information.

- **Format**

**debug ospf show detail external\_link**



## 20. Debug Software Command List

### ● Parameters

None.

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To display all AS external LSAs with detail information:

```
Zxxx0:admin#debug ospf show detail external_link
Command: debug ospf show detail external_link

OSPF Phase2 External Link:

=====
AREA 0.0.0.0:

AS-External LSA:
Link-State ID: 192.168.205.0
Advertising Router: 1.1.1.1
LS Age: 10 Seconds
Options: 0x2
.... 0 = 0 Bit Isn't Set
.... 1 = E: ExternalRoutingCapability
.... 0.. = MC: NOT Multicast Capable
.... 0... = N/P: NSSA Bit
...0 .... = EA: Not Support Rcv And Fwd EA_LSA
..0. .... = DC: Not Support Handling Of Demand Circuits
.0.. .... = O: O Bit Isn't Set
0... .... = 7 Bit Isn't Set
LS Sequence Number: 0x80000001
Length: 36
Netmask: 255.255.255.0
Metric: 20
Forwarding Address: 10.90.90.101
External Route Tag: 0
Internal Field:
Del_flag: 0x0 I_ref_count: 0 Seq: 0x80000001 Csum: 0xd08e
Rxtime: 384 Txtime: 0 Orgage: 0
Current Time: 394

Zxxx0:admin#
```

## 20.18. debug ospf show detail net\_link

---

### ● Description

This command is used to display all Network LSAs with detail information.

### ● Format

**debug ospf show detail net\_link**

### ● Parameters

None.

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

Only Administrator level users can issue this command.

```
Zxxx0:admin#debug ospf show detail net_link
Command: debug ospf show detail net_link

OSPF Phase2 NET Link:

=====
AREA 0.0.0.0:
  Network LSA:
  Link-State ID: 10.90.90.123
  Netmask: 255.0.0.0
  Advertising Router: 10.90.90.91
  LS Age: 109 Seconds
  Options: 0x2
  .... 0 = 0 Bit Isn't Set
  .... 1 = E: ExternalRoutingCapability
  .... 0 = MC: NOT Multicast Capable
  .... 0 = N/P: NSSA Bit
  ...0 .... = EA: Not Support Rcv And Fwd EA_LSA
  ..0. .... = DC: Not Support Handling Of Demand Circuits
  .0.. .... = O: O Bit Isn't Set
  0... .... = 7 Bit Isn't Set
  LS Sequence Number: 0x80000001
  Length: 32
  Attached Router: 10.90.90.91
  Attached Router: 1.1.1.1
  Internal Field:
  Del_flag: 0x0 I_ref_count: 0 Seq: 0x80000001 Csum: 0x4e99
  Rxtime: 4 Txtime: 4 Orgage: 1
  Current Time: 112

Zxxx0:admin#
```

## 20.19. debug ospf show detail rt\_link

---

- **Description**

This command is used to display all Router LSAs with detail information.

- **Format**

`debug ospf show detail rt_link`

- **Parameters**

None.

- **Restrictions**

Only Administrator-level users can issue this command.

- **Example**

To display all Router LSAs with detail information:

```

Zxxx0:admin#debug ospf show detail rt_link
Command: debug ospf show detail rt_link

OSPF Phase2 RT Link:

=====
AREA 0.0.0.0:
  Router LSA:
    Link-State ID: 1.1.1.1
    Advertising Router: 1.1.1.1
    LS Age: 10 Seconds
    Options: 0x2
    .... 0 = 0 Bit Isn't Set
    .... 1 = E: ExternalRoutingCapability
    .... 0 = MC: NOT Multicast Capable
    .... 0 = N/P: NSSA Bit
    ...0 .... = EA: Not Support Rcv And Fwd EA_LSA
    ..0. .... = DC: Not Support Handling Of Demand Circuits
    .0.. .... = O: O Bit Isn't Set
    0... .... = 7 Bit Isn't Set
    LS Sequence Number: 0x80000002
    Length: 36
    Flags: 0x0
    .... 0 = B: Not Area Border Router
    .... 0 = E: Not AS Boundary Router
    .... 0 = V: Not Virtual Link Endpoint
    Number Of Links: 1
    Type: Transit      ID: 10.90.90.123      Data: 10.90.90.91      Metric: 1
    Internal Field:
    Del_flag: 0x0  I_ref_count: 0  Seq: 0x80000002  Csum: 0xd81d
    Rxtime: 5  Txtime: 0  Orgage: 0
    Current Time: 15

Zxxx0:admin#

```

## **20.20. debug ospf show detail summary\_link**

### ● Description

This command is used to display all Summary LSAs with detail information.

### ● Format

**debug ospf show detail summary\_link**

### ● Parameters

None.

### ● Restrictions

Only Administrator-level users can issue this command.

## 20. Debug Software Command List

### ● Example

To display all Summary LSAs with detail information:

```
Zxxx0:admin#debug ospf show detail summary_link
Command: debug ospf show detail summary_link

OSPF Phase2 Summary Link:

=====
AREA 0.0.0.0:
  Summary LSA:
  Link-State ID: 20.1.1.0
  Advertising Router: 10.90.90.91
  LS Age: 10 Seconds
  Options: 0x2
  .... 0 = 0 Bit Isn't Set
  .... 1 = E: ExternalRoutingCapability
  .... 2 = MC: NOT Multicast Capable
  .... 3 = N/P: NSSA Bit
  .... 4 = EA: Not Support Rcv And Fwd EA_LSA
  .... 5 = DC: Not Support Handling Of Demand Circuits
  .... 6 = O: O Bit Isn't Set
  .... 7 = 7 Bit Isn't Set
  LS Sequence Number: 0x80000001
  Length: 28
  Netmask: 255.255.255.0
  Metric: 1
  Internal Field:
  Del_flag: 0x0  I_ref_count: 0  Seq: 0x80000001  Csum: 0x8f9c
  Rxtime: 246  Txtime: 246  Orgage: 1
  Current Time: 255

Zxxx0:admin#
```

## **20.21. debug ospf show detail type7\_link**

---

### ● Description

This command is used to display all type-7 LSAs with detail information.

### ● Format

**debug ospf show detail type7\_link**

### ● Parameters

None.

### ● Restrictions

Only Administrator-level users can issue this command.

## ● Example

To display all type-7 LSAs with detail information:

```
Zxxx0:admin#debug ospf show detail type7_link
Command: debug ospf show detail type7_link

OSPF Phase2 NSSA-External Link:

=====
AREA 0.0.0.1:

NSSA-External LSA:
Link-State ID: 0.0.0.0
Advertising Router: 10.90.90.91
LS Age: 855 Seconds
Options: 0x2
.... ...0 = 0 Bit Isn't Set
.... ..1. = E: ExternalRoutingCapability
.... .0.. = MC: NOT Multicast Capable
.... 0... = N/P: NSSA Bit
...0 .... = EA: Not Support Rcv And Fwd EA_LSA
..0. .... = DC: Not Support Handling Of Demand Circuits
.0.. .... = O: O Bit Isn't Set
0... .... = 7 Bit Isn't Set
LS Sequence Number: 0x80000002
Length: 36
Netmask: 0.0.0.0
Metric: 0
Forwarding Address: 0.0.0.0
External Route Tag: 0
Internal Field:
Del_flag: 0x0 I_ref_count: 0 Seq: 0x80000002 Csum: 0x77be
Rxtime: 2301 Txtime: 0 Orgage: 0
Current Time: 3156

Zxxx0:admin#
```

## 20.22. debug ospf show flag

---

### ● Description

This command is used to display the OSPF debug flag setting.

### ● Format

**debug ospf show flag**

### ● Parameters

None.

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To show the current OSPF debug flag setting:

```
Zxxx0:admin# debug ospf show flag
Command: debug ospf show flag

Global State: Enabled

Current OSPF Flags Setting:

Neighbor State Change
Interface State Change
LSA Originating
LSA Operating
LSA Receiving
LSA Flooding
Packet Receiving
Packet Sending
Retransmission
Timer
DR Selection
Route
Redistribution
Virtual Link
SPF Intra
SPF Inter
SPF Extern

Zxxx0:admin#
```

## 20.23. debug ospf show log state

---

- **Description**

This command is used to display the OSPF debug log state.

- **Format**

`debug ospf show log state`

- **Parameters**

None.

- **Restrictions**

Only Administrator-level users can issue this command.

- **Example**

To display the debug OSPF log state:

```
Zxxx0:admin# debug ospf show log state
Command: debug ospf show log state

OSPF Log State : Enabled

Zxxx0:admin#
```

## 20.24. debug ospf show redistribution

---

- **Description**

This command is used to display the current internal OSPF redistribute list.

- **Format**

`debug ospf show redistribution`

- **Parameters**

None.

- **Restrictions**

Only Administrator-level users can issue this command.

- **Example**

To display the current OSPF redistribution list:



## 20. Debug Software Command List

```
Zxxx0:admin# debug ospf show redistribution
Command: debug ospf show redistribution

OSPF Redistribution List:

IP                Nexthop           State Type Tag
-----
1.1.1.0/24        0.0.0.0          ON    2    0.0.0.0

OSPF ASE Table:

IP                Nexthop           State Type Tag
-----
1.1.1.0/24        0.0.0.0          ON    2    0.0.0.0

Zxxx0:admin#
```

### **20.25. debug ospf show request\_list**

- **Description**

This command is used to display the current internal OSPF request list.

- **Format**

**debug ospf show request\_list**

- **Parameters**

None.

- **Restrictions**

Only Administrator-level users can issue this command.

- **Example**

To display the current OSPF request list:

```
Zxxx0:admin# debug ospf show request_list
Command: debug ospf show request_list

OSPF Request List:

Area 0.0.0.0:
Circuit: 1.1.1.1
Neighbor: 90.2.0.1 IP: 1.1.1.2
LSID: 192.194.134.0 RTID: 90.2.0.1
LSID: 192.194.135.0 RTID: 90.2.0.1
LSID: 192.194.136.0 RTID: 90.2.0.1
LSID: 192.194.137.0 RTID: 90.2.0.1
LSID: 192.194.138.0 RTID: 90.2.0.1

Zxxx0:admin#
```

## 20.26. debug ospf show summary\_list

---

### ● Description

This command is used to display the current internal OSPF summary list.

### ● Format

**debug ospf show summary\_list**

### ● Parameters

None.

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To display the current OSPF summary list:

```
Zxxx0:admin# debug ospf show summary_list
Command: debug ospf show summary_list

OSPF Summary List:

Area 0.0.0.0:
Circuit: 1.1.1.1
Neighbor: 90.2.0.1 IP: 1.1.1.2
LSID: 1.1.1.1 RTID: 1.1.1.1

Circuit: 2.2.2.1

Circuit: 10.1.1.6

Zxxx0:admin#
```

## 20.27. debug ospf state

---

### ● Description

This command is used to set the OSPF debug global state.

### ● Format

**debug ospf state [enable | disable]**

### ● Parameters

---

|                |                                                              |
|----------------|--------------------------------------------------------------|
| <b>state</b>   | Specifies the OSPF debug global state.                       |
| <b>enable</b>  | Specifies that the OSPF debug global state will be enabled.  |
| <b>disable</b> | Specifies that the OSPF debug global state will be disabled. |

---

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To enable the OSPF debug global state:

```
Zxxx0:admin# debug ospf state enable
Command: debug ospf state enable

Success.

Zxxx0:admin# debug ospf show flag
Command: debug ospf show flag

Global State: Enabled

Current OSPF Flags Setting:

Neighbor State Change

Zxxx0:admin#
```

## 20.28. debug vrrp

---

### ● Description

This command is used to set VRRP debug flags.

### ● Format

**debug vrrp** [vr\_state\_change | packet [all | {receiving | sending}(1)] | mac\_addr\_update | interface\_change | timers] state [enable | disable]

### ● Parameters

---

#### **vr\_state\_change**

Specifies the state of the VRRP change debug flags.

---

#### **packet** Specifies to set the VRRP packet flags.

**all** Sets VRRP all packet debug flags.

#### **receiving**

(Optional) Set the VRRP packet receiving flag.

#### **sending**

(Optional) Set the VRRP packet sending flag.

---

#### **mac\_addr\_update**

Specifies the state of VRRP MAC debug flags.

---

#### **interface\_change**

Specifies the state of VRRP interface debug flags.

---

#### **timers** Specifies the state of VRRP timer's debug flags.

---

#### **state** Specifies the state of the configured VRRP debug flags.

#### **enable**

Specifies that the configure VRRP debug flag will be enabled.

#### **disable**

Specifies that the configure VRRP debug flag will be disabled.

---

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To enable the VRRP virtual router state change debug flag:

```
Zxxx0:admin# debug vrrp vr_state_change state enable
Command: debug vrrp vr_state_change state enable

Success.

Zxxx0:admin#
```

To enable all VRRP packet debug flags:

## 20. Debug Software Command List

```
Zxxx0:admin# debug vrrp packet all state enable
Command: debug vrrp packet all state enable

Success.

Zxxx0:admin#
```

To enable VRRP virtual MAC address update debug flags:

```
Zxxx0:admin# debug vrrp mac_addr_update state enable
Command: debug vrrp mac_addr_update state enable

Success.

Zxxx0:admin#
```

To enable VRRP interface state change debug flags:

```
Zxxx0:admin# debug vrrp interface_change state enable
Command: debug vrrp interface_change state enable

Success.

Zxxx0:admin#
```

To enable VRRP timer debug flags:

```
Zxxx0:admin# debug vrrp timers state enable
Command: debug vrrp timers state enable

Success.

Zxxx0:admin#
```

## 20.29. debug vrrp clear counter

---

### ● Description

This command is used to reset the VRRP debug statistic counters.

### ● Format

**debug vrrp clear counter**

### ● Parameters

None.

## ● Restrictions

Only Administrator-level users can issue this command.

## ● Example

To clear VRRP statistic counters:

```
Zxxx0:admin# debug vrrp clear counter
Command: debug vrrp clear counter

Success

Zxxx0:admin#
```

# 20.30. debug vrrp log state

## ● Description

This command is used to enable or disable the VRRP debug log state.

## ● Format

**debug vrrp log state [enable | disable]**

## ● Parameters

|                |                                                                       |
|----------------|-----------------------------------------------------------------------|
| <b>state</b>   | Specifies the state of the VRRP log. The default setting is disabled. |
| <b>enable</b>  | Specifies that the VRRP log state will be enabled.                    |
| <b>disable</b> | Specifies that the VRRP log state will be disabled.                   |

## ● Restrictions

Only Administrator-level users can issue this command.

## ● Example

To enable the VRRP debug log state:

```
Zxxx0:admin# debug vrrp log state enable
Command: debug vrrp log state enable

Success.

Zxxx0:admin#
```

## 20.31. debug vrrp show counter

---

### ● Description

This command is used to display the VRRP debug statistic counters.

### ● Format

debug vrrp show counter

### ● Parameters

None.

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To display VRRP statistic counters:

```
Zxxx0:admin# debug vrrp show counter
Command: debug vrrp show counter

VRRP debug statistic counters
Received ADV : 9
Drop         : 52
Auth fail    : 0
Sent ADV     : 0

Zxxx0:admin#
```

## 20.32. debug vrrp show flag

---

### ● Description

This command is used to display VRRP debug flag settings.

### ● Format

debug vrrp show flag

### ● Parameters

None.

### ● Restrictions

Only Administrator-level users can issue this command.

- **Example**

To display VRRP debug flag settings:

```
Zxxx0:admin#debug vrrp show flag
Command: debug vrrp show flag

Global State: Disabled

Current VRRP debug level setting:

virtual router state change
packet receiving
packet sending
mac address update
interface change
timer

Zxxx0:admin#
```

## 20.33. debug vrrp show log state

---

- **Description**

The command is used to display the VRRP debug log state.

- **Format**

**debug vrrp show log state**

- **Parameters**

None.

- **Restrictions**

Only Administrator-level users can issue this command.

- **Example**

To display the VRRP debug log state:

```
Zxxx0:admin# debug vrrp show log state
Command: debug vrrp show log state

VRRP Debug Log State: Disabled

Zxxx0:admin#
```



## 20.34. debug vrrp state

---

### ● Description

The command is used to enable or disable the VRRP debug state.

### ● Format

**debug vrrp state [enable | disable]**

### ● Parameters

---

|                |                                                                               |
|----------------|-------------------------------------------------------------------------------|
| <b>state</b>   | Specifies the state of the VRRP debug state. The default setting is disabled. |
| <b>enable</b>  | Specifies that the VRRP debug state will be enabled.                          |
| <b>disable</b> | Specifies that the VRRP debug state will be disabled.                         |

---

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To enable the VRRP debug state:

```
Zxxx0:admin# debug vrrp state enable
Command: debug vrrp state enable

Success.

Zxxx0:admin#
```

## 20.35. debug dhcpv6\_relay state enable

---

### ● Description

This command is used to enable the DHCPv6 relay Debug function.

### ● Format

**debug dhcpv6\_relay state enable**

### ● Parameters

None.

- **Restrictions**

Only Administrator-level users can issue this command.

- **Example**

To enabled DHCPv6 relay debug function:

```
Zxxx0:admin# debug dhcpv6_relay state enable
Command:  debug dhcpv6_relay state enable

Success.

Zxxx0:admin#
```

## **20.36. debug dhcpv6\_relay state disable**

- **Description**

This command is used to disable the DHCPv6 relay Debug function.

- **Format**

**debug dhcpv6\_relay state disable**

- **Parameters**

None.

- **Restrictions**

Only Administrator-level users can issue this command.

- **Example**

To disabled DHCPv6 relay debug function:

```
Zxxx0:admin# debug dhcpv6_relay state disable
Command:  debug dhcpv6_relay state disable

Success.

Zxxx0:admin#
```

## 20.37. debug dhcpv6\_relay hop\_count state

---

### ● Description

This command is used to enable or disable debug information flag about the hop count.

### ● Format

debug dhcpv6\_relay hop\_count state [enable | disable]

### ● Parameters

---

|                |                                                      |
|----------------|------------------------------------------------------|
| <b>state</b>   | Specifies the hop count debugging state.             |
| <b>enable</b>  | Specifies that the hop count state will be enabled.  |
| <b>disable</b> | Specifies that the hop count state will be disabled. |

---

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To enable debug information flag about the hop count:

```
Zxxx0:admin# debug dhcpv6_relay hop_count state enable
Command: debug dhcpv6_relay hop_count state enable

Success.

Zxxx0:admin#
```

## 20.38. debug dhcpv6\_relay output

---

### ● Description

Used to set debug message to output to buffer or console.

### ● Format

debug dhcpv6\_relay output [buffer | console]

## ● Parameters

---

|                |                                                     |
|----------------|-----------------------------------------------------|
| <b>output</b>  | Specifies the location of the debug message output. |
| <b>buffer</b>  | Let the debug message output to buffer.             |
| <b>console</b> | Let the debug message output to console.            |

---

## ● Restrictions

Only Administrator-level users can issue this command.

## ● Example

To set debug information to output to console:

```
Zxxx0:admin# debug dhcpv6_relay output console
Command: debug dhcpv6_relay output console

Success.

Zxxx0:admin#
```

# 20.39. debug dhcpv6\_relay packet

---

## ● Description

Used to enable or disable debug information flag for DHCPv6 relay packet, including packet receiving and sending.

## ● Format

**debug dhcpv6\_relay packet {all | receiving | sending} state [enable | disable]**

## ● Parameters

---

|                  |                                                                         |
|------------------|-------------------------------------------------------------------------|
| <b>all</b>       | (Optional) Set packet receiving and sending debug flags.                |
| <b>receiving</b> | (Optional) Set packet receiving debug flag.                             |
| <b>sending</b>   | (Optional) Set packet sending debug flag.                               |
| <b>state</b>     | Specifies if the designated flags function will be enabled or disabled. |
| <b>enable</b>    | Enable the designated flags.                                            |
| <b>disable</b>   | Disable the designated flags.                                           |

---

## ● Restrictions

Only Administrator-level users can issue this command.

## 20. Debug Software Command List

### ● Example

To enabled DHCPv6 relay packet sending debug:

```
Zxxx0:admin# debug dhcpv6_relay packet sending state enable
Command: debug dhcpv6_relay packet sending state enable

Success.

Zxxx0:admin#
```

## 20.40. debug dhcpv6\_server packet

### ● Description

This command is used to enable or disable the debug information flag of the DHCPv6 server packet, including packets receiving and sending.

### ● Format

**debug dhcpv6\_server packet** [all | receiving | sending] state [enable | disable]

### ● Parameters

|                  |                                               |
|------------------|-----------------------------------------------|
| <b>all</b>       | Set packet receiving and sending debug flags. |
| <b>receiving</b> | Set packet receiving debug flag.              |
| <b>sending</b>   | Set packet sending debug flag.                |
| <b>state</b>     | Specifies the state of the designated flags.  |
| <b>enable</b>    | Enable the designated flags.                  |
| <b>disable</b>   | Disable the designated flags.                 |

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To enabled the DHCPv6 server packet sending debug:

```
Zxxx0:admin# debug dhcpv6_server packet sending state enable
Command: debug dhcpv6_server packet sending state enable

Success.

Zxxx0:admin#
```

## 20.41. debug dhcpv6\_server state disable

---

- **Description**

This command is used to disable the DHCPv6 server debug functions.

- **Format**

debug dhcpv6\_server state disable

- **Parameters**

None.

- **Restrictions**

Only Administrator-level users can issue this command.

- **Example**

To disabled the DHCPv6 server debug function:

```
Zxxx0:admin# debug dhcpv6_server state disable
Command: debug dhcpv6_server state disable

Success.

Zxxx0:admin#
```

## 20.42. debug dhcpv6\_server state enable

---

- **Description**

This command is used to enable the DHCPv6 server debug functions.

- **Format**

debug dhcpv6\_server state enable

- **Parameters**

None.

- **Restrictions**

Only Administrator-level users can issue this command.

- **Example**

To enabled the DHCPv6 server debug function:

## 20. Debug Software Command List

```
Zxxx0:admin# debug dhcpv6_server state enable
Command: debug dhcpv6_server state enable

Success.

Zxxx0:admin#
```

### 20.43. debug pim ssm

---

#### ● Description

This command is used to enable the PIM-SSM debug function.

#### ● Format

**debug pim ssm**

#### ● Parameters

None.

#### ● Restrictions

Only Administrator-level users can issue this command.

#### ● Example

To enable the PIM-SSM debug function:

```
Zxxx0:admin# debug pim ssm
Command: debug pim ssm

Success.

Zxxx0:admin#
```

Once the PIM-SSM debug enabled, the debug information maybe outputted.

```
Zxxx0:admin# Group Record mode 2 for SSM group 232.1.1.1 from 192.168.2.14, ignored

Output truncated...
```

## 20.44. no debug pim ssm

---

### ● Description

This command is used to disable the PIM-SSM debug function.

### ● Format

no debug pim ssm

### ● Parameters

None.

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To disable the PIM-SSM debug function:

```
Zxxx0:admin# no debug pim ssm
Command: no debug pim ssm

Success.

Zxxx0:admin#
```

## 20.45. debug show status

---

### ● Description

Show the debug handler state and the specified module's debug status.

If the input module list is empty, the states of all registered modules which support debug module will be shown.

### ● Format

debug show status {module <module\_list>}

### ● Parameters

---

**module** (Optional) Specifies the module list.  
     <module\_list>  
         Enter the module list here.

---



## 20. Debug Software Command List

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To show the specified module's debug state:

```
Prompt# debug show status module MSTP
Command: debug show status module MSTP

Debug Global State: Enable

MSTP                : Enable

Prompt#
```

To show the debug state:

```
Prompt# debug show status
Command: debug show status

Debug Global State: Enable

SYS      : Enable
OS       : Enable
MSTP     : Enable
ACL      : Disable
CLI      : Enable
SNMP     : Disable
IGMP     : Enable

Prompt#
```

## 21.DHCP Local Relay Commands

DHCP (Dynamic Host Configuration Protocol) is a function to obtain an IP address from the DHCP server when the client is booted. In general, a series of packets to obtain an IP address is broadcasted.

DHCP Local Relay is a function to add option 82 information (the Switching Hub's MAC address and the client's connection port number) to DHCP packets if the client and DHCP server are on the same VLAN. A DHCP server supporting option 82 can use option 82 information to apply the policy required to assign an IP address. Original option 82 information is also added to return packets from the DHCP server, so that the packets to the client are transferred to the destination port instead of being broadcasted.

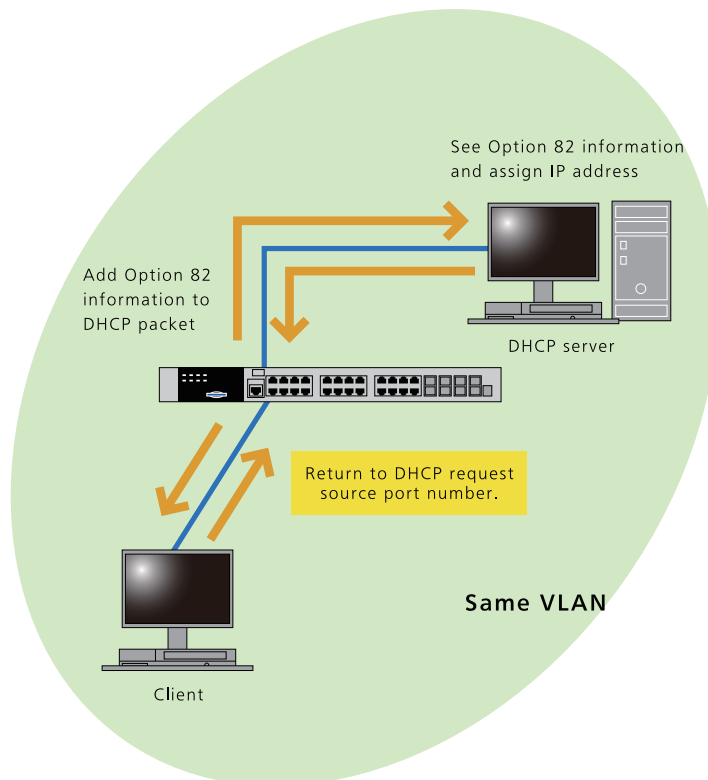


Figure 21-1 DHCP Local Relay overview

To use this function, the DHCP relay function needs to be enabled separately.

Refer to "DHCP Relay Commands."

## 21. DHCP Local Relay Commands

---

```
config dhcp_local_relay vlan <vlan_name 32> state [enable | disable]
config dhcp_local_relay vlan vlanid <vlan_id> state [enable | disable]
enable dhcp_local_relay
disable dhcp_local_relay
show dhcp_local_relay
```

---

### 21.1. config dhcp\_local\_relay vlan

---

#### ● Description

This command is used to enable or disable the DHCP local relay function for a specified VLAN. When DHCP local relay is enabled for the VLAN, the DHCP packet will be relayed as a broadcast without changing the source MAC address and gateway address. DHCP option 82 will be automatically added.

#### ● Format

```
config dhcp_local_relay vlan <vlan_name 32> state [enable | disable]
```

#### ● Parameters

---

|                             |                                                                  |
|-----------------------------|------------------------------------------------------------------|
| <b>&lt;vlan_name 32&gt;</b> | Specify the name of the VLAN to be enabled for DHCP local relay. |
| <b>state</b>                | Enable or disable DHCP local relay for a specified VLAN.         |
| <b>enable</b>               | Enable DHCP local relay for a specified VLAN.                    |
| <b>disable</b>              | Disable DHCP local relay for a specified VLAN.                   |

---

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To enable DHCP local relay for the default VLAN:

```
Zxxx0:admin#config dhcp_local_relay vlan default state enable
Command: config dhcp_local_relay vlan default state enable

Success.

Zxxx0:admin#
```

## 21.2. `config dhcp_local_relay vlan vlanid`

### ● Description

This command is used to enable or disable the DHCP local relay function for a specified VLAN ID.

### ● Format

`config dhcp_local_relay vlan vlanid <vlan_id> state [enable | disable]`

### ● Parameters

|               |                                                                                                                                                                                                |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlanid</b> | Specifies the VLAN ID used to enabled DHCP local relay.<br><b>&lt;vlan_id&gt;</b><br>Enter the VLAN ID used here.                                                                              |
| <b>state</b>  | Enable or disable DHCP local relay for a specified VLAN.<br><b>enable</b><br>Enable DHCP local relay for a specified VLAN.<br><b>disable</b><br>Disable DHCP local relay for a specified VLAN. |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable DHCP local relay for the default VLAN:

```
Zxxx0:admin#config dhcp_local_relay vlan vlanid 1 state enable
Command: config dhcp_local_relay vlan vlanid 1 state enable

Success.

Zxxx0:admin#
```

## 21.3. `enable dhcp_local_relay`

### ● Description

This command is used to globally enable the DHCP local relay function on the Switching Hub.

### ● Format

`enable dhcp_local_relay`

## 21. DHCP Local Relay Commands

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable the DHCP local relay function:

```
Zxxx0:admin#enable dhcp_local_relay
Command: enable dhcp_local_relay

Success.

Zxxx0:admin#
```

## 21.4. disable dhcp\_local\_relay

---

### ● Description

This command is used to globally disable the DHCP local relay function on the Switching Hub.

### ● Format

**disable dhcp\_local\_relay**

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To disable the DHCP local relay function:

```
Zxxx0:admin#disable dhcp_local_relay
Command: disable dhcp_local_relay

Success.

Zxxx0:admin#
```

## 21.5. show dhcp\_local\_relay

---

### ● Description

This command is used to display the current DHCP local relay configuration on the Switching Hub.

### ● Format

`show dhcp_local_relay`

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display the local DHCP relay status:

```
Zxxx0:admin#show dhcp_local_relay
Command: show dhcp_local_relay

DHCP/BOOTP Local Relay Status      : Disabled
DHCP/BOOTP Local Relay VID List    : 1,3-4

Zxxx0:admin#
```

---

## 22. DHCP Relay Commands

---

DHCP (Dynamic Host Configuration Protocol) is a function to obtain an IP address from the DHCP server when the client is booted. In general, a series of packets to obtain an IP address is broadcasted. For this reason, the client and DHCP server must be on the same network. DHCP Relay is a function to transfer DHCP packets to a DHCP server on a different network. This does no longer require a DHCP server installed for each network, making it easier for you to manage the DHCP server.

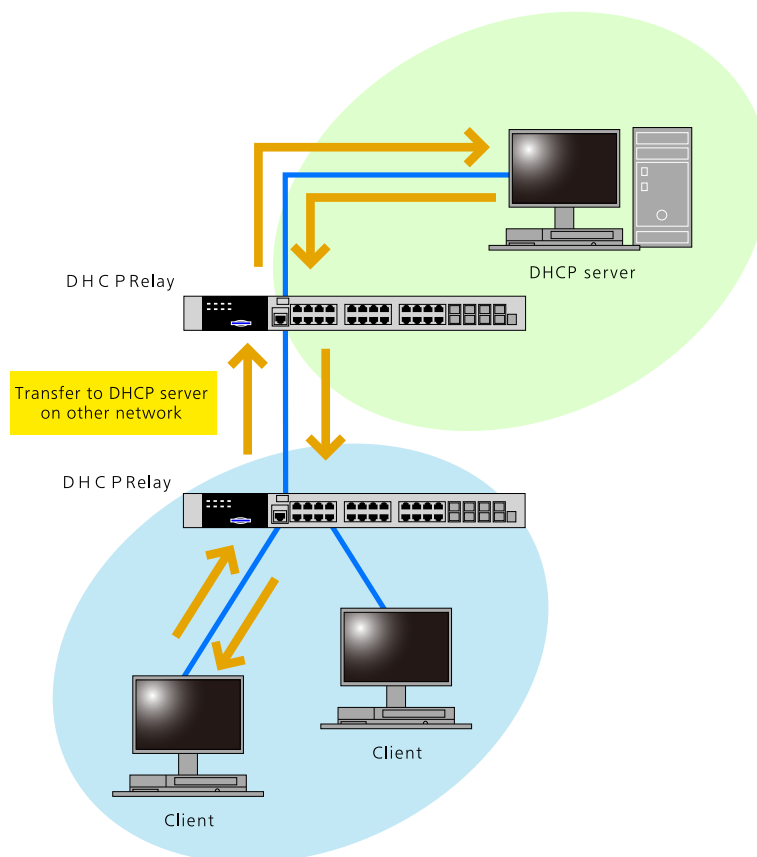


Figure 22-1 DHCP Relay overview

### ● option 82

This is a function to add the Switching Hub's MAC address and the client's connection port number to packets when relaying the DHCP packets. A DHCP server supporting option 82 can use option 82 information to apply the policy required to assign an IP address. Original option 82 information is also added to return packets from the DHCP server, so that the packets to the client are transferred to the destination port instead of being broadcasted.

## ● Option 60/61

This is client identification information added to DHCP packets. For example, IP phone model number.

You can configure the relay destination or change information, such as an IP address assigned by the DHCP server, according to the client environment based on this information.

---

```

config dhcp_relay {hops <int 1-16> | time <sec 0-65535>}(1)
config dhcp_relay add ipif <ipif_name 12> <ipaddr>
config dhcp_relay delete ipif <ipif_name 12> <ipaddr>
config dhcp_relay option_60 add string <multiword 255> relay <ipaddr> [exact-match | partial-match]
config dhcp_relay option_60 default [relay <ipaddr> | mode [relay | drop]]
config dhcp_relay option_60 delete [string <multiword 255> {relay <ipaddr>} | ipaddress <ipaddr> | all | default {<ipaddr>}]
config dhcp_relay option_60 state [enable | disable]
config dhcp_relay option_61 add [mac_address <macaddr> | string <desc_long 255>] [relay <ipaddr> | drop]
config dhcp_relay option_61 default [relay <ipaddr> | drop]
config dhcp_relay option_61 delete [mac_address <macaddr> | string <desc_long 255> | all]
config dhcp_relay option_61 state [enable | disable]
config dhcp_relay option_82 check [enable | disable]
config dhcp_relay option_82 policy [replace | drop | keep]
config dhcp_relay option_82 remote_id [default | user_define <desc 32>]
config dhcp_relay option_82 state [enable | disable]
enable dhcp_relay
disable dhcp_relay
show dhcp_relay {ipif <ipif_name 12>}
show dhcp_relay option_60 {[string <multiword 255> | ipaddress <ipaddr> | default]}
show dhcp_relay option_61

```

---



### 22.1. config dhcp\_relay

---

#### ● Description

This command is used to configure the DHCP relay feature of the Switching Hub.

#### ● Format

`config dhcp_relay {hops <int 1-16> | time <sec 0-65535>}(1)`

#### ● Parameters

---

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>hops</b> | Specify the maximum number of router hops that the DHCP/BOOTP packets can cross. The range is 1 to 16. The default value is 4.<br><b>&lt;int 1-16&gt;</b><br>Specify the maximum number of router hops that the DHCP/BOOTP packets can cross. The maximum number of hops value must be between 1 and 16.                                                                                                                                                         |
| <b>time</b> | Specify the minimum time in seconds within which the Switching Hub must relay the DHCP/BOOTP request. If this time is larger than the DHCP packet's time, the Switching Hub will drop the DHCP/BOOTP packet. The range is 0 to 65535. The default value is 0.<br><b>&lt;sec 0-65535&gt;</b><br>Specify the minimum time in seconds within which the Switching Hub must relay the DHCP/BOOTP request. The minimum time value must be between 0 and 65535 seconds. |

---

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To configure the DHCP relay:

```
Zxxx0:admin#config dhcp_relay hops 4 time 2
Command: config dhcp_relay hops 4 time 2

Success.

Zxxx0:admin#
```

## 22.2. config dhcp\_relay add ipif

---

### ● Description

This command is used to add an IP destination address to the Switching Hub's DHCP relay table.

### ● Format

config dhcp\_relay add ipif <ipif\_name 12> <ipaddr>

### ● Parameters

---

<ipif\_name 12>

Specify the name of the IP interface which contains the IP address below.

---

<ipaddr> Specify the DHCP/BOOTP server IP address.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To add an IP destination address to the Switching Hub's DHCP relay table:

```
Zxxx0:admin#config dhcp_relay add ipif System 10.43.21.12
Command: config dhcp_relay add ipif System 10.43.21.12

Success.

Zxxx0:admin#
```

## 22.3. config dhcp\_relay delete ipif

---

### ● Description

This command is used to delete an IP destination address from the Switching Hub's DHCP relay table.

### ● Format

config dhcp\_relay delete ipif <ipif\_name 12> <ipaddr>

### ● Parameters

---

<ipif\_name 12>

Specify the name of the IP interface which contains the IP address below.

---

<ipaddr> Specify the DHCP/BOOTP server IP address.

---

## 22. DHCP Relay Commands

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete an IP destination address from the Switching Hub's DHCP relay table:

```
Zxxx0:admin#config dhcp_relay delete ipif System 10.43.21.12
Command: config dhcp_relay delete ipif System 10.43.21.12

Success.

Zxxx0:admin#
```

## **22.4. config dhcp\_relay option\_60 add string**

### ● Description

This command is used to configure the Option 60 relay rules. Note that different strings can be specified with the same relay server, and the same string can be specified with multiple relay servers. The system will relay the packet to all the matching servers.

### ● Format

**config dhcp\_relay option\_60 add string <multiword 255> relay <ipaddr> [exact-match | partial-match]**

### ● Parameters

---

**<multiword 255>**

Specify a string.

---

**relay** Specify a relay server IP address.

**<ipaddr>**

Enter the IP address here.

---

**exact-match**

The Option 60 string in the packet must fully match the specified string.

---

**partial-match**

The Option 60 string in the packet only need partially match the specified string.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure DHCP Option 60 to decide to relay which DHCP server:

```
Zxxx0:admin#config dhcp_relay option_60 add string "abc" relay 10.90.90.1 exact-match
Command: config dhcp_relay option_60 add string "abc" relay 10.90.90.1 exact-match

Success.

Zxxx0:admin#
```

## 22.5. `config dhcp_relay option_60 default`

### ● Description

This command is used to configure DHCP relay Option 60 default relay servers. When there are no match servers found for the packet based on Option 60, the relay servers will be determined by the default relay server setting. When drop is specified, the packet with no matching rules found will be dropped without further processing. If the setting is no-drop, then the packet will be processed further based on Option 61. The final relay servers will be the union of Option 60 default relay servers and the relay servers determined by Option 61.

### ● Format

`config dhcp_relay option_60 default [relay <ipaddr> | mode [relay | drop]]`

### ● Parameters

|              |                                                                                                                                                                                                 |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>relay</b> | Specify a relay server IP for the packet that has matching Option 60 rules.<br><b>&lt;ipaddr&gt;</b><br>Enter the server IP address here.                                                       |
| <b>mode</b>  | Specify the mode to relay or drop packets.<br><b>relay</b> The packet will be relayed based on the relay rules.<br><b>drop</b> Specify to drop the packet that has no matching Option 60 rules. |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure a DHCP Option 60 default drop action:

```
Zxxx0:admin#config dhcp_relay option_60 default mode drop
Command: config dhcp_relay option_60 default mode drop

Success.

Zxxx0:admin#
```

## 22.6. config dhcp\_relay option\_60 delete

### ● Description

This command is used to delete a DHCP Option 60 entry. When all is specified, all rules excluding the default rules are deleted.

### ● Format

**config dhcp\_relay option\_60 delete** [**string** <multiword 255> {**relay** <ipaddr>} | **ipaddress** <ipaddr> | **all** | **default** {<ipaddr>}]

### ● Parameters

|                  |                                                                                                                                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>string</b>    | Delete all the entries whose string is equal to the string specified if the IP address is not specified.<br><b>&lt;multiword 255&gt;</b><br>The string value can be up to 255 characters long. |
| <b>relay</b>     | (Optional) Delete one entry, whose string and IP address are equal to the string and IP address specified by the user.<br><b>&lt;ipaddr&gt;</b><br>Enter the IP address here.                  |
| <b>ipaddress</b> | Delete all the entries whose IP address are equal to the specified IP address.<br><b>&lt;ipaddr&gt;</b><br>Enter the IP address here.                                                          |
| <b>all</b>       | Specify to have all rules, excluding the default rules, deleted.                                                                                                                               |
| <b>default</b>   | Delete the default relay IP address that is specified by the user.<br><b>&lt;ipaddr&gt;</b><br>(Optional) Enter the IP address here.                                                           |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete a DHCP Option 60 entry:

```
Zxxx0:admin# config dhcp_relay option_60 delete string "abc" relay 10.90.90.1
Command: config dhcp_relay option_60 delete string "abc" relay 10.90.90.1

Success.

Zxxx0:admin#
```

## 22.7. `config dhcp_relay option_60 state`

---

### ● Description

This command is used to decide whether DHCP relay will process the DHCP Option 60 or not. When Option 60 is enabled, if the packet does not have Option 60, then the relay servers cannot be determined based on Option 60. The relay servers will be determined based on either Option 61 or per IPIF configured servers.

### ● Format

`config dhcp_relay option_60 state [enable | disable]`

### ● Parameters

---

|                |                                                                                              |
|----------------|----------------------------------------------------------------------------------------------|
| <b>enable</b>  | Specify to enable the DHCP relay function to use option 60 rules to relay DHCP packets.      |
| <b>disable</b> | Specify to disable the DHCP relay function from using option 60 rules to relay DHCP packets. |

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the DHCP Option 60 state:

```
Zxxx0:admin#config dhcp_relay option_60 state enable
Command: config dhcp_relay option_60 state enable

Success.

Zxxx0:admin#
```

## 22.8. config dhcp\_relay option\_61 add

### ● Description

This command adds a rule to determine the relay server based on Option 61. The match rule can be based on either MAC address or a user-specified string. Only one relay server can be specified for a MAC address or a string. If relay servers are determined based on Option 60, and one relay server is determined based on Option 61, the final relay servers will be the union of these two sets of the servers.

### ● Format

**config dhcp\_relay option\_61 add [mac\_address <macaddr> | string <desc\_long 255>] [relay <ipaddr> | drop]**

### ● Parameters

|                    |                                                                                                                                                                                                                                    |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mac_address</b> | Specify the client's client-ID, which is the hardware address of the client.<br><b>&lt;macaddr&gt;</b><br>Specify the client's client-ID, which is the MAC address of the client.                                                  |
| <b>string</b>      | Specify the client's client-ID, which is specified by administrator.<br><b>&lt;desc_long 255&gt;</b><br>Specify the client's client-ID, which is specified by administrator The client-ID string can be up to 255 characters long. |
| <b>relay</b>       | Specify to relay the packet to an IP address.<br><b>&lt;ipaddr&gt;</b><br>Specify to relay the packet to an IP address by entering the IP address here.                                                                            |
| <b>drop</b>        | Specify to drop the packet.                                                                                                                                                                                                        |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure DHCP Option 61 to decide how to process DHCP packets:

```
Zxxx0:admin#config dhcp_relay option_61 add mac_address 00-11-22-33-44-55 drop
Command: config dhcp_relay option_61 add mac_address 00-11-22-33-44-55 drop

Success.

Zxxx0:admin#
```

## 22.9. config dhcp\_relay option\_61 default

### ● Description

This command is used to determine the rule to process those packets that have no Option 61 matching rules. The default default-rule is drop.

### ● Format

config dhcp\_relay option\_61 default [relay <ipaddr> | drop]

### ● Parameters

|              |                                                                                                                                       |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>relay</b> | Specify to relay the packet that has no option matching 61 matching rules to an IP address.<br><ipaddr><br>Enter the IP address here. |
| <b>drop</b>  | Specify to drop the packet that have no Option 61 matching rules.                                                                     |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the DHCP Option 61 default action to drop:

```
Zxxx0:admin#config dhcp_relay option_61 default drop
Command: config dhcp_relay option_61 default drop

Success.

Zxxx0:admin#
```

## 22.10. config dhcp\_relay option\_61 delete

### ● Description

This command is used to delete Option 61 rules.

### ● Format

config dhcp\_relay option\_61 delete [mac\_address <macaddr> | string <desc\_long 255> | all]



## 22. DHCP Relay Commands

### ● Parameters

|                    |                                                                                                                               |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>mac_address</b> | The entry with the specified MAC address will be deleted<br><macaddr><br>Enter the MAC address here.                          |
| <b>string</b>      | The entry with the specified string will be deleted.<br><desc_long 255><br>The string value can be up to 255 characters long. |
| <b>all</b>         | All rules excluding the default rule will be deleted.                                                                         |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete a DHCP Option 61 entry:

```
Zxxx0:admin#config dhcp_relay option_61 delete mac_address 00-11-22-33-44-55
Command: config dhcp_relay option_61 delete mac_address 00-11-22-33-44-55

Success.

Zxxx0:admin#
```

## 22.11. config dhcp\_relay option\_61 state

### ● Description

This command is used to decide whether DHCP relay will process the DHCP Option 61 or not. When Option 61 is enabled, if the packet does not have Option 61, then the relay servers cannot be determined based on Option 61. If the relay servers are determined based on Option 60 or Option 61, then per IPIF configured servers will be ignored. If the relay servers are not determined either by Option 60 or Option 61, then per IPIF configured servers will be used to determine the relay servers.

### ● Format

config dhcp\_relay option\_61 state [enable | disable]

### ● Parameters

|                |                                                                                          |
|----------------|------------------------------------------------------------------------------------------|
| <b>enable</b>  | Specify to enable the DHCP relay function to use option 61 rules to relay DHCP packets.  |
| <b>disable</b> | Specify to disable the DHCP relay function to use option 61 rules to relay DHCP packets. |

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure the state of DHCP relay Option 61:

```
Zxxx0:admin#config dhcp_relay option_61 state enable
Command: config dhcp_relay option_61 state enable

Success.

Zxxx0:admin#
```

# 22.12. config dhcp\_relay option\_82 check

## ● Description

This command is used to configure the checking mechanism of the DHCP relay agent information Option 82 of the Switching Hub.

## ● Format

config dhcp\_relay option\_82 check [enable | disable]

## ● Parameters

|                |                                                                                                                                                                               |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>enable</b>  | When the state is enabled, for a packet coming from the client side, the packet should not have the Option 82 field. If the packet has this option field, it will be dropped. |
| <b>disable</b> | The default setting is disabled.                                                                                                                                              |

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure the checking mechanism of the DHCP relay agent information Option 82:

```
Zxxx0:admin#config dhcp_relay option_82 check disable
Command: config dhcp_relay option_82 check disable

Success.

Zxxx0:admin#
```

### 22.13. config dhcp\_relay option\_82 policy

#### ● Description

This option takes effect only when the check status is disabled. The relay agent does this operation because the packet cannot contain two Option 82s. The default setting is replace.

#### ● Format

config dhcp\_relay option\_82 policy [replace | drop | keep]

#### ● Parameters

|                |                                                                                                                                                                                                                                                                                                                                                               |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>replace</b> | Replace the existing option 82 field in the packet.                                                                                                                                                                                                                                                                                                           |
| <b>drop</b>    | Specifies to discard if the packet has the Option 82 field. If the packet, that comes from the client side, contains an Option 82 value, then the packet will be dropped. If the packet, that comes from the client side doesn't contain an Option 82 value, then insert it's own Option 82 value into the packet.                                            |
| <b>keep</b>    | Specifies to retain the existing Option 82 field in the packet. The default setting is replace. If the packet, that comes from the client side, and contains an Option 82 value, then keep the old Option 82 value. If the packet, that comes from the client side, doesn't contain an Option 82 value, then insert it's own Option 82 value into the packet. |

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To configure the policy of DHCP relay agent information Option 82:

```
Zxxx0:admin#config dhcp_relay option_82 policy replace
Command: config dhcp_relay option_82 policy replace

Success

Zxxx0:admin#
```

## 22.14. `config dhcp_relay option_82 remote_id`

### ● Description

This command is used to configure the remote ID string of the DHCP relay agent information Option 82 of the Switch.

### ● Format

`config dhcp_relay option_82 remote_id [default | user_define <desc 32>]`

### ● Parameters

---

**default** Use the Switching Hub's system MAC address as remote ID.

---

**user\_define**

Use the user-defined string as remote ID. Space characters are allowed in the string.

**<desc 32>**

The user-defined string can be up to 32 characters long.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the remote ID string of the DHCP relay agent information Option 82:

```
Zxxx0:admin#config dhcp_relay option_82 remote_id user_define Switch
Command: config dhcp_relay option_82 remote_id user_define Switch

Success.

Zxxx0:admin#
```

### 22.15. config dhcp\_relay option\_82 state

---

#### ● Description

This command is used to configure the state of the DHCP relay agent information Option 82 of the Switching Hub. The default settings is disabled.

#### ● Format

config dhcp\_relay option\_82 state [enable | disable]

#### ● Parameters

|                |                                                                                                                                                                                                                       |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>enable</b>  | When the state is enabled, the DHCP packet will be inserted with the Option 82 field before being relayed to server. The DHCP packet will be processed based on the behavior defined in the check and policy setting. |
| <b>disable</b> | When the state is disabled, the DHCP packet will be relayed directly to the server without further check and processing of the packet.                                                                                |

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To configure the state of the DHCP relay agent information Option 82:

```
Zxxx0:admin#config dhcp_relay option_82 state enable
Command: config dhcp_relay option_82 state enable

Success.

Zxxx0:admin#
```

### 22.16. enable dhcp\_relay

---

#### ● Description

This command is used to enable the DHCP relay function on the Switching Hub.

#### ● Format

enable dhcp\_relay

#### ● Parameters

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To enable the DHCP relay function:

```
Zxxx0:admin#enable dhcp_relay
Command: enable dhcp_relay

Success.

Zxxx0:admin#
```

## **22.17. disable dhcp\_relay**

---

- **Description**

This command is used to disable the DHCP relay function on the Switching Hub.

- **Format**

**disable dhcp \_relay**

- **Parameters**

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To disable the DHCP relay function:

```
Zxxx0:admin#disable dhcp_relay
Command: disable dhcp_relay

Success.

Zxxx0:admin#
```

## 22.18. show dhcp\_relay

### ● Description

This command is used to display the current DHCP relay configuration.

### ● Format

**show dhcp\_relay {ipif <ipif\_name 12>}**

### ● Parameters

---

|             |                                                                                                                                                                   |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b> | (Optional) Specify the IP interface name.<br><b>&lt;ipif_name 12&gt;</b><br>Specify the IP interface name. The IP interface name can be up to 12 characters long. |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---



---

**NOTE** If no parameter is specified, the system will display all DHCP relay configurations.

---

### ● Restrictions

None.

### ● Example

To display the DHCP relay status:

```
Zxxx0:admin#show dhcp_relay
Command: show dhcp_relay

DHCP/BOOTP Relay Status      : Disabled
DHCP/BOOTP Hops Count Limit  : 4
DHCP/BOOTP Relay Time Threshold : 0
DHCP Vendor Class Identifier Option 60 State: Disabled
DHCP Client Identifier Option 61 State: Disabled
DHCP Relay Agent Information option 82 State : Disabled
DHCP Relay Agent Information option 82 Check : Disabled
DHCP Relay Agent Information option 82 Policy : Replace
DHCP Relay Agent Information option 82 Remote ID : Switch

Interface      Server 1      Server 2      Server 3      Server 4
-----
System         10.1.1.1      192.168.0.1
Zxxx0:admin#
```

## 22.19. show dhcp\_relay option\_60

### ● Description

This command is used to display the DHCP relay option 60 entries.

### ● Format

**show dhcp\_relay option\_60** {[string <multiword 255> | ipaddress <ipaddr> | default]}

### ● Parameters

|                  |                                                                                                                                       |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>string</b>    | (Optional) Display the entry whose string equals the string specified.<br><multiword 255>The string can be up to 255 characters long. |
| <b>ipaddress</b> | (Optional) Display the entry whose IP ipaddress equals the specified IP address.<br><ipaddr><br>Enter the IP address here.            |
| <b>default</b>   | (Optional) Display the default behaviour of DHCP relay option 60.                                                                     |

**NOTE** If no parameter is specified, all DHCP option 60 entries will be displayed.

### ● Restrictions

None.

### ● Example

To display the DHCP option 60 entries:

```
Zxxx0:admin#show dhcp_relay option_60
Command: show dhcp_relay option_60

Default Processing Mode: Drop

Default Servers:
  10.90.90.100
  10.90.90.101
  10.90.90.102

Matching Rules:

String                Match Type            IP Address
-----
abc                   Exact Match           10.90.90.1
abcde                 Partial Match         10.90.90.2
abcdefg              Exact Match           10.90.90.3

Total Entries: 3

Zxxx0:admin#
```



### 22.20. show dhcp\_relay option\_61

---

#### ● Description

This command is used to display all the DHCP relay option 61 rules.

#### ● Format

show dhcp\_relay option\_61

#### ● Parameters

None.

#### ● Restrictions

None.

#### ● Example

To display the DHCP option 61 entries:

```
Zxxx0:admin#show dhcp_relay option_61
Command: show dhcp_relay option_61

Default Relay Rule:Drop

Matching Rules:

Client-ID                                Type                Relay Rule
-----                                ----                -
abc                                     String              Drop
abcde                                  String              10.90.90.1
00-11-22-33-44-55                      MAC Address         Drop

Total Entries: 3

Zxxx0:admin#
```

## 23. DHCP Server Commands

DHCP (Dynamic Host Configuration Protocol) is a function to obtain an IP address from the DHCP server when the client is booted. This Switching Hub can be used as a DHCP server.

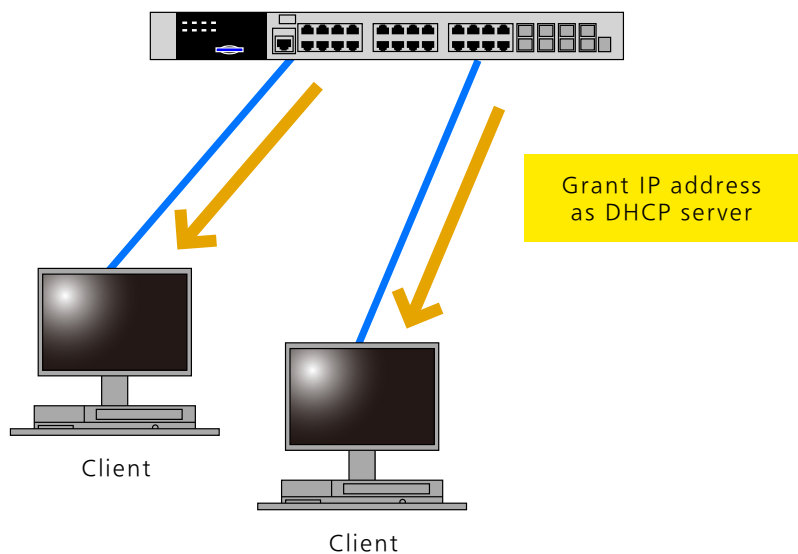


Figure 23-1

To use this Switching Hub as a DHCP server, you need to configure the range and expiration time of an IP address assigned to the client.

For devices using a static IP address, you can create a mapping between MAC addresses and IP addresses and assign it to the devices.

Setting changes are applied after this Switching Hub is rebooted.

```
create dhcp excluded_address begin_address <ipaddr> end_address <ipaddr>
delete dhcp excluded_address [begin_address <ipaddr> end_address <ipaddr> | all]
show dhcp excluded_address
create dhcp pool <pool_name 12>
delete dhcp pool [<pool_name 12> | all]
config dhcp pool network_addr <pool_name 12> <network_address>
config dhcp pool domain_name <pool_name 12> {<domain_name 64>}
config dhcp pool dns_server <pool_name 12> {<ipaddr>} {<ipaddr>} {<ipaddr>}
config dhcp pool netbios_name_server <pool_name 12> {<ipaddr>} {<ipaddr>} {<ipaddr>}
config dhcp pool netbios_node_type <pool_name 12> [broadcast | peer_to_peer | mixed | hybrid]
config dhcp pool default_router <pool_name 12> {<ipaddr>} {<ipaddr>} {<ipaddr>}
config dhcp pool lease <pool_name 12> [<day 0-365> <hour 0-23> <minute 0-59> | infinite]
config dhcp pool boot_file <pool_name 12> {<file_name 64>}
config dhcp pool next_server <pool_name 12> {<ipaddr>}
config dhcp ping_packets <number 0-10>
config dhcp ping_timeout <millisecond 10-2000>
create dhcp pool manual_binding <pool_name 12> <ipaddr> hardware_address <macaddr> {type
    [ethernet | ieee802]}
delete dhcp pool manual_binding <pool_name 12> [<ipaddr> | all]
```

## 23. DHCP Server Commands

---

```
clear dhcp binding [<pool_name 12> [<ipaddr> | all] | all]
show dhcp binding {<pool_name 12>}
show dhcp pool {<pool_name 12>}
show dhcp pool manual_binding {<pool_name 12>}
enable dhcp_server
disable dhcp_server
show dhcp_server
clear dhcp conflict_ip [<ipaddr> | all]
show dhcp conflict_ip {<ipaddr>}
```

---

### 23.1. create dhcp excluded\_address

---

#### ● Description

This command is used to create a DHCP server exclude address. The DHCP server assumes that all IP addresses in a DHCP pool subnet are available for assigning to DHCP clients. Use this command to specify the IP address that the DHCP server should not assign to clients. This command can be used multiple times in order to define multiple groups of excluded addresses.

#### ● Format

**create dhcp excluded\_address begin\_address <ipaddr> end\_address <ipaddr>**

#### ● Parameters

---

**begin\_address**

Specify the starting address of the IP address range.

**<ipaddr>**

Specify the starting address of the IP address range.

---

**end\_address**

Specify the ending address of the IP address range.

**<ipaddr>**

Specify the ending address of the IP address range.

---

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To specify the IP address that DHCP server should not assign to clients:

```
Zxxx0:admin#create dhcp excluded_address begin_address 10.10.10.1 end_address
10.10.10.10
Command: create dhcp excluded_address begin_address 10.10.10.1 end_address
10.10.10.10

Success.

Zxxx0:admin#
```

## 23.2. delete dhcp excluded\_address

### ● Description

This command is used to delete a DHCP server exclude address.

### ● Format

**delete dhcp excluded\_address [begin\_address <ipaddr> end\_address <ipaddr> | all]**

### ● Parameters

#### **begin\_address**

Specify the starting address of the IP address range.

**<ipaddr>**

Specify the starting address of the IP address range.

#### **end\_address**

Specify the ending address of the IP address range.

**<ipaddr>**

Specify the ending address of the IP address range.

#### **all**

Specify to delete all IP addresses.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete a DHCP server exclude address:

```
Zxxx0:admin#delete dhcp excluded_address begin_address 10.10.10.1 end_address
10.10.10.10
Command: delete dhcp excluded_address begin_address 10.10.10.1 end_address
10.10.10.10

Success.

Zxxx0:admin#
```

## 23.3. show dhcp excluded\_address

---

### ● Description

This command is used to display the groups of IP addresses which are excluded from being a legal assigned IP address.

### ● Format

show dhcp excluded\_address

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display the DHCP server excluded addresses:

```
Zxxx0:admin#show dhcp excluded_address
Command: show dhcp excluded_address

Index   Begin Address   End Address
-----
1        192.168.0.1     192.168.0.100
2        10.10.10.10     10.10.10.11

Total Entries : 2

Zxxx0:admin#
```

## 23.4. create dhcp pool

---

### ● Description

This command is used to create a DHCP pool by specifying a name. After creating a DHCP pool, use other DHCP pool configuration commands to configure parameters for the pool.

### ● Format

create dhcp pool <pool\_name 12>

## ● Parameters

---

**<pool\_name 12>**

Specify the name of the DHCP pool.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To create a DHCP pool:

```
Zxxx0:admin#create dhcp pool nyknicks
Command: create dhcp pool nyknicks

Success.

Zxxx0:admin#
```

# 23.5. delete dhcp pool

---

## ● Description

This command is used to delete a DHCP pool.

## ● Format

**delete dhcp pool [<pool\_name 12> | all]**

## ● Parameters

---

**<pool\_name 12>**

Specify the name of the DHCP pool.

---

**all**

Specify to delete all the DHCP pools.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To delete a DHCP pool:

```
Zxxx0:admin#delete dhcp pool nyknicks
Command: delete dhcp pool nyknicks

Success.

Zxxx0:admin#
```

## 23.6. `config dhcp pool network_addr`

---

### ● Description

This command is used to specify the network for the DHCP pool. The addresses in the network are free to be assigned to the DHCP client. The prefix length specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/). When the DHCP server receives a request from the client, the server will automatically find a pool to allocate the address. If the request is relayed to the server by the intermediate device, the server will match the gateway IP address carried in the packet against the network of each DHCP pool. The pool which has the longest match will be selected. If the request packet is not through relay, then the server will match the IP address of the IPIF that received the request packet against the network of each DHCP pool.

### ● Format

`config dhcp pool network_addr <pool_name 12> <network_address>`

### ● Parameters

---

`<pool_name 12>`

Specify the DHCP pool name.

---

`<network_address>`

Specify the IP address that the DHCP server may assign to clients.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the address range of the DHCP address pool:

```
Zxxx0:admin#config dhcp pool network_addr nyknicks 10.10.10.0/24
Command: config dhcp pool network_addr nyknicks 10.10.10.0/24

Success.

Zxxx0:admin#
```

## 23.7. `config dhcp pool domain_name`

### ● Description

This command is used to specify the domain name for the client if the server allocates the address for the client from this pool. The domain name configured here will be used as the default domain name by the client. By default, the domain name is empty. If the domain name is empty, the domain name information will not be provided to the client.

### ● Format

`config dhcp pool domain_name <pool_name 12> {<domain_name 64>}`

### ● Parameters

---

`<pool_name 12>`

Specify the DHCP pool name.

---

`<domain_name 64>`

(Optional) Specify the domain name of the client.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the domain name option of the DHCP pool:

```
Zxxx0:admin#config dhcp pool domain_name nyknicks nba.com
Command: config dhcp pool domain_name nyknicks nba.com

Success.

Zxxx0:admin#
```

## 23.8. `config dhcp pool dns_server`

### ● Description

This command is used to specify the IP address of a DNS server that is available to a DHCP client. Up to three IP addresses can be specified on one command line. If DNS server is not specified, the DNS server information will not be provided to the client. If this command is input twice for the same pool, the second command will overwrite the first command.

### ● Format

`config dhcp pool dns_server <pool_name 12> {<ipaddr>} {<ipaddr>} {<ipaddr>}`



## 23. DHCP Server Commands

### ● Parameters

---

**<pool\_name 12>**

Specify the DHCP poll name.

---

**<ipaddr>** (Optional) Specify the IP address of the DNS server. Up to three IP addresses can be specified on one command line.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the DNS server's IP address:

```
Zxxx0:admin#config dhcp pool dns_server nyknicks 10.10.10.1
Command: config dhcp pool dns_server nyknicks 10.10.10.1

Success.

Zxxx0:admin#
```

## **23.9. config dhcp pool netbios\_name\_server**

### ● Description

This command is used to specify the NetBIOS WINS server that is available to a Microsoft DHCP client. Up to three IP addresses can be specified on one command line.

Windows Internet Naming Service (WINS) is a name resolution service that Microsoft DHCP clients use to correlate host names to IP addresses within a general grouping of networks. If a NetBIOS name server is not specified, the NetBIOS name server information will not be provided to the client. If this command is input twice for the same pool, the second command will overwrite the first command.

### ● Format

**config dhcp pool netbios\_name\_server <pool\_name 12> {<ipaddr>} {<ipaddr>} {<ipaddr>}**

### ● Parameters

---

**<pool\_name 12>** - Specify the DHCP pool name.

**<ipaddr>** - (Optional) Specify the IP address of the WINS server. Up to three IP addresses can be specified on one command line.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure a WINS server IP address:

```
Zxxx0:admin#config dhcp pool netbios_name_server knicks 10.10.10.1
Command: config dhcp pool netbios_name_server knicks 10.10.10.1

Success.

Zxxx0:admin#
```

## **23.10. config dhcp pool netbios\_node\_type**

### ● Description

This command is used to specify the NetBIOS node type for a Microsoft DHCP client. The NetBIOS node type for Microsoft DHCP clients can be one of four settings: broadcast, peer-to-peer, mixed, or hybrid. Use this command to configure a NetBIOS over TCP/IP device that is described in RFC 1001/1002. By default, the NetBIOS node type is broadcast.

### ● Format

**config dhcp pool netbios\_node\_type <pool\_name 12> [broadcast | peer\_to\_peer | mixed | hybrid]**

### ● Parameters

|                             |                                                                           |
|-----------------------------|---------------------------------------------------------------------------|
| <b>&lt;pool_name 12&gt;</b> | Specify the DHCP pool name.                                               |
| <b>broadcast</b>            | Specify the NetBIOS node type for Microsoft DHCP clients as broadcast.    |
| <b>peer_to_peer</b>         | Specify the NetBIOS node type for Microsoft DHCP clients as peer_to_peer. |
| <b>mixed</b>                | Specify the NetBIOS node type for Microsoft DHCP clients as mixed.        |
| <b>hybrid</b>               | Specify the NetBIOS node type for Microsoft DHCP clients as hybrid.       |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the NetBIOS node type:

## 23. DHCP Server Commands

```
Zxxx0:admin#config dhcp pool netbios_node_type knicks hybrid
Command: config dhcp pool netbios_node_type knicks hybrid

Success.

Zxxx0:admin#
```

### 23.11. config dhcp pool default\_router

#### ● Description

This command is used to specify the IP address of the default router for a DHCP client. Up to three IP addresses can be specified on one command line.

After a DHCP client has booted, the client begins sending packets to its default router. The IP address of the default router should be on the same subnet as the client. If the default router is not specified, the default router information will not be provided to the client. If this command is input twice for the same pool, the second command will overwrite the first command. The default router must be within the range the network defined for the DHCP pool.

#### ● Format

`config dhcp pool default_router <pool_name 12> {<ipaddr>} {<ipaddr>} {<ipaddr>}`

#### ● Parameters

---

**<pool\_name 12>**

Specify the DHCP pool name.

---

**<ipaddr>** (Optional) Specify the IP address of the default router. Up to three IP addresses can be specified on one command line.

---

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To configure the default router:

```
Zxxx0:admin#config dhcp pool default_router nyknicks 10.10.10.1
Command: config dhcp pool default_router nyknicks 10.10.10.1

Success.

Zxxx0:admin#
```

## 23.12. config dhcp pool lease

---

### ● Description

This command is used to specify the duration of the DHCP pool lease.

By default, each IP address assigned by a DHCP server comes with a one-day lease, which is the amount of time that the address is valid.

### ● Format

`config dhcp pool lease <pool_name 12> [<day 0-365> <hour 0-23> <minute 0-59> | infinite]`

### ● Parameters

---

**<pool\_name 12>**

Specify the DHCP pool's name.

---

**<day 0-365>**

Specify the number of days of the lease.

---

**<hour 0-23>**

Specify the number of hours of the lease.

---

**<minute 0-59>**

Specify the number of minutes of the lease.

---

**infinite** Specify a lease of unlimited duration.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the lease of a pool:

```
Zxxx0:admin#config dhcp pool lease nyknicks infinite
Command: config dhcp pool lease nyknicks infinite

Success.

Zxxx0:admin#
```

## 23.13. config dhcp pool boot\_file

---

### ● Description

This command is used to specify the name of the file that is used as a boot image. The boot file is used to store the boot image for the client. The boot image is generally the operating system the client uses to load. If this command is input twice for the same pool, the second command will overwrite the first command. If the bootfile is not specified, the boot file information will not be provided to the client.

### ● Format

config dhcp pool boot\_file <pool\_name 12> {<file\_name 64>}

### ● Parameters

---

<pool\_name 12>

Specify the DHCP pool name.

---

<file\_name 64>

(Optional) Specify the file name of the boot image.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the boot file:

```
Zxxx0:admin#config dhcp pool boot_file engineering boot.rom
Command: config dhcp pool boot_file engineering boot.rom

Success.

Zxxx0:admin#
```

## 23.14. config dhcp pool next\_server

---

### ● Description

This command is used by the F boot process, typically a TFTP server. If next server information is not specified, it will not be provided to the client. If this command is input twice for the same pool, the second command will overwrite the first command.

### ● Format

config dhcp pool next\_server <pool\_name 12> {<ipaddr>}

### ● Parameters

---

**<pool\_name 12>**

Specify the DHCP pool name.

---

**<ipaddr>**(Optional) Specify the IP address of the next server.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the next server:

```
Zxxx0:admin#config dhcp pool next_server engineering 192.168.0.1
Command: config dhcp pool next_server engineering 192.168.0.1

Success.

Zxxx0:admin#
```

## 23.15. config dhcp ping\_packets

---

### ● Description

This command is used to specify the number of ping packets the DHCP server sends to an IP address before assigning this address to a requesting client.

By default, the DHCP server pings a pool address twice before assigning the address to a DHCP client. If the ping is unanswered, the DHCP server assumes (with a high probability) that the address is not in use and assigns the address to the requesting client. If the ping is answered, the server will discard the current IP address and try another IP address.

### ● Format

**config dhcp ping\_packets <number 0-10>**

### ● Parameters

---

**<number 0-10>**

Specify the number of ping packets. 0 means there is no ping test. The default value is 2.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure ping packets:

## 23. DHCP Server Commands

```
Zxxx0:admin#config dhcp ping_packets 4
Command: config dhcp ping_packets 4

Success.

Zxxx0:admin#
```

### 23.16. config dhcp ping\_timeout

---

#### ● Description

This command is used to specify the amount of time the DHCP server must wait before timing out a ping packet.

By default, the DHCP server waits 100 milliseconds before timing out a ping packet.

#### ● Format

`config dhcp ping_timeout <millisecond 10-2000>`

#### ● Parameters

---

**<millisecond 10-2000>**

Specify the amount of time the DHCP server must wait before timing out a ping packet.  
The default value is 100.

---

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To configure the time out value for ping packets:

```
Zxxx0:admin#config dhcp ping_timeout 500
Command: config dhcp ping_timeout 500

Success.

Zxxx0:admin#
```

## 23.17. create dhcp pool manual\_binding

---

### ● Description

This command is used to specify the distinct identification of the client in dotted-hexadecimal notation or hardware address.

An address binding is a mapping between the IP address and MAC address of a client. The IP address of a client can be assigned manually by an administrator or assigned automatically from a pool by a DHCP server.

The IP address specified in the manual binding entry must be in a range within that the network uses for the DHCP pool. If the user specifies a conflict IP address, an error message will be returned. If a number of manual binding entries are created, and the network address for the pool is changed such that conflicts are generated, those manual binding entries which conflict with the new network address will be automatically deleted.

### ● Format

```
create dhcp pool manual_binding <pool_name 12> <ipaddr> hardware_address <macaddr>
{type [ethernet | ieee802]}
```

### ● Parameters

---

**<pool\_name 12>**

Specify the DHCP pool name.

---

**<ipaddr>** Specify the IP address which will be assigned to a specified client.

---

**hardware\_address**

Specify the hardware MAC address.

**<macaddr>**

Enter the MAC address here.

---

**type** (Optional) Specify the DHCP pool manual binding type.

**ethernet**

Specify Ethernet type.

**ieee802**

Specify IEEE802 type.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure manual bindings:



## 23. DHCP Server Commands

```
Zxxx0:admin#create dhcp pool manual_binding engineering 10.10.10.1  
hardware_address 00-80-C8-02-02-02 type ethernet  
Command: create dhcp pool manual_binding engineering 10.10.10.1 hardware_address  
00-80-C8-02-02-02 type ethernet
```

Success.

Zxxx0:admin#

### 23.18. delete dhcp pool manual\_binding

#### ● Description

This command is used to delete DHCP server manual binding.

#### ● Format

**delete dhcp pool manual\_binding <pool\_name 12> [<ipaddr> | all]**

#### ● Parameters

---

**<pool\_name 12>**

Specify the DHCP pool name.

---

**<ipaddr>** Specify the IP address which will be assigned to a specified client.

---

**all** Specify to delete all IP addresses.

---

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To delete DHCP server manual binding:

```
Zxxx0:admin#delete dhcp pool manual_binding engineering 10.10.10.1  
Command: delete dhcp pool manual_binding engineering 10.10.10.1
```

Success.

Zxxx0:admin#

## 23.19. clear dhcp binding

---

### ● Description

This command is used to clear a binding entry or all binding entries in a pool or clears all binding entries in all pools. Note that this command will not clear the dynamic binding entry which matches a manual binding entry.

### ● Format

**clear dhcp binding [<pool\_name 12> [<ipaddr> | all] | all]**

### ● Parameters

---

**<pool\_name 12>**

Specify the DHCP pool name to clear.

**<ipaddr>**

Specify the IP address to clear.

**all** Specify to clear all IP addresses for the specified pool.

---

**all** Specify to clear all binding entries in all pools

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To clear dynamic binding entries in the pool named "engineering":

```
Zxxx0:admin#clear dhcp binding engineering 10.20.3.4
Command: clear dhcp binding engineering 10.20.3.4

Success.

Zxxx0:admin#
```

## 23.20. show dhcp binding

---

### ● Description

This command is used to display dynamic binding entries.

### ● Format

**show dhcp binding {<pool\_name 12>}**

## 23. DHCP Server Commands

### ● Parameters

---

**<pool\_name 12>**

(Optional) Specify a DHCP pool name.

---

### ● Restrictions

None.

### ● Example

To display dynamic binding entries for "engineering":

```
Zxxx0:admin#show dhcp binding engineering
Command: show dhcp binding engineering
```

| Pool Name   | IP Addresss | Hardware Address  | Type     | Status    | Lifetime |
|-------------|-------------|-------------------|----------|-----------|----------|
| engineering | 192.168.0.1 | 00-80-C8-08-13-88 | Ethernet | Manual    | 86400    |
| engineering | 192.168.0.2 | 00-80-C8-08-13-99 | Ethernet | Automatic | 86400    |
| engineering | 192.168.0.3 | 00-80-C8-08-13-A0 | Ethernet | Automatic | 86400    |
| engineering | 192.168.0.4 | 00-80-C8-08-13-B0 | Ethernet | Automatic | 86400    |

```
Total Entries: 4

Zxxx0:admin#
```

## 23.21. show dhcp pool

---

### ● Description

This command is used to display the information for DHCP pool. If pool name is not specified, information for all pools will be displayed.

### ● Format

**show dhcp pool {<pool\_name 12>}**

### ● Parameters

---

**<pool\_name 12>**

(Optional) Specify the DHCP pool name.

---

### ● Restrictions

None.

### ● Example

To display the current DHCP pool information for "engineering":

```

Zxxx0:admin#show dhcp pool engineering
Command: show dhcp pool engineering

Pool Name       : engineering
Network Address : 10.10.10.0/24
Domain Name     : manager.com
DNS Server      : 10.10.10.1
NetBIOS Name Server : 10.10.10.1
NetBIOS Node Type : Broadcast
Default Router  : 10.10.10.1
Pool Lease      : 10 Days, 0 Hours, 0 Minutes
Boot File       : boot.bin
Next Server     : 10.10.10.2

Zxxx0:admin#

```

## 23.22. show dhcp pool manual\_binding

### ● Description

This command is used to display the configured manual binding entries.

### ● Format

**show dhcp pool manual\_binding {<pool\_name 12>}**

### ● Parameters

---

**<pool\_name 12>**  
(Optional) Specify the DHCP pool name.

---

### ● Restrictions

None.

### ● Example

To display the configured manual binding entries:

```

Zxxx0:admin#show dhcp pool manual_binding
Command: show dhcp pool manual_binding

Pool Name      IP Address      Hardware Address  Type
-----
p1             192.168.0.1     00-80-C8-08-13-88 Ethernet
p1             192.168.0.2     00-80-C8-08-13-99 Ethernet

Total Entries : 2

Zxxx0:admin#

```

## 23.23. enable dhcp\_server

---

### ● Description

This command is used to enable the DHCP server function.

If DHCP relay is enabled, DHCP server cannot be enabled. The opposite is also true. For Layer 2 Switching Hubs, if DHCP client is enabled on the only interface, then DHCP server cannot be enabled. For layer 3 Switching Hubs, when the System interface is the only interface then can DHCP client be enabled. If the DHCP client is enabled, then the DHCP server cannot be enabled.

### ● Format

`enable dhcp_server`

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable DHCP server:

```
Zxxx0:admin#enable dhcp_server
Command: enable dhcp_server

Success.

Zxxx0:admin#
```

## 23.24. disable dhcp\_server

---

### ● Description

This command is used to disable the DHCP server function on the Switching Hub.

### ● Format

`disable dhcp_server`

### ● Parameters

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To disable the Switch's DHCP server:

```
Zxxx0:admin#disable dhcp_server
Command: disable dhcp_server

Success.

Zxxx0:admin#
```

## 23.25. show dhcp\_server

---

- **Description**

This command is used to display the current DHCP server configuration.

- **Format**

show dhcp\_server

- **Parameters**

None.

- **Restrictions**

None.

- **Example**

To display the DHCP server status:

```
Zxxx0:admin#show dhcp_server
Command: show dhcp_server

  DHCP Server Global State: Disabled
  Ping Packet Number       : 2
  Ping Timeout             : 100 ms

Zxxx0:admin#
```

## 23.26. clear dhcp conflict\_ip

---

### ● Description

This command is used to clear an entry or all entries from the conflict IP database.

### ● Format

clear dhcp conflict\_ip [<ipaddr> | all]

### ● Parameters

---

|          |                                                |
|----------|------------------------------------------------|
| <ipaddr> | Specify the IP address to be cleared.          |
| all      | Specify that all IP addresses will be cleared. |

---

### ● Restrictions

None.

### ● Example

To clear an IP address 10.20.3.4 from the conflict database:

```
Zxxx0:admin#clear dhcp conflict_ip 10.20.3.4
Command: clear dhcp conflict_ip 10.20.3.4

Success.

Zxxx0:admin#
```

## 23.27. show dhcp conflict\_ip

---

### ● Description

This command is used to display the IP address that has been identified as being in conflict. The DHCP server will use ping packet to determine whether an IP address is conflicting with other hosts before binding this IP. The IP address which has been identified in conflict will be moved to the conflict IP database. The system will not attempt to bind the IP address in the conflict IP database unless the user clears it from the conflict IP database.

### ● Format

show dhcp conflict\_ip {<ipaddr>}

### ● Parameters

---

|          |                                         |
|----------|-----------------------------------------|
| <ipaddr> | Specify the IP address to be displayed. |
|----------|-----------------------------------------|

---

- **Restrictions**

None.

- **Example**

To display the entries in the DHCP conflict IP database:

```
Zxxx0:admin#show dhcp conflict_ip
Command: show dhcp conflict_ip

  IP Address      Detection Method  Detection Time
  -----
172.16.1.32      Ping             2007/08/30 17:06:59
172.16.1.32      Gratuitous ARP   2007/09/10 19:38:01

Zxxx0:admin#
```



## 24. DHCP Snooping Commands

The commands are used to allow only clients with a regular IP address assigned by the DHCP server to communicate.

When this function is enabled, all ports are set to "untrusted." You need to change the DHCP server and DHCP relay ports to "trusted." In communications from clients connected on "untrusted" ports, only DHCP packets are authenticated first and other packets are discarded. The Switching Hub monitors communications with the DHCP server on a "trusted" port and stores a mapping between assigned IP addresses and MAC addresses in the Binding Table in the Switching Hub.

Only clients with an IP address and MAC address stored in the Binding Table are authorized for normal communication.

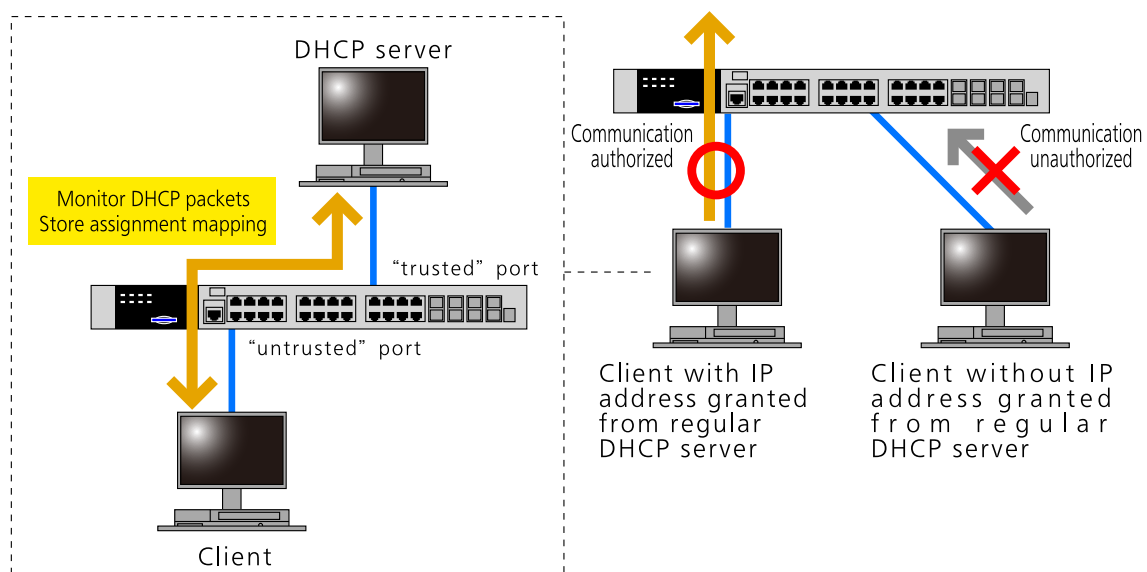


Figure 24-1

```
enable dhcp_snoop
disable dhcp_snoop
show dhcp_snoop
show dhcp_snoop binding_entry { [ port <port> | vlan <vlan_name 32> | vlanid <vidlist> |
ipaddress <ipaddr> | mac_address <macaddr> ] }
```

## 24.1. enable dhcp\_snoop

---

### ● Description

This command is used to enable DHCP snooping operation on the Switching Hub. This is a global control for the DHCP snooping function. By default, the DHCP snooping function is disabled.

### ● Format

`enable dhcp_snoop`

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable the DHCP snooping function globally:

```
Zxxx0:admin# enable dhcp_snoop
Command: enable dhcp_snoop

Success.

Zxxx0:admin#
```

### 24.2. **disable dhcp\_snoop**

---

#### ● Description

This command is used to disable DHCP snooping operation on the Switching Hub. This command disables the DHCP snooping function. By default, the DHCP snooping function is disabled.

#### ● Format

**disable dhcp\_snoop**

#### ● Parameters

None.

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To disable the DHCP snooping function globally:

```
Zxxx0:admin# disable dhcp_snoop
Command: disable dhcp_snoop

Success.

Zxxx0:admin#
```

## 24.3. show dhcp\_snoop

---

- **Description**

This command is used to display the DHCP snooping configuration status.

- **Format**

show dhcp\_snoop

- **Parameters**

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To display the DHCP snooping configuration status:

```
Zxxx0:admin# show dhcp_snoop
Command: show dhcp_snoop

DHCP Snooping Status : Enabled

Zxxx0:admin#
```

## 24.4. show dhcp\_snoop binding\_entry

### ● Description

The show dhcp\_snoop binding command displays the DHCP snooping binding table information.

### ● Format

show dhcp\_snoop binding\_entry { [ port <port> | vlan <vlan\_name 32> | vlanid <vidlist> | ipaddress <ipaddr> | mac\_address <macaddr> ] }

### ● Parameters

---

<port> Displays the entries for one port.

---

<vlan\_name>  
Displays the entries for a specific VLAN.

---

<vlanid> Display the entries for the VLANs indicated by VID list.

---

<ipaddress>  
Displays the entries for a specific IP address.

---

<mac\_address>  
Displays the entries for a specific MAC address.

---

If no parameter is specified, system will display the whole DHCP snooping binding table.

### ● Restrictions

Only Administrator, Operator, Power-User level users and users can issue this command.

### ● Example

To display the DHCP snooping binding table:

```
Zxxx0:admin# admin# show dhcp_snoop binding
Command: show dhcp_snoop binding
```

| Port | VID | IP Address | MAC Address       | Lease Time |
|------|-----|------------|-------------------|------------|
| 1    | 2   | 10.0.0.1   | 00-00-00-00-00-01 | 00:23:59   |
| 1    | 2   | 10.0.0.4   | 00-00-00-00-00-02 | 00:23:59   |
| 1    | 2   | 10.0.0.5   | 00-00-00-00-00-03 | 00:23:59   |
| 1    | 2   | 10.0.0.6   | 00-00-00-00-00-04 | 00:23:59   |
| 1    | 2   | 10.0.0.7   | 00-00-00-00-00-05 | 00:23:59   |
| 1    | 2   | 10.0.0.8   | 00-00-00-00-00-06 | 00:23:59   |
| 1    | 2   | 10.0.0.9   | 00-00-00-00-00-07 | 00:23:59   |

```

Total Entries : 7

Zxxx0:admin#
```

---

## 25. DHCPv6 Relay Command List

---

This is a DHCP Relay function for IPv6. This function is used to configure a DHCPv6 server address on the relay destination for each interface.

---

```
enable dhcpv6_relay
disable dhcpv6_relay
config dhcpv6_relay hop_count <value 1-32>
config dhcpv6_relay [add | delete] ipif <ipif_name 12> <ipv6addr>
config dhcpv6_relay ipif [<ipif_name 12> | all] state [enable | disable]
show dhcpv6_relay {ipif <ipif_name 12>}
```

---

### 25.1. enable dhcpv6\_relay

---

#### ● Description

This command is used to enable the DHCPv6 relay function on the Switch.

#### ● Format

```
enable dhcpv6_relay
```

#### ● Parameters

None.

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To configure the DHCPv6 relay global state to enable:

```
Zxxx0:admin# enable dhcpv6_relay
Command: enable dhcpv6_relay

Success.

Zxxx0:admin#
```

## 25.2. disable dhcpv6\_relay

---

### ● Description

This command is used to disable the DHCPv6 relay function on the Switch.

### ● Format

disable dhcpv6\_relay

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the DHCPv6 relay global state to disable:

```
Zxxx0:admin# disable dhcpv6_relay
Command: disable dhcpv6_relay

Success.

Zxxx0:admin#
```

## 25.3. config dhcpv6\_relay hop\_count

---

### ● Description

Configure the DHCPv6 relay hop\_count of the Switching Hub.

### ● Format

config dhcpv6\_relay hop\_count <value 1-32>

### ● Parameters

---

hop\_count

Specifies the number of relay agents that have relayed this message. The default value is 4.

<value 1-32>

Enter the hop count number here. This value must be between 1 and 32.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure the maximum hops of a DHCPv6 relay packet could be transferred to 4:

```
Zxxx0:admin# config dhcpv6_relay hop_count 4
Command: config dhcpv6_relay hop_count 4

Success.

Zxxx0:admin#
```

# 25.4. config dhcpv6\_relay

## ● Description

The command could add/delete an IPv6 address which is a destination to forward (relay) DHCPv6 packets.

## ● Format

**config dhcpv6\_relay [add | delete] ipif <ipif\_name 12> <ipv6addr>**

## ● Parameters

|                         |                                                                                                                                                                                     |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>add</b>              | Add an IPv6 destination to the DHCPv6 relay table.                                                                                                                                  |
| <b>delete</b>           | Delete an IPv6 destination from the DHCPv6 relay table                                                                                                                              |
| <b>ipif</b>             | The name of the IP interface in which DHCPv6 relay is to be enabled.<br><b>&lt;ipif_name 12&gt;</b><br>Enter the IP interface name here. This name can be up to 12 characters long. |
| <b>&lt;ipv6addr&gt;</b> | The DHCPv6 server IP address.                                                                                                                                                       |

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To add a DHCPv6 server to the relay table:

```
Zxxx0:admin# config dhcpv6_relay add ipif System
2001:DB8:1234:0:218:FEFF:FEFB:CC0E
Command: config dhcpv6_relay add ipif System 2001:DB8:1234:0:218:FEFF:FEFB:CC0E

Success.

Zxxx0:admin#
```



## 25.5. config dhcpv6\_relay ipif

---

### ● Description

The command is used to configure the DHCPv6 relay state of one specific interface or all interfaces.

### ● Format

**config dhcpv6\_relay ipif [<ipif\_name 12> | all] state [enable | disable]**

### ● Parameters

|                |                                                                                                                                                             |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b>    | Specifies the name of the IP interface.<br><b>&lt;ipif_name 12&gt;</b><br>Enter the IP interface name used here. This name can be up to 12 characters long. |
| <b>all</b>     | Specifies that all the configured IP interfaces will be used.                                                                                               |
| <b>state</b>   | Specifies if the DHCPv6 relay state will be enabled or disabled.                                                                                            |
| <b>enable</b>  | Choose this parameter to enable the DHCPv6 relay state of the interface.                                                                                    |
| <b>disable</b> | Choose this parameter to disable the DHCPv6 relay state of the interface.                                                                                   |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the DHCPv6 relay state of the System interface to enable:

```
Zxxx0:admin# config dhcpv6_relay ipif System state enable
Command: config dhcpv6_relay ipif System state enable

Success.

Zxxx0:admin#
```

## 25.6. show dhcpv6\_relay

---

### ● Description

This command will display the current DHCPv6 relay configuration of all interfaces, or if an IP interface name is specified, the DHCPv6 relay configuration for that IP interface.

### ● Format

**show dhcpv6\_relay {ipif <ipif\_name 12>}**

### ● Parameters

---

|             |                                                                                                                                     |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b> | (Optional) The name of the IP interface for which to display the current DHCPv6 relay configuration.<br><b>&lt;ipif_name 12&gt;</b> |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------|

---

Enter the IP interface name used here. This name can be up to 12 characters long.

---

If no IP interface is specified, all configured DHCPv6 relay interfaces are displayed.

### ● Restrictions

None.

### ● Example

To show the DHCPv6 relay configuration of all interfaces:

```
Zxxx0:admin# show dhcpv6_relay
Command: show dhcpv6_relay

DHCPv6 Relay Global State : Disabled
DHCPv6 Hops Count Limit   : 4
-----
IP Interface               : n81
DHCPv6 Relay Status       : Enabled
Server Address             :

IP Interface               : n90
DHCPv6 Relay Status       : Enabled
Server Address             :

IP Interface               : n1000
DHCPv6 Relay Status       : Enabled
Server Address             :

Total Entries : 3

Zxxx0:admin#
```

To show the DHCPv6 relay configuration of System interface:

## 25. DHCPv6 Relay Command List

```
Zxxx0:admin# show dhcpv6_relay ipif System
Command: show dhcpv6_relay ipif System

DHCPv6 Relay Global State : Disabled
DHCPv6 Hops Count Limit   : 4
-----
IP Interface               : System
DHCPv6 Relay Status        : Enabled
Server Address             : 2001:DB8:1234::218:FEFF:FEFB:CC0E
Server Address             : 3000:90:1::6

Zxxx0:admin#
```

## 26. DHCPv6 Server Commands

The commands are used to configure this Switching Hub as a DHCP server for IPv6.

```
create dhcpv6 pool <pool_name 12>
delete dhcpv6 pool [<pool_name 12> | all]
show dhcpv6 pool {<pool_name 12>}
config dhcpv6 pool ipv6network_addr <pool_name 12> begin <ipv6networkaddr> end
    <ipv6networkaddr>
config dhcpv6 pool domain_name <pool_name 12> <domain_name 255>
config dhcpv6 pool dns_server <pool_name 12> <ipv6addr> {<ipv6addr>}
config dhcpv6 pool lifetime <pool_name 12> preferred_lifetime <sec 60-4294967295>
    valid_lifetime <sec 60-4294967295>
config dhcpv6 pool manual_binding <pool_name 12> [add <ipv6addr> client_duid <string 28> |
    delete [<ipv6addr> | all]]
show dhcpv6 manual_binding {<pool_name 12>}
show dhcpv6 binding {<pool_name 12>}
clear dhcpv6 binding {<pool_name 12>}
enable dhcpv6_server
disable dhcpv6_server
show dhcpv6_server {ipif <ipif_name 12>}
config dhcpv6 pool excluded_address <pool_name 12> [add begin <ipv6addr> end <ipv6addr> |
    delete [begin <ipv6addr> end <ipv6addr> | all]]
show dhcpv6 excluded_address {<pool_name 12>}
config dhcpv6_server ipif [<ipif_name 12> | all] state [enable | disable]
```

### 26.1. create dhcpv6 pool

#### ● Description

This command is used to create a DHCPv6 pool for the DHCPv6 server.

#### ● Format

```
create dhcpv6 pool <pool_name 12>
```

#### ● Parameters

|             |                                                                                                                                               |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>pool</b> | Specifies the pool to be created with this command.<br><pool_name 12><br>Enter the pool name here. This name can be up to 12 characters long. |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------|

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## 26. DHCPv6 Server Commands

### ● Example

To create a DHCPv6 pool pool1:

```
Zxxx0:admin# create dhcpv6 pool pool1
Command : create dhcpv6 pool pool1

success

Zxxx0:admin#
```

## 26.2. delete dhcpv6 pool

---

### ● Description

This command is used to delete one or all DHCPv6 pools.

### ● Format

**delete dhcpv6 pool [<pool\_name 12> | all]**

### ● Parameters

---

|             |                                                                                                                                                                      |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>pool</b> | Specifies the DHCPv6 pool to be removed.<br><b>&lt;pool_name 12&gt;</b><br>Enter the DHCPv6 pool name to be removed here. This name can be up to 12 characters long. |
| <b>all</b>  | Specifies that all the DHCPv6 pools will be removed.                                                                                                                 |

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete the DHCPv6 pool by specifying the pool name pool1:

```
Zxxx0:admin# delete dhcpv6 pool pool1
Command: delete dhcpv6 pool pool1

Success.

Zxxx0:admin#
```

## 26.3. show dhcpv6 pool

---

### ● Description

This command is used to display one or all DHCPv6 pools configuration.

### ● Format

**show dhcpv6 pool {<pool\_name 12>}**

### ● Parameters

---

|             |                                                                                                                                                                                     |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>pool</b> | Specifies the DHCPv6 pool to be displayed.<br><b>&lt;pool_name 12&gt;</b><br>(Optional) Enter the DHCPv6 pool name to be displayed here. This name can be up to 12 characters long. |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

If no parameters are specified, all the DHCPv6 pools will be displayed.

### ● Restrictions

None.

### ● Example

To show the DHCPv6 pool by specifying the pool name pool1:

```
Zxxx0:admin# show dhcpv6 pool pool1
Command: show dhcpv6 pool pool1

Pool Name           : pool1
Begin Network Address : 2000::1/64
End Network Address  : 2000::200/64
Domain Name          : domain.com
DNS Server Address   : 2000::ff
                     : 2000::fe
Preferred Lifetime    : 604800 (sec)
Valid Lifetime        : 2592000 (sec)

Total Pool Entry: 1

Zxxx0:admin#
```

## 26.4. **config dhcpv6 pool ipv6network\_addr**

### ● Description

This command is used to configure the range of IPv6 network addresses for the DHCPv6 pool. The IPv6 addresses in the range are free to be assigned to any DHCPv6 client. When the DHCPv6 server receives a request from the client, the server will automatically find an available pool to allocate an IPv6 address.

The `begin_networkaddr` and `end_networkaddr` must observe some rules as followed:

The prefix of the `begin_networkaddr` and `end_networkaddr` are not consistent, otherwise, the Switching Hub will print an error message: The prefix of `begin_networkaddr` and `end_networkaddr` must be consistent. (e.g.: the `begin_networkaddr` is 2000::1/64, and the `end_networkaddr` is 3000::100/64)

The begin address must not be larger than end address, otherwise, the Switching Hub will print an error message: The begin IPv6 address must be lower than or equal to the end IPv6 address. (e.g.: the `begin_networkaddr` is 2000::200/64, and the `end_networkaddr` is 2000::100/64)

There must not be intersection between the IPv6 address ranges of two pools, otherwise, the Switch will print an error message: IPv6network address collision. (e.g.: pool1: 2000::1/64 — 2000::100/64, pool2: 2000::50/64 — 2000::200/64)

The IPv6 network address can't be Link-local address and Multicast address, otherwise, the Switch will print an error message: "The IPv6 network address can't be Link-local address or Multicast address. " (e.g.: pool1: FE80::1/64 — FE80::100/64, pool2: FE80::200/64 — FE80::300/64)

### ● Format

```
config dhcpv6 pool ipv6network_addr <pool_name 12> begin <ipv6networkaddr> end
<ipv6networkaddr>
```

### ● Parameters

|                             |                                                                                                                                                                         |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;pool_name 12&gt;</b> | Enter the DHCPv6 pool name used here. This name can be up to 12 characters long.                                                                                        |
| <b>begin</b>                | Specifies the beginning IPv6 network address of the DHCPv6 pool.<br><b>&lt;ipv6networkaddr&gt;</b><br>Enter the beginning IPv6 network address of the DHCPv6 pool here. |
| <b>end</b>                  | Specifies the ending IPv6 network address of the DHCPv6 pool.<br><b>&lt;ipv6networkaddr&gt;</b><br>Enter the ending IPv6 network address of the DHCPv6 pool here.       |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the range of ipv6network address for the DHCPv6 pool pool1:

```
Zxxx0:admin# config dhcpv6 pool ipv6network_addr pool1 begin 2000::1/64 end
2000::32/64
Command: config dhcpv6 pool ipv6network_addr pool1 begin 2000::1/64 end 2000::32/64

success

Zxxx0:admin#
```

## 26.5. config dhcpv6 pool domain\_name

### ● Description

This command is used to configure the domain name for the DHCPv6 pool of the Switch. The domain name configured here will be used as the default domain name by the client.

By default, the domain name is empty. If domain name is empty, the domain name information will not be provided to the client.

### ● Format

config dhcpv6 pool domain\_name <pool\_name 12> <domain\_name 255>

### ● Parameters

---

<pool\_name 12>

Enter the DHCPv6 pool name used here. This name can be up to 12 characters long.

---

<domain\_name 255>

Enter the domain name used here. This name can be up to 255 characters long.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the domain name for the DHCPv6 pool pool1:

```
Zxxx0:admin# config dhcpv6 pool domain_name pool1 manager.com
Command: config dhcpv6 pool domain_name pool1 manager.com

Success.

Zxxx0:admin#
```



## 26.6. config dhcpv6 pool dns\_server

---

### ● Description

This command is used to configure the DNS server's IPv6 addresses for a specific DHCPv6 pool. Users may add up to two DNS Server addresses. If DNS server is not specified, the DNS server information will not be provided to the client. Users could delete a DNS server address in the method of setting the DNS server address to zero.

### ● Format

**config dhcpv6 pool dns\_server <pool\_name 12> <ipv6addr> {<ipv6addr>}**

### ● Parameters

---

**<pool\_name 12>**

Enter the DHCPv6 pool name used here. This name can be up to 12 characters long.

---

**<ipv6addr>**

Enter the primary DNS Server IPv6 address used for this pool here.

---

**<ipv6addr>**

(Optional) Enter the secondary DNS Server IPv6 address used for this pool here.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the DNS server address for a DHCPv6 pool:

```
Zxxx0:admin# config dhcpv6 pool dns_server pool1 2000::200 2000::201
Command: config dhcpv6 pool dns_server pool1 2000::200 2000::201

Success.

Zxxx0:admin#
```

## 26.7. config dhcpv6 pool lifetime

---

### ● Description

This command is used to configure the preferred-lifetime and valid-lifetime of IPv6 address within a DHCPv6 pool.

**Preferred lifetime** - the length of time that a valid address is preferred (i.e., the time until deprecation). When the preferred lifetime expires, the address becomes deprecated.

**Valid lifetime** - the length of time an address remains in the valid state (i.e., the time until invalidation). When the valid lifetime expires, the address becomes invalid.

The valid lifetime must be greater than or equal to the preferred lifetime.

### ● Format

```
config dhcpv6 pool lifetime <pool_name 12> preferred_lifetime <sec 60-4294967295>
valid_lifetime <sec 60-4294967295>
```

### ● Parameters

---

**<pool\_name 12>**

Enter the DHCPv6 pool name used here. This name can be up to 12 characters long.

---

**preferred\_lifetime**

Specifies the length of time that a valid address is preferred to.

**<sec 60-4294967295>**

Enter the preferred lifetime value here. This value must be between 60 and 4294967295 seconds.

---

**valid\_lifetime**

Specifies the length of time an address remains in the valid state.

**<sec 60-4294967295>**

Enter the valid lifetime value here. This value must be between 60 and 4294967295 seconds.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the preferred-lifetime and valid-lifetime for the DHCPv6 pool:

```
Zxxx0:admin# config dhcpv6 pool lifetime pool1 preferred_lifetime 80 valid_lifetime
100
Command: config dhcpv6 pool lifetime pool1 preferred_lifetime 80 valid_lifetime 100

Success.

Zxxx0:admin#
```

## 26.8. config dhcpv6 pool manual\_binding

### ● Description

This command is used to configure a DHCPv6 pool manual binding entry. An address binding is a mapping between the IPv6 address and DUID (A DHCPv6 Unique Identifier for a DHCPv6 participant) of a client. The IPv6 address specified in the manual binding entry must be in the range of the DHCPv6 pool.

### ● Format

**config dhcpv6 pool manual\_binding <pool\_name 12> [add <ipv6addr> client\_duid <string 28> | delete [<ipv6addr> | all]]**

### ● Parameters

|                             |                                                                                                                   |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>&lt;pool_name 12&gt;</b> | Enter the DHCPv6 pool name used here. This name can be up to 12 characters long.                                  |
| <b>add</b>                  | Specifies the IPv6 address that will statically be bound to a device.                                             |
| <b>&lt;ipv6addr&gt;</b>     | Enter the IPv6 address used for the static bind here.                                                             |
| <b>client_duid</b>          | Specifies the DUID of the device that will statically be bound to the IPv6 address entered in the previous field. |
| <b>&lt;string 28&gt;</b>    | Enter the client DUID used here. This string can be up to 28 characters long.                                     |
| <b>delete</b>               | Specifies to delete the manual binding entry.                                                                     |
| <b>&lt;ipv6addr&gt;</b>     | Enter the IPv6 address of the manual binding entry to be deleted here.                                            |
| <b>all</b>                  | Specifies that all manual binding entries will be deleted.                                                        |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To add a manual binding DHCPv6 entry:

```
Zxxx0:admin# config dhcpv6 pool manual_binding pool1 add 2000::3 client_duid
00010006124dd5840021918d4d9f
Command: config dhcpv6 pool manual_binding pool1 add 2000::3 client_duid
00010006124dd5840021918d4d9f

success

Zxxx0:admin#
```

## 26.9. show dhcpv6 manual\_binding

---

### ● Description

This command will display the manual binding entries for the selected or all DHCPv6 pools.

### ● Format

**show dhcpv6 manual\_binding {<pool\_name 12>}**

### ● Parameters

---

**<pool\_name 12>**

(Optional) Enter the DHCPv6 pool name used here. This name can be up to 12 characters long.

---

If no parameter is specified, then all the entries will be displayed.

### ● Restrictions

None.

### ● Example

To display the manual binding entries of the DHCPv6 pool:

```
Zxxx0:admin# show dhcpv6 manual_binding
Command: show dhcpv6 manual_binding

Pool Name :net100
Entry 1
  IPv6 Address: 3000:100:1::ABCD
  DUID          : 00030006001572200700

Pool Name :net91
Entry 1
  IPv6 Address: 3000:91:1::100
  DUID          : 00030006aabbcc000000

Entry 2
  IPv6 Address: 3000:91:1::101
  DUID          : 00030006aabbcc000001

Total Entries: 3

Zxxx0:admin#
```

## 26.10. show dhcpv6 binding

---

### ● Description

This command is used to show the DHCPv6 dynamic binding information. Entering the command without the pool name will display all information regarding DHCPv6 dynamic binding on the Switching Hub. This command only displays the dynamic binding information, not including manual binding information.

### ● Format

**show dhcpv6 binding {<pool\_name 12>}**

### ● Parameters

---

**<pool\_name 12>**

(Optional) Enter the DHCPv6 pool name used here. This name can be up to 12 characters long.

---

### ● Restrictions

None.

### ● Example

To display the DHCPv6 dynamic binding information on the Switch:

```
Zxxx0:admin# show dhcpv6 binding
Command: show dhcpv6 binding

Pool Name: net90          IPv6 Address: 3000:90:1::7
                        DUID       : 0003000600cd14517000
                        Preferred(s): 120           Valid(s): 240

Pool Name: net100-2       IPv6 Address: 3000:100:1::1
                        DUID       : 00030006001572200300
                        Preferred(s): 120           Valid(s): 240

Total Entries : 2

Zxxx0:admin#
```

## 26.11. clear dhcpv6 binding

---

### ● Description

This command is used to clear the DHCPv6 dynamic binding information.

### ● Format

clear dhcpv6 binding {<pool\_name 12>}

### ● Parameters

---

<pool\_name 12>

(Optional) Enter the DHCPv6 pool name used here. This name can be up to 12 characters long.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To clear the DHCPv6 dynamic binding information on the Switch:

```
Zxxx0:admin# clear dhcpv6 binding
Command: clear dhcpv6 binding

Success.

Zxxx0:admin#
```

## 26.12. enable dhcpv6\_server

---

### ● Description

This command is used to enable the DHCPv6 server function on the Switch

### ● Format

enable dhcpv6\_server

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## 26. DHCPv6 Server Commands

### ● Example

To configure the DHCPv6 server global state to enable:

```
Zxxx0:admin# enable dhcpv6_server
Command: enable dhcpv6_server

Success.

Zxxx0:admin#
```

## 26.13. disable dhcpv6\_server

---

### ● Description

This command is used to disable the DHCPv6 server function on the Switch

### ● Format

**disable dhcpv6\_server**

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the DHCPv6 server global state to disable:

```
Zxxx0:admin# disable dhcpv6_server
Command: disable dhcpv6_server

Success.

Zxxx0:admin#
```

## 26.14. show dhcpv6\_server

---

### ● Description

This command is used to display the DHCPv6 server setting.

### ● Format

**show dhcpv6\_server {ipif <ipif\_name 12>}**

### ● Parameters

---

|             |                                                                                                                                                                                            |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b> | (Optional) Specifies the IP interface name to be displayed.<br><b>&lt;ipif_name 12&gt;</b><br>Enter the IP interface name to be displayed here. This name can be up to 12 characters long. |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### ● Restrictions

None.

### ● Example

To display the DHCPv6 server setting:

```
Zxxx0:admin# show dhcpv6_server
Command: show dhcpv6_server

DHCPv6 Server Global State: Disabled
-----
IP Interface           : System
DHCPv6 Server State    : Enabled

IP Interface           : ipif1
DHCPv6 Server State    : Enabled

Total Entries          : 2

Zxxx0:admin#
```



## 26.15. config dhcpv6 pool excluded\_address

### ● Description

This command is used to configure the reserved IPv6 addresses on the DHCPv6 server.

### ● Format

**config dhcpv6 pool excluded\_address <pool\_name 12> [add begin <ipv6addr> end <ipv6addr> | delete [begin <ipv6addr> end <ipv6addr> | all]]**

### ● Parameters

|                             |                                                                                                                                                                                    |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;pool_name 12&gt;</b> | Enter the DHCPv6 pool name used here. This name can be up to 12 characters long.                                                                                                   |
| <b>add</b>                  | Specifies to add an excluded address range for a specified pool.                                                                                                                   |
| <b>begin</b>                | Specifies the beginning IPv6 address of the range of IPv6 addresses to be excluded from the DHCPv6 pool.<br><b>&lt;ipv6addr&gt;</b><br>Enter the beginning IPv6 address used here. |
| <b>end</b>                  | Specifies the ending IPv6 address of the range of IPv6 addresses to be excluded from the DHCPv6 pool.<br><b>&lt;ipv6addr&gt;</b><br>Enter the ending IPv6 address used here.       |
| <b>delete</b>               | Specifies to delete one or all excluded address ranges of a specified pool.                                                                                                        |
| <b>begin</b>                | Specifies the beginning IPv6 address of the range of IPv6 addresses to be excluded from the DHCPv6 pool.<br><b>&lt;ipv6addr&gt;</b><br>Enter the beginning IPv6 address used here. |
| <b>end</b>                  | Specifies the ending IPv6 address of the range of IPv6 addresses to be excluded from the DHCPv6 pool.<br><b>&lt;ipv6addr&gt;</b><br>Enter the ending IPv6 address used here.       |
| <b>all</b>                  | Specifies to delete all excluded address ranges of a specified pool.                                                                                                               |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To add the IPv6 addresses range that DHCPv6 server should not assign to clients:

```
Zxxx0:admin# config dhcpv6 pool excluded_address pool1 add begin 2000::3 end 2000::8
Command: config dhcpv6 pool excluded_address pool1 add begin 2000::3 end 2000::8

Success.

Zxxx0:admin#
```

## 26.16. show dhcpv6 excluded\_address

---

### ● Description

This command is used to display the groups of IPv6 addresses which are excluded from the legal assigned IPv6 address

### ● Format

**show dhcpv6 excluded\_address {<pool\_name 12>}**

### ● Parameters

---

**<pool\_name 12>**

(Optional) Enter the DHCPv6 pool name used here. This name can be up to 12 characters long.

---

### ● Restrictions

None.

### ● Example

To display the excluded address information:

```
Zxxx0:admin# show dhcpv6 excluded_address
Command: show dhcpv6 excluded_address
```

```
Pool Name: net100
```

```
Range 1
```

```
Begin Address: 3000:100:1::1
```

```
End Address : 3000:100:1::7
```

```
Pool Name: net110
```

```
Range 1
```

```
Begin Address: 3000:110:1::1
```

```
End Address : 3000:110:1::7
```

```
Range 2
```

```
Begin Address: 3000:110:1::9
```

```
End Address : 3000:110:1::9
```

```
Range 3
```

```
Begin Address: 3000:110:1::11
```

```
End Address : 3000:110:1::11
```

```
Range 4
```

```
Begin Address: 3000:110:1::13
```

```
End Address : 3000:110:1::13
```

```
Total Entries : 5
```

```
Zxxx0:admin#
```

## 26.17. config dhcpv6\_server ipif

---

### ● Description

This command is used to configure the DHCPv6 Server state per interface.

### ● Format

**config dhcpv6\_server ipif** [<ipif\_name 12> | all] **state** [enable | disable]

### ● Parameters

|                |                                                                                                                                                 |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b>    | Specifies the IP interface used.<br><b>&lt;ipif_name 12&gt;</b><br>Enter the IP interface name used. This name can be up to 12 characters long. |
| <b>all</b>     | Specifies that all the IP interfaces will be used.                                                                                              |
| <b>state</b>   | Specifies the DHCPv6 server state for the specified interface.                                                                                  |
| <b>enable</b>  | Specifies that the DHCPv6 server state for the specified interface will be enabled.                                                             |
| <b>disable</b> | Specifies that the DHCPv6 server state for the specified interface will be disabled.                                                            |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the DHCPv6 Server state of System Interface to enable:

```
Zxxx0:admin# config dhcpv6_server ipif System state enable
Command: config dhcpv6_server ipif System state enable

Success.

Zxxx0:admin#
```

## 27.Distance Vector Multicast Routing Protocol (DVMRP) Commands

Sending data simultaneously to multiple destinations is called "multicast" and used for music and video distribution.

DVMRP (Distance Vector Multicast Routing Protocol) is one of multicast routing protocols. It exchanges route information from the distribution source to the distribution destination with adjacent routers and manages the shortest route in a routing table like RIP.

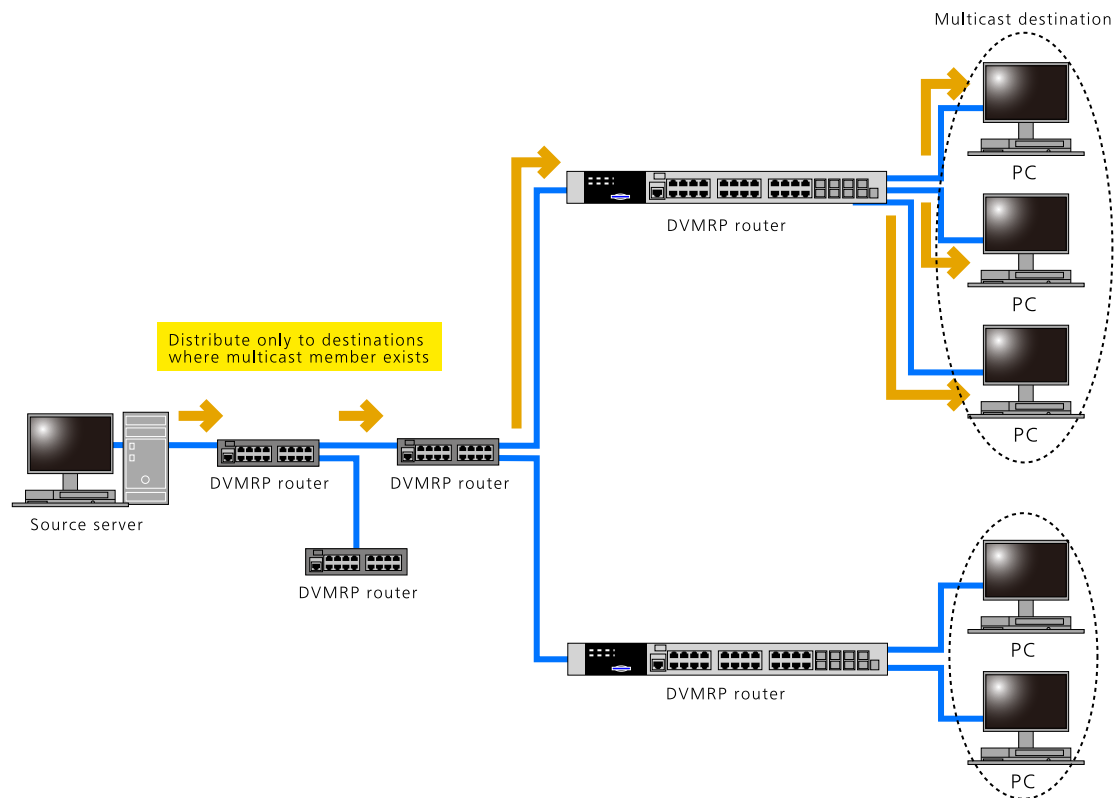


Figure 27-1 DVMRP routing

This Switching Hub supports DVMRP version 3 and enables/disables DVMRP for each interface.

DVMRP does not always have a fast transmission speed. Therefore, it is used in a relatively low-bandwidth network where some delay is not a problem. If a high transmission speed is required, consider using other multicast routing protocols such as PIM (Protocol Independent Multicast routing).

## 27. Distance Vector Multicast Routing Protocol (DVMRP) Commands

---

```
config dvmrp [ipif <ipif_name 12> | all] {metric <value 1-31> | probe <sec 1-65535> |  
    neighbor_timeout <sec 1-65535> | state [enable | disable]}  
enable dvmrp  
disable dvmrp  
show dvmrp {ipif <ipif_name 12>}  
show dvmrp neighbor {ipif <ipif_name 12> | ipaddress <network_address>}  
show dvmrp nexthop {ipaddress <network_address> | ipif <ipif_name 12>}  
show dvmrp routing_table {ipaddress <network_address>}
```

---

### 27.1. config dvmrp

---

#### ● Description

This command is used to configure DVMRP configurations.

#### ● Format

```
config dvmrp [ipif <ipif_name 12> | all] {metric <value 1-31> | probe <sec 1-65535> |  
neighbor_timeout <sec 1-65535> | state [enable | disable]}
```

#### ● Parameters

---

|             |                                                                                                                                                           |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b> | Specifies the IP interface name used.<br><b>&lt;ipif_name 12&gt;</b><br>Enter the IP interface name used here. This name can be up to 12 characters long. |
| <b>all</b>  | Specifies that all the IP interfaces will be used.                                                                                                        |

---

|               |                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>metric</b> | (Optional) Allows the assignment of a DVMRP route cost to the above IP interface. A DVMRP route cost is a relative number that represents the real cost of using this route in the construction of a multicast delivery tree. It is similar to, but not defined as, the hop count in RIP.<br><b>&lt;value 1-31&gt;</b><br>Enter the metric value used here. This value must be between 1 and 31. The default value is 1. |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

|              |                                                                                                                                                                                                                                            |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>probe</b> | (Optional) Specifies the time in seconds between the DVMRP Probe message transmissions.<br><b>&lt;sec 1-65535&gt;</b><br>Enter the probe value used here. This value must be between 1 and 65535 seconds. The default value is 10 seconds. |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

|                         |                                                                                                                                                                                                                                                                                      |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>neighbor_timeout</b> | (Optional) Specifies the time period for DVMRP will hold Neighbor Router reports before issuing poison route messages.<br><b>&lt;sec 1-65535&gt;</b><br>Enter the neighbor timeout value used here. This value must be between 1 and 65535 seconds. The default value is 35 seconds. |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

|              |                                                                                                                                                                                                                                             |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>state</b> | (Optional) Specifies the DVMRP state of the IP interface.<br><b>enable</b><br>Specifies that DVMRP of the specified IP interface will be enabled.<br><b>disable</b><br>Specifies that DVMRP of the specified IP interface will be disabled. |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure DVMRP configurations of IP interface called 'System':

```
Zxxx0:admin# config dvmrp ipif System neighbor_timeout 30 metric 1 probe 5
Command: config dvmrp ipif System neighbor_timeout 30 metric 1 probe 5

Success

Zxxx0:admin#
```

## 27.2. enable dvmrp

---

### ● Description

This command is used to enable the DVMRP global state on the Switch.

### ● Format

enable dvmrp

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable DVMRP:

```
Zxxx0:admin# enable dvmrp
Command: enable dvmrp

Success.

Zxxx0:admin#
```

## 27.3. disable dvmrp

---

### ● Description

This command is used to disable the DVMRP global state on the Switch.

### ● Format

**disable dvmrp**

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To disable DVMRP:

```
Zxxx0:admin# disable dvmrp
Command: disable dvmrp

Success.

Zxxx0:admin#
```

## 27.4. show dvmrp

---

### ● Description

This command is used to display DVMRP configurations.

### ● Format

**show dvmrp {ipif <ipif\_name 12>}**

### ● Parameters

---

|                             |                                                                                                   |
|-----------------------------|---------------------------------------------------------------------------------------------------|
| <b>ipif</b>                 | (Optional) Specifies the IP interface name used for the display.                                  |
| <b>&lt;ipif_name 12&gt;</b> | Enter the IP interface name used for the display here. This name can be up to 12 characters long. |

---

If no parameter is specified, then all the IP interfaces will be displayed.

## ● Restrictions

None.

## ● Example

To display DVMRP configurations:

```
Zxxx0:admin#show dvmrp
Command: show dvmrp

DVMRP Global State : Disabled

Interface      IP Address      Neighbor Timeout  Probe  Metric  State
-----
System         192.168.69.123  35                10     1       Disabled

Total Entries: 1

Zxxx0:admin#
```

## 27.5. show dvmrp neighbor

### ● Description

This command is used to display the DVMRP neighbor table.

### ● Format

**show dvmrp neighbor {ipif <ipif\_name 12> | ipaddress <network\_address>}**

### ● Parameters

---

**ipif** (Optional) Specifies the IP interface name used for the display.  
**<ipif\_name 12>**  
 Enter the IP interface name used for the display here. This name can be up to 12 characters long.

---

**ipaddress** (Optional) Specifies the IP address and netmask of the destination used.  
**<network\_address>**  
 Enter the IP address and netmask of the destination used here.

---

If no parameter is specified, the system will display the whole DVMRP neighbor table.

## ● Restrictions

None.

## ● Example

To display DVMRP neighbor table:



## 27. Distance Vector Multicast Routing Protocol (DVMRP) Commands

```
Zxxx0:admin# show dvmrp neighbor
Command: show dvmrp neighbor

DVMRP Neighbor Address Table
Interface      Neighbor Address  Generation ID  Expire Time
-----
System         10.48.74.123     86             32

Total Entries : 1

Zxxx0:admin#
```

### 27.6. show dvmrp nexthop

---

#### ● Description

This command is used to display the DVMRP routing next hop table.

#### ● Format

**show dvmrp nexthop {ipaddress <network\_address> | ipif <ipif\_name 12>}**

#### ● Parameters

---

##### ipaddress

(Optional) Specifies the IP address and netmask of the destination used.

**<network\_address>**

Enter the IP address and netmask of the destination used here.

---

##### ipif

(Optional) Specifies the IP interface name used for the display.

**<ipif\_name 12>**

Enter the IP interface name used for the display here. This name can be up to 12 characters long.

---

If no parameter is specified, the system will display all the DVMRP routing next hop tables.

#### ● Restrictions

None.

#### ● Example

To display DVMRP routing next hop table:

## 27. Distance Vector Multicast Routing Protocol (DVMRP) Commands

```
Zxxx0:admin# show dvmrp nexthop
Command: show dvmrp nexthop
```

| Source Address/NetMask | Interface Name | Type |
|------------------------|----------------|------|
| 10.0.0.0/8             | ip2            | Leaf |
| 10.0.0.0/8             | ip3            | Leaf |
| 20.0.0.0/8             | System         | Leaf |
| 20.0.0.0/8             | ip3            | Leaf |
| 30.0.0.0/8             | System         | Leaf |
| 30.0.0.0/8             | ip2            | Leaf |

```
Total Entries : 6
```

```
Zxxx0:admin#
```

### 27.7. show dvmrp routing\_table

#### ● Description

This command is used to display the DVMRP routing table.

#### ● Format

**show dvmrp routing\_table {ipaddress <network\_address>}**

#### ● Parameters

---

**ipaddress**

(Optional) Specifies the IP address and netmask of the destination used.

**<network\_address>**

Enter the IP address and netmask of the destination used here.

---

If no parameter is specified, the system will display the whole DVMRP routing table.

#### ● Restrictions

None.

#### ● Example

To display DVMRP routing table:

## 27. Distance Vector Multicast Routing Protocol (DVMRP) Commands

```
Zxxx0:admin# show dvmrp routing_table  
Command: show dvmrp routing_table
```

### DVMRP Routing Table

| Source Address/Netmask | Upstream Neighbor | Metric | Learned | Interface | Expire |
|------------------------|-------------------|--------|---------|-----------|--------|
| 10.0.0.0/8             | 10.90.90.90       | 2      | Local   | System    | -      |
| 20.0.0.0/16            | 20.1.1.1          | 2      | Local   | ip2       | -      |
| 30.0.0.0/24            | 30.1.1.1          | 2      | Local   | ip3       | -      |

```
Total Entries : 3
```

```
Zxxx0:admin#
```

## 28. Domain Name System (DNS) Relay Commands

DNS (Domain Name System) is a function to manage server domain names.

Domain names are named based on hierarchical structure rules. The DNS server, which corresponds to domain name hierarchies, manages a mapping between domain names and IP addresses. Access to a web server becomes available after sending an inquiry to the DNS server and obtaining an IP address from the domain name (name resolution). The DNS relay is a function that allows this Switching Hub to receive a name resolution request from the client and transfer it to the original DNS server.

TCP/IP network requires a DNS server specified for each client. The DNS relay function allows you to configure this Switching Hub as a DNS server.

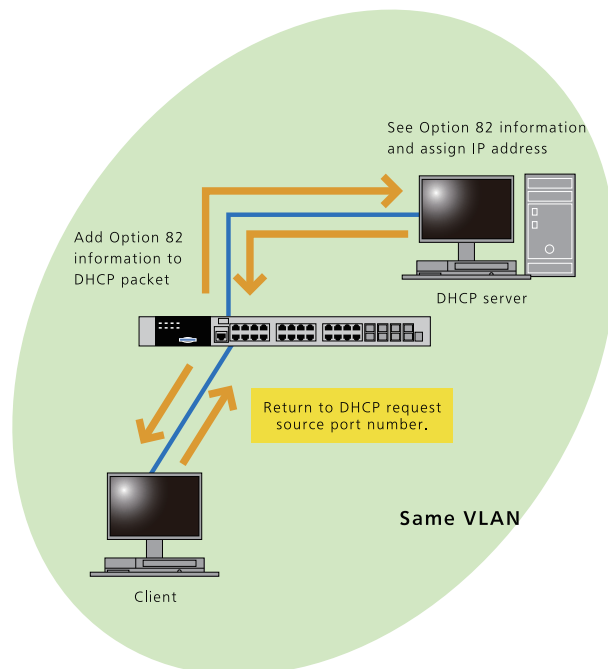


Figure 28-1 DNS relay function overview

In addition, you can improve the name resolution efficiency using DNS cache and configure a static DNS table.

## 28. Domain Name System (DNS) Relay Commands

---

```
config dnsr [[primary | secondary] nameserver <ipaddr> | [add | delete] static <domain_name 32>
<ipaddr>]
enable dnsr {[cache | static]}
disable dnsr {[cache | static]}
show dnsr {static}
```

---

### 28.1. config dnsr

---

#### ● Description

This command is used to add or delete a static entry into the Switch's DNS resolution table, or set up the relay server.

#### ● Format

```
config dnsr [[primary | secondary] nameserver <ipaddr> | [add | delete] static
<domain_name 32> <ipaddr>]
```

#### ● Parameters

---

|                |                                                                                         |
|----------------|-----------------------------------------------------------------------------------------|
| <b>primary</b> | Specify to indicate that the IP address below is the address of the primary DNS server. |
|----------------|-----------------------------------------------------------------------------------------|

|                  |
|------------------|
| <b>secondary</b> |
|------------------|

|                                                                                           |
|-------------------------------------------------------------------------------------------|
| Specify to indicate that the IP address below is the address of the secondary DNS server. |
|-------------------------------------------------------------------------------------------|

---

|                   |
|-------------------|
| <b>nameserver</b> |
|-------------------|

|                                               |
|-----------------------------------------------|
| Specify the IP address of the DNS nameserver. |
|-----------------------------------------------|

|                       |
|-----------------------|
| <b>&lt;ipaddr&gt;</b> |
|-----------------------|

|                                               |
|-----------------------------------------------|
| Specify the IP address of the DNS nameserver. |
|-----------------------------------------------|

---

|            |                                        |
|------------|----------------------------------------|
| <b>add</b> | Specify to add the DNS relay function. |
|------------|----------------------------------------|

---

|               |                                           |
|---------------|-------------------------------------------|
| <b>delete</b> | Specify to delete the DNS relay function. |
|---------------|-------------------------------------------|

---

|               |                                       |
|---------------|---------------------------------------|
| <b>static</b> | Specify the domain name of the entry. |
|---------------|---------------------------------------|

|                              |
|------------------------------|
| <b>&lt;domain_name32&gt;</b> |
|------------------------------|

|                          |
|--------------------------|
| Specify the domain name. |
|--------------------------|

|                       |
|-----------------------|
| <b>&lt;ipaddr&gt;</b> |
|-----------------------|

|                                      |
|--------------------------------------|
| Specify the IP address of the entry. |
|--------------------------------------|

---

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To set IP address 10.24.22.5 as the primary DNS server:

```
Zxxx0:admin# config dnsr primary nameserver 10.24.22.5
Command: config dnsr primary nameserver 10.24.22.5

Success.

Zxxx0:admin#
```

To add the entry "dns1" with IP address 10.24.22.5 to the DNS static table:

```
Zxxx0:admin#config dnsr add static dns1 10.24.22.5
Command: config dnsr add static dns1 10.24.22.5

Success.

Zxxx0:admin#
```

To delete the entry "dns1" with IP address 10.24.22.5 from the DNS static table:

```
Zxxx0:admin#config dnsr delete static dns1 10.24.22.5
Command: config dnsr delete static dns1 10.24.22.5

Success.

Zxxx0:admin#
```

## 28.2. enable dnsr

---

### ● Description

This command is used to enable DNS relay.

### ● Format

**enable dnsr** {[cache | static]}

### ● Parameters

|               |                                                                                   |
|---------------|-----------------------------------------------------------------------------------|
| <b>cache</b>  | Specify to enable the cache lookup for the DNS relay on the Switching Hub.        |
| <b>static</b> | Specify to enable the static table lookup for the DNS relay on the Switching Hub. |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable DNS relay:

```
Zxxx0:admin#enable dnsr
Command: enable dnsr

Success.

Zxxx0:admin#
```

## 28. Domain Name System (DNS) Relay Commands

To enable cache lookup for DNS relay:

```
Zxxx0:admin#enable dnsr cache
Command: enable dnsr cache

Success.

Zxxx0:admin#
```

To enable static table lookup for DNS relay:

```
Zxxx0:admin#enable dnsr static
Command: enable dnsr static

Success.

Zxxx0:admin#
```

### 28.3. disable dnsr

---

#### ● Description

This command is used to disable DNS relay on the Switching Hub.

#### ● Format

**disable dnsr** {[cache | static]}

#### ● Parameters

|               |                                                                                               |
|---------------|-----------------------------------------------------------------------------------------------|
| <b>cache</b>  | (Optional) Specify to disable the cache lookup for the DNS relay on the Switching Hub.        |
| <b>static</b> | (Optional) Specify to disable the static table lookup for the DNS relay on the Switching Hub. |

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To disable the status of DNS relay:

```
Zxxx0:admin#disable dnsr
Command: disable dnsr

Success.

Zxxx0:admin#
```

To disable cache lookup for DNS relay:

```
Zxxx0:admin#disable dnsr cache
Command: disable dnsr cache

Success.

Zxxx0:admin#
```

To disable static table lookup for DNS relay:

```
Zxxx0:admin#disable dnsr static
Command: disable dnsr static

Success.

Zxxx0:admin#
```

### 28.4. show dnsr

---

#### ● Description

This command is used to display the current DNS relay configuration and static entries.

#### ● Format

**show dnsr {static}**

#### ● Parameters

---

|               |                                                                                                                                                      |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>static</b> | (Optional) Specify to display the static entries in the DNS relay table. If this parameter is omitted, the entire DNS relay table will be displayed. |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------|

---

#### ● Restrictions

None.

#### ● Example

To display the DNS relay status:



## 28. Domain Name System (DNS) Relay Commands

```
Zxxx0:admin#show dnsr
```

```
Command: show dnsr
```

```
DNSR Status           : Disabled  
Primary Name Server    : 0.0.0.0  
Secondary Name Server  : 0.0.0.0  
DNSR Cache Status      : Disabled  
DNSR Static Table Status : Disabled
```

```
DNS Relay Static Table
```

| Domain Name | IP Address   |
|-------------|--------------|
| -----       | -----        |
| www.123.com | 10.12.12.123 |

```
Total Entries: 1
```

```
Zxxx0:admin#
```

## 29. DNS Resolver Commands

DNS (Domain Name System) is function to manage server domain names. Domain names are named based on hierarchical structure rules. The DNS server, which corresponds to domain name hierarchies, manages a mapping between domain names and IP addresses. Access to a web server becomes available after sending an inquiry to the DNS server and obtaining an IP address from the domain name (name resolution).

A resolver is a client that sends a name resolution request to the DNS server.

In this chapter, you will configure a DNS server used when this Switching Hub requires name resolution.

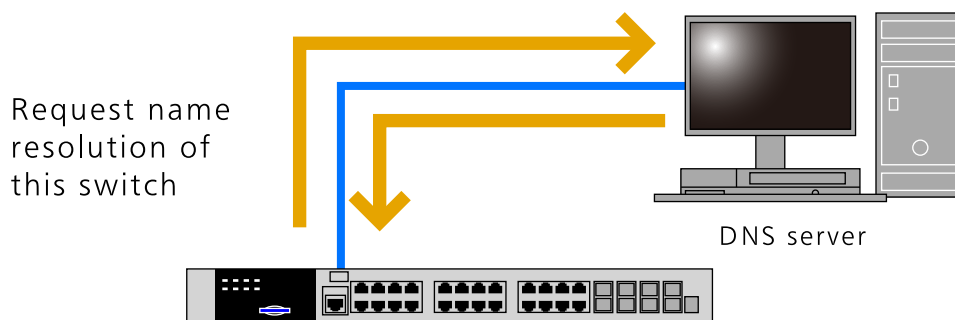


Figure 29-1 Name resolution of this Switching Hub

You can also configure the response waiting time (1 to 60 seconds) from the DNS server, register a static DNS table, and check and delete DNS cache.

```
config name_server add <ipaddr> { primary }
config name_server delete <ipaddr> { primary }
config name_server timeout <second 1-60>
show name_server
create host_name <name 255> <ipaddr>
delete host_name [<name 255> | all]
show host_name { static | dynamic }
enable dns_resolver
disable dns_resolver
```

## 29.1. config name\_server add

---

### ● Description

This command is used to add a DNS resolver name server to the Switch.

### ● Format

config name\_server add <ipaddr> {primary}

### ● Parameters

---

<ipaddr> Enter the DNS Resolver name server IP address used here.

---

primary (Optional) Specifies that the name server is a primary name server.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To add DNS Resolver primary name server 10.10.10.10:

```
Zxxx0:admin# config name_server add 10.10.10.10 primary
Command: config name_server add 10.10.10.10 primary

Success.

Zxxx0:admin#
```

## 29.2. config name\_server delete

---

### ● Description

This command is used to delete a DNS resolver name server from the Switch.

### ● Format

config name\_server delete <ipaddr> {primary}

### ● Parameters

---

<ipaddr> Enter the DNS Resolver name server IP address used here.

---

primary (Optional) Specifies that the name server is a primary name server.

---

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To delete DNS Resolver name server 10.10.10.1:

```
Zxxx0:admin# config name_server delete 10.10.10.10
Command: config name_server delete 10.10.10.10

Success.

Zxxx0:admin#
```

## 29.3. **config name\_server timeout**

---

- **Description**

This command is used to configure the timeout value of a DNS Resolver name server.

- **Format**

config name\_server timeout <second 1-60>

- **Parameters**

---

|                            |                                                                                 |
|----------------------------|---------------------------------------------------------------------------------|
| <b>timeout</b>             | Specifies the maximum time waiting for a response from a specified name server. |
| <b>&lt;second 1-60&gt;</b> | Enter the timeout value used here. This value must be between 1 and 60 seconds. |

---

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To configure DNS Resolver name server time out to 10 seconds:

```
Zxxx0:admin# config name_server timeout 10
Command: config name_server timeout 10

Success.

Zxxx0:admin#
```

## 29.4. show name\_server

---

### ● Description

This command is used to display the current DNS Resolver name servers and name server time out on the Switch.

### ● Format

show name\_server

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display the current DNS Resolver name servers and name server time out:

```
Zxxx0:admin# show name_server
Command: show name_server

Name Server Time Out: 3 seconds

Static Name Server Table:
Server IP Address      Priority
-----
20.20.20.20            Secondary
10.1.1.1               Primary

Dynamic Name Server Table:
Server IP Address      Priority
-----
10.48.74.122          Primary

Zxxx0:admin#
```

## 29.5. create host\_name

---

### ● Description

This command is used to create the static host name entry of the Switch.

### ● Format

create host\_name <name 255> <ipaddr>

### ● Parameters

---

<name 255>

Enter the hostname used here.

This name can be up to 255 characters long.

---

<ipaddr> Enter the host IP address used here.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create static host name "www.example.com":

```
Zxxx0:admin# create host_name www.example.com 10.10.10.10
Command: create host_name www.example.com 10.10.10.10

Success.

Zxxx0:admin#
```

## 29.6. delete host\_name

---

### ● Description

This command is used to delete the static or dynamic host name entries of the Switch.

### ● Format

delete host\_name [<name 255> | all]

### ● Parameters

---

<name 255>

Enter the hostname used here.

This name can be up to 255 characters long.

---

all Specifies that all the hostnames will be deleted.

---

## 29. DNS Resolver Commands

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete the static host name entry "www.example.com":

```
Zxxx0:admin# delete host_name www.example.com
Command: delete host_name www.example.com

Success.

Zxxx0:admin#
```

## 29.7. show host\_name

---

### ● Description

This command is used to display the current host name.

### ● Format

show host\_name {static | dynamic}

### ● Parameters

---

|               |                                                               |
|---------------|---------------------------------------------------------------|
| <b>static</b> | (Optional) Specifies to display the static host name entries. |
|---------------|---------------------------------------------------------------|

---

|                |                                                                |
|----------------|----------------------------------------------------------------|
| <b>dynamic</b> | (Optional) Specifies to display the dynamic host name entries. |
|----------------|----------------------------------------------------------------|

---

### ● Restrictions

None.

### ● Example

To display the static and dynamic host name entries:

```

Zxxx0:admin# show host_name
Command: show host_name

Static Host Name Table
Host Name                               IP Address
-----
www.example.com                        10.10.10.10
www.exempla.com                        20.20.20.20

Total Static Entries: 2

Dynamic Host Name Table
Host Name                               IP Address      TTL
-----
www.examp1c.com                        30.30.30.30      60 minutes
www.examp1d.com                        40.40.40.40      10 minutes

Total Dynamic Entries: 2

Zxxx0:admin#

```

## 29.8. enable dns\_resolver

### ● Description

This command is used to enable the DNS Resolver state of the Switch.

### ● Format

enable dns\_resolver

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the DNS Resolver state to enabled:

```

Zxxx0:admin# enable dns_resolver
Command: enable dns_resolver

Success.

Zxxx0:admin#

```



## 29.9. disable dns\_resolver

---

### ● Description

This command is used to disable the DNS Resolver state of the Switch.

### ● Format

disable dns\_resolver

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the DNS Resolver state to disabled:

```
Zxxx0:admin# disable dns_resolver
Command: disable dns_resolver

Success.

Zxxx0:admin#
```

## 30. FDB Commands

Forwarding Database (FDB) is a mapping table between the MAC addresses of network devices and the destination VLANs or ports. A Switching Hub accesses FDB using the MAC address information of a receive packet and determines the destination VLAN or port.

| VID | VLAN Name | MAC Address       | Port | Type    |
|-----|-----------|-------------------|------|---------|
| 1   | default   | 00-00-00-00-00-01 | 1:25 | Dynamic |
| 1   | default   | 00-00-00-00-00-02 | 1:25 | Dynamic |
| 1   | default   | 00-00-00-00-00-03 | T1   | Static  |
| 1   | default   | 00-00-00-00-00-04 | T1   | Static  |
| 1   | default   | 00-00-00-00-00-0A | CPU  | Self    |
| 1   | default   | 00-00-00-00-00-06 | -    | Static  |

FDB is usually created automatically from receive packet information. However, it can also be registered manually by the administrator. FDB is created not only for unicast, which sends to one destination, but also for multicast, which sends to multiple destinations. You can also configure which ports join or not join a multicast group.

### ● Multicast filtering function

In multicast where data is simultaneously sent to multiple destinations, multicast data may be sent even to unnecessary ports if a multicast group does not exist. When the multicast filtering function is enabled, you can configure not to send data to any port other than router ports even if a multicast group is not created.

---

```

create fdb <vlan_name 32> <macaddr> [port <port> | drop]
create fdb vlanid <vidlist> <macaddr> [port <port> | drop]
create multicast_fdb <vlan_name 32> <macaddr>
config multicast_fdb <vlan_name 32> <macaddr> [add | delete] <portlist>
config fdb aging_time <sec 10-1000000>
config multicast_vlan_filtering_mode [vlanid <vidlist> | vlan <vlan_name 32> | all]
    [forward_all_groups | forward_unregistered_groups | filter_unregistered_groups]
delete fdb <vlan_name 32> <macaddr>
clear fdb [vlan <vlan_name 32> | port <port> | all]
show multicast_fdb {[vlan <vlan_name 32> | vlanid <vidlist>] | mac_address <macaddr>}
show fdb {[port <port> | vlan <vlan_name 32> | vlanid <vidlist> | mac_address <macaddr> | static
    | aging_time | security]}
show multicast_vlan_filtering_mode {[vlanid <vidlist> | vlan <vlan_name 32>]}
  
```

---

## 30.1. create fdb

---

### ● Description

This command is used to make an entry into the Switching Hub's unicast MAC address forwarding database.

### ● Format

**create fdb <vlan\_name 32> <macaddr> [port <port> | drop]**

### ● Parameters

---

**<vlan\_name 32>**

Specify a VLAN name associated with a MAC address. The maximum length is 32 characters.

---

**<macaddr>**

Specify the MAC address to be added to the static forwarding table.

---

**port**

The Switching Hub will always forward traffic to the specified device through this port.

**<port>** Specify the port number corresponding to the MAC destination address.

**drop** Specify to have the Switching Hub drop traffic.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create an unicast MAC forwarding:

```
Zxxx0:admin#create fdb default 00-00-00-00-01-02 port 1:5
Command: create fdb default 00-00-00-00-01-02 port 1:5

Success.
Zxxx0:admin#
```

## 30.2. create fdb vlanid

---

### ● Description

This command is used to create an entry into the Switching Hub's unicast MAC address forwarding database using the VLAN ID.

### ● Format

**create fdb vlanid <vidlist> <macaddr> [port <port> | drop]**

## ● Parameters

---

**<vidlist>** Enter the VLAN ID used here.

---

**<macaddr>**

Specify the MAC address to be added to the static forwarding table.

---

**port** The Switching Hub will always forward traffic to the specified device through this port.  
**<port>** Specify the port number corresponding to the MAC destination address.  
**drop** Specify to have the Switching Hub drop traffic.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To create an unicast MAC forwarding:

```
Zxxx0:admin#create fdb vlanid 1 00-11-22-33-44-55 port 1:5
Command: create fdb vlanid 1 00-11-22-33-44-55 port 1:5

Success.

Zxxx0:admin#
```

# 30.3. create multicast\_fdb

---

## ● Description

This command is used to make an entry into the Switching Hub's multicast MAC address forwarding database.

## ● Format

**create multicast\_fdb <vlan\_name 32> <macaddr>**

## ● Parameters

---

**<vlan\_name 32>**

Specify the name of the VLAN on which the MAC address resides. The maximum length is 32 characters.

---

**<macaddr>**

Specify the multicast MAC address to be added to the static forwarding table.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## 30. FDB Commands

### ● Example

To create multicast MAC forwarding:

```
Zxxx0:admin# create multicast_fdb default 01-00-00-00-01-01
Command: create multicast_fdb default 01-00-00-00-01-01

Success.

Zxxx0:admin#
```

## 30.4. config multicast\_fdb

---

### ● Description

This command is used to configure the multicast MAC address forwarding table.

### ● Format

**config multicast\_fdb <vlan\_name 32> <macaddr> [add | delete] <portlist>**

### ● Parameters

|                             |                                                                                                          |
|-----------------------------|----------------------------------------------------------------------------------------------------------|
| <b>&lt;vlan_name 32&gt;</b> | Specify the name of the VLAN on which the MAC address resides. The maximum name length is 32 characters. |
| <b>&lt;macaddr&gt;</b>      | Specify the MAC address that will be added or deleted to the forwarding table.                           |
| <b>add</b>                  | Specify to add ports.                                                                                    |
| <b>delete</b>               | Specify to delete ports.                                                                                 |
| <b>&lt;portlist&gt;</b>     | Specifies a range of ports to be configured.                                                             |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To add multicast MAC forwarding:

```
Zxxx0:admin# config multicast_fdb default 01-00-00-00-01-01 add 1-5
Command: config multicast_fdb default 01-00-00-00-01-01 add 1-5

Success.

Zxxx0:admin#
```

## 30.5. config fdb aging\_time

---

### ● Description

This command is used to set the age-out timer for the Switching Hub's dynamic unicast MAC address forwarding tables.

### ● Format

config fdb aging\_time <sec 10-1000000>

### ● Parameters

---

<sec 10-1000000> - Specify the time in seconds that a dynamically learned MAC address will remain in the Switching Hub's MAC address forwarding table without being accessed, before being dropped from the database. The range of the value is 10 to 1000000. The default value is 300.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure MAC address aging time:

```
Zxxx0:admin#config fdb aging_time 300
Command: config fdb aging_time 300

Success.

Zxxx0:admin#
```

## 30.6. config multicast vlan\_filtering\_mode

### ● Description

This command is used to configure the multicast packet filtering mode for VLANs.

### ● Format

config multicast vlan\_filtering\_mode [vlanid <vidlist> | vlan <vlan\_name 32> | all]  
[forward\_all\_groups | forward\_unregistered\_groups | filter\_unregistered\_groups]

### ● Parameters

|                                    |                                                                                    |
|------------------------------------|------------------------------------------------------------------------------------|
| <b>vlanid</b>                      | Specify the VLAN ID list to set.<br><vidlist><br>Specify the VLAN ID list to set.  |
| <b>vlan</b>                        | Specify the VLAN to set.<br><vlan_name 32><br>The maximum length is 32 characters. |
| <b>all</b>                         | Specify to set all VLANs.                                                          |
| <b>forward_all_groups</b>          | Specifies that all multicast groups will be forwarded based on the VLAN.           |
| <b>forward_unregistered_groups</b> | Specify the filtering mode as forward_unregistered_groups. This is the default.    |
| <b>filter_unregistered_groups</b>  | Specify the filtering mode as filter_unregistered_groups.                          |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the the multicast packet filtering mode for all VLANs:

```
Zxxx0:admin#config multicast vlan_filtering_mode all forward_unregistered_groups
Command: config multicast port filtering_mode all forward_unregistered_groups

Success.

Zxxx0:admin#
```

## 30.7. delete fdb

---

### ● Description

This command is used to delete a permanent FDB entry.

### ● Format

`delete fdb <vlan_name 32> <macaddr>`

### ● Parameters

---

**<vlan\_name 32>**

Specify the name of the VLAN on which the MAC address resides. The maximum length is 32 characters.

---

**<macaddr>**

Specify the MAC address to be deleted from the static forwarding table.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete a permanent FDB entry:

```
Zxxx0:admin#delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

Zxxx0:admin#
```



## 30.8. clear fdb

---

### ● Description

This command is used to clear the Switching Hub's forwarding database of all dynamically learned MAC addresses.

### ● Format

**clear fdb** [vlan <vlan\_name 32> | port <port> | all ]

### ● Parameters

|             |                                                                                                                                                                      |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan</b> | Specify the name of the VLAN on which the MAC address resides.<br><vlan_name 32><br>The maximum length is 32 characters.                                             |
| <b>port</b> | Specify the port number corresponding to the dynamically learned MAC address.<br><port>Specify the port number corresponding to the dynamically learned MAC address. |
| <b>all</b>  | Specify to clear all VLANs and ports.                                                                                                                                |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To clear all FDB dynamic entries:

```
Zxxx0:admin#clear fdb all
Command: clear fdb all

Success.

Zxxx0:admin#
```

## 30.9. show multicast\_fdb

---

### ● Description

This command is used to display the contents of the Switching Hub's multicast forwarding database.

### ● Format

**show multicast\_fdb** {[vlan <vlan\_name 32> | vlanid <vidlist>] | mac\_address <macaddr>}

## ● Parameters

---

**vlan** (Optional) Specify the name of the VLAN on which the MAC address resides.  
**<vlan\_name 32>**

The maximum length is 32 characters.

---

**vlanid** (Optional) Specifies the VLAN ID on which the MAC address resides.  
**<vidlist>**

Enter the VLAN ID used here.

---

**mac\_address**

(Optional) Specify a MAC address, for which FDB entries will be displayed.

**<macaddr>**

Specify a MAC address, for which FDB entries will be displayed.

---



---

**NOTE** If no parameter is specified, all multicast FDB entries will be displayed.

---

## ● Restrictions

None.

## ● Example

To display multicast MAC address table:

```
Zxxx0:admin#show multicast_fdb
Command: show multicast_fdb

VLAN Name      : default
MAC Address    : 01-00-00-00-01-01
Egress Ports   : 1-5,26
Mode           : Static

Total Entries  : 1

Zxxx0:admin#
```

## 30.10. show fdb

---

### ● Description

This command is used to display the current unicast MAC address forwarding database.

### ● Format

**show fdb {[port <port> | vlan <vlan\_name 32> | vlanid <vidlist> | mac\_address <macaddr> | static | aging\_time | security]}**

## 30. FDB Commands

### ● Parameters

|                    |                                                                                                                            |
|--------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>port</b>        | (Optional) Specify the entries for one port.<br><port>Specify the entries for one port.                                    |
| <b>vlan</b>        | (Optional) Specify to display the entries for a specific VLAN.<br><vlan_name 32><br>The maximum length is 32 characters.   |
| <b>vlanid</b>      | (Optional) Specify to display the entries by VLAN ID list.<br><vidlist><br>Specify to display the entries by VLAN ID list. |
| <b>mac_address</b> | (Optional) Specify the MAC address.<br><macaddr><br>Specify the MAC address.                                               |
| <b>static</b>      | (Optional) Specify to display all permanent entries.                                                                       |
| <b>aging_time</b>  | Specify to display the unicast MAC address aging time.                                                                     |
| <b>security</b>    | Specify to display the security settings.                                                                                  |

**NOTE** If no parameter is specified, all unicast FDB entries will be displayed.

### ● Restrictions

None.

### ● Example

To display unicast MAC address table:

```
Zxxx0:admin#show fdb
Command: show fdb

Unicast MAC Address Aging Time = 300

VID  VLAN Name                MAC Address          Port  Type      Status
----  -
1    default                    00-01-02-03-04-00  CPU   Self      Forward
1    default                    00-26-5A-AE-CA-1C  21    Dynamic  Forward

Total Entries: 2

Zxxx0:admin#
```

## 30.11. show multicast vlan\_filtering\_mode

### ● Description

This command is used to display the multicast packet filtering mode for VLANs.

### ● Format

**show multicast vlan\_filtering\_mode** {[vlanid <vidlist> | vlan <vlan\_name 32>]}

### ● Parameters

---

|               |                                                                         |
|---------------|-------------------------------------------------------------------------|
| <b>vlanid</b> | (Optional) Specify to display the entries by VLAN ID list.<br><vidlist> |
|---------------|-------------------------------------------------------------------------|

Specify to display the entries by VLAN ID list.

---

|             |                                                                                  |
|-------------|----------------------------------------------------------------------------------|
| <b>vlan</b> | (Optional) Specify to display the entries for a specific VLAN.<br><vlan_name 32> |
|-------------|----------------------------------------------------------------------------------|

The maximum length is 32 characters.

---

### ● Restrictions

None.

### ● Example

To show multicast filtering mode for ports:

```
Zxxx0:admin#show multicast vlan_filtering_mode
Command: show multicast filtering_mode

VLAN ID/VLAN Name          Multicast Filter Mode
-----
default                    forward_unregistered_groups

Zxxx0:admin#
```

## 31. File System Management Commands

The commands are used to manage storage media files on this Switching Hub and mounted SD card.

You can check/format media information, change the drive, create/change/delete a directory, and display/rename/delete/copy/move a file.

---

```

show storage_media_info {[unit <unit_id> | all]}
md {{unit <unit_id>} <drive_id>} <pathname>
rd {{unit <unit_id>} <drive_id>} <pathname>
cd {<pathname>}
dir {{unit <unit_id>} <drive_id>} {<pathname>}
rename {{unit <unit_id>} <drive_id>} <pathname> <filename>
erase {{unit <unit_id>} <drive_id>} <pathname>
format {unit <unit_id>} <drive_id> {[fat16 | fat32]} {<label_name>}
del {{unit <unit_id>} <drive_id>} <pathname> {recursive}
move {{unit <unit_id>} <drive_id>} <pathname> {{unit <unit_id>} <drive_id>} <pathname>
copy {{unit <unit_id>} <drive_id>} <pathname> {{unit <unit_id>} <drive_id>} <pathname>
change drive {unit <unit_id>} <drive_id>
  
```

---

### 31.1. show storage\_media\_info

#### ● Description

This command is used to display storage media information.

#### ● Format

**show storage\_media\_info** {[unit <unit\_id> | all]}

#### ● Parameters

---

|             |                                                                                                                                             |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>unit</b> | Specifies the unit ID in the stacking system. If not specified, it refers to the master unit.<br><unit_id><br>Enter the unit ID value here. |
| <b>all</b>  | Specifies that all the units, in the stacking system's storage media information will be displayed.                                         |

---

#### ● Restrictions

None.

#### ● Example

To display storage media information:

```
Zxxx0:admin#show storage_media_info
Command: show storage_media_info

Unit   Drive  Media Type      Size  Label      FS Type
-----
  1    c:    Flash          123 MB      FFS

Zxxx0:admin#
```

## 31.2. md

### ● Description

This command is used to create a directory.

### ● Format

**md** {{unit <unit\_id>} <drive\_id>} <pathname>

### ● Parameters

|                         |                                                                                                                                                                                                  |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>unit</b>             | Specifies the unit ID in the stacking system. If not specified, it refers to the master unit.<br><b>&lt;unit_id&gt;</b><br>Enter the unit ID value here.                                         |
| <b>&lt;drive_id&gt;</b> | Specifies the drive ID. If not specified, it refers to the current drive.                                                                                                                        |
| <b>&lt;pathname&gt;</b> | Specify the directory to be created. The path name can be specified either as a full path name or partial name. For a partial path name, it indicates the directory is in the current directory. |

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To create a directory:

```
Zxxx0:admin#md c:/abc
Command: md c:/abc

Success.

Zxxx0:admin#
```

### 31.3. rd

---

#### ● Description

This command is used to remove a directory. If there are files and directories still existing in the directory, this command will fail and return an error message.

#### ● Format

**rd** {{unit <unit\_id>} <drive\_id>} <pathname>

#### ● Parameters

---

|                         |                                                                                                                                                                                             |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>unit</b>             | Specifies the unit ID in the stacking system. If not specified, it refers to the master unit.<br><b>&lt;unit_id&gt;</b><br>Enter the unit ID value here.                                    |
|                         | <b>&lt;drive_id&gt;</b><br>Specifies the drive ID. If not specified, it refers to the current drive.                                                                                        |
| <b>&lt;pathname&gt;</b> | Specify the directory to be removed. The path name can be specified either as a full path name or partial name. For a partial path name, it indicates the file is in the current directory. |

---

#### ● Restrictions

Only Administrator and Operator-level users can issue this command.

#### ● Example

To delete an empty directory:

```
Zxxx0:admin#rd c:/abc
Command: rd c:/abc

Success.

Zxxx0:admin#
```

## 31.4. cd

---

### ● Description

This command is used to change the current directory. The user can change the current directory to another drive using this command. The current drive and current directory will be displayed if the **<pathname>** is not specified.

### ● Format

**cd {<pathname>}**

### ● Parameters

---

**<pathname>**

(Optional) Specify the directory to be changed. The path name can be specified either as a full path name or partial name. For a partial path name, it indicates the file is in the current directory.

---

### ● Restrictions

None.

### ● Example

To change a work directory:

```
Zxxx0:admin#cd d1
Command: cd d1

Current work directory: "c:/d1"

Zxxx0:admin#
```

## 31.5. dir

---

### ● Description

This command is used to list all of the files located in a directory of a drive. If a path name is not specified, then all of the files in the specified drive will be displayed. If none of the parameters are specified, the files in the current directory will be displayed. If a user lists the system directory, the used space will be shown.

### ● Format

**dir [{unit <unit\_id>} <drive\_id>] {<pathname>}**



## 31. File System Management Commands

### ● Parameters

---

|             |                                                                                                                                                                                                                                                                  |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>unit</b> | Specifies the unit ID in the stacking system. If not specified, it refers to the master unit.<br><b>&lt;unit_id&gt;</b><br>Enter the unit ID value here.<br><b>&lt;drive_id&gt;</b><br>Specifies the drive ID. If not specified, it refers to the current drive. |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

|                         |                                                                                                                                                                                                                                                                                        |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;pathname&gt;</b> | (Optional) Specify the directory to be listed. The path name can be specified either as a full path name or partial name. For a partial path name, it indicates the file is in the current directory. The drive ID also included in this parameter, for example: d:/config/bootup.cfg. |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### ● Restrictions

None.

### ● Example

To list a directory:

```
Zxxx0:admin#dir
Command: dir

Directory of c:/
Idx Info      Attr Size      Update Time      Name
---
  1 RUN(*)    -rw- 4796564  2000/01/22 03:52:03 runtime.rom
  2 CFG(*)    -rw- 24120    2000/01/22 23:22:58 config.cfg
  3 CFG(b)    -rw- 24120    2000/01/23 06:59:39 1
  4          d---          2000/01/23 22:52:50 system
30608 KB total (25700 KB free)

(*) -with boot up info      (b) -with backup info

Zxxx0:admin#
```

To list a system directory:

```
Zxxx0:admin#dir c:/system
Command: dir c:/system

System reserved directory. Used space 89KB.

Zxxx0:admin#
```

## 31.6. rename

---

### ● Description

This command is used to rename a file in the file system. The pathname specifies the file (in path form) to be renamed and the file name specifies the new file name. If the path name is not a full path, then it refers to a path under the current directory for the drive. The renamed file will stay in the same directory.

### ● Format

**rename** [{unit <unit\_id>} <drive\_id>} <pathname> <filename>

### ● Parameters

|                         |                                                                                               |
|-------------------------|-----------------------------------------------------------------------------------------------|
| <b>unit</b>             | Specifies the unit ID in the stacking system. If not specified, it refers to the master unit. |
| <b>&lt;unit_id&gt;</b>  | Enter the unit ID value here.                                                                 |
| <b>&lt;drive_id&gt;</b> | Specifies the drive ID. If not specified, it refers to the current drive.                     |
| <b>&lt;pathname&gt;</b> | Specify the file (in path form) to be renamed.                                                |
| <b>&lt;filename&gt;</b> | Specify the new name of the file.                                                             |

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To rename a file or directory:

```
Zxxx0:admin#rename run.rom run1.rom
Command: rename run.rom run1.rom

Success.

Zxxx0:admin#
```

### 31.7. erase

---

#### ● Description

This command is used to delete a file stored in the file system. The system will prompt if the target file is a bootup image/configuration or the last image.

#### ● Format

**erase** { {unit <unit\_id>} <drive\_id>} <pathname>

#### ● Parameters

|                         |                                                                                                                                                          |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>unit</b>             | Specifies the unit ID in the stacking system. If not specified, it refers to the master unit.<br><b>&lt;unit_id&gt;</b><br>Enter the unit ID value here. |
|                         | <b>&lt;drive_id&gt;</b><br>Specifies the drive ID. If not specified, it refers to the current drive.                                                     |
| <b>&lt;pathname&gt;</b> | Specify the file to be deleted. If it is specified in the associated form, then it is related to the current directory.                                  |

#### ● Restrictions

Only Administrator and Operator-level users can issue this command.

#### ● Example

To delete a file:

```
Zxxx0:admin#erase cfg
Command: erase cfg

Are you sure to remove the boot up Configuration from this device? (y/n)y

Success.

Zxxx0:admin#
```

## 31.8. format

---

### ● Description

This command is used to format a specific drive.

### ● Format

**format** {unit <unit\_id>} <drive\_id> {[fat16 | fat32]} {<label\_name>}

### ● Parameters

|                           |                                                                                                                                                                                      |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>unit</b>               | Specifies the unit ID in the stacking system. If not specified, it refers to the master unit.<br><unit_id><br>Enter the unit ID value here.<br><drive_id><br>Specifies the drive ID. |
| <b>fat16</b>              | (Optional) Specifies that the drive will be formatted to support a FAT16 file system.                                                                                                |
| <b>fat32</b>              | (Optional) Specifies that the drive will be formatted to support a FAT32 file system.                                                                                                |
| <b>&lt;label_name&gt;</b> | (Optional) Enter the label name used for this drive here.                                                                                                                            |

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To format media:

```
Zxxx0:admin#format d: fat32
Command: format d: fat32

Formatting..... Done!

Zxxx0:admin#
```

### 31.9. del

---

#### ● Description

This command is used to delete a file. It is also used to delete a directory and its contents. The system will prompt if the target file is a bootup image/configuration or the last image.

#### ● Format

**del** [{unit <unit\_id>} <drive\_id>} <pathname> {recursive}

#### ● Parameters

---

|             |                                                                                                                                                          |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>unit</b> | Specifies the unit ID in the stacking system. If not specified, it refers to the master unit.<br><b>&lt;unit_id&gt;</b><br>Enter the unit ID value here. |
|             | <b>&lt;drive_id&gt;</b><br>Specifies the drive ID. If not specified, it refers to the current drive.                                                     |

---

|                         |                                                                                                                                      |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;pathname&gt;</b> | Specify the file or directory to be deleted. If it is specified in the associated form, then it is related to the current directory. |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------|

---

|                             |                                                                                        |
|-----------------------------|----------------------------------------------------------------------------------------|
| <b>recursive</b> (Optional) | Used on the directory, to delete a directory and its contents even if it is not empty. |
|-----------------------------|----------------------------------------------------------------------------------------|

---

#### ● Restrictions

Only Administrator and Operator-level users can issue this command.

#### ● Example

To delete a file:

```
Zxxx0:admin#del cfg
Command: del cfg

Are you sure to remove the boot up Configuration from this device? (y/n)y

Success.

Zxxx0:admin#
```

To delete a a directory with the parameter "recursive":

```
Zxxx0:admin# del d1 recursive
Command: del d1 recursive

Success.

Zxxx0:admin#
```

## 31.10. move

---

### ● Description

This command is used to move a file around the file system. Note that when a file is moved, it can be specified whether to be renamed at the same time.

### ● Format

```
move {{unit <unit_id>} <drive_id>} <pathname> {{unit <unit_id>} <drive_id>}
<pathname>
```

### ● Parameters

---

|             |                                                                                                                         |
|-------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>unit</b> | Specifies the unit ID in the stacking system. If not specified, it refers to the master unit.<br><b>&lt;unit_id&gt;</b> |
|-------------|-------------------------------------------------------------------------------------------------------------------------|

Enter the unit ID value here.

**<drive\_id>**

Specifies the drive ID. If not specified, it refers to the current drive.

---

**<pathname>**

Specify the file to be moved. The path name can be specified either as a full path name or partial name. For a partial path name, it indicates the file is in the current directory.

---

|             |                                                                                                                         |
|-------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>unit</b> | Specifies the unit ID in the stacking system. If not specified, it refers to the master unit.<br><b>&lt;unit_id&gt;</b> |
|-------------|-------------------------------------------------------------------------------------------------------------------------|

Enter the unit ID value here.

**<drive\_id>**

Specifies the drive ID. If not specified, it refers to the current drive.

---

**<pathname>**

Specify the new path where the file will be moved. The path name can be specified either as a full path name or partial name. For a partial path name, it indicates the file is in the current directory.

---

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To move a file or directory:

```
Zxxx0:admin#move c:/log.txt c:/abc/log1.txt
Command: move c:/log.txt c:/abc/log1.txt

Success.

Zxxx0:admin#
```

## 31.11. copy

---

### ● Description

This command is used to copy a file to another file in the file system.

### ● Format

copy {{unit <unit\_id>} <drive\_id>} <pathname> {{unit <unit\_id>} <drive\_id>}  
<pathname>

### ● Parameters

|             |                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>unit</b> | Specifies the unit ID in the stacking system. If not specified, it refers to the master unit.<br><b>&lt;unit_id&gt;</b><br>Enter the unit ID value here.<br><b>&lt;drive_id&gt;</b><br>Specifies the drive ID. If not specified, it refers to the current drive.<br><b>&lt;pathname&gt;</b><br>Specify the file to be copied. If it is specified in the associated form, then it is related to the current directory. |
| <b>unit</b> | Specifies the unit ID in the stacking system. If not specified, it refers to the master unit.<br><b>&lt;unit_id&gt;</b><br>Enter the unit ID value here.<br><b>&lt;drive_id&gt;</b><br>Specifies the drive ID. If not specified, it refers to the current drive.<br><b>&lt;pathname&gt;</b><br>Specify the file to copy to. If it is specified in the associated form, then it is related to the current directory    |

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To copy a file:

```
Zxxx0:admin#copy c:/log.txt c:/log1.txt
Command: copy c:/log.txt c:/log1.txt

Copying..... Done!

Zxxx0:admin#
```

## 31.12. change drive

---

### ● Description

This command is used to change the current drive.

### ● Format

change drive {unit <unit\_id>} <drive\_id>

### ● Parameters

---

|             |                                                                                                          |
|-------------|----------------------------------------------------------------------------------------------------------|
| <b>unit</b> | (Optional) Specifies the unit ID in the stacking system. If not specified, it refers to the master unit. |
|-------------|----------------------------------------------------------------------------------------------------------|

**<unit\_id>**

Enter the unit ID value here.

---

**<drive\_id>**

Specifies the drive ID. The format of drive\_id is 'c:', or 'd:'.

---

### ● Restrictions

None.

### ● Example

To display the storage media's information:

```
Zxxx0:admin# change drive unit 3 c:
Command: change drive unit 3 c:

Current work directory: "/unit3:/c:".

Zxxx0:admin#
```



## 32. Filter Commands

The commands are used to filter packets from the DHCP server and NetBIOS over TCP/IP and NetBIOS packets.

The DHCP server packet filtering allows you to limit the number of DHCP servers to be used if there are multiple DHCP servers on the network. It also can detect unauthorized DHCP servers and log them or report them to the management server as a SNMP trap.

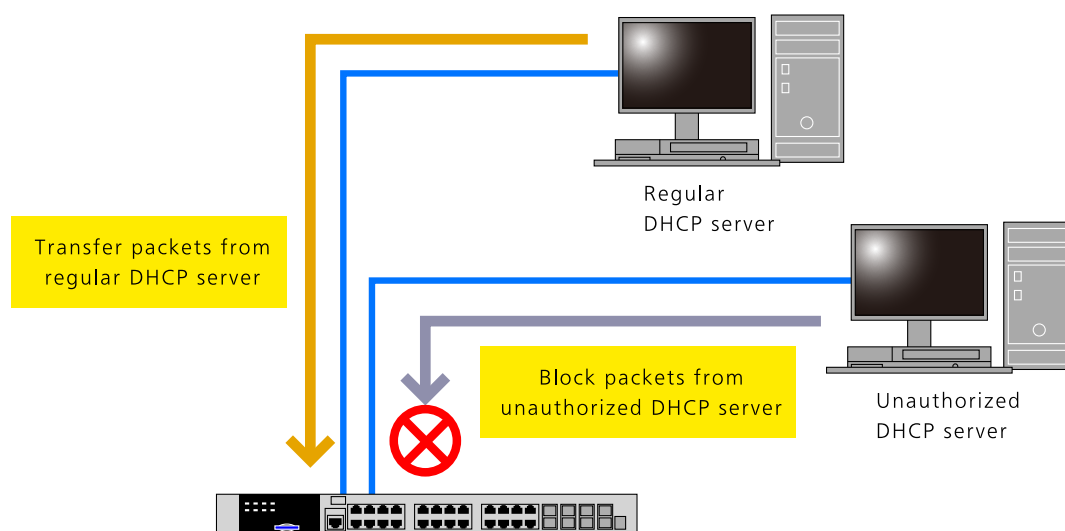


Figure 32-1 DHCP server packet filtering

```

config filter dhcp_server [add permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist>
| all] | delete permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | ports
 [<portlist> | all] state [enable | disable] | illegal_server_log_suppress_duration [1min | 5min |
 30min] | trap_log [enable | disable]]
show filter dhcp_server
config filter extensive_netbios [<portlist> | all] state [enable | disable]
show filter extensive_netbios
config filter netbios [<portlist> | all] state [enable | disable]
show filter netbios

```

## 32.1. config filter dhcp\_server

---

### ● Description

This command has two purposes: to specify to filter all DHCP server packets on the specific port and to specify to allow some DHCP server packets with pre-defined server IP addresses and client MAC addresses. With this function, we can restrict the DHCP server to service specific DHCP clients. This is useful when two DHCP servers are present on the network; one of them can provide the private IP address and the other can provide the public IP address.

Enabling filter DHCP server port state will create one access profile and create one access rule per port (UDP port = 67). Filter commands in this file will share the same access profile. Addition of a permit DHCP entry will create one access profile and create one access rule. Filter commands in this file will share the same access profile.

### ● Format

```
config filter dhcp_server [add permit server_ip <ipaddr> {client_mac <macaddr>} ports
[<portlist> | all] | delete permit server_ip <ipaddr> {client_mac <macaddr>} ports
[<portlist> | all] | ports [<portlist> | all] state [enable | disable] |
illegal_server_log_suppress_duration [1min | 5min | 30min] | trap_log [enable |
disable]]
```

### ● Parameters

---

#### add permit server\_ip

Specify the IP address of the DHCP server to be permitted.

**<ipaddr>**

Specify the IP address.

**client\_mac**

(Optional) Specify the MAC address of the DHCP client.

**<macaddr>**

Specify the MAC address.

**ports** Specify the ports.

**<portlist>**

Specify a range of ports to be configured.

**all** Specify to configure all ports.

---

## 32. Filter Commands

---

### **delete permit server\_ip**

Specify the delete permit server IP address.

**<ipaddr>**

Specify the IP address.

**client\_mac**

(Optional) Specify the MAC address of the DHCP client.

**<macaddr>**

Specify the MAC address.

**ports** Specify the ports.

**<portlist>**

Specify a range of ports to be configured.

**all** Specify to configure all ports.

---

**ports** Specify the ports.

**<portlist>** Specify a range of ports to be configured.

**all** Specify to configure all ports.

**state** Specify the port status.

**enable**

Enable the state.

**disable**

Disable the state.

---

### **illegal\_server\_log\_suppress\_duration**

Specify the illegal server log suppression duration.

**1min** Specify an illegal server log suppression duration of 1 minute.

**5min** Specify an illegal server log suppression duration of 5 minutes.

**30min** Specify an illegal server log suppression duration of 30 minutes.

---

**trap\_log** Specify the trap log status.

**enable** Enable the trap log feature.

**disable** Disable the trap log feature.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To add an entry from the DHCP server/client filter list in the Switching Hub's database:

```
Zxxx0:admin#config filter dhcp_server add permit server_ip 10.1.1.1 client_mac 00-00-00-00-01 port 1-26
Command: config filter dhcp_server add permit server_ip 10.1.1.1 client_mac 00-00-00-00-01 port 1-26

Success.

Zxxx0:admin#
```

To configure the filter DHCP server state:

```
Zxxx0:admin#config filter dhcp_server ports 1-10 state enable
Command: config filter dhcp_server ports 1-10 state enable

Success.

Zxxx0:admin#
```

## 32.2. show filter dhcp\_server

---

### ● Description

This command is used to display the DHCP server/client filter list created on the Switching Hub.

### ● Format

**show filter dhcp\_server**

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display the DHCP server/client filter list created on the Switching Hub:

```
Zxxx0:admin#show filter dhcp_server
Command: show filter dhcp_server

Enabled Ports: 1,28
Trap & Log State: Enabled
Illegal Server Log Suppress Duration: 1 minutes
Permit DHCP Server/Client Table
Server IP Address Client MAC Address  Port
-----
Total Entries: 0

Zxxx0:admin#
```

## 32.3. config filter extensive\_netbios

---

### ● Description

This command is used to configure the Switching Hub to deny NetBIOS packets over 802.3 frames on the network. Enabling the filterNetBIOS packets over 802.3 frames will create one access profile and one access rule per port automatically. Filter commands in this file will share the same access profile.

### ● Format

**config filter extensive\_netbios [<portlist> | all] state [enable | disable]**

### ● Parameters

|                                                                    |                                                                                      |
|--------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| <b>&lt;portlist&gt;</b> Specify a range of ports to be configured. |                                                                                      |
| <b>all</b>                                                         | Specify to configure all ports.                                                      |
| <b>state</b>                                                       | Specify the status of the filter to block the NetBIOS packets over 802.3 frames.     |
|                                                                    | <b>enable</b><br>Enable the filter to block the NetBIOS packets over 802.3 frames.   |
|                                                                    | <b>disable</b><br>Disable the filter to block the NetBIOS packets over 802.3 frames. |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the extensive NetBIOS filter state on ports 1 to 10:

```
Zxxx0:admin#config filter extensive_netbios 1-10 state enable
Command: config filter extensive_netbios 1-10 state enable

Success.

Zxxx0:admin#
```

## 32.4. show filter extensive\_netbios

---

### ● Description

This command is used to display the extensive NetBIOS filter state on the Switching Hub.

### ● Format

**show filter extensive\_netbios**

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display the extensive NetBIOS filter state on the Switching Hub:

```
Zxxx0:admin#show filter extensive_netbios
Command: show filter extensive_netbios

Enabled Ports: 1-3

Zxxx0:admin#
```

## 32.5. config filter netbios

### ● Description

This command is used to configure the Switch to deny NetBIOS packets on the network. Enabling of the filter NetBIOS state will create one access profile and three access rules per port automatically (UDP ports 137 and 138 and TCP port 139). Filter commands in this file will share the same access profile.

### ● Format

**config filter netbios [<portlist> | all] state [enable | disable]**

### ● Parameters

|                         |                                                            |
|-------------------------|------------------------------------------------------------|
| <b>&lt;portlist&gt;</b> | Specify a range of ports to be configured.                 |
| <b>all</b>              | Specify to configure all ports.                            |
| <b>state</b>            | Specify the status of the filter to block NetBIOS packets. |
| <b>enable</b>           | Enable the filter to block NetBIOS packets.                |
| <b>disable</b>          | Disable the filter to block NetBIOS packets.               |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## 32. Filter Commands

### ● Example

To configure the NetBIOS filter state:

```
Zxxx0:admin#config filter netbios 1-10 state enable
Command: config filter netbios 1-10 state enable

Success.

Zxxx0:admin#
```

## 32.6. show filter netbios

---

### ● Description

This command is used to display the NetBIOS filter state on the Switching Hub.

### ● Format

**show filter netbios**

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display the NetBIOS filter state:

```
Zxxx0:admin#show filter netbios
Command: show filter netbios

Enabled Ports: 1-3

Zxxx0:admin#
```

## 33. Gratuitous ARP Commands

ARP (Address Resolution Protocol) is used to calculate a MAC address from an IP address if the destination MAC address is unknown.

Gratuitous ARP is a special ARP packet sent when an IP interface is booted, sending an inquiry by setting its own IP address instead of the destination IP address. If other device responds to Gratuitous ARP, it means the IP address is duplicated.

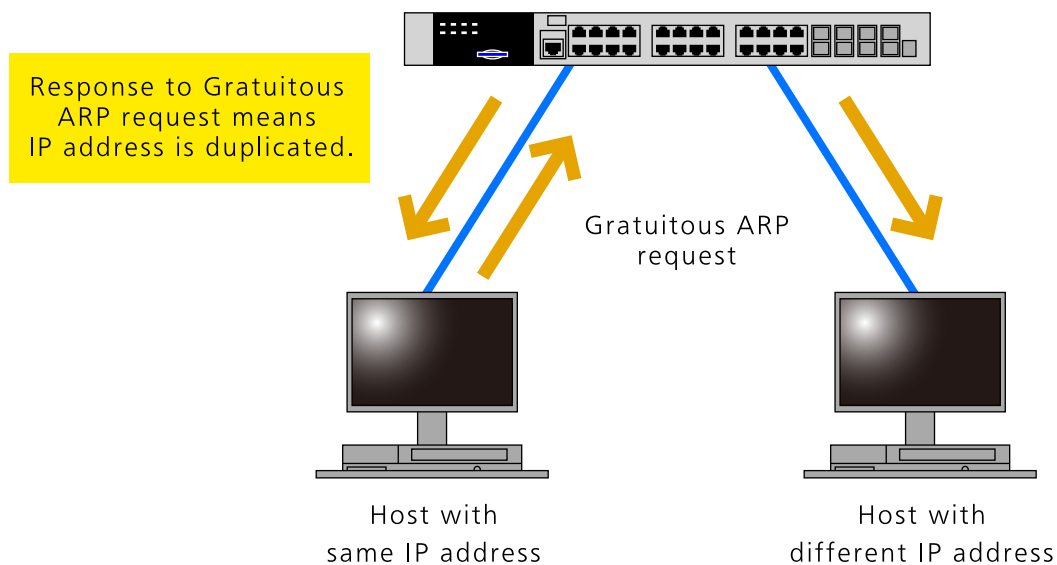


Figure 33-1 Gratuitous ARP overview

```
enable gratuitous_arp {ipif <ipif_name 12>} {trap | log}(1)
disable gratuitous_arp {ipif <ipif_name 12>} {trap | log}(1)
config gratuitous_arp learning [enable | disable]
config gratuitous_arp send dup_ip_detected [enable | disable]
config gratuitous_arp send ipif_status_up [enable | disable]
config gratuitous_arp send periodically ipif <ipif_name 12> interval <value 0-65535>
show gratuitous_arp {ipif <ipif_name 12>}
```



### 33.1. enable gratuitous\_arp

---

#### ● Description

This command is used to enable the gratuitous ARP trap and log state. The Switching Hub can trap and log the IP conflict event to inform the administrator.

#### ● Format

**enable gratuitous\_arp {ipif <ipif\_name 12>} {trap | log}(1)**

#### ● Parameters

|             |                                                                                                                                                              |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b> | (Optional) The interface name of the L3 interface.<br><b>&lt;ipif_name 12&gt;</b><br>Specify the name of the interface. The maximum length is 12 characters. |
| <b>trap</b> | Specify trap. The trap is disabled by default.                                                                                                               |
| <b>log</b>  | Specify log. The even log is enabled by default.                                                                                                             |

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To enable gratuitous ARP:

```
Zxxx0:admin#enable gratuitous_arp ipif System trap log
Command: enable gratuitous_arp ipif System trap log

Success.

Zxxx0:admin#
```

### 33.2. disable gratuitous\_arp

---

#### ● Description

This command is used to disable the gratuitous ARP trap and log state.

#### ● Format

**disable gratuitous\_arp {ipif <ipif\_name 12>} {trap | log}(1)**

### ● Parameters

|             |                                                                                                                                                              |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b> | (Optional) The interface name of the L3 interface.<br><b>&lt;ipif_name 12&gt;</b><br>Specify the name of the interface. The maximum length is 12 characters. |
| <b>trap</b> | Specify trap. The trap is disabled by default.                                                                                                               |
| <b>log</b>  | Specify log. The even log is enabled by default.                                                                                                             |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To disable gratuitous ARP, the trap, and the log state:

```
Zxxx0:admin#disable gratuitous_arp ipif System trap log
Command: disable gratuitous_arp ipif System trap log

Success.

Zxxx0:admin#
```

## 33.3. config gratuitous\_arp learning

### ● Description

This command is used to enable or disable learning of ARP entries in the ARP cache based on the received gratuitous ARP packets.

### ● Format

config gratuitous\_arp learning [enable | disable]

### ● Parameters

|                |                                                                               |
|----------------|-------------------------------------------------------------------------------|
| <b>enable</b>  | Enable learning of ARP entries based on the received gratuitous ARP packets.  |
| <b>disable</b> | Disable learning of ARP entries based on the received gratuitous ARP packets. |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable learning of ARP entries in the ARP cache based on the received gratuitous ARP packets:

## 33. Gratuitous ARP Commands

```
Zxxx0:admin# config gratuitous_arp learning enable
Command: config gratuitous_arp learning enable

Success.

Zxxx0:admin#
```

### 33.4. config gratuitous\_arp send dup\_ip\_detected

---

#### ● Description

This command is used to enable or disable the sending of gratuitous ARP requests when a duplicate IP address is detected. By default, the state is disabled. For this command, duplicate IP detected means that the system received an ARP request packet that is sent by an IP address that matches the system's own IP address. In this case, the system knows that somebody out there is using an IP address that conflicts with that of the system. In order to reclaim the correct host of this IP address, the system can send out the gratuitous ARP request packet for this duplicate IP address.

#### ● Format

`config gratuitous_arp send dup_ip_detected [enable | disable]`

#### ● Parameters

|                |                                                                                 |
|----------------|---------------------------------------------------------------------------------|
| <b>enable</b>  | Enable the sending of gratuitous ARP requests when a duplicate IP is detected.  |
| <b>disable</b> | Disable the sending of gratuitous ARP requests when a duplicate IP is detected. |

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To enable the sending of gratuitous ARP requests when a duplicate IP address is detected:

```
Zxxx0:admin#config gratuitous_arp send dup_ip_detected enable
Command: config gratuitous_arp send dup_ip_detected enable

Success.

Zxxx0:admin#
```

## 33.5. config gratuitous\_arp send ipif\_status\_up

---

### ● Description

This command is used to enable or disable the sending of gratuitous ARP requests when the IP interface status becomes up. This is used to automatically announce the interface's IP address to other nodes. By default, the state is disabled. When the state is enabled and IP interface is linked up, one gratuitous ARP packet will be broadcast.

### ● Format

config gratuitous\_arp send ipif\_status\_up [enable | disable]

### ● Parameters

|                |                                                                                 |
|----------------|---------------------------------------------------------------------------------|
| <b>enable</b>  | Enable the sending of gratuitous ARP requests when the IPIF status becomes up.  |
| <b>disable</b> | Disable the sending of gratuitous ARP requests when the IPIF status becomes up. |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable the sending of gratuitous ARP requests when the IP interface status becomes up:

```
Zxxx0:admin#config gratuitous_arp send ipif_status_up enable
Command: config gratuitous_arp send ipif_status_up enable

Success.

Zxxx0:admin#
```

## 33.6. config gratuitous\_arp send periodically ipif

---

### ● Description

This command is used to configure the interval for the periodical sending of gratuitous ARP request packets.

### ● Format

config gratuitous\_arp send periodically ipif <ipif\_name 12> interval <value 0-65535>

### ● Parameters

---

<ipif\_name 12>

Specify the interface name of the L3 interface. The maximum length is 12 characters.

---

interval The periodically send gratuitous ARP interval time, in seconds.

<value 0-65535>

Specify the value between 0 and 65535. 0 (zero) means not to send gratuitous ARP request packets periodically. By default, the interval is 0 (zero).

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the gratuitous ARP interval to 5 for the IPIF System:

```
Zxxx0:admin#config gratuitous_arp send periodically ipif System interval 5
Command: config gratuitous_arp send periodically ipif System interval 5

Success.

Zxxx0:admin#
```

## 33.7. show gratuitous\_arp

---

### ● Description

This command is used to display gratuitous ARP configuration.

### ● Format

**show gratuitous\_arp {ipif <ipif\_name 12>}**

### ● Parameters

---

|             |                                                                                   |
|-------------|-----------------------------------------------------------------------------------|
| <b>ipif</b> | (Optional) The interface name of the L3 interface.<br><b>&lt;ipif_name 12&gt;</b> |
|-------------|-----------------------------------------------------------------------------------|

---

Specify the name of the interface. The maximum length is 12 characters.

---

### ● Restrictions

None.

### ● Example

To display the gratuitous ARP log and trap state:

```
Zxxx0:admin#show gratuitous_arp
Command: show gratuitous_arp

Send on IPIF Status Up      : Disabled
Send on Duplicate IP Detected : Disabled
Gratuitous ARP Learning     : Disabled

IP Interface Name : System
    Gratuitous ARP Trap           : Disabled
    Gratuitous ARP Log            : Enabled
    Gratuitous ARP Periodical Send Interval : 0

Total Entries: 1

Zxxx0:admin#
```

## 34. Internet Group Management Protocol (IGMP) Commands

In multicast where data is simultaneously sent to multiple destinations, destinations are managed in a unit called "group." Each group has its own unique multicast IP address and multicast MAC address assigned. A client that wants to join multicast can be a member of the group after sending a notification that it joins a specific multicast group to neighbor routers. IGMP is a protocol to maintain and manage multicast groups. It is used for clients to join or leave a group or used to exchange group information between routers.

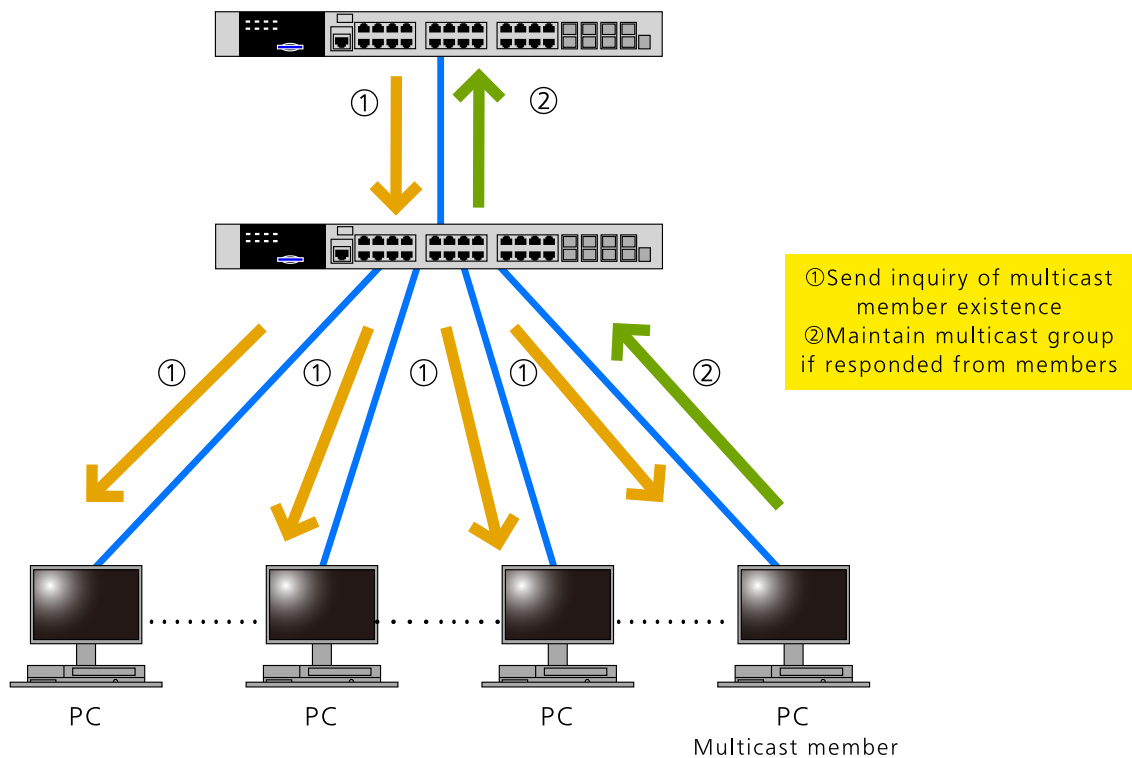


Figure 34-1 IGMP overview

```
config igmp [ipif <ipif_name 12> | all] {version <value 1-3> | query_interval <sec 1-31744> |
max_response_time <sec 1-25> | robustness_variable <value 1-7> |
last_member_query_interval <value 1-25> | state [enable | disable]}
show igmp {ipif <ipif_name 12>}
show igmp group {group <group> | ipif <ipif_name 12>}
config igmp check_subscriber_source_network [ipif <ipif_name 12> | all] [enable | disable]
show igmp check_subscriber_source_network {ipif <ipif_name 12>}
create igmp static_group ipif <ipif_name 12> group <ipaddr>
delete igmp static_group ipif <ipif_name 12> [group <ipaddr> | all]
show igmp static_group {ipif <ipif_name 12>}
```

## 34.1. config igmp

---

### ● Description

This command is used to configure IGMP on the Switch.

### ● Format

**config igmp** [**ipif** <ipif\_name 12> | **all**] {**version** <value 1-3> | **query\_interval** <sec 1-31744> | **max\_response\_time** <sec 1-25> | **robustness\_variable** <value 1-7> | **last\_member\_query\_interval** <value 1-25> | **state** [**enable** | **disable**]}

### ● Parameters

|                                   |                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b>                       | Specifies the IP interface name used for this configuration.<br><ipif_name 12><br>Enter the IP interface name used for this configuration here. This name can be up to 12 characters long.                                                                                                                                                          |
| <b>all</b>                        | Specifies that all the IP interfaces will be used.                                                                                                                                                                                                                                                                                                  |
| <b>version</b>                    | (Optional) Specifies the IGMP version used.<br><value 1-3><br>Enter the IGMP version number used here. This value must be between 1 and 3. The default value is 3.                                                                                                                                                                                  |
| <b>query_interval</b>             | (Optional) Specifies the time in seconds between general query transmissions.<br><sec 1-31744><br>Enter the query interval time here. This value must be between 1 and 31744 seconds. The default value is 125.                                                                                                                                     |
| <b>max_response_time</b>          | (Optional) Specifies the maximum time in seconds to wait for reports from members.<br><sec 1-25><br>Enter the maximum response time here. This value must be between 1 and 25 seconds. The default value is 10.                                                                                                                                     |
| <b>robustness_variable</b>        | (Optional) Specifies the permitted packet loss that guarantees IGMP.<br><value 1-7><br>Enter the robustness variable here. This value must be between 1 and 7. The default value is 2.                                                                                                                                                              |
| <b>last_member_query_interval</b> | (Optional) Specifies the maximum Response Time inserted into the Group-Specific Queries that are sent in response to Leave Group messages, which is also the amount of time between Group-Specific Query messages.<br><value 1-25><br>Enter the last member query interval value here. This value must be between 1 and 25. The default value is 1. |
| <b>state</b>                      | (Optional) Specifies the IGMP state on a router interface.<br><b>enable</b><br>Specifies that the IGMP state will be enabled.<br><b>disable</b><br>Specifies that the IGMP state will be disabled.                                                                                                                                                  |



## 34. Internet Group Management Protocol (IGMP) Commands

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable IGMP version 1 for the IP interface "System":

```
Zxxx0:admin# config igmp ipif System version 1 state enable
Command: config igmp ipif System version 1 state enable

Success.

Zxxx0:admin#
```

To configure IGMPv2 for all IP interfaces:

```
Zxxx0:admin# config igmp all version 2
Command: config igmp all version 2

Success.

Zxxx0:admin#
```

## 34.2. show igmp

---

### ● Description

This command is used to display the IGMP configuration.

### ● Format

**show igmp {ipif <ipif\_name 12>}**

### ● Parameters

---

|             |                                                                                                                                                                                                                    |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b> | (Optional) Specifies the IP interface name used for this configuration.<br><b>&lt;ipif_name 12&gt;</b><br>Enter the IP interface name used for this configuration here. This name can be up to 12 characters long. |
| <b>all</b>  | Specifies that all the IP interfaces will be used.                                                                                                                                                                 |

---

If no parameter is specified, the system will display all IGMP configurations.

### ● Restrictions

None.

### ● Example

To display the IGMP configuration for all interfaces:

## 34. Internet Group Management Protocol (IGMP) Commands

```
Zxxx0:admin#show igmp
Command: show igmp

IGMP Interface Configurations

Interface      IP Address/Netmask  Ver- Query  Maximum  Robust-  Last      State
                sion          Response  ness     Member
                Time         Value     Query
                Interval
-----
System         10.90.90.90/8       3    125     10       2        1      Disabled

Total Entries: 1

Zxxx0:admin#
```

### 34.3. show igmp group

#### ● Description

This command is used to display the Switching Hub's IGMP group table.

#### ● Format

**show igmp group {group <group> | ipif <ipif\_name 12>}**

#### ● Parameters

---

**group** (Optional) Specifies the multicast group ID.  
**<group>**

Enter the multicast group ID value here.

---

**ipif** (Optional) Specifies the IP interface name used for this configuration.  
**<ipif\_name 12>**

Enter the IP interface name used for this configuration here. This name can be up to 12 characters long.

**all** Specifies that all the IP interfaces will be used.

---

If no parameter is specified, the system will display all IGMP group tables.

#### ● Restrictions

None.

#### ● Example

To display the IGMP group table:

## 34. Internet Group Management Protocol (IGMP) Commands

```
Zxxx0:admin# show igmp group
Command: show igmp group

Interface      Multicast Group  Last Reporter   IP Querier      IP Expire
-----
System         224.0.0.2        10.42.73.111    10.48.74.122    260
System         224.0.0.9        10.20.53.1      10.48.74.122    260
System         224.0.1.24       10.18.1.3       10.48.74.122    259
System         224.0.1.41       10.1.43.252     10.48.74.122    259
System         224.0.1.149      10.20.63.11     10.48.74.122    259

Total Entries : 5

Zxxx0:admin#
```

### 34.4. config igmp check\_subscriber\_source\_network

#### ● Description

This command is used to configure the flag that determines whether or not to check the subscriber source IP when an IGMP report or leave message is received. When this command is enabled on an interface, any IGMP report or leave messages received by the interface will be checked to determine whether its source IP is in the same network as the interface. If the check failed for a received report or leave message, the message won't be processed by IGMP protocol. If the check is disabled, the IGMP report or leave message with any source IP will be processed by the IGMP protocol.

#### ● Format

**config igmp check\_subscriber\_source\_network [ipif <ipif\_name 12> | all] [enable | disable]**

#### ● Parameters

|                |                                                                                                                                                                                                         |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b>    | Specifies the IP interface name used for this configuration.<br><b>&lt;ipif_name 12&gt;</b><br>Enter the IP interface name used for this configuration here. This name can be up to 12 characters long. |
| <b>all</b>     | Specifies that all the IP interfaces will be used.                                                                                                                                                      |
| <b>enable</b>  | Specifies that the check state will be enabled.                                                                                                                                                         |
| <b>disable</b> | Specifies that the check state will be disabled.                                                                                                                                                        |

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable the checking of subscriber source IP addresses when an IGMP report or leave message is received on the interface called 'System':

```
Zxxx0:admin# config igmp check_subscriber_source_network ipif System enable
Command: config igmp check_subscriber_source_network ipif System enable

Success.

Zxxx0:admin#
```

## 34.5. show igmp check\_subscriber\_source\_network

### ● Description

This command is used to display the status of the IGMP report/leave message source IP check.

### ● Format

show igmp check\_subscriber\_source\_network {ipif <ipif\_name 12>}

### ● Parameters

|             |                                                                                                                                                                                                       |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b> | (Optional) Specifies the IP interface name used for this configuration.<br><ipif_name 12><br>Enter the IP interface name used for this configuration here. This name can be up to 12 characters long. |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

If no parameter is specified, the system will display all interfaces.

### ● Restrictions

None.

### ● Example

To show the status of the check subscriber for the received IGMP report/leave messages on interface "n20":

```
Zxxx0:admin# show igmp check_subscriber_source_network ipif n20
Command: show igmp check_subscriber_source_network ipif n20

Interface      IP Address/Netmask  Check Subscriber Source Network
-----
n20            20.1.1.1/8          Disabled

Total Entries: 1

Zxxx0:admin#
```

## 34. Internet Group Management Protocol (IGMP) Commands

To show the status of the check subscriber for the received IGMP report/leave messages on all interfaces:

```
Zxxx0:admin# show igmp check_subscriber_source_network
Command: show igmp check_subscriber_source_network

Interface      IP Address/Netmask  Check Subscriber Source Network
-----
System         10.90.90.90/8       Enabled
n1             1.1.1.1/8           Disabled
n11            11.1.1.1/8          Disabled
n20            20.1.1.1/8          Disabled
n100           100.3.2.2/8         Disabled

Total Entries: 5

Zxxx0:admin#
```

### 34.6. create igmp static\_group ipif

#### ● Description

This command is used to create an IGMP static group on the Switch.

#### ● Format

**create igmp static\_group ipif <ipif\_name 12> group <ipaddr>**

#### ● Parameters

|              |                                                                                                                                                                                                         |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b>  | Specifies the IP interface name used for this configuration.<br><b>&lt;ipif_name 12&gt;</b><br>Enter the IP interface name used for this configuration here. This name can be up to 12 characters long. |
| <b>group</b> | Specifies the multicast IP address used.<br><b>&lt;ipaddr&gt;</b><br>Enter the multicast IP address used here.                                                                                          |

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To create an IGMP static group, with the multicast IP address 225.0.0.2 on the IP interface "System":

```
Zxxx0:admin# create igmp static_group ipif System group 225.0.0.2
Command: create igmp static_group ipif System group 225.0.0.2

Success.

Zxxx0:admin#
```

## 34.7. delete igmp static\_group ipif

---

### ● Description

This command is used to delete an IGMP static group on the Switch.

### ● Format

**delete igmp static\_group ipif <ipif\_name 12> [group <ipaddr> | all]**

### ● Parameters

|              |                                                                                                                                                                                                         |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b>  | Specifies the IP interface name used for this configuration.<br><b>&lt;ipif_name 12&gt;</b><br>Enter the IP interface name used for this configuration here. This name can be up to 12 characters long. |
| <b>group</b> | Specifies the multicast IP address used.<br><b>&lt;ipaddr&gt;</b><br>Enter the multicast IP address used here.                                                                                          |
| <b>all</b>   | <b>Specifies that all the multicast IP addresses will be deleted.</b>                                                                                                                                   |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete the IGMP static group, with the multicast IP address 225.0.0.2 on the IP interface "System".

```
Zxxx0:admin# delete igmp static_group ipif System group 225.0.0.2
Command: delete igmp static_group ipif System group 225.0.0.2

Success.

Zxxx0:admin#
```

To delete all IGMP static groups on the IP interface "n2".

```
Zxxx0:admin# delete igmp static_group ipif n2 all
Command: delete igmp static_group ipif n2 all

Success.

Zxxx0:admin#
```

### 34.8. show igmp static\_group

---

#### ● Description

This command is used to display IGMP static groups on the Switch.

#### ● Format

**show igmp static\_group {ipif <ipif\_name 12>}**

#### ● Parameters

---

|             |                                                                                                                                                                                                                    |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b> | (Optional) Specifies the IP interface name used for this configuration.<br><b>&lt;ipif_name 12&gt;</b><br>Enter the IP interface name used for this configuration here. This name can be up to 12 characters long. |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

#### ● Restrictions

None.

#### ● Example

To display all IGMP static groups on the interface "n20":

```
Zxxx0:admin# show igmp static_group ipif n20
Command: show igmp static_group ipif n20

Interface      Multicast Group
-----
n20            239.0.0.3

Total Entries: 1

Zxxx0:admin#
```

To display all IGMP static groups on all interfaces:

```
Zxxx0:admin# show igmp static_group
Command: show igmp static_group

Interface      Multicast Group
-----
System        225.0.0.1
System        225.0.0.2
n20           239.0.0.3

Total Entries: 3

Zxxx0:admin#
```

## 35.IGMP Proxy Commands

IGMP (Internet Group Management Protocol) is a protocol to manage multicast groups.

IGMP proxy is a function to transfer IGMP packets from multicast members to the upstream router. If a multicast transmission route is fixed, this function can transfer multicast packets between routers on the fixed route without using a multicast routing protocol. If a multicast server does not exist on the topology uplink, use the multicast routing function.

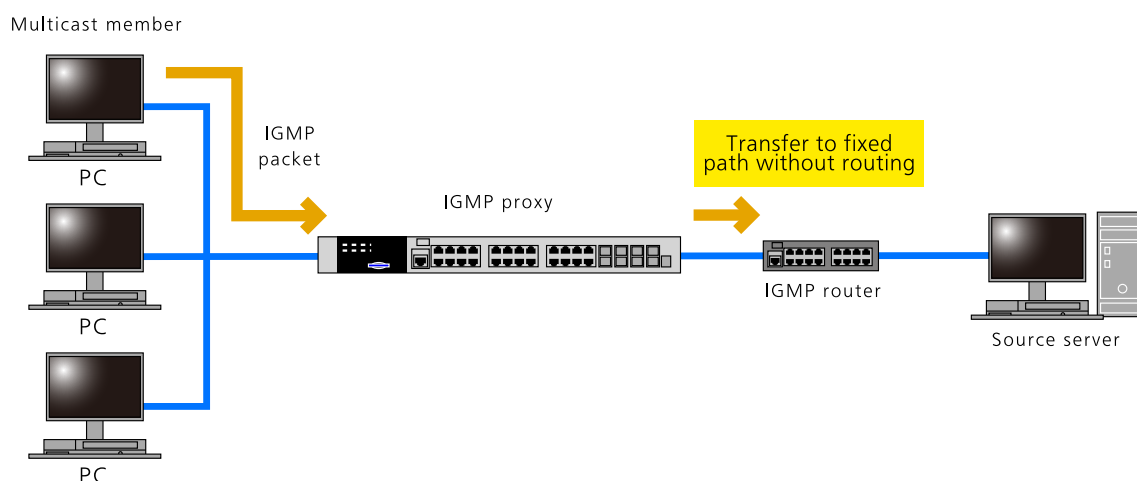


Figure 35-1 IGMP proxy overview

```
enable igmp_proxy
disable igmp_proxy
config igmp_proxy downstream_if [add | delete] vlan [<vlan_name 32> | vlanid <vidlist>]
config igmp_proxy upstream_if {vlan [<vlan_name 32> | vlanid <vlanid 1-4094>] | router_ports
    [add | delete] <portlist> | source_ip <ipaddr> | unsolicited_report_interval <sec 0-25>}(1)
show igmp_proxy {group}
```

### 35.1. enable igmp\_proxy

#### ● Description

This command is used to enable the IGMP proxy on the Switching Hub.

#### ● Format

```
enable igmp_proxy
```



## 35. IGMP Proxy Commands

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable the IGMP proxy:

```
Zxxx0:admin#enable igmp_proxy
Command: enable igmp_proxy

Success.

Zxxx0:admin#
```

## **35.2. disable igmp\_proxy**

---

### ● Description

This command is used to disable the IGMP proxy on the Switching Hub.

### ● Format

**disable igmp\_proxy**

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To disable the IGMP proxy:

```
Zxxx0:admin#disable igmp_proxy
Command: disable igmp_proxy

Success.

Zxxx0:admin#
```

## 35.3. config igmp\_proxy downstream\_if

● Description

This command is used to configure the IGMP proxy downstream interfaces. The IGMP proxy plays the server role on the downstream interfaces. The downstream interface must be an IGMP-snooping enabled VLAN.

● Format

config igmp\_proxy downstream\_if [add | delete] vlan [<vlan\_name 32> | vlanid <vidlist>]

● Parameters

|        |                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| add    | Specify to add a downstream interface.                                                                                                                                                                                                                                                                                                                                                                                      |
| delete | Specify to delete a downstream interface .                                                                                                                                                                                                                                                                                                                                                                                  |
| vlan   | Specify the VLAN by name or ID.<br><vlan_name 32><br>Specify a name of VLAN which will be added to or deleted from the IGMP proxy downstream interface. The maximum length is 32 characters.<br>vlanidSpecify a list of VLAN IDs to be added to or deleted from the IGMP proxy downstream interface.<br><vidlist><br>Specify a list of VLAN IDs which will be added to or deleted from the IGMP proxy downstream interface. |

● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

● Example

To configure the IGMP proxy's downstream interface:

```
Zxxx0:admin#config igmp_proxy downstream_if add vlan vlanid 2-7
Command: config igmp_proxy downstream_if add vlan vlanid 2-7

Success.

Zxxx0:admin#
```

## 35.4. config igmp\_proxy upstream\_if

---

### ● Description

This command is used to configure the setting for the IGMP proxy's upstream interface. The IGMP proxy plays the host role on the upstream interface. It will send IGMP report packets to the router port.

The source IP address determines the source IP address to be encoded in the IGMP protocol packet.

If the router port is empty, the upstream will send the IGMP protocol packet to all member ports on the upstream interface.

### ● Format

```
config igmp_proxy upstream_if {vlan [<vlan_name 32> | vlanid <vlanid 1-4094>] |
router_ports [add | delete] <portlist> | source_ip <ipaddr> |
unsolicited_report_interval <sec 0-25>} (1)
```

### ● Parameters

---

|               |                                                                                                                                 |
|---------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan</b>   | Specify the VLAN for the upstream interface.<br><b>&lt;vlan_name 32&gt;</b><br>Specify a VLAN name between 1 and 32 characters. |
| <b>vlanid</b> | Specify the VLAN ID for the upstream interface.<br><b>&lt;1-4094&gt;</b><br>Specify the VLAN ID between 1 and 4094.             |

---

|                         |                                                                          |
|-------------------------|--------------------------------------------------------------------------|
| <b>router_ports</b>     | Specify a list of ports that are connected to multicast-enabled routers. |
| <b>add</b>              | Specify to add the router ports.                                         |
| <b>delete</b>           | Specify to delete the router ports.                                      |
| <b>&lt;portlist&gt;</b> | Specify a range of ports to be configured.                               |

---

|                  |                                                                                                                                                                                                            |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>source_ip</b> | Specify the source IP address of the upstream protocol packet. If it is not specified, zero IP address will be used as the protocol source IP address.<br><b>&lt;ipaddr&gt;</b><br>Specify the IP address. |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

|                                    |                                                                                                                                                                                                                                              |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>unsolicited_report_interval</b> | Specify the time between repetitions of the host's initial report of membership in a group. The default is 10 seconds. If set to 0, only one report packet is sent.<br><b>&lt;sec 0-25&gt;</b><br>Specify the time between 0 and 25 seconds. |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the router port of IGMP proxy's upstream interface:

```
Zxxx0:admin#config igmp_proxy upstream_if vlan default router_ports add 3
Command: config igmp_proxy upstream_if vlan default router_ports add 3

Success.

Zxxx0:admin#
```

## 35.5. show igmp\_proxy

---

### ● Description

This command displays IGMP proxy configuration information or group information on the Switching Hub. The display status item means group entry is determined by whether or not the chip is inserted.

### ● Format

**show igmp\_proxy {group}**

### ● Parameters

---

|              |                                           |
|--------------|-------------------------------------------|
| <b>group</b> | (Optional) Specify the group information. |
|--------------|-------------------------------------------|

---

---

**NOTE** If the group is not specified, the IGMP proxy configuration will be displayed.

---

### ● Restrictions

None.

## 35. IGMP Proxy Commands

### ● Example

To display IGMP proxy information:

```
Zxxx0:admin#show igmp_proxy
Command: show igmp_proxy

IGMP Proxy Global State      : Enabled

Upstream Interface
VLAN ID                     : 1
Dynamic Router Ports        : 1-4
Static Router Ports         : 5-6
Unsolicited Report Interval : 10
Source IP Address           : 0.0.0.0

Downstream Interface
VLAN List                   : 2-4

Zxxx0:admin#
```

To display the IGMP proxy's group information:

```
Zxxx0:admin#show igmp_proxy group
Command: show igmp_proxy group

Dest-V : The destination VLAN.
A       : Active
I       : Inactive

Dest IP      Source IP  Dest-V  Member Ports  Status
-----
224.2.2.2    NULL      4       3, 6          A
              2       2-4          I
227.3.1.5    NULL      2       2, 5, 8       I
              3       5, 7, 9      A

Total Entries: 2

Zxxx0:admin#
```

## 36.IGMP Snooping Commands

IGMP (Internet Group Management Protocol) is a protocol to manage multicast groups.

IGMP snooping is a filtering function to monitor IGMP packets flowing on ports of the Switching Hub and prevent data from flowing to unnecessary ports. This filtering function allows to efficiently process a large amount of data, such as video distribution.

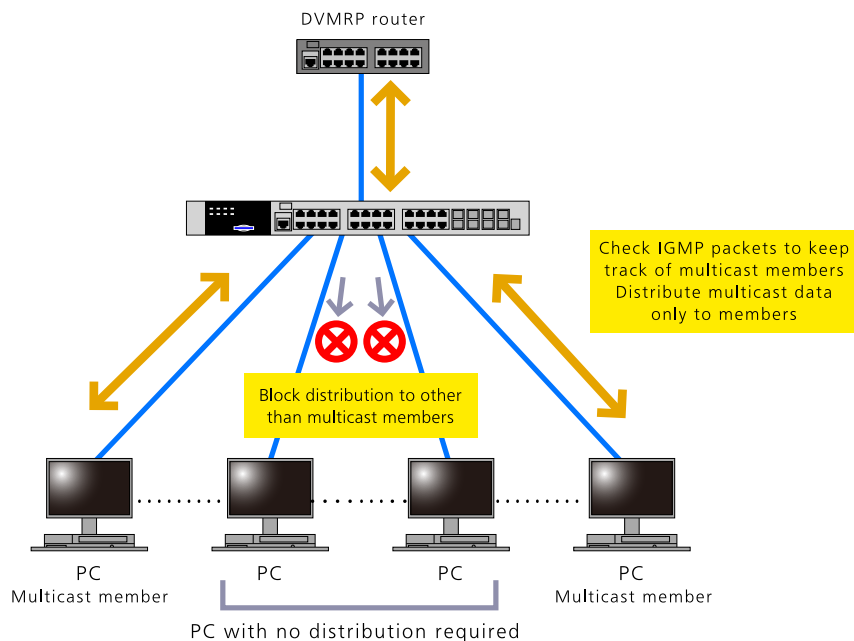


Figure 36-1 IGMP Snooping overview

```

config igmp_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable |
  disable] | fast_leave [enable | disable] | proxy_reporting {state [enable | disable] | source_ip
  <ipaddr>}(1)}
config igmp_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all]
  {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value
  1-7> | last_member_query_interval <sec 1-25> | state [enable | disable] | version <value 1-
  3>}(1)
config router_ports [<vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>
config router_ports forbidden [<vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>
enable igmp_snooping
disable igmp_snooping
show igmp_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}
show igmp_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>]
  {<ipaddr>}}
config igmp_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>] [<value 1-1000> | no_limit]
show igmp_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>]
create igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>
  
```

## 36. IGMP Snooping Commands

---

```
config igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr> [add |
delete] <portlist>
delete igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>
show igmp_snooping static_group {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>}
show igmp_snooping statistic counter [vlan <vlan_name 32> | vlanid <vlanid_list> | ports
<portlist>]
clear igmp_snooping statistics counter
show igmp_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}
show router_ports [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static | dynamic |
forbidden]}
config igmp_snooping unknow_data_learning [all | vlan_name <vlan_name 32> | vlanid
<vlanid_list>] {state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-
65535>}
config igmp_snooping unknow_data_learning max_learned_entry <value 1-1024>
clear igmp_snooping data_learning_group [all | [vlan_name <vlan_name 32> | vlanid <vlanid_list>]
[<ipaddr> | all]]
```

---

### 36.1. config igmp\_snooping

---

#### ● Description

This command is used to configure IGMP snooping on the Switching Hub.

#### ● Format

```
config igmp_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state
[enable | disable] | fast_leave [enable | disable] | proxy_reporting {state [enable |
disable] | source_ip <ipaddr>}(1)}
```

#### ● Parameters

---

|                  |                                                                                                                                                                                    |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan_name</b> | Specify the name of the VLAN for which IGMP snooping is to be configured.<br><b>&lt;vlan_name 32&gt;</b><br>Specify the VLAN name. The maximum length is 32 characters.            |
| <b>vlanid</b>    | Specify the VLAN ID list.<br><b>&lt;vlanid_list&gt;</b><br>Specify the VLAN ID list.                                                                                               |
| <b>all</b>       | Specify to configure all VLANs.                                                                                                                                                    |
| <b>state</b>     | Enable or disable IGMP snooping for the chosen VLAN.<br><b>enable</b><br>Enable IGMP snooping for the chosen VLAN.<br><b>disable</b><br>Disable IGMP snooping for the chosen VLAN. |

---

**fast\_leave**

Enable or disable the IGMP snooping fast leave function. If enabled, the membership is immediately removed when the system receive the IGMP leave message.

**enable**

Enable the IGMP snooping fast leave function.

**disable**

Disable the IGMP snooping fast leave function.

**proxy\_reporting**

Specifies the proxy reporting option.

**state** Specifies the proxy reporting state.

**enable**

Specifies that the proxy reporting option will be enabled.

**disable**

Specifies that the proxy reporting option will be disabled.

**source\_ip**

Specifies the source IP address used.

**<ipaddr>**

Enter the source IP addres used here.

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure IGMP snooping:

```
Zxxx0:admin#config igmp_snooping vlan_name default state enable fast_leave enable
Command: config igmp_snooping vlan_name default state enable fast_leave enable

Success.

Zxxx0:admin#
```

## 36.2. config igmp\_snooping querier

### ● Description

This command is used to configure the IGMP snooping querier.

### ● Format

```
config igmp_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all]
{query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable
<value 1-7> | last_member_query_interval <sec 1-25> | state [enable | disable] |
version <value 1-3>} (1)
```



## 36. IGMP Snooping Commands

### ● Parameters

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan_name</b>                  | Specify the name of the VLAN for which IGMP snooping querier is to be configured.<br><b>&lt;vlan_name 32&gt;</b><br>Specify the VLAN name. The maximum length is 32 characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>vlanid</b>                     | Specify the VLAN ID list.<br><b>&lt;vlanid_list&gt;</b><br>Specify the VLAN ID list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>all</b>                        | Specify to configure all VLANs and VLAN IDs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>query_interval</b>             | Specify the amount of time in seconds between general query transmissions.<br><b>&lt;sec 1-65535&gt;</b><br>Specify the amount of time in seconds between general query transmissions. The default setting is 125 seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>max_response_time</b>          | Specify the maximum time in seconds to wait for reports from members.<br><b>&lt;sec 1-25&gt;</b><br>Specify the maximum time in seconds to wait for reports from members. The default setting is 10 seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>robustness_variable</b>        | <p>Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following IGMP message intervals:</p> <ul style="list-style-type: none"><li>• Group member interval - Amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows:<br/><br/><math display="block">(\text{robustness variable} \times \text{query interval}) + (1 \times \text{query response interval}).</math></li><li>• Other querier present interval - Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows:<br/><br/><math display="block">(\text{robustness variable} \times \text{query interval}) + (0.5 \times \text{query response interval}).</math></li><li>• 3.Last member query count - Number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable.</li></ul> <b>&lt;value 1-7&gt;</b><br>Specify the value between 1 and 7. Increase the value if you expect a subnet to be lossy. The robustness variable is set to 2 by default. |
| <b>last_member_query_interval</b> | Specify the maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last member of a group.<br><b>&lt;sec 1-25&gt;</b><br>Specify the time between 1 and 25 seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>state</b>   | <p>If the state is enable, it allows the Switching Hub to be selected as a IGMP Querier (sends IGMP query packets). If the state is disabled, then the Switching Hub can not play the role as a querier. Note that if the Layer 3 router connected to the Switching Hub provides only the IGMP proxy function but does not provide the multicast routing function, then this state must be configured as disabled. Otherwise, if the Layer 3 router is not selected as the querier, it will not send the IGMP query packet. Since it will not also send the multicast-routing protocol packet, the port will be timed out as a router port.</p> <p><b>enable</b><br/>Allows the Switching Hub to be selected as an IGMP Querier (sends IGMP query packets).</p> <p><b>disable</b><br/>When disabled, the Switching Hub can not play the role as a querier.</p> |
| <b>version</b> | <p>Specify the version of IGMP packet that will be sent by this port. If a IGMP packet received by the interface has a version higher than the specified version, this packet will be forward from the router's ports or VLAN flooding.</p> <p><b>&lt;value 1-3&gt;</b><br/>Specify the values between 1 and 3.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the IGMP snooping querier:

```
Zxxx0:admin#config igmp_snooping querier vlan_name default query_interval 125
state enable
Command: config igmp_snooping querier vlan_name default query_interval 125 state
enable

Success.

Zxxx0:admin#
```

## 36.3. config router\_ports

### ● Description

This command is used to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router, regardless of protocol.

### ● Format

config router\_ports [<vlan\_name 32> | vlanid <vlanid\_list>] [add | delete] <portlist>

### ● Parameters

**<vlan\_name 32>**  
Specify the name of the VLAN on which the router port resides.

## 36. IGMP Snooping Commands

|                         |                                                                                      |
|-------------------------|--------------------------------------------------------------------------------------|
| <b>vlanid</b>           | Specify the VLAN ID list.<br><b>&lt;vlanid_list&gt;</b><br>Specify the VLAN ID list. |
| <b>add</b>              | Specify to add the router ports.                                                     |
| <b>delete</b>           | Specify to delete the router ports.                                                  |
| <b>&lt;portlist&gt;</b> | Specify a range of ports to be configured.                                           |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To set up static router ports:

```
Zxxx0:admin#config router_ports default add 1-10
Command: config router_ports default add 1-10

Success.

Zxxx0:admin#
```

## 36.4. config router\_ports\_forbidden

### ● Description

This command is used to designate a range of ports as being not connected to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.

### ● Format

**config router\_ports\_forbidden [<vlan\_name 32> | vlanid <vlanid\_list>] [add | delete] <portlist>**

### ● Parameters

|                             |                                                                                      |
|-----------------------------|--------------------------------------------------------------------------------------|
| <b>&lt;vlan_name 32&gt;</b> | Specify the name of the VLAN on which the router port resides.                       |
| <b>vlanid</b>               | Specify the VLAN ID list.<br><b>&lt;vlanid_list&gt;</b><br>Specify the VLAN ID list. |
| <b>add</b>                  | Specify to add the router ports.                                                     |
| <b>delete</b>               | Specify to delete the router ports.                                                  |
| <b>&lt;portlist&gt;</b>     | Specify a range of ports to be configured.                                           |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To set up port range 1 to 7 to be forbidden router ports of the default VLAN:

```
Zxxx0:admin#config router_ports_forbidden default add 1-7
Command: config router_ports_forbidden default add 1-7

Success.

Zxxx0:admin#
```

## 36.5. enable igmp\_snooping

---

- **Description**

This command allows you to enable IGMP snooping on the Switching Hub.

- **Format**

enable igmp\_snooping

- **Parameters**

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To enable IGMP snooping on the Switching Hub:

```
Zxxx0:admin#enable igmp_snooping
Command: enable igmp_snooping

Success.

Zxxx0:admin#
```

## 36.6. disable igmp\_snooping

---

- **Description**

This command is used to disable IGMP snooping on the Switching Hub. IGMP snooping can be disabled only if IP multicast routing is not being used. Disabling IGMP snooping allows all IGMP and IP multicast traffic to flood within a given IP interface.

- **Format**

disable igmp\_snooping

- **Parameters**

None.

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To disable IGMP snooping:

```
Zxxx0:admin#disable igmp_snooping
Command: disable igmp_snooping

Success.

Zxxx0:admin#
```

# 36.7. show igmp\_snooping

## ● Description

This command is used to display the current IGMP snooping configuration on the Switching Hub.

## ● Format

show igmp\_snooping {[vlan <vlan\_name 32> | vlanid <vlanid\_list>]}

## ● Parameters

|               |                                                                                                                                                                      |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan</b>   | (Optional) Specify the name of the VLAN to display the IGMP snooping configuration.<br><vlan_name 32><br>Specify the VLAN name. The maximum length is 32 characters. |
| <b>vlanid</b> | (Optional) Specify the VLAN ID to display the IGMP snooping configuration.<br><vlanid_list><br>Specify a range of VLAN IDs.                                          |

---

**NOTE** If no parameter is specified, the system will display all current IGMP snooping configuration.

---

## ● Restrictions

None.

## ● Example

To show IGMP snooping:

## 36. IGMP Snooping Commands

```
Zxxx0:admin#show igmp_snooping
Command: show igmp_snooping

IGMP Snooping Global State           : Disabled

VLAN Name                           : default
Query Interval                       : 125
Max Response Time                     : 10
Robustness Value                     : 2
Last Member Query Interval           : 1
Querier State                        : Disable
Querier Role                         : Non-Querier
Querier IP                           : 0.0.0.0
Querier Expiry Time                  : 0 secs
State                               : Disable
Fast Leave                          : Disable
Proxy Reporting                      : Enable
Proxy Reporting Source IP            : 0.0.0.0
Rate Limit                          : No Limitation
Version                             : 3

Total Entries: 1

Zxxx0:admin#
```

### 36.8. show igmp\_snooping group

#### ● Description

This command is used to display the current IGMP snooping group configuration on the Switching Hub.

#### ● Format

**show igmp\_snooping group** {[vlan <vlan\_name 32> | vlanid <vlanid\_list> | ports <portlist>] {<ipaddr>}}

#### ● Parameters

|               |                                                                                                                                                                                                                 |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan</b>   | (Optional) Specify the name of the VLAN for which you want to view IGMP snooping group configuration information.<br><b>&lt;vlan_name 32&gt;</b><br>Specify the VLAN name. The maximum length is 32 characters. |
| <b>vlanid</b> | (Optional) Specify the ID of the VLAN for which to view IGMP snooping group information.<br><b>&lt;vlanid_list&gt;</b><br>Specify the VLAN ID list.                                                             |
| <b>ports</b>  | (Optional) Specify the list of ports for which to view IGMP snooping group information.<br><b>&lt;portlist&gt;</b><br>Specify a range of ports to be configured.                                                |

---

**<ipaddr>**(Optional) Specify the group IP address for which to view IGMP snooping group information.

---



---

**NOTE** If no parameter is specified, the system will display all of the current IGMP snooping group configuration of the Switching Hub.

---

## ● Restrictions

None.

## ● Example

To display IGMP snooping groups:

```
Zxxx0:admin#show igmp_snooping group
Command: show igmp_snooping group

Source/Group      : NULL / 224.106.0.211
VLAN Name/VID     : default/1
Member Ports      : 1
UP Time           : 223
Expiry Time       : 37
Filter Mode       : EXCLUDE

Source/Group      : NULL / 234.54.163.75
VLAN Name/VID     : default/1
Member Ports      : 1
UP Time           : 223
Expiry Time       : 37
Filter Mode       : EXCLUDE

Source/Group      : 110.56.32.100 / 235.10.160.5
VLAN Name/VID     : default/1
Member Ports      : 2
UP Time           : 221
Expiry Time       : 0
Filter Mode       : EXCLUDE

Total Entries : 3

Zxxx0:admin#
```



### 36.9. **config igmp\_snooping rate\_limit**

---

#### ● Description

This command is used to configure the upper limit per second for ingress IGMP control packets.

#### ● Format

**config igmp\_snooping rate\_limit [ports <portlist> | vlanid <vlanid\_list>] [<value 1-1000> | no\_limit]**

#### ● Parameters

|                             |                                                                                                                                                                                                            |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ports</b>                | Specify a range of ports to be configured.<br><b>&lt;portlist&gt;</b><br>Specify a range of ports to be configured.                                                                                        |
| <b>vlanid</b>               | Specify a range of VLANs to be configured.<br><b>&lt;vlanid_list&gt;</b><br>Specify the VLAN ID list.                                                                                                      |
| <b>&lt;value 1-1000&gt;</b> | Specify the rate of IGMP control packets that the Switching Hub can process on a specific port/VLAN. The rate is specified in packet per second. The packets that exceed the limited rate will be dropped. |
| <b>no_limit</b>             | The default setting is no limit.                                                                                                                                                                           |

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To configure the IGMP snooping rate limit for ports 1-2 to have no limit:

```
Zxxx0:admin#config igmp_snooping rate_limit ports 1-2 no_limit
Command: config igmp_snooping rate_limit ports 1-2 no_limit

Success.

Zxxx0:admin#
```

## 36.10. show igmp\_snooping rate\_limit

### ● Description

This command is used to display the IGMP snooping rate limit setting.

### ● Format

**show igmp\_snooping rate\_limit** [**ports** <portlist> | **vlanid** <vlanid\_list>]

### ● Parameters

|               |                                                            |
|---------------|------------------------------------------------------------|
| <b>ports</b>  | Specify a range of ports to be displayed.<br><portlist>    |
|               | Specify a range of ports to be displayed.                  |
| <b>vlanid</b> | Specify a range of VLANs to be displayed.<br><vlanid_list> |
|               | Specify the VLAN ID list.                                  |

### ● Restrictions

None.

### ● Example

To display the IGMP snooping rate limit for ports 1-2:

```
Zxxx0:admin#show igmp_snooping rate_limit ports 1-2
Command: show igmp_snooping rate_limit ports 1-2

Port      Rate Limit
-----
1          No Limit
2          No Limit

Total Entries: 2
Zxxx0:admin#
```

## 36.11. create igmp\_snooping static\_group

### ● Description

This command allows users to create an IGMP snooping static group. Member ports can be added to the static group. The static member and the dynamic member port form the member ports of a group. The static group will only take effect when IGMP snooping is enabled on the VLAN. For those static member ports, the device needs to emulate the IGMP protocol operation to the querier, and forward the traffic destined to the multicast group to the member ports.

For a layer 3 device, the device is also responsible to route the packet destined for this specific group to static member ports. The static member port will only affect V2 IGMP operation. The Reserved IP multicast address 224.0.0.X must be excluded from the configured group. The VLAN must be created first before a static group can be created.

### ● Format

**create igmp\_snooping static\_group [vlan <vlan\_name 32> | vlanid <vlanid\_list>]  
<ipaddr>**

### ● Parameters

|                       |                                                                                                                                                              |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan</b>           | Specify the name of the VLAN on which the router port resides.<br><b>&lt;vlan_name 32&gt;</b><br>Specify the VLAN name. The maximum length is 32 characters. |
| <b>vlanid</b>         | Specify the VLAN ID list.<br><b>&lt;vlanid_list&gt;</b><br>Specify the VLAN ID list.                                                                         |
| <b>&lt;ipaddr&gt;</b> | Specify the multicast group IP address (for Layer 3 Switching Hub).                                                                                          |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create an IGMP snooping static group on default VLAN, group 239.1.1.1:

```
Zxxx0:admin#create igmp_snooping static_group vlan default 239.1.1.1
Command: create igmp_snooping static_group vlan default 239.1.1.1

Success.

Zxxx0:admin#
```

## 36.12. config igmp\_snooping static\_group

### ● Description

This command is used to configure an IGMP snooping static group on the Switching Hub. When a port is configured as a static member port, the IGMP protocol will not operate on this port. Therefore, suppose that a port is a dynamic member port learned by IGMP. If this port is configured as a static member later, then the IGMP protocol will stop operating on this port. The IGMP protocol will resume once this port is removed from static member ports. The static member port will only affect V2 IGMP operation.

### ● Format

config igmp\_snooping static\_group [vlan <vlan\_name 32> | vlanid <vlanid\_list>]  
<ipaddr> [add | delete] <portlist>

### ● Parameters

|                         |                                                                                                                                                  |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan</b>             | Specify the name of the VLAN on which the static group resides.<br><vlan_name 32><br>Specify the VLAN name. The maximum length is 32 characters. |
| <b>vlanid</b>           | Specify the ID of the VLAN on which the static group resides.<br><vlanid_list><br>Specify the VLAN ID list.                                      |
| <b>&lt;ipaddr&gt;</b>   | Specify the multicast group IP address (for Layer 3 Switching Hub).                                                                              |
| <b>add</b>              | Specify to add the member ports.                                                                                                                 |
| <b>delete</b>           | Specify to delete the member ports.                                                                                                              |
| <b>&lt;portlist&gt;</b> | Specify a range of ports to be configured.                                                                                                       |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To add port 9 to 10 to be IGMP snooping static member ports for group 239.1.1.1 on default VLAN:

```
Zxxx0:admin#config igmp_snooping static_group vlan default 239.1.1.1 add 9-10
Command: config igmp_snooping static_group vlan default 239.1.1.1 add 9-10

Success.

Zxxx0:admin#
```

### 36.13. delete igmp\_snooping static\_group

#### ● Description

This command is used to delete an IGMP snooping static group on the Switching Hub. The deletion of an IGMP snooping static group will not affect the IGMP snooping dynamic member ports for a group.

#### ● Format

**delete igmp\_snooping static\_group [vlan <vlan\_name 32> | vlanid <vlanid\_list>]  
<ipaddr>**

#### ● Parameters

|                       |                                                                                                                                                              |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan</b>           | Specify the name of the VLAN on which the router port resides.<br><b>&lt;vlan_name 32&gt;</b><br>Specify the VLAN name. The maximum length is 32 characters. |
| <b>vlanid</b>         | Specify the VLAN ID list on which the router port resides.<br><b>&lt;vlanid_list&gt;</b><br>Specify the VLAN ID list.                                        |
| <b>&lt;ipaddr&gt;</b> | Specify the multicast group IP address (for Layer 3 Switching Hub).                                                                                          |

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To delete an IGMP snooping static group from the default VLAN, group 239.1.1.1:

```
Zxxx0:admin#delete igmp_snooping static_group vlan default 239.1.1.1
Command: delete igmp_snooping static_group vlan default 239.1.1.1

Success.

Zxxx0:admin#
```

## 36.14. show igmp\_snooping static\_group

### ● Description

This command is used to display the IGMP snooping static multicast group.

### ● Format

**show igmp\_snooping static\_group** {[vlan <vlan\_name 32> | vlanid <vlanid\_list>]  
<ipaddr>}

### ● Parameters

|                       |                                                                                                                                                 |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan</b>           | Specify the name of the VLAN on which the router port resides.<br><vlan_name 32><br>Specify the VLAN name. The maximum length is 32 characters. |
| <b>vlanid</b>         | Specify the VLAN ID list on which the router port resides.<br><vlanid_list><br>Specify the VLAN ID list.                                        |
| <b>&lt;ipaddr&gt;</b> | Specify the multicast group IP address (for Layer 3 Switching Hub).                                                                             |

### ● Restrictions

None.

### ● Example

To display all the IGMP snooping static groups:

```
Zxxx0:admin#show igmp_snooping static_group
Command: show igmp_snooping static_group

VLAN ID/Name                IP Address      Static Member Ports
-----
1/Default                    239.1.1.1      9-10

Total Entries : 1

Zxxx0:admin#
```

## 36.15. show igmp\_snooping statistic counter

---

### ● Description

This command is used to display the IGMP snooping statistics counter for IGMP protocol packets that are transmitted or received by the Switching Hub since IGMP snooping was enabled.

### ● Format

**show igmp\_snooping statistic counter [vlan <vlan\_name 32> | vlanid <vlanid\_list> | ports <portlist>]**

### ● Parameters

---

|               |                                                                                                                               |
|---------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan</b>   | Specify a VLAN to be displayed.<br><b>&lt;vlan_name 32&gt;</b><br>Specify the VLAN name. The maximum length is 32 characters. |
| <b>vlanid</b> | Specify a list of VLANs to be displayed.<br><b>&lt;vlanid_list&gt;</b><br>Specify the VLAN ID list.                           |
| <b>ports</b>  | Specify a list of ports to be displayed.<br><b>&lt;portlist&gt;</b><br>Specify a list of ports.                               |

---

### ● Restrictions

None.

### ● Example

To display the IGMP snooping statistics counter for port 1:

## 36. IGMP Snooping Commands

```
Zxxx0:admin#show igmp_snooping statistic counter ports 1
Command: show igmp_snooping statistic counter ports 1
```

```
Port #           : 1
-----
```

```
Group Number     : 0
```

### Receive Statistics

#### Query

|                            |     |
|----------------------------|-----|
| IGMP v1 Query              | : 0 |
| IGMP v2 Query              | : 0 |
| IGMP v3 Query              | : 0 |
| Total                      | : 0 |
| Dropped By Rate Limitation | : 0 |
| Dropped By Multicast VLAN  | : 0 |

#### Report & Leave

|                                 |     |
|---------------------------------|-----|
| IGMP v1 Report                  | : 0 |
| IGMP v2 Report                  | : 0 |
| IGMP v3 Report                  | : 0 |
| IGMP v2 Leave                   | : 0 |
| Total                           | : 0 |
| Dropped By Rate Limitation      | : 0 |
| Dropped By Max Group Limitation | : 0 |
| Dropped By Group Filter         | : 0 |
| Dropped By Multicast VLAN       | : 0 |

### Transmit Statistics

#### Query

|               |     |
|---------------|-----|
| IGMP v1 Query | : 0 |
| IGMP v2 Query | : 0 |
| IGMP v3 Query | : 8 |
| Total         | : 8 |

#### Report & Leave

|                |     |
|----------------|-----|
| IGMP v1 Report | : 0 |
| IGMP v2 Report | : 0 |
| IGMP v3 Report | : 0 |
| IGMP v2 Leave  | : 0 |
| Total          | : 0 |

```
Total Entries : 1
```

```
Zxxx0:admin#
```



## **36.16. clear igmp\_snooping statistics counter**

### ● Description

This command is used to clear the IGMP snooping statistics counter on the Switching Hub.

### ● Format

**clear igmp\_snooping statistics counter**

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To clear the IGMP snooping statistic counter:

```
Zxxx0:admin#clear igmp_snooping statistics counter
Command: clear igmp_snooping statistics counter

Success.

Zxxx0:admin#
```

## **36.17. show igmp\_snooping forwarding**

### ● Description

This command is used to display the Switching Hub's current IGMP snooping forwarding table. It provides an easy way for users to check the list of ports that the multicast group comes from in terms of specific sources. The packets come from the source VLAN. They will be forwarded to the forwarding ports.

### ● Format

**show igmp\_snooping forwarding {[vlan <vlan\_name 32> | vlanid <vlanid\_list>]}**

### ● Parameters

---

|             |                                                                           |
|-------------|---------------------------------------------------------------------------|
| <b>vlan</b> | (Optional) Specify a VLAN to be displayed.<br><b>&lt;vlan_name 32&gt;</b> |
|             | Specify the VLAN name. The maximum length is 32 characters.               |

---

---

**vlanid** (Optional) Specify a list of VLANs to be displayed.  
**<vlanid\_list>**  
 Specify the VLAN ID list.

---



---

**NOTE** If no parameter is specified, the system will display all current IGMP snooping forwarding table entries of the Switching Hub.

---

## ● Restrictions

None.

## ● Example

To display all IGMP snooping forwarding entries located on the Switching Hub:

```
Zxxx0:admin#show igmp_snooping forwarding
Command: show igmp_snooping forwarding

VLAN Name      : default
Source IP       : 10.90.90.114
Multicast Group : 225.0.0.0
Port Member    : 2,7

VLAN Name      : default
Source IP       : 10.90.90.10
Multicast Group : 225.0.0.1
Port Member    : 2,5

Total Entries  : 2

Zxxx0:admin#
```

## 36.18. show router\_ports

---

### ● Description

This command is used to display the current router ports on the Switching Hub.

### ● Format

**show router\_ports** [vlan <vlan\_name 32> | vlanid <vlanid\_list> | all] {[static | dynamic | forbidden]}

### ● Parameters

---

**vlan** Specify the name of the VLAN on which the router port resides.  
**<vlan\_name 32>**  
 Specify the VLAN name. The maximum length is 32 characters.

---

## 36. IGMP Snooping Commands

|                  |                                                                                                                         |
|------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>vlanid</b>    | Specify the ID of the VLAN on which the router port resides.<br><b>&lt;vlanid_list&gt;</b><br>Specify the VLAN ID list. |
| <b>all</b>       | Specifies that all the VLAN's will be displayed.                                                                        |
| <b>static</b>    | (Optional) Display router ports that have been statically configured.                                                   |
| <b>dynamic</b>   | (Optional) Display router ports that have been dynamically registered.                                                  |
| <b>forbidden</b> | (Optional) Display forbidden router ports that have been statically configured.                                         |

**NOTE** If no parameter is specified, the system will display all the current router ports on the Switch.

### ● Restrictions

None.

### ● Example

To display the router ports on the default VLAN:

```
Zxxx0:admin#show router_ports vlan default
Command: show router_ports vlan default

VLAN Name           : default
Static Router Port   :
Dynamic Router Port  :
Router IP            :
Forbidden Router Port:

Total Entries: 1

Zxxx0:admin#
```

## 37. IP Multicasting Commands

The commands are used to display multicast routing information stored in this Switching Hub. IP multicast forwarding table and IP multicast forwarding cache information are displayed.

You can display the IP multicast forwarding table with routing protocols (DVMRP, PIM) and currently disabled items specified.

```
Interface --- IP Address ----- Multicast Routing↵
-----↵
System ----- 10.90.90.90 ----- INACT↵
n1 ----- 1.3.2.3 ----- PIM-SM -----↵
n2 ----- 2.3.2.3 ----- PIM-SM-DM -----↵
n3 ----- 3.3.2.3 ----- PIM-DM -----↵
n4 ----- 4.3.2.3 ----- DVMRP -----↵
```

---

```
show ipmc {ipif <ipif_name 12> | protocol [inactive | dvmrp | pim]}
```

```
show ipmc cache {group <group>} {ipaddress <network_address>}
```

---

### 37.1. show ipmc

#### ● Description

This command is used to display the IP Multicast interface table.

#### ● Format

```
show ipmc {ipif <ipif_name 12> | protocol [inactive | dvmrp | pim]}
```

#### ● Parameters

---

|                 |                                                                                                                                                                      |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b>     | (Optional) Specifies the IP interface name used.<br><b>&lt;ipif_name 12&gt;</b><br>Enter the IP interface name used here. This name can be up to 12 characters long. |
| <b>protocol</b> | (Optional) Specifies which kind of routing protocol interface table will be displayed.                                                                               |
| <b>inactive</b> | Specifies that the protocol display will be inactive.                                                                                                                |
| <b>dvmrp</b>    | Specifies that the DVMRP protocol will be displayed.                                                                                                                 |
| <b>pim</b>      | Specifies that the PIM protocol will be displayed.                                                                                                                   |

---

## 37. IP Multicasting Commands

### ● Restrictions

None.

### ● Example

To display the IP Multicast interface table:

```
Zxxx0:admin# show ipmc
Command: show ipmc

Interface      IP Address      Multicast Routing
-----
System        10.90.90.90     INACT
n1            1.3.2.3         PIM-SM
n2            2.3.2.3         PIM-SM-DM
n3            3.3.2.3         PIM-DM
n4            4.3.2.3         DVMRP

Total Entries : 5

Zxxx0:admin#
```

## 37.2. show ipmc cache

### ● Description

This command is used to display the IP multicast forwarding cache.

### ● Format

**show ipmc cache {group <group>} {ipaddress <network\_address>}**

### ● Parameters

---

**group** (Optional) Specifies the multicast group.  
**<group>**

Enter the multicast group used here.

---

**ipaddress** (Optional) Specifies the IP address used.  
**<network\_address>**

Enter the IP address used here.

---

### ● Restrictions

None.

### ● Example

To display the IP multicast forwarding cache:

### 37. IP Multicasting Commands

```
Zxxx0:admin# show ipmc cache
```

```
Command: show ipmc cache
```

| Multicast<br>Group | Source<br>Address/Netmask | Upstream<br>Neighbor | Expire<br>Time | Routing<br>Protocol |
|--------------------|---------------------------|----------------------|----------------|---------------------|
| -----              | -----                     | -----                | -----          | -----               |
| 224.1.1.1          | 10.48.74.121/8            | 10.48.75.63          | 30             | DVMRP               |
| 224.1.1.1          | 20.48.74.25/8             | 20.48.75.25          | 20             | PIM_DM              |
| 224.1.2.3          | 10.48.75.3/8              | 10.48.76.6           | 30             | DVMRP               |

```
Total Entries : 3
```

```
Zxxx0:admin#
```

## 38. IP Routing Commands

IP routing is a process to transfer packets based on the destination IP address in TCP/IP network. Destination information is managed in a routing table in this Switching Hub.

In this chapter, you will display/delete a routing table and register items manually.

You can configure each table for IPv4 and IPv6.

### IPv4 routing table

| IP Address/Netmask | Gateway | Interface | Cost  | Protocol |
|--------------------|---------|-----------|-------|----------|
| -----              | -----   | -----     | ----- | -----    |
| 10.0.0.0/8         | 0.0.0.0 | System    | 1     | Local    |

### IPv6 routing table

|                    |                  |           |
|--------------------|------------------|-----------|
| IPv6 Prefix: ::/0  | Protocol: Static | Metric: 1 |
| Next Hop : FEC0::5 | IPIF : System    |           |

In addition, you can configure whether to use or not routing algorithm ECMP (Equal Cost Multi Path) for OSPF (Open Shortest Path First), a protocol that automatically determines routing.

```

create iproute [default | <network_address>] [null0 | <ipaddr> {<metric 1-65535>} {[primary |
  backup | weight <value 1-4>}]} | ip_tunnel <tunnel_name 12>]
delete iproute [default | <network_address>] [null0 | <ipaddr> | ip_tunnel <tunnel_name 12>]
show iproute {[<network_address> | <ipaddr>]} {[static | rip | ospf | hardware]}
create ipv6route [default | <ipv6networkaddr>] [[<ipif_name 12> <ipv6addr> | <ipv6addr>]
  {<metric 1-65535>} {[primary | backup]} | ip_tunnel <tunnel_name 12>]
delete ipv6route [[default | <ipv6networkaddr>] [<ipif_name 12> <ipv6addr> | <ipv6addr> |
  ip_tunnel <tunnel_name 12>] | all]
show ipv6route {[<ipv6networkaddr> | <ipv6addr>]} {[static | ospfv3 | hardware]}
enable ecmp ospf
disable ecmp ospf
config ecmp algorithm {ip_destination | [ip_source | crc_low | crc_high] | tcp_udp_port}
show ecmp algorithm

```

## 38.1. create iproute

---

### ● Description

This command is used to create an IP route entry in the Switching Hub's IP routing table. This command creates an IP route entry in the Switching Hub's IP routing table. "Primary" and "backup" are mutually exclusive. Users can select only one when creating one new route. If a user sets neither of these, the system will try to set the new route first by primary and second by backup and not set this route to be a multipath route.

### ● Format

```
create iproute [default | <network_address>] [null0 | <ipaddr> {<metric 1-65535>}
{[primary | backup | weight <value 1-4>}] | ip_tunnel <tunnel_name 12>]
```

### ● Parameters

|                                |                                                                                                                                                                                                                                                                 |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>default</b>                 | Create a default IP route entry.                                                                                                                                                                                                                                |
| <b>&lt;network_address&gt;</b> | The IP address and netmask of the IP interface that is the destination of the route. Specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/16).                                    |
| <b>null0</b>                   | Specifies the null interface as the next hop.                                                                                                                                                                                                                   |
| <b>&lt;ipaddr&gt;</b>          | Specify the IP address for the next hop router.                                                                                                                                                                                                                 |
| <b>&lt;metric 1-65535&gt;</b>  | (Optional) The default setting is 1. That is, the default hop cost is 1.                                                                                                                                                                                        |
| <b>primary</b>                 | (Optional) Specifies the route as the primary route to the destination.                                                                                                                                                                                         |
| <b>backup</b>                  | (Optional) Specifies the route as the backup route to the destination. If the route is not specified as the primary route or the backup route, then it will be auto-assigned by the system. The first created is the primary, the second created is the backup. |
| <b>weight</b>                  | (Optional) Specifies the weight value of the IP route.                                                                                                                                                                                                          |
| <b>&lt;value 1-4&gt;</b>       | Enter the weight value used here. This value must be between 1 and 4.                                                                                                                                                                                           |
| <b>ip_tunnel</b>               | Specifies the IP tunnel used.                                                                                                                                                                                                                                   |
| <b>&lt;tunnel_name 12&gt;</b>  | Enter the IP tunnel name used here. This name can be up to 12 characters long.                                                                                                                                                                                  |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To add a default route with a nexthop of 10.48.74.21:



## 38. IP Routing Commands

```
Zxxx0:admin#create iproute default 10.48.74.121
Command: create iproute default 10.48.74.121

Success.

Zxxx0:admin#
```

### 38.2. delete iproute

---

#### ● Description

This command is used to delete an IP route entry from the Switching Hub's IP routing table.

#### ● Format

**delete iproute** [default | <network\_address>] [null0 | <ipaddr> | ip\_tunnel <tunnel\_name 12>]

#### ● Parameters

---

**default** Delete a default IP route entry.

---

**<network\_address>**

The IP address and netmask of the IP interface that is the destination of the route. Specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8).

---

**null0** Specifies the null interface as the next hop.

---

**<ipaddr>** Specify the IP address for the next hop router.

---

**ip\_tunnel**

Specifies the IP tunnel used.

**<tunnel\_name 12>**

Enter the IP tunnel name used here. This name can be up to 12 characters long.

---

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To delete a default route from the routing table:

```
Zxxx0:admin#delete iproute default 10.48.74.121
Command: delete iproute default 10.48.74.121

Success.

Zxxx0:admin#
```

## 38.3. show iproute

### ● Description

This command is used to display the Switching Hub's current IP routing table.

### ● Format

**show iproute** {[<network\_address> | <ipaddr>]} {[static | rip | ospf | hardware]}

### ● Parameters

|                                |                                                                                                                                      |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;network_address&gt;</b> | (Optional) Specify the destination network address of the route want to be displayed.                                                |
| <b>&lt;ipaddr&gt;</b>          | (Optional) Specify the destination IP address of the route want to be displayed. The longest prefix matched route will be displayed. |
| <b>static</b>                  | (Optional) Specify to display only static routes. One static route may be active or inactive.                                        |
| <b>rip</b>                     | (Optional) Specify to display only RIP routes.                                                                                       |
| <b>ospf</b>                    | (Optional) Specify to display only OSPF routes.                                                                                      |
| <b>hardware</b>                | (Optional) Specify to display only the routes that have been written into the chip.                                                  |

### ● Restrictions

None.

### ● Example

To display the contents of the IP routing table:

```
Zxxx0:admin#show iproute
Command: show iproute

Routing Table

IP Address/Netmask  Gateway          Interface        Cost    Protocol
-----
10.0.0.0/8          0.0.0.0          System           1       Local

Total Entries : 1

Zxxx0:admin#
```

## 38.4. create ipv6route

### ● Description

This command is used to create an IPv6 static route in the Switching Hub's IP routing table. If the next hop is a global address, it is not necessary to indicate the interface name. If the next hop is a link local address, then the interface name must be specified.

### ● Format

```
create ipv6route [default | <ipv6networkaddr>] [[<ipif_name 12> <ipv6addr> |
<ipv6addr>] [<metric 1-65535>] {[primary | backup]} | ip_tunnel <tunnel_name 12>]
```

### ● Parameters

|                                              |                                                                                                                                                                                                                                                    |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>default</b>                               | Specify the default route.                                                                                                                                                                                                                         |
| <b>&lt;ipv6networkaddr&gt;</b>               | Specify the destination network for the route.                                                                                                                                                                                                     |
| <b>&lt;ipif_name 12&gt; &lt;ipv6addr&gt;</b> | Specify the interface for the route.                                                                                                                                                                                                               |
| <b>&lt;ipv6addr&gt;</b>                      | Specify the next hop address for this route.                                                                                                                                                                                                       |
| <b>&lt;metric 1-65535&gt;</b>                | (Optional) The default setting is 1.                                                                                                                                                                                                               |
| <b>primary</b>                               | (Optional) Specify the route as the primary route to the destination.                                                                                                                                                                              |
| <b>backup</b>                                | Specify the route as the backup route to the destination. If the route is not specified as the primary route or the backup route, then it will be auto-assigned by the system. The first created is the primary, the second created is the backup. |
| <b>ip_tunnel</b>                             | Specifies the IPv6 tunnel name used.                                                                                                                                                                                                               |
| <b>&lt;tunnel_name 12&gt;</b>                | Enter the IPv6 tunnel name used here. This name can be up to 12 characters long.                                                                                                                                                                   |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create an IPv6 default route:

```
Zxxx0:admin#create ipv6route default System FEC0::5
Command: create ipv6route default System FEC0::5

Success.

Zxxx0:admin#
```

# 38.5. delete ipv6route

## ● Description

This command is used to delete an IPv6 static route from the Switching Hub's IP routing table. If the next hop is a global address, it is not necessary to indicate the interface name. If the next hop is a link local address, then the interface name must be specified.

## ● Format

delete ipv6route [[default | <ipv6networkaddr>] [<ipif\_name 12> <ipv6addr> | <ipv6addr> | ip\_tunnel <tunnel\_name 12>] | all]

## ● Parameters

|                           |                                                                                  |
|---------------------------|----------------------------------------------------------------------------------|
| default                   | Specify the default route.                                                       |
| <ipv6networkaddr>         | Specify the IPv6 network address.                                                |
| <ipif_name 12> <ipv6addr> | Specify the IP interface name.                                                   |
| <ipv6addr>                | Specify the next hop address for the IPv6 route                                  |
| ip_tunnel                 | Specifies the IPv6 tunnel name used.                                             |
| <tunnel_name 12>          | Enter the IPv6 tunnel name used here. This name can be up to 12 characters long. |
| all                       | All static created routes will be deleted.                                       |

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To delete an IPv6 static route:

```
Zxxx0:admin#delete ipv6route default System FEC0::5
Command: delete ipv6route default System FEC0::5

Success.

Zxxx0:admin#
```

## 38.6. show ipv6route

---

### ● Description

This command is used to display the Switching Hub's current IPv6 routing table.

### ● Format

**show ipv6route** {[<ipv6networkaddr> | <ipv6addr>]} {[static | ospfv3 | hardware]}

### ● Parameters

---

**<ipv6networkaddr>**

Enter the IPv6 destination network address of the route.

---

**<ipv6addr>**

Enter the IPv6 address.

---

**static**     Display the static route entries.

---

**ospfv3**    Display the OSPFv3 route entries.

---

**hardware**

Display the route entries which have been written into hardware table.

---

### ● Restrictions

None.

### ● Example

To display an IPv6 route:

```
Zxxx0:admin#show ipv6route
Command: show ipv6route

IPv6 Prefix: ::/0                      Protocol: Static  Metric: 1
Next Hop   : FEC0::5                  IPIF      : System

Total Entries: 1

Zxxx0:admin#
```

## 38.7. enable ecmp ospf

---

### ● Description

This command is used to activate the OSPF ECMP function.

### ● Format

enable ecmp ospf

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable the OSPF ECMP function:

```
Zxxx0:admin# enable ecmp ospf
Command: enable ecmp ospf

Success.

Zxxx0:admin#
```

## 38.8. disable ecmp ospf

---

### ● Description

This command is used to disable the OSPF ECMP function.

### ● Format

disable ecmp ospf

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## 38. IP Routing Commands

### ● Example

To disable the OSPF ECMP function:

```
Zxxx0:admin# disable ecmp ospf
Command: disable ecmp ospf

Success.

Zxxx0:admin#
```

## 38.9. config ecmp algorithm

---

### ● Description

This command is used to configure the ECMP route load-balancing algorithm.

### ● Format

**config ecmp algorithm {ip\_destination | [ip\_source| crc\_low | crc\_high] | tcp\_udp\_port}**

### ● Parameters

---

**ip\_destination**

(Optional) Specifies that the ECMP algorithm will include the destination IP. It is set by default.

---

**ip\_source**

(Optional) Specifies that the ECMP algorithm will include the lower 5 bits of the source IP. This attribution is mutually exclusive with **crc\_low** and **crc\_high**. If it is set, **crc\_low** and **crc\_high** will be excluded. It is not set by default.

---

**crc\_low** (Optional) Specifies that the ECMP algorithm will include the lower 5 bits of the CRC. This attribution is mutually exclusive with **crc\_high** and **ip\_source**. If it is set, **crc\_high** and **ip\_source** will be excluded. It is set by default.

---

**crc\_high** (Optional) Specifies that the ECMP algorithm will include the upper 5 bits of the CRC. This attribution is mutually exclusive with **ip\_source** and **crc\_low**. If it is set, **crc\_low** and **ip\_source** will be excluded. It is not set by default.

---

**tcp\_udp\_port**

(Optional) Specifies that the ECMP algorithm will include the TCP or UDP port. It is not set by default.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To set the ECMP hash algorithm:

```
Zxxx0:admin# config ecmp algorithm ip_destination ip_source
Command: config ecmp algorithm ip_destination ip_source

Success.

Zxxx0:admin#
```

## 38.10. show ecmp algorithm

---

### ● Description

This command is used to display the ECMP related settings.

### ● Format

**show ecmp algorithm**

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To show current ECMP related settings:

```
Zxxx0:admin#show ecmp algorithm
Command: show ecmp algorithm

ECMP for OSPF : Enabled
ECMP Load Balance Algorithm :
  Destination IP : used.
  Source IP : not used.
  CRC_Low  : used.
  CRC_High : not used.
  TCP_UDP_Port : not used.

Zxxx0:admin#
```



## 39. IP Source Address Verify Commands

---

```

config ip_verify_source ports [<portlist> | all] state [enable | disable]
config arp_inspection ports [<portlist> | all] state [enable | disable]
create ip_source_binding ipaddress [<ipaddr>mac_address<macaddr> port <port>]
delete ip_source_binding [ipaddress<ipaddr>mac_address<macaddr> | all]
config ip_source_binding ipaddress [<ipaddr>mac_address<macaddr> port <port>]
show ip_source_binding [all | ipaddress<ipaddr>mac_address<macaddr>]
show ip_verify_source { ports {<portlist>} }
enable dhcp_snoop
disable dhcp_snoop
clear dhcp_snoop binding_entry ports [<portlist> | all]
show dhcp_snoop {[max_entry {ports <portlist>} | binding_entry {port <port>}}]
config dhcp_snoopmax_entry ports [<portlist> | all] limit [<value 1-n> | no_limit]
enable ip_verify_source log
disable ip_verify_source log

```

---

### 39.1. config ip\_verify\_source ports

#### ● Description

This command is used to configure the per port state of IPSG on the Switching Hub. If a port has been configured as group member of an aggregated link, then the IPSG function cannot be enabled. When the IPSG is enabled on the port, all IP packets will be checked. The legal IP packets will be forwarded, while the illegal IP packets will be dropped. All non-IP packets (L2 packets, ARP, etc.) will be forwarded by default.

#### ● Format

```
config ip_verify_source ports [<portlist> | all] state [enable | disable]
```

#### ● Parameters

---

**state**

**enable**

Enable the IPSG function. The legal IP packets will be forwarded, while the illegal IP packets will be dropped.

**disable**

Disable the IPSG function. The default value is **disable**.

---

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To enable IPSG on port1:

```
Zxxx0:admin# config ip_verify_source ports 1 state enable
Command: config ip_verify_source ports 1 state enable

Success.

Zxxx0:admin#
```

## 39.2. config arp\_inspection ports

### ● Description

This command is used to configure the per port state of dynamic ARP inspection on the Switching Hub. If a port has been configured as group member of an aggregated link, then the dynamic ARP inspection function cannot be enabled. When the dynamic ARP inspection is enabled on the port, all ARP packets will be checked under this mode. In this mode, the legal ARP packets will be forwarded, while the illegal packets will be dropped.

### ● Format

config arp\_inspection ports [<portlist> | all] state [enable | disable]

### ● Parameters

---

**state**

**enable**

Enable the dynamic ARP inspection function. The legal ARP packets will be forwarded, while the illegal ARP packets will be dropped.

**disable**

Disable the dynamic ARP inspection function. The default value is **disable**.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To enable dynamic ARP inspection on port1:

```
Zxxx0:admin# config arp_inspection ports 1 state enable
Command: config arp_inspection ports 1 state enable

Success.

Zxxx0:admin#
```

## 39.3. create ip\_source\_binding

---

### ● Description

This command is used to create an IPSG entry. One MAC address can be mapped to multiple IP addresses.

### ● Format

**create ip\_source\_binding ipaddress <ipaddr> mac\_address <macaddr> port <port>**

### ● Parameters

---

|               |                                                 |
|---------------|-------------------------------------------------|
| <b>ipaddr</b> | Specify the IP address used for the IPSG entry. |
|---------------|-------------------------------------------------|

---

|                |                                                  |
|----------------|--------------------------------------------------|
| <b>macaddr</b> | Specify the MAC address used for the IPSG entry. |
|----------------|--------------------------------------------------|

---

|             |                                                |
|-------------|------------------------------------------------|
| <b>port</b> | Specify the port that the entry will apply to. |
|-------------|------------------------------------------------|

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create an IPSG entry that binds the IP address 10.1.1.1 to the MAC address 00-00-00-00-00-11 on port 3:

```
Zxxx0:admin# create ip_source_binding ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11 port 3
Command: create ip_source_binding ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11 port 3

Success

Zxxx0:admin#
```

## 39.4. delete ip\_source\_binding

---

### ● Description

This command is used to create an to delete an IPSG entry.

### ● Format

**delete ip\_source\_binding [ipaddress <ipaddr> mac\_address <macaddr> | all]**

### ● Parameters

|                |                                         |
|----------------|-----------------------------------------|
| <b>ipaddr</b>  | Specify the IP address of the entry.    |
| <b>macaddr</b> | Specify the MAC address of the entry.   |
| <b>all</b>     | Delete all IPSG manual binding entries. |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete an IPSG entry that binds the IP address 10.1.1.1 to the MAC address 00-00-00-00-11:

```
Zxxx0:admin# delete ip_source_binding ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11
Command: delete ip_source_binding ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11

Success.

Zxxx0:admin#
```

## 39.5. config ip\_source\_binding

---

### ● Description

This command is used to update an IPSG entry.

### ● Format

**config ip\_source\_binding ipaddress <ipaddr> mac\_address <macaddr> port <port>]**

### ● Parameters

---

**ipaddr** Specify the IP address of the entry being updated.

---

**macaddr** Specify the MAC address of the entry being updated.

---

**ports** Specify which ports that will use the updated IPSG entry.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure an IPSG entry so that the IP address 10.1.1.1 is bound to the MAC address 00-00-00-00-00-11 on port 10:

```
Zxxx0:admin# config address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11 port 10
Command: config address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11 port 10

Success.

Zxxx0:admin#
```

## 39.6. show ip\_source\_binding

### ● Description

This command is used to show the binding entries.

### ● Format

**show ip\_source\_binding** [**all** | **ipaddress** <ipaddr> **mac\_address** <macaddr>]

### ● Parameters

---

**ipaddr** Specify the learned IP address of the entry in the database.

---

**macaddr** Specify the MAC address of the entry or the blocked MAC address.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To show the binding entries:

The ACL status will display regardless of whether the hardware ACL is active or not.

```
Zxxx0:admin# show ip_source_binding all
Command: show ip_source_binding all

M(Mode) - D:DHCP,S:Static    ACL - A:Active I:Inactive

IP Address                      MAC Address      M  ACL Port
-----
10.1.1.1                        00-00-00-00-00-11 S  I    3
10.1.1.2                        00-00-00-00-00-12 S  A    1
10.1.1.10                       00-00-00-00-00-aa D  A    1

Total Entries : 3

Zxxx0:admin#
```

## 39. IP Source Address Verify Commands

To display the binding entry by IP address and MAC address:

```
Zxxx0:admin# show ip_source_binding ipaddress10.1.1.1 mac_address 00-00-00-00-00-11
Command: show ip_source_binding ipaddress10.1.1.1 mac_address 00-00-00-00-00-11

M(Mode) - D:DHCP,S:Static   ACL - A:Active I:Inactive

IP Address                      MAC Address          M  ACL Port
-----
10.1.1.1                        00-00-00-00-00-11  S  I    3

Total Entries : 1

Zxxx0:admin#
```

### 39.7. show ip\_verify\_source

#### ● Description

This command is used to show the IP Source Address Verify information.

#### ● Format

`show ip_verify_source { ports {<portlist>} }`

#### ● Parameters

|              |                                                                                                              |
|--------------|--------------------------------------------------------------------------------------------------------------|
| <b>ports</b> | Specify the ports that the information will be displayed for. If not specified, all ports will be displayed. |
|--------------|--------------------------------------------------------------------------------------------------------------|

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To show the IP Source Address Verify global configuration:

```
Zxxx0:admin# show ip_verify_source
Command: show ip_verify_source

Log           : Enabled
DHCP Snoop    : Disabled

Zxxx0:admin#
```

To show the IP Source Address Verify ports:

```
Zxxx0:admin# show ip_verify_source ports
Command: show ip_verify_source ports
```

| Port | ARP Inspection | IP Verify Source |
|------|----------------|------------------|
| 1    | Disabled       | Disabled         |
| 2    | Enabled        | Disabled         |
| 3    | Enabled        | Enabled          |
| 4    | Disabled       | Disabled         |
| 5    | Disabled       | Enabled          |
| 6    | Disabled       | Enabled          |
| 7    | Disabled       | Enabled          |
| 8    | Disabled       | Disabled         |
| 9    | Disabled       | Disabled         |
| 10   | Disabled       | Disabled         |
| 11   | Disabled       | Enabled          |
| 12   | Disabled       | Enabled          |

```
Zxxx0:admin#
```

## 39.8. enable dhcp\_snoop

---

### ● Description

This command is used to enable DHCP snooping. By default, DHCP snooping is disabled. If a user enables DHCP snooping, Switching Hub will learn the IP address through the DHCP packets and build up the DHCP binding entries on the ports that either IP Source Guard or Dynamic ARP Inspection enabled.

### ● Format

**enable dhcp\_snoop**

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.



## 39. IP Source Address Verify Commands

### ● Example

To enable DHCP snooping mode:

```
Zxxx0:admin# admin# enable dhcp_snoop
Command: enable dhcp_snoop

Success.

Zxxx0:admin#
```

## 39.9. disable dhcp\_snoop

---

### ● Description

This command is used to disable DHCP snooping.

When the DHCP snooping function is disabled, all of the DHCP snooping binding entries will be removed.

### ● Format

**disable dhcp\_snoop**

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To disable DHCP snooping mode:

```
Zxxx0:admin# disable dhcp_snoop
Command: disable dhcp_snoop

Success.

Zxxx0:admin#
```

## 39.10. clear dhcp\_snoop binding\_entry

---

### ● Description

This command is used to clear the DHCP Snooping entries learned for the specified ports.

### ● Format

**clear dhcp\_snoop binding\_entry ports [<portlist>|all]**

### ● Parameters

---

|              |                                                                            |
|--------------|----------------------------------------------------------------------------|
| <b>ports</b> | Specify the list of ports used to clear the DHCP snooping entries learned. |
|--------------|----------------------------------------------------------------------------|

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To clear the DHCP snooping entries on ports 1-3:

```
Zxxx0:admin# clear dhcp_snoop binding_entry ports 1-3
Command: clear dhcp_snoop binding_entry ports 1-3

Success.

Zxxx0:admin#
```

## 39.11. show dhcp\_snoop

---

### ● Description

This command is used to show all the DHCP snooping configuration and learning databases.

### ● Format

**show dhcp\_snoop {[max\_entry {ports <portlist>} | binding\_entry {port <port>}}]**

### ● Parameters

---

|                      |                                                                                                                      |
|----------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>max_entry</b>     | Display the maximum number of entries per port.                                                                      |
| <b>binding_entry</b> | Display the DHCP snooping binding entries on ports. If no ports are specified all binding entries will be displayed. |

---

## 39. IP Source Address Verify Commands

---

If no parameters are specified, all the DHCP snooping configuration.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To show the DHCP snooping state:

```
Zxxx0:admin# show dhcp_snoop
Command: show dhcp_snoop

DHCP_Snoop : Enabled

Zxxx0:admin#
```

To display the DHCP snooping maximum entry configuration:

```
Zxxx0:admin# show dhcp_snoop max_entry
Command: show dhcp_snoop max_entry

Port          Max Entry
-----
1             10
2             10
3             10
4             No Limit
5             No Limit
6             No Limit
7             No Limit
8             No Limit
9             No Limit
10            No Limit
11            No Limit
12            No Limit

Zxxx0:admin#
```

To display the DHCP snooping binding entries:

---

|             |                                                                                            |
|-------------|--------------------------------------------------------------------------------------------|
| <b>NOTE</b> | "Inactive" indicates that the entry is currently inactive due to the port link being down. |
|-------------|--------------------------------------------------------------------------------------------|

---

## 39.12. config dhcp\_snoop max\_entry

---

### ● Description

This command is used to specify the maximum number of entries that can be learned by a specified port. By default, the maximum number of port entries is unlimited. This command specifies the maximum number of entries that can be learned by the specified ports.

### ● Format

**config dhcp\_snoop max\_entry ports [<portlist> | all] limit [<value 1-n> | no\_limit]**

### ● Parameters

|                          |                                                                                                                                        |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>portlist</b>          | Specify the list of ports that needs a restriction on the maximum number of DHCP snooping address binding entries that can be learned. |
| <b>all</b>               | Indicates that all the ports on the Switch will be used.                                                                               |
| <b>limit</b>             |                                                                                                                                        |
| <b>&lt;value 1-n&gt;</b> | Specify the maximum number.                                                                                                            |
| <b>no_limit</b>          | Specify that the maximum number of learned entries is unlimited.                                                                       |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To set the maximum number of DHCP snooping entries that can be learned on ports 1-3 to 10:

```
Zxxx0:admin# config dhcp_snoop max_entry ports 1-3 limit 10.
Command: config dhcp_snoop max_entry ports 1-3 limit 10.

Success.

Zxxx0:admin#
```

## 39.13. enable ip\_verify\_source log

---

### ● Description

This command is used to enable IP Source Address Verify logs.

This command is used to generate logs when the IP Source Address Verify modules detect an illegal IP and MAC address.

### ● Format

enable ip\_verify\_source log

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable the IP Source Address Verify logs function:

```
Zxxx0:admin# enable ip_verify_source log
Command: enable ip_verify_source log

Success.

Zxxx0:admin#
```

## 39.14. disable ip\_verify\_source log

---

- **Description**

This command is used to disable the IP Source Address Verify logs.

- **Format**

disable ip\_verify\_source log

- **Parameters**

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To disable IP Source Address Verify logs:

```
Zxxx0:admin#  disable ip_verify_source log
Command: disable ip_verify_source log

Success.

Zxxx0:admin#
```

## 40. IPv6 NDP Commands

In IPv6, a protocol called NDP (Neighbor Discovery Protocol) is used to configure the global IP address of a device connected to the router. The router periodically sends packets called RA (Router Advertisement) to a specified interface. An RA packet includes parameters such as network prefix and hop limit. A device receiving RA packets combines the network prefix and its link-local address to create an IPv6 address. The transmission source of RA packets is managed as a default router. Device information with the address added is registered in a NDP table in the router.

In this chapter, you will display/delete a NDP table and register items manually. You will also configure parameters about RA operations.

```
create ipv6 neighbor_cache ipif <ipif_name 12> <ipv6addr> <macaddr>
delete ipv6 neighbor_cache ipif [<ipif_name 12> | all] [<ipv6addr> | static | dynamic | all]
show ipv6 neighbor_cache ipif [<ipif_name 12> | all] [ipv6address <ipv6addr> | static | dynamic |
all] {hardware}
config ipv6 nd ns ipif <ipif_name 12> retrans_time <millisecond 0-4294967295>
config ipv6 nd ra ipif <ipif_name 12> {state [enable | disable] | life_time <sec 0-9000> |
reachable_time <millisecond 0-3600000> | retrans_time <millisecond 0-4294967295> |
hop_limit <value 0-255> | managed_flag [enable | disable] | other_config_flag [enable |
disable] | min_rtr_adv_interval <sec 3-1350> | max_rtr_adv_interval <sec 4-1800>}(1)
config ipv6 nd ra prefix_option ipif <ipif_name 12> <ipv6networkaddr> {preferred_life_time <sec 0-
4294967295> | valid_life_time <sec 0-4294967295> | on_link_flag [enable | disable] |
autonomous_flag [enable | disable]}(1)
show ipv6 nd {ipif <ipif_name 12>}
```

### 40.1. create ipv6 neighbor\_cache ipif

#### ● Description

This command is used to add a static neighbor on an IPv6 interface.

#### ● Format

```
create ipv6 neighbor_cache ipif <ipif_name 12> <ipv6addr> <macaddr>
```

#### ● Parameters

```
<ipif_name 12>
```

Specify the interface's name.

---

**<ipv6addr>**

Specify the IPv6 address of the neighbor.

---

**<macaddr>**

Specify the MAC address of the neighbor.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To add a static entry into the NDP table:

```
Zxxx0:admin#create ipv6 neighbor_cache ipif System 3ffc::1 00:01:02:03:04:05
Command: create ipv6 neighbor_cache ipif System 3FFC::1 00-01-02-03-04-05

Success.

Zxxx0:admin#
```

## 40.2. delete ipv6 neighbor\_cache ipif

---

### ● Description

This command is used to delete a neighbor cache entry or static neighbor cache entries from the address cache or all address cache entries on this IP interface. Both static and dynamic entries can be deleted.

### ● Format

**delete ipv6 neighbor\_cache ipif [<ipif\_name 12> | all] [<ipv6addr> | static | dynamic | all]**

### ● Parameters

---

**<ipif\_name 12>**

Specify the IPv6 interface name.

---

**all**

Specify all IPv6 interfaces.

---

**<ipv6addr>**

Specify the IPv6 address of the neighbor.

---

**static**

Specify to delete the IPv6 static entries.

---

**dynamic**

Specify to delete the IPv6 dynamic entries.

---

**all**

Specify all IPv6 entries, including static and dynamic, to be deleted.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.



## 40. IPv6 NDP Commands

### ● Example

To delete the neighbor cache entry for IPv6 address 3ffc::1 on the IP interface "System":

```
Zxxx0:admin#delete ipv6 neighbor_cache ipif System 3ffc::1
Command: delete ipv6 neighbor_cache ipif System 3FFC::1

Success.

Zxxx0:admin#
```

## 40.3. show ipv6 neighbor\_cache ipif

### ● Description

This command is used to display the neighbor cache entry for the specified interface. Users can display a specific entry, all static entries, all dynamic entries, or all entries.

### ● Format

**show ipv6 neighbor\_cache ipif** [<ipif\_name 12> | all] [ipv6address <ipv6addr> | static | dynamic | all] {hardware}

### ● Parameters

|                             |                                                                                                          |
|-----------------------------|----------------------------------------------------------------------------------------------------------|
| <b>&lt;ipif_name 12&gt;</b> | Specify the IPv6 interface name.                                                                         |
| <b>all</b>                  | Specify all the IPv6 interface names.                                                                    |
| <b>ipv6address</b>          | Specify the IPv6 address of the neighbor.                                                                |
| <b>&lt;ipv6addr&gt;</b>     | Specify the IPv6 address                                                                                 |
| <b>static</b>               | Specify to display the IPv6 static neighbor cache entries.                                               |
| <b>dynamic</b>              | Specify to display the IPv6 dynamic entries.                                                             |
| <b>all</b>                  | Specify to display all IPv6 addresses, static and dynamic.                                               |
| <b>hardware</b>             | (Optional) Specify to display all the neighbor cache entries which were written into the hardware table. |

### ● Restrictions

None.

### ● Example

To display all neighbor cache entries for the IP interface "System":

```

Zxxx0:admin#show ipv6 neighbor_cache ipif System all
Command: show ipv6 neighbor_cache ipif System all

FE80::215:72FF:FE36:104          State: Reachable
MAC Address : 00-15-72-36-01-04   Port : 1:21
Interface   : System             VID  : 1

Total Entries: 1

Zxxx0:admin#

```

## 40.4. config ipv6 nd ns ipif

### ● Description

This command is used to configure the NS retransmit time of a specified interface.

### ● Format

**config ipv6 nd ns ipif <ipif\_name 12> retrans\_time <millisecond 0-4294967295>**

### ● Parameters

**<ipif\_name 12>**

Specify the name of the interface. The maximum length is 12 characters.

**retrans\_time**

Specify the neighbor solicitation's retransmit timer in milliseconds. It has the same value as ra retrans\_time in the config ipv6 nd ra command. If one is configured, the other will change too.

**<millisecond 0-4294967295>**

Specify the neighbor solicitation's retransmit timer in milliseconds. It has the same value as ra retrans\_time in the config ipv6 nd ra command. If one is configured, the other will change too. Specify a time between 0 and 4294967295 milliseconds.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the NS retransmit time of a specified interface:

```

Zxxx0:admin#config ipv6 nd ns ipif System retrans_time 400
Command: config ipv6 nd ns ipif System retrans_time 400

Success.

Zxxx0:admin#

```

## 40.5. config ipv6 nd ra ipif

---

### ● Description

This command is used to configure the RA parameters of a specified interface.

### ● Format

```
config ipv6 nd ra ipif <ipif_name 12> {state [enable | disable] | life_time <sec 0-9000> |
reachable_time <millisecond 0-3600000> | retrans_time <millisecond 0-4294967295> |
hop_limit <value 0-255> | managed_flag [enable | disable] | other_config_flag [enable
| disable] | min_rtr_adv_interval <sec 3-1350> | max_rtr_adv_interval <sec 4-1800>}(1)
```

### ● Parameters

|                                         |                                                                                                                                                                                                                       |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;ipif_name 12&gt;</b>             | Specify the interface's name.                                                                                                                                                                                         |
| <b>state</b>                            | Specify the router advertisement status.                                                                                                                                                                              |
| <b>enable</b>                           | Enable the router advertisement state.                                                                                                                                                                                |
| <b>disable</b>                          | Disable the router advertisement state.                                                                                                                                                                               |
| <b>life_time</b>                        | Specify the lifetime of the router as the default router, in seconds.                                                                                                                                                 |
| <b>&lt;sec 0-9000&gt;</b>               | Specify the time between 0 and 9000 seconds.                                                                                                                                                                          |
| <b>reachable_time</b>                   | Specifies the amount of time that a node can consider a neighboring node reachable after receiving a reachability confirmation in millisecond.                                                                        |
| <b>&lt;millisecond 0-3600000&gt;</b>    | Specify the time between 0 and 3600000 milliseconds.                                                                                                                                                                  |
| <b>retrans_time</b>                     | Specifies the amount of time between retransmissions of router advertisement message in millisecond, and the router advertisement packet will take it to host.                                                        |
| <b>&lt;millisecond 0-4294967295&gt;</b> | Specify the time between 0 and 4294967295 milliseconds.                                                                                                                                                               |
| <b>hop_limit</b>                        | Specify the default value of the hop limit field in the IPv6 header for packets sent by hosts that receive this RA message.                                                                                           |
| <b>&lt;value 0-255&gt;</b>              | Specify the value between 0 and 255.                                                                                                                                                                                  |
| <b>managed_flag</b>                     | Specify to enable or disable the function.                                                                                                                                                                            |
| <b>enable</b>                           | When set to enable, it indicates that hosts receiving this RA must use a stateful address configuration protocol to obtain an address, in addition to the addresses derived from the stateless address configuration. |
| <b>disable</b>                          | Set to disable to stop hosts receiving the RA from using a stateful address configuration to obtain an address.                                                                                                       |

---

**other\_config\_flag**

Specify to enable or disable the function.

**enable**

When set to enable, it indicates that hosts receiving this RA must use a stateful address configuration protocol to obtain on-address configuration information.

**disable**

Set to disable to stop hosts receiving this RA from using a stateful address configuration protocol to obtain on-address configuration information.

---

**min\_rtr\_adv\_interval**

Specify the minimum time allowed between sending unsolicited multicast Router Advertisements from the interface, in seconds. It must be no less than 3 seconds and no greater than  $.75 * \text{MaxRtrAdvInterval}$ . The default is  $0.33 * \text{MaxRtrAdvInterval}$ .

**<sec 3-1350>**

Specify the time between 3 and 1350 seconds.

---

**max\_rtr\_adv\_interval**

Specify the maximum time allowed between sending unsolicited multicast Router Advertisements from the interface, in seconds. It must be no less than 4 seconds and no greater than 1800 seconds. The default is 600 seconds.

**<sec 4-1800>**

Specify the time between 4 and 1800 seconds.

---

**● Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

**● Example**

To configure the RA state as enabled and the life\_time of the "tiberius" interface to be 1000 seconds:

```
Zxxx0:admin#config ipv6 nd ra ipif tiberius state enable life_time 1000
Command: config ipv6 nd ra ipif tiberius state enable life_time 1000

Success.

Zxxx0:admin#
```

## **40.6. config ipv6 nd ra prefix\_option ipif**

---

**● Description**

This command is used to configure the prefix option for the router advertisement function.

**● Format**

```
config ipv6 nd ra prefix_option ipif <ipif_name 12> <ipv6networkaddr>
{preferred_life_time <sec 0-4294967295> | valid_life_time <sec 0-4294967295> |
on_link_flag [enable | disable] | autonomous_flag [enable | disable]}(1)
```

## 40. IPv6 NDP Commands

### ● Parameters

---

**<ipif\_name 12>**

Specify the interface's name. The maximum length is 12 characters.

---

**<ipv6networkaddr>**

Specify the IPv6 network address.

---

**preferred\_life\_time**

Specify the number in seconds that an address, based on the specified prefix using the stateless address configuration, remains in preferred state.

**<sec 0-4294967295>**

Specify the time between 0 and 4294967295 seconds. For an infinite valid lifetime the value can be set to 4294967295.

---

**valid\_life\_time**

Specify the number of seconds that an address, based on the specified prefix, using the stateless address configuration, remains valid.

**<sec 0-4294967295>**

Specify the time between 0 and 4294967295 seconds. For an infinite valid lifetime the value can be set to 4294967295.

---

**on\_link\_flag**

Specify to enable or disable the function.

**enable**

Setting this field to enable will denote, within the IPv6 packet, that the IPv6 prefix configured here is assigned to this link-local network. Once traffic has been successfully sent to these nodes with this specific IPv6 prefix, the nodes will be considered reachable on the link-local network.

**disable**

When set to disable, the addresses implied by the specified prefix are not available on the link where the RA message is received.

---

**autonomous\_flag**

Specify to enable or disable the function.

**enable**

Setting this field to enable will denote that this prefix may be used to autoconfigure IPv6 addresses on the link-local network.

**disable**

When set to disable, the specified prefix will not be used to create an autonomous address configuration.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the value of the preferred\_life\_time of prefix option to be 1000 seconds for the prefix 3ffe:501:ffff:100::/64, which is the prefix of the ip1 interface:

```
Zxxx0:admin#config ipv6 nd ra prefix_option ipif ip1 3ffe:501:ffff:100::/64
preferred_life_time 1000
Command: config ipv6 nd ra prefix_option ipif ip1 3ffe:501:ffff:100::/64
preferred_life_time 1000
```

Success.

Zxxx0:admin#

## 40.7. show ipv6 nd

### ● Description

This command is used to display IPv6 Neighbor Discover related configuration.

### ● Format

**show ipv6 nd {ipif <ipif\_name 12>}**

### ● Parameters

---

**ipif** (Optional) Specify the interface name.

---

**<ipif\_name 12>**

Specify the interface's name. The maximum length is 12 characters.

---



---

**NOTE** If no IP interface is specified, the IPv6 ND related configuration of all interfaces will be displayed.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To display IPv6 Neighbor Discover related configuration:

## 40. IPv6 NDP Commands

```
Zxxx0:admin#show ipv6 nd ipif System
```

```
Command: show ipv6 nd ipif System
```

```
Interface Name      : System
```

```
Hop Limit           : 64
```

```
NS Retransmit Time  : 400 (ms)
```

```
Router Advertisement : Disabled
```

```
RA Max Router AdvInterval : 600 (sec)
```

```
RA Min Router AdvInterval : 198 (sec)
```

```
RA Router Life Time : 1800 (sec)
```

```
RA Reachable Time    : 1200000 (ms)
```

```
RA Retransmit Time   : 400 (ms)
```

```
RA Managed Flag       : Disabled
```

```
RA Other Configure Flag : Disabled
```

| Prefix                   | Preferred | Valid   | OnLink  | Autonomous |
|--------------------------|-----------|---------|---------|------------|
| 1000:A111:B111:C111::/64 | 604800    | 2592000 | Enabled | Enabled    |

```
Zxxx0:admin#
```

## 41. Jumbo Frame Commands

In Ethernet, communication data is divided into fixed-size units called "frames" and transmitted. The standard frame has a fixed-size of 1518 bytes. A frame called jumbo frame is larger than the standard frame for more efficient data transmission.

This Switching Hub supports a jumbo frame with up to 13000 bytes and allows you to configure the setting for all ports or each port.

To transmit with jumbo frames, all devices on the route, including this Switching Hub, must support jumbo frames. If there are some devices not supporting jumbo frames, data is transmitted with the standard frame size.

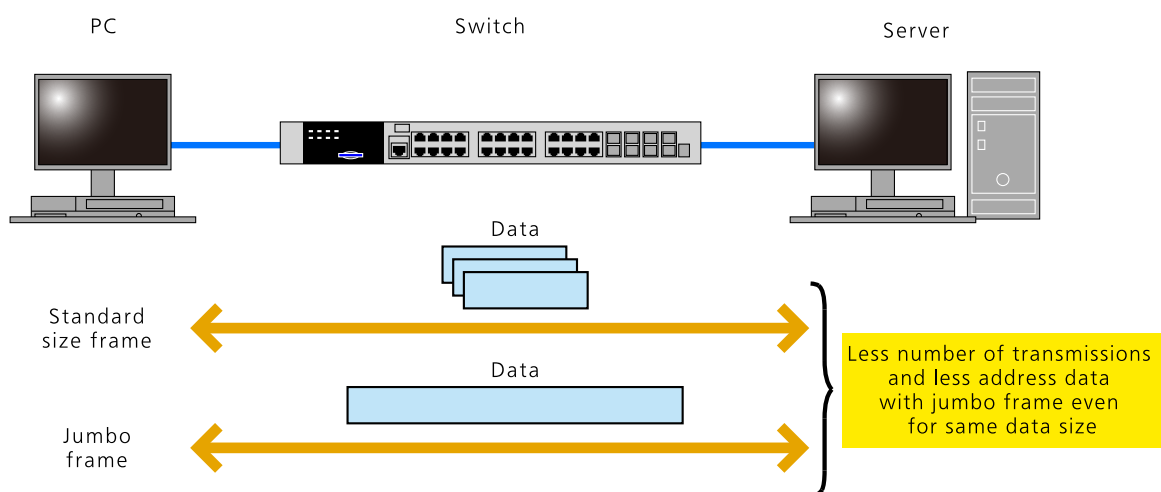


Figure 41-1 Jumbo frame overview

```
enable jumbo_frame
disable jumbo_frame
config jumbo_frame ports [<portlist> | all] state [enable | disable]
show jumbo_frame {<portlist>}
```



## 41.1. enable jumbo\_frame

---

### ● Description

This command is used to enable support of Jumbo Frames.

### ● Format

enable jumbo\_frame

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable Jumbo Frames:

```
Zxxx0:admin#enable jumbo_frame
Command: enable jumbo_frame

Zxxx0:admin#
```

## 41.2. disable jumbo\_frame

---

### ● Description

This command is used to disable support of Jumbo Frames.

### ● Format

disable jumbo\_frame

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To disable Jumbo Frames:

```
Zxxx0:admin#disable jumbo_frame
Command: disable jumbo_frame

Success.

Zxxx0:admin#
```

## 41.3. config jumbo\_frame ports

### ● Description

This command is used to configure the jumbo frame state on specified ports.

### ● Format

config jumbo\_frame ports [<portlist> | all] state [enable | disable]

### ● Parameters

---

**<portlist>** Enter the list of ports used for this configuration here.

---

**all** Specifies that all the ports will be used for this configuration.

---

**state** Specifies the jumbo frame state to be applied to a range of ports specified.

**enable** Specifies that the jumbo frame state will be enabled.

**disable** Specifies that the jumbo frame state will be disabled.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable jumbo frames on ports 1:1-1:5:

```
Zxxx0:admin# config jumbo_frame ports 1:1-1:5 state enable
Command: config jumbo_frame ports 1:1-1:5 state enable

Success.

Zxxx0:admin#
```

## 41.4. show jumbo\_frame

---

### ● Description

This command is used to display Jumbo Frames.

### ● Format

show jumbo\_frame {<portlist>}

### ● Parameters

---

<portlist>(Optional) Enter the list of ports to be displayed here.

---

### ● Restrictions

None.

### ● Example

To display Jumbo Frames for port 1 to 5:

```
Zxxx0:admin#show jumbo_frame 1-5
Command: show jumbo_frame 1-5

Jumbo Frame Global State : Disabled

Maximum Jumbo Frame Size : 1518 Bytes

Port          Jumbo Frame State
-----
1             Enabled
2             Enabled
3             Enabled
4             Enabled
5             Enabled

Zxxx0:admin#
```

## 42. LACP Configuration Commands

Link aggregation is a technology to connect two Switching Hubs with multiple ports and bundle them as one port. This provides path redundancy and enhanced bandwidth.

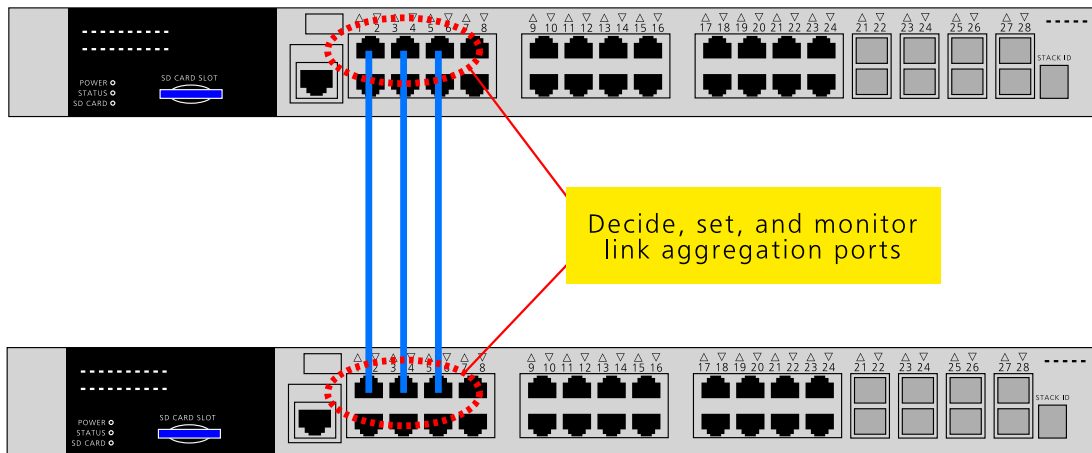


Figure 42-1 LACP overview

LACP (Link Aggregate Control Protocol) is a protocol to automatically decide, set, and monitor the port connection status in link aggregation.

The LACP operation mode needs to be configured for each port.

- Active: Port sending LACP frames
- Passive: Port receiving LACP frames

**NOTE** For more information about how to enable link aggregation, refer to "Link Aggregation Commands."

```
config lacp_port <portlist> mode [active | passive]
show lacp_port {<portlist>}
```

### 42.1. config lacp\_port

#### • Description

This command is used to configure per-port LACP mode.

#### • Format

```
config lacp_port <portlist> mode [active | passive]
```

## 42. LACP Configuration Commands

### ● Parameters

---

**<portlist>** Specify a range of ports to be configured.

---

**mode** Specify the port mode.

**active** Specify the mode as active.

**passive** Specify the mode as passive.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure port LACP mode for ports 1 to 3:

```
Zxxx0:admin#config lacp_port 1-3 mode active
Command: config lacp_port 1-3 mode active
```

```
Success.
```

```
Zxxx0:admin#
```

## 42.2. show lacp\_port

---

### ● Description

This command is used to display per-port LACP mode.

### ● Format

show lacp\_port {<portlist>}

### ● Parameters

---

**<portlist>**(Optional) Specify a range of ports to be displayed.

---

---

**NOTE** If no parameter is specified, the system will display current LACP mode for all ports.

---

### ● Restrictions

None.

### ● Example

To display the current LACP mode for ports 1 to 3 on the Switching Hub:

## 42. LACP Configuration Commands

```
Zxxx0:admin#show lacp_port 1-3  
Command: show lacp_port 1-3
```

| Port | Activity |
|------|----------|
| 1    | Active   |
| 2    | Active   |
| 3    | Active   |

```
Zxxx0:admin#
```

---

## 43. Layer 2 Protocol Tunneling (L2PT) Command List

---

L2PT is a function to enable transferring of L2 protocol frames, such as STP and GVRP, to different networks.

In this chapter, you will configure L2PT.

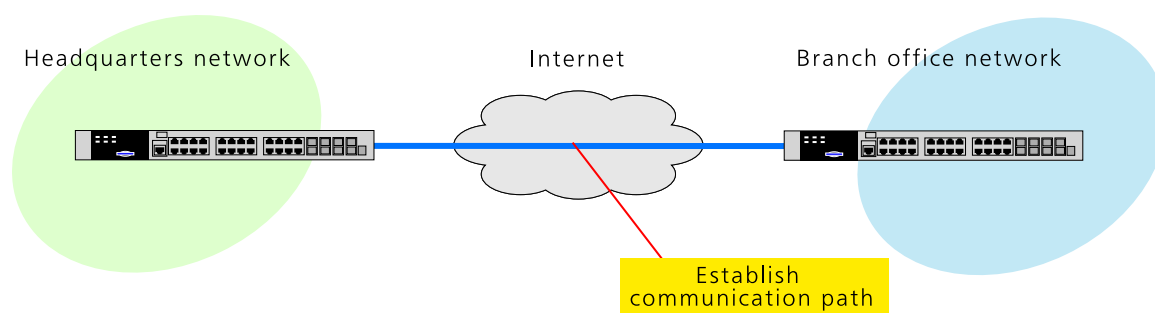


Figure 43-1 L2PT overview

---

```
config l2protocol_tunnel ports [<portlist> | all] type [uni tunneled_protocol [{stp | gvrp |  
    protocol_mac [01-00-0C-CC-CC-CC | 01-00-0C-CC-CC-CD]}(1) | all] {threshold <value 0-  
    65535>} | nni | none]  
show l2protocol_tunnel {[uni | nni]}  
enable l2protocol_tunnel  
disable l2protocol_tunnel
```

---

### 43.1. config l2protocol\_tunnel ports

---

#### ● Description

This command is used to configure Layer 2 protocol tunneling on ports.

Layer 2 protocol tunneling is used to tunnel Layer 2 protocol packet.

If a Layer 2 protocol is tunnel-enabled on an UNI, once received the PDU on this port, the multicast destination address of the PDU will be replaced by Layer 2 protocol tunneling multicast address. The Layer 2 protocol tunneling multicast address for STP is 01-05-5D-00-00-00, for GVRP is 01-05-5D-00-00-21, for Layer 2 protocols MAC 01-00-0C-CC-CC-CC is 01-05-5D-00-00-10 and for protocol MAC 01-00-0C-CC-CC-CD is 01-05-5D-00-00-11.

## ● Format

**config l2protocol\_tunnel ports [<portlist> | all] type [uni tunneled\_protocol [{stp | gvrp | protocol\_mac [01-00-0C-CC-CC-CC | 01-00-0C-CC-CC-CD]}(1) | all] {threshold <value 0-65535>} | nni | none]**

## ● Parameters

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ports</b>             | Specify the ports on which the Layer 2 protocol tunneling will be configured.<br><b>&lt;portlist&gt;</b><br>Enter a list of ports to be configured here.<br><b>all</b> Specify to use this configuration on all the ports.                                                                                                                                                                                                                                        |
| <b>type</b>              | Specify the type of the ports.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>uni</b>               | Specify the port is UNI port                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>tunneled_protocol</b> | Specify tunneled protocols on this UNI port. If specified all, all tunnel-able Layer 2 protocols will be tunneled on this port.<br><b>stp</b> (Optional) Specify to use the STP protocol.<br><b>gvrp</b> (Optional) Specify to use the GVRP protocol.<br><b>protocol_mac</b><br>(Optional) Specify which protocol MAC address to use.<br>01-00-0C-CC-CC-CCSpecify to use this protocol MAC address.<br>01-00-0C-CC-CC-CDSpecify to use this protocol MAC address. |
| <b>all</b>               | Specify to use all the MAC addresses.                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>threshold</b>         | (Optional) Specify the drop threshold for packets-per-second accepted on this UNI port. The port drops the PDU if the protocol's threshold is exceeded. The range of the threshold value is 0 to 65535 (packet/second). The value 0 means on limit. By default, the value is 0.<br><b>&lt;value 0-65535&gt;</b><br>Enter the threshold packets-per-seconds value here. This value must be between 0 and 65535.                                                    |
| <b>nni</b>               | Specify the port is NNI port                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>none</b>              | Disables tunnel on it. By default, a port is none port.                                                                                                                                                                                                                                                                                                                                                                                                           |

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure the STP tunneling on ports 1-4:

```
Zxxx0:admin# config l2protocol_tunnel ports 1-4 type uni tunneled_protocol stp
Command: config l2protocol_tunnel ports 1-4 type uni tunneled_protocol stp

Success.

Zxxx0:admin#
```



## 43.2. show l2protocol\_tunnel

### ● Description

This command is used to show Layer 2 protocol tunneling information.

### ● Format

**show l2protocol\_tunnel** {[uni | nni]}

### ● Parameters

|            |                                                                                              |
|------------|----------------------------------------------------------------------------------------------|
| <b>uni</b> | (Optional) Specify show UNI detail information, include tunneled and dropped PDU statistic.  |
| <b>nni</b> | (Optional) Specify show NNI detail information, include de-capsulated Layer 2 PDU statistic. |

### ● Restrictions

None.

### ● Example

To show Layer 2 protocol tunneling information summary:

```
Zxxx0:admin# show l2protocol_tunnel
Command: show l2protocol_tunnel

Global State: Enabled
UNI Ports: 1-2
NNI Ports: 3-4

Zxxx0:admin#
```

To show Layer 2 protocol tunneling detail information on UNI ports:

```
Zxxx0:admin# show l2protocol_tunnel uni
Command: show l2protocol_tunnel uni

UNI      Tunneled      Threshold
Port     Protocol      (packet/sec)
----      -
1:1      STP            10
         GVRP          10
         01-00-0C-CC-CC-CC 10
1:2      STP            20
         GVRP          20
         01-00-0C-CC-CC-CC 20
1:3      STP            0
1:4      STP            0

Zxxx0:admin#
```

To show Layer 2 protocol tunneling detail information on NNI ports:

```
Zxxx0:admin# show l2protocol_tunnel nni
Command: show l2protocol_tunnel nni
```

| NNI<br>Port | Protocol          |
|-------------|-------------------|
| ----        | -----             |
| 1           | STP               |
|             | GVRP              |
|             | 01-00-0C-CC-CC-CC |
|             | 01-00-0C-CC-CC-CD |
| 2           | STP               |
|             | GVRP              |
|             | 01-00-0C-CC-CC-CC |
|             | 01-00-0C-CC-CC-CD |

```
Zxxx0:admin#
```

## 43.3. enable l2protocol\_tunnel

### ● Description

Used to enable the Layer 2 protocol tunneling function.

### ● Format

**enable l2protocol\_tunnel**

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable the Layer 2 protocol tunneling function:

```
Zxxx0:admin# enable l2protocol_tunnel
Command: enable l2protocol_tunnel
```

```
Success.
```

```
Zxxx0:admin#
```

## 43.4. **disable l2protocol\_tunnel**

---

- **Description**

Used to disable the Layer 2 protocol tunneling function.

- **Format**

**disable l2protocol\_tunnel**

- **Parameters**

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To disable the Layer 2 protocol tunneling function:

```
Zxxx0:admin# disable l2protocol_tunnel
Command: disable l2protocol_tunnel

Success.

Zxxx0:admin#
```

## 44. Limited Multicast IP Address Commands

The commands are used to configure multicast packet filtering out of the target of IGMP/MLD snooping or layer-3 function.

```
create mcast_filter_profile {[ipv4 | ipv6]} profile_id <value 1-60> profile_name <name 32>
config mcast_filter_profile [profile_id <value 1-60> | profile_name <name 32>] {profile_name
    <name 32> | [add | delete] <mcast_address_list>}(1)
config mcast_filter_profile ipv6 [profile_id <value 1-60> | profile_name <name 32>] {profile_name
    <name 32> | [add | delete] <mcastv6_address_list>}(1)
delete mcast_filter_profile {[ipv4 | ipv6]} [profile_id [<value 1-60> | all] | profile_name <name
    32>]
show mcast_filter_profile {[ipv4 | ipv6]} {[profile_id <value 1-60> | profile_name <name 32>]}
config limited_multicast_addr [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]} {[add | delete]
    [profile_id <value 1-60> | profile_name <name 32>] | access [permit | deny]}(1)
show limited_multicast_addr [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]}
config max_mcast_group [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]} {max_group
    [<value 1-1024> | infinite] | action [drop | replace]} (1)
show max_mcast_group [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]}
```

### 44.1. create mcast\_filter\_profile

#### ● Description

This command is used to create a multicast address profile. If the IPv4 or IPv6 option is not specified, IPv4 is implied.

#### ● Format

```
create mcast_filter_profile {[ipv4 | ipv6]} profile_id <value 1-60> profile_name <name
32>
```

#### ● Parameters

|             |                                                        |
|-------------|--------------------------------------------------------|
| <b>ipv4</b> | (Optional) Specifies to add an IPv4 multicast profile. |
|-------------|--------------------------------------------------------|

|             |                                                        |
|-------------|--------------------------------------------------------|
| <b>ipv6</b> | (Optional) Specifies to add an IPv6 multicast profile. |
|-------------|--------------------------------------------------------|

|                   |                                  |
|-------------------|----------------------------------|
| <b>profile_id</b> | Specifies the ID of the profile. |
|-------------------|----------------------------------|

**<value 1-60>**

The profile ID range must be from 1 to 60

|                     |                                                    |
|---------------------|----------------------------------------------------|
| <b>profile_name</b> | Provides a meaningful description for the profile. |
|---------------------|----------------------------------------------------|

**<name 32>**

The profile name can be up to 32 characters long.

## 44. Limited Multicast IP Address Commands

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create a multicast address profile named MOD:

```
Zxxx0:admin#create mcast_filter_profile profile_id 2 profile_name MOD
Command: create mcast_filter_profile profile_id 2 profile_name MOD

Success.

Zxxx0:admin#
```

## 44.2. config mcast\_filter\_profile

---

### ● Description

This command is used to modify the profile name, add or delete a range of previously defined multicast IP addresses to or from the profile.

### ● Format

**config mcast\_filter\_profile** [**profile\_id** <value 1-60> | **profile\_name** <name 32>]  
{**profile\_name** <name 32> | [**add** | **delete**] <mcast\_address\_list>}(1)

### ● Parameters

---

**profile\_id**Specify the ID of the profile.

**<value 1-60>**

The profile ID must be between 1 and 60.

---

**profile\_name**

Specifies the name of the profile.

**<name 32>**

The profile name can be up to 32 characters long.

---

**profile\_name**

Specify a new name of the profile.

**<name 32>**

The profile name can be up to 32 characters long.

**add** Specify to add a range of multicast IP addresses.

**delete**Specify to delete a range of multicast IP addresses.

**<mcast\_address\_list>**

List of the multicast addresses to be added to or deleted from the profile.

Either specify a single multicast IP address or a range of multicast addresses using a hyphen.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To add a range of multicast addresses to a profile:

```
Zxxx0:admin#config mcast_filter_profile profile_id 2 add 225.1.1.1 - 225.1.1.100
Command: config mcast_filter_profile profile_id 2 add 225.1.1.1 - 225.1.1.100

Success.

Zxxx0:admin#
```

## 44.3. config mcast\_filter\_profile ipv6

---

### ● Description

This command is used to add or delete a range of previously defined IPv6 multicast IP addresses to or from the profile.

### ● Format

**config mcast\_filter\_profile ipv6** [**profile\_id** <value 1-60> | **profile\_name** <name 32>]  
**{profile\_name** <name 32> | [**add** | **delete**] <mcastv6\_address\_list>}(1)

### ● Parameters

---

**profile\_id** Specify the ID of the profile.

**<value 1-60>**

The profile ID must be between 1 and 60.

---

**profile\_name**

Specifies the name of the profile.

**<name 32>**

The profile name can be up to 32 characters long.

---

**profile\_name**

Specify a new name of the profile.

**<name 32>**

The profile name can be up to 32 characters long.

**add** Specify to add a range of multicast IP addresses.

**delete** Specify to delete a range of multicast IP addresses.

**<mcastv6\_address\_list>**

List of the IPv6 multicast addresses to be added to or deleted from the profile. Either specify a single IPv6 multicast IP address or a range of IPv6 multicast addresses using a hyphen.

---

## 44. Limited Multicast IP Address Commands

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To add the IPv6 multicast address range FF0E::100:0:0:20 - FF0E::100:0:0:22 to profile ID 3:

```
Zxxx0:admin#config mcast_filter_profile ipv6 profile_id 3 add FF0E::100:0:0:20 -  
FF0E::100:0:0:22  
Command: config mcast_filter_profile ipv6 profile_id 3 add FF0E::100:0:0:20 -  
FF0E::100:0:0:22  
  
Success.  
  
Zxxx0:admin#
```

## 44.4. delete mcast\_filter\_profile

### ● Description

This command is used to delete a multicast address profile. If the IPv4 or IPv6 option is not specified, IPv4 is implied.

### ● Format

**delete mcast\_filter\_profile** {[ipv4 | ipv6]} [profile\_id [<value 1-60> | all] | profile\_name <name 32>]

### ● Parameters

|                     |                                                                                                                       |
|---------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>ipv4</b>         | (Optional) Specify to delete an IPv4 multicast profile.                                                               |
| <b>ipv6</b>         | (Optional) Specify to delete an IPv6 multicast profile.                                                               |
| <b>profile_id</b>   | Specify the ID of the profile. The range is from 1 to 60.<br><value 1-60><br>The profile ID must be between 1 and 60. |
| <b>all</b>          | All multicast address profiles will be deleted.                                                                       |
| <b>profile_name</b> | Specify a profile based on the profile name.<br><name 32><br>The profile name can be up to 32 characters long.        |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete a multicast profile with a profile ID of 3:

```
Zxxx0:admin#delete mcast_filter_profile profile_id 3
Command: delete mcast_filter_profile profile_id 3

Success.

Zxxx0:admin#
```

To delete a multicast profile with a profile named MOD:

```
Zxxx0:admin#delete mcast_filter_profile profile_name MOD
Command: delete mcast_filter_profile profile_name MOD

Success.

Zxxx0:admin#
```

## 44.5. show mcast\_filter\_profile

### ● Description

This command is used to display defined multicast address profiles. If the IPv4 or IPv6 option is not specified, IPv4 is implied.

### ● Format

**show mcast\_filter\_profile** {[ipv4 | ipv6]} {[profile\_id <value 1-60> | profile\_name <name 32>]}

### ● Parameters

---

**ipv4** (Optional) Specify to display an IPv4 multicast profile.

---

**ipv6** (Optional) Specify to display an IPv6 multicast profile.

---

**profile\_id**(Optional) Specify the ID of the profile. If both profile\_id and profile\_name are not specified, all profiles will be displayed.  
**<value 1-60>**

The profile ID must be between 1 and 60.

---

**profile\_name**

(Optional) Specify to display a profile based on the profile name. If both profile\_id and profile\_name are not specified, all profiles will be displayed.  
**<name 32>**

The profile name can be up to 32 characters long.

---

### ● Restrictions

None.

### ● Example

To display all the defined multicast address profiles:



## 44. Limited Multicast IP Address Commands

```
Zxxx0:admin#show mcast_filter_profile
Command: show mcast_filter_profile

Profile ID Name                               Multicast Addresses
-----
1          MOD                               234.1.1.1 - 238.244.244.244
2          customer                         224.19.62.34 - 224.19.162.200

Total Entries: 2

Zxxx0:admin#
```

### 44.6. config limited\_multicast\_addr

#### ● Description

This command is used to configure the multicast address filtering function on a port or VLAN. When there are no profiles specified with a port or VLAN, the limited function is not effective. When the function is configured on a port or VLAN, it limits the multicast group operated by the IGMP/MLD snooping function and layer 3 function. If the IPv4 or IPv6 option is not specified, IPv4 is implied.

#### ● Format

```
config limited_multicast_addr [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]}
{[add | delete] [profile_id <value 1-60> | profile_name <name 32>] | access [permit |
deny]](1)
```

#### ● Parameters

|                   |                                                                                                                                                                                                                                                |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ports</b>      | Specify a range of ports to configure the multicast address filtering function.<br><b>&lt;portlist&gt;</b><br>Specify a range of ports to be configured.                                                                                       |
| <b>vlanid</b>     | Specify the VLAN ID of the VLAN that the multicast address filtering function will be configured on.<br><b>&lt;vlanid_list&gt;</b><br>Enter the VLAN ID of the VLAN that the multicast address filtering functions will be configured on here. |
| <b>ipv4</b>       | (Optional) Specify the IPv4 multicast profile.                                                                                                                                                                                                 |
| <b>ipv6</b>       | (Optional) Specify the IPv6 multicast profile.                                                                                                                                                                                                 |
| <b>add</b>        | (Optional) Add a multicast address profile to a port or VLAN.                                                                                                                                                                                  |
| <b>delete</b>     | (Optional) Delete a multicast address profile from a port or VLAN.                                                                                                                                                                             |
| <b>profile_id</b> | (Optional) Specify a profile ID to be added to or deleted from the port or VLAN.<br><b>&lt;value 1-60&gt;</b><br>The profile ID must be between 1 and 60.                                                                                      |

|                     |                                                                                                                                                                   |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>profile_name</b> | (Optional) Specify a profile name to be added to or deleted from the port or VLAN.<br><b>&lt;name 32&gt;</b><br>The profile name can be up to 32 characters long. |
| <b>access</b>       | (Optional) Specify whether the access is permit or deny.                                                                                                          |
| <b>permit</b>       | Specify that the packets that match the addresses defined in the profiles will be permitted.                                                                      |
| <b>deny</b>         | Specify that the packets that match the addresses defined in the profiles will be denied.                                                                         |

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To add multicast address profile 2 to ports 1 and 3:

```
Zxxx0:admin#config limited_multicast_addr ports 1,3 add profile_id 2
Command: config limited_multicast_addr ports 1,3 add profile_id 2

Success.

Zxxx0:admin#
```

# 44.7. show limited\_multicast\_addr

## ● Description

This command is used to display a multicast address range by ports or by VLANs. When the function is configured on a port or VLAN, it limits the multicast group operated by the IGMP/MLD snooping function and layer 3 function. If the IPv4 or IPv6 option is not specified, IPv4 is implied.

## ● Format

**show limited\_multicast\_addr [ ports <portlist> | vlanid <vlanid\_list>] {[ipv4 | ipv6]}**

## ● Parameters

|               |                                                                                                                                                                                       |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ports</b>  | Specify a range of ports to show the limited multicast address configuration.<br><b>&lt;portlist&gt;</b><br>Specify a range of ports to be displayed.                                 |
| <b>vlanid</b> | Specify the VLAN ID of VLANs that require information displaying about the multicast address filtering function.<br><b>&lt;vlanid_list&gt;</b><br>Enter the VLAN ID of the VLAN here. |
| <b>ipv4</b>   | (Optional) Specify to display the IPv4 multicast profile associated with the port or VLAN.                                                                                            |
| <b>ipv6</b>   | (Optional) Specify to display the IPv6 multicast profile associated with the port or VLAN.                                                                                            |

## 44. Limited Multicast IP Address Commands

### ● Restrictions

None.

### ● Example

To display the limited multicast address range on VLAN 1:

```
Zxxx0:admin#show limited_multicast_addr vlanid 1
Command: show limited_multicast_addr vlanid 1

VLAN      : 1
Access    : Deny

Profile ID      Name                Multicast Addresses
-----
1              customer            224.19.62.34 - 224.19.162.200

Zxxx0:admin#
```

To display the limited multicast address range on ports 1 and 3:

```
Zxxx0:admin#show limited_multicast_addr ports 1,3
Command: show limited_multicast_addr ports 1,3

Port      : 1
Access    : Deny

Profile ID      Name                Multicast Addresses
-----
1              customer            224.19.62.34 - 224.19.162.200

Port      : 3
Access    : Deny

Profile ID      Name                Multicast Addresses
-----
1              customer            224.19.62.34 - 224.19.162.200

Zxxx0:admin#
```

## 44.8. config max\_mcast\_group

---

### ● Description

This command is used to configure the maximum number of multicast groups a port or VLAN can join. If the IPv4 or IPv6 option is not specified, IPv4 is implied. When the joined groups for a port or a VLAN have reached the maximum number, the newly learned group will be dropped if the action is specified as drop. The newly learned group will replace the oldest group if the action is specified as replace.

### ● Format

```
config max_mcast_group [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]}
{max_group [<value 1-1024> | infinite] | action [drop | replace]} (1)
```

### ● Parameters

|                  |                                                                                                                                                                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ports</b>     | Specify a range of ports to configure the maximum multicast group.<br><b>&lt;portlist&gt;</b><br>Specify a range of ports to be configured.                                                                                      |
| <b>vlanid</b>    | Specify the VLAN ID to configure the maximum multicast group.<br><b>&lt;vlanid_list&gt;</b><br>Enter the VLAN ID of the VLAN here.                                                                                               |
| <b>ipv4</b>      | (Optional) Specify that the maximum number of IPv4 learned addresses should be limited.                                                                                                                                          |
| <b>ipv6</b>      | (Optional) Specify that the maximum number of IPv6 learned addresses should be limited.                                                                                                                                          |
| <b>max_group</b> | (Optional) Specify the maximum number of the multicast groups.<br><b>&lt;value 1-1024&gt;</b><br>The range is from 1 to 1024 or infinite.<br><b>infinite</b><br>Infinite is the default setting.                                 |
| <b>action</b>    | (Optional) Specify the action for handling newly learned groups when the register is full.<br><b>drop</b> The new group will be dropped.<br><b>replace</b><br>The new group will replace the oldest group in the register table. |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the maximum number of multicast groups that ports 1 and 3 can join to 100:

## 44. Limited Multicast IP Address Commands

```
Zxxx0:admin# config max_mcast_group ports 1, 3 max_group 100
Command: config max_mcast_group ports 1, 3 max_group 100

Success.

Zxxx0:admin#
```

### 44.9. show max\_mcast\_group

#### ● Description

This command is used to display the maximum number of multicast groups that a port or VLAN can join. If the IPv4 or IPv6 option is not specified, IPv4 is implied.

#### ● Format

**show max\_mcast\_group [ports <portlist> | vlanid <vlanid\_list>] {[ipv4 | ipv6]}**

#### ● Parameters

|               |                                                                                                                                        |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>ports</b>  | Specify a range of ports to display the maximum number of multicast groups.<br><portlist><br>Specify a range of ports to be displayed. |
| <b>vlanid</b> | Specify the VLAN ID for displaying the maximum number of multicast groups.<br><vlanid_list><br>Enter the VLAN ID of the VLAN here.     |
| <b>ipv4</b>   | (Optional) Specify to display the maximum number of IPv4 learned addresses.                                                            |
| <b>ipv6</b>   | (Optional) Specify to display the maximum number of IPv6 learned addresses.                                                            |

#### ● Restrictions

None.

#### ● Example

To display the maximum number of multicast groups for ports 1-2:

```
Zxxx0:admin# show max_mcast_group ports 1-2
Command: show max_mcast_group ports 1-2

Port      Max Multicast Group Number  Action
-----
1         Infinite                  Drop
2         Infinite                  Drop

Total Entries : 2
Zxxx0:admin#
```

## 45. Link Aggregation Commands

Link aggregation is a technology to connect two Switching Hubs with multiple ports and bundle them as one port. This provides path redundancy and enhanced bandwidth.

You can select how to distribute communications to bundled ports from several methods.

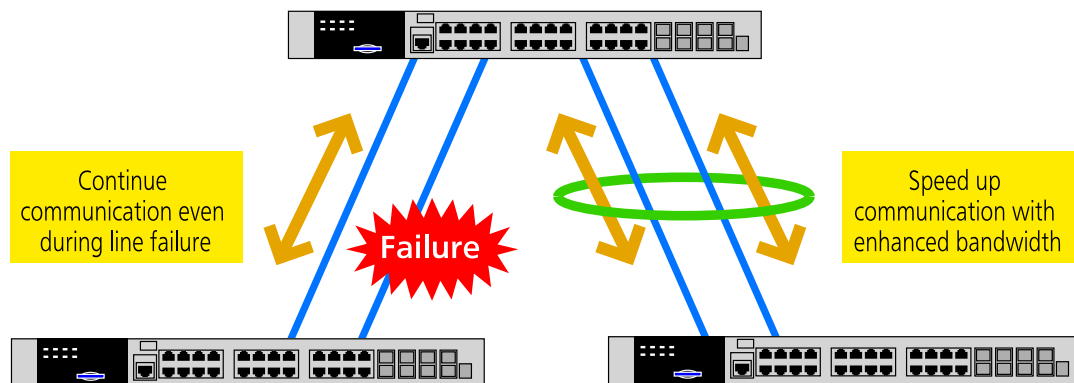


Figure 45-1 Link aggregation overview

**NOTE** To use the LACP protocol, which automatically configures and monitors link aggregation, enable the use of LACP in this chapter and configure the protocol settings by referring to "LACP Configuration Commands."

```
create link_aggregation group_id <value 1-48> { type [lacp | static] }
delete link_aggregation group_id <value 1-48>
config link_aggregation group_id <value 1-48> { master_port <port> | ports <portlist> | state
    [enable | disable] } (1)
config link_aggregation algorithm [mac_source | mac_destination | mac_source_dest | ip_source
    | ip_destination | ip_source_dest | l4_src_port | l4_dest_port | l4_src_dest_port]
show link_aggregation { group_id <value 1-48> | algorithm }
```

### 45.1. create link\_aggregation group\_id

#### ● Description

This command is used to create a link aggregation group.

#### ● Format

```
create link_aggregation group_id <value 1-48> { type [lacp | static] }
```

## 45. Link Aggregation Commands

### ● Parameters

---

**<value 1-48>**

Specify the group ID. The group number identifies each of the groups. The Switching Hub allows up to 48 link aggregation groups to be configured.

---

**type** (Optional) Specify the group type belongs to static or LACP. If type is not specified, the default is the static type.

**lacp** Specify the group type as LACP.

**static** Specify the group type as static.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create a link aggregation group:

```
Zxxx0:admin#create link_aggregation group_id 1 type lacp
```

```
Command: create link_aggregation group_id 1 type lacp
```

```
Success
```

```
Zxxx0:admin#
```

## **45.2. delete link\_aggregation group\_id**

### ● Description

This command is used to delete a previously configured link aggregation group.

### ● Format

**delete link\_aggregation group\_id <value 1-48>**

### ● Parameters

---

**<value 1-48>**

Specify the group ID. The group number identifies each of the groups. The Switching Hub allows up to 48 link aggregation groups to be configured.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To delete a link aggregation group:

```
Zxxx0:admin#delete link_aggregation group_id 3
Command: delete link_aggregation group_id 3

Success.

Zxxx0:admin#
```

## 45.3. config link\_aggregation group\_id

### ● Description

This command allows you to configure a link aggregation group that was created with the **create link\_aggregation** command above.

### ● Format

**config link\_aggregation group\_id <value 1-48> {master\_port <port> | ports <portlist> | state [enable | disable]} (1)**

### ● Parameters

#### <value 1-48>

Specify the group ID. The group number identifies each of the groups. The Switching Hub allows up to 48 link aggregation groups to be configured.

#### master\_port

Specify which port (by port number) of the link aggregation group will be the master port. All of the ports in a link aggregation group will share the port configuration with the master port.

#### <port>

Specify the master port ID.

#### ports

Specify a range of ports that will belong to the link aggregation group. The port list should include the master port.

#### <portlist>

Specify a range of ports to be configured.

#### state

Enable or disable the specified link aggregation group. If LACP group state is enabled, the ports' state machine will start.

#### enable

Enable the specified link aggregation group.

#### disable

Disable the specified link aggregation group.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.



## 45. Link Aggregation Commands

### ● Example

To configure a link aggregation group, group-id 1, master port 7, member ports 5-7:

```
Zxxx0:admin#config link_aggregation group_id 1 master_port 7 ports 5-7
Command: config link_aggregation group_id 1 master_port 7 ports 5-7

Success.

Zxxx0:admin#
```

## 45.4. config link\_aggregation algorithm

### ● Description

This command is used to configure the part of the packet examined by the Switching Hub when selecting the egress port for transmitting load-sharing data.

If the load sharing algorithm is based on IP information and the packet is a non-IP packet, it will be based on the source MAC.

If the load sharing algorithm is based on L4 information and the packet is not a TCP/UDP packet:

- 1) If the packet is a non-IP packet, it will be based on the source MAC.
- 2) If the packet is an IP packet, it will use the default value of "0" for the TCP/UDP port. It means that if it is not a TCP/UDP IP packet, it will deal with it the same as way as the TCP/UDP packets, but just the TCP/UDP value is 0.

### ● Format

```
config link_aggregation algorithm [mac_source | mac_destination | mac_source_dest
| ip_source | ip_destination | ip_source_dest | l4_src_port | l4_dest_port |
l4_src_dest_port]
```

### ● Parameters

---

**mac\_source**

Indicates that the Switching Hub should examine the MAC source address.

---

**mac\_destination**

Indicates that the Switching Hub should examine the MAC destination address.

---

**mac\_source\_dest**

Indicates that the Switching Hub should examine the MAC source and destination address.

---

**ip\_source**

Indicate that the Switching Hub should examine the IP source address.

---

**ip\_destination**

Indicate that the Switching Hub should examine the IP destination address.

---

**ip\_source\_dest**

Indicate that the Switching Hub should examine the IP source and destination address.

---

---

**l4\_src\_port**

Indicate that the Switching Hub should examine the Layer 4 source port.

---

**l4\_dest\_port**

Indicate that the Switching Hub should examine the Layer 4 destination port.

---

**l4\_src\_dest\_port**Indicate that the Switching Hub should examine the Layer 4 source and destination port.

---

**● Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

**● Example**

To configure the link aggregation algorithm to mac-source-dest:

```
Zxxx0:admin#config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

Zxxx0:admin#
```

## 45.5. show link\_aggregation

---

**● Description**

This command is used to display the current link aggregation configuration of the Switching Hub.

**● Format**

**show link\_aggregation {group\_id <value 1-48> | algorithm}**

**● Parameters**

---

**group\_id**(Optional) Specify the group ID. The group number identifies each of the groups.**<value 1-48>**

The Switching Hub allows up to 48 link aggregation groups to be configured.

---

**algorithm**(Optional) Specify the display of link aggregation by the algorithm in use by that group.

---

---

**NOTE**

If no parameter is specified, the system will display all the link aggregation information.

---

**● Restrictions**

None.

## 45. Link Aggregation Commands

### ● Example

To display the current link aggregation configuration when link aggregation is enabled:

```
Zxxx0:admin#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC_Source_Dest

Group ID      : 1
Type          : LACP
Master Port   : 1
Member Port   : 1-8
Active Port   : 7
Status        : Enabled
Flooding Port : 7

Total Entries: 1

Zxxx0:admin#
```

To display the current link aggregation configuration when link aggregation is disabled:

```
Zxxx0:admin#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-Source-Dest
Group ID      : 1
Type          : LACP
Master Port   : 1
Member Port   : 1-8
Active Port   :
Status        : Disabled
Flooding Port :

Total Entries: 1

Zxxx0:admin#
```

## 46. LLDP Commands

LLDP (Link Layer Discovery Protocol) is a function to periodically collect connected device information. If devices, such as an IP phone, printer, and network camera, support LLDP, you can learn what devices are connected where. This function also allows you to identify configuration errors based on collected information and change the protocol settings or Switching Hub operations according to the information.

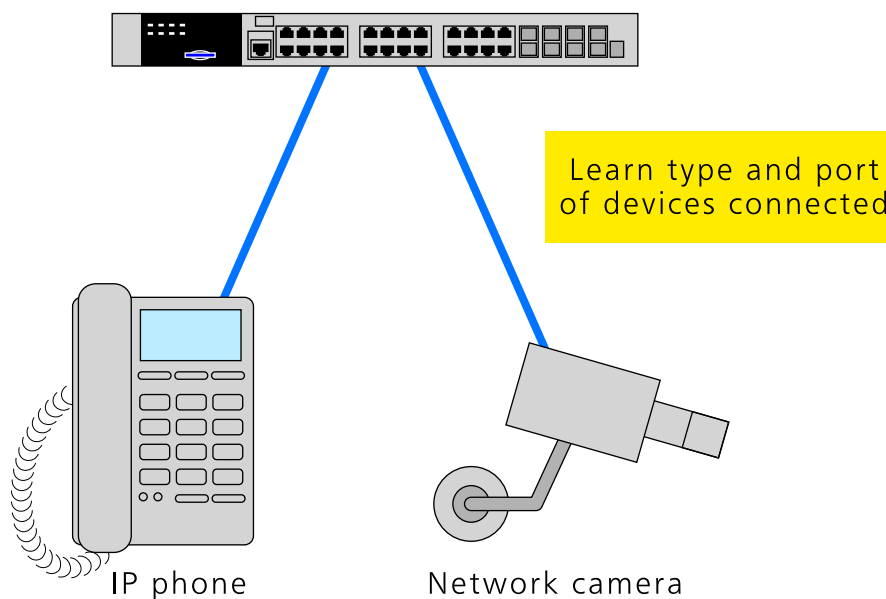


Figure 46-1 LLDP overview

```
enable lldp
disable lldp
config lldp [message_tx_interval <sec 5-32768> | message_tx_hold_multiplier <int 2-10> |
tx_delay <sec 1-8192> | reinit_delay <sec 1-10>]
show lldp
config lldp forward_message [enable | disable]
config lldp notification_interval <sec 5-3600>
config lldp ports [<portlist> | all] [notification [enable | disable] | admin_status [tx_only | rx_only |
tx_and_rx | disable] | mgt_addr [ipv4 <ipaddr> | ipv6 <ipv6addr>] [enable | disable] |
basic_tlvs [{all} | {port_description | system_name | system_description |
system_capabilities}] [enable | disable] | dot1_tlv_pvid [enable | disable] |
dot1_tlv_protocol_vid [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable] |
dot1_tlv_vlan_name [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable] |
dot1_tlv_protocol_identity [all | {eapol | lacp | gvrp | stp}] [enable | disable] | dot3_tlvs
[{all} | {mac_phy_configuration_status | link_aggregation | maximum_frame_size}] [enable
| disable]]
show lldp ports {<portlist>}
config lldp_med fast_start_repeat_count <value 1-10>
config lldp_med log_state [enable | disable]
config lldp_med notification topo_change ports [<portlist> | all] state [enable | disable]
```

## 46. LLDP Commands

---

```
config lldp_med ports [<portlist> | all] med_transmit_capabilities [all | {capabilities |  
    network_policy | inventory}(1)] state [enable | disable]  
show lldp_med ports {<portlist>}  
show lldp_med  
show lldp_med local_ports {<portlist>}  
show lldp_med remote_ports {<portlist>}  
show lldp local_ports {<portlist>} {mode [brief | normal | detailed]}  
show lldp mgt_addr {[ipv4 <ipaddr> | ipv6 <ipv6addr>]}  
show lldp remote_ports {<portlist>} {mode [brief | normal | detailed]}  
show lldp statistics  
show lldp statistics ports {<portlist>}
```

---

### 46.1. enable lldp

---

#### ● Description

This command is used to enable LLDP. This is a global control for the LLDP function. When this function is enabled, the Switching Hub can start to transmit LLDP packets and receive and process the LLDP packets. The specific function of each port will depend on the per port LLDP setting. For the advertisement of LLDP packets, the Switching Hub announces the information to its neighbor through ports. For the receiving of LLDP packets, the Switching Hub will learn the information from the LLDP packets advertised from the neighbor in the neighbor table. The default state for LLDP is disabled.

#### ● Format

enable lldp

#### ● Parameters

None.

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To enable LLDP:

```
Zxxx0:admin#enable lldp  
Command: enable lldp  
  
Success.  
  
Zxxx0:admin#
```

## 46.2. disable lldp

---

### ● Description

This command is used to disable LLDP. The Switching Hub will stop the sending and receiving of LLDP advertisement packets.

### ● Format

disable lldp

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To disable LLDP:

```
Zxxx0:admin#disable lldp
Command: disable lldp

Success.

Zxxx0:admin#
```

## 46.3. config lldp

---

### ● Description

This command is used to configure LLDP timer values. The message TX interval controls how often active ports retransmit advertisements to their neighbors. The message TX hold multiplier is a multiplier on the msgTxInterval that is used to compute the TTL value of txTTL in an LLDPDU. The TTL will be carried in the LLDPDU packet. The lifetime will be the minimum of 65535 and (message\_tx\_interval \* message\_tx\_hold\_multiplier). On the partner Switching Hub, when the time-to-live for a given advertisement expires, the advertised data is deleted from the neighbor Switching Hub's MIB. The TX delay is used to change the minimum time (delay-interval) any LLDP port will delay advertising successive LLDP advertisements due to a change in LLDP MIB content. The TX delay defines the minimum interval between sending of LLDP messages due to the constantly changing MIB content. A re-enabled LLDP port will wait for the reinit delay after the last disable command before reinitializing.

## 46. LLDP Commands

### ● Format

**config lldp [message\_tx\_interval <sec 5-32768> | message\_tx\_hold\_multiplier <int 2-10> | tx\_delay <sec 1-8192> | reinit\_delay <sec 1-10>]**

### ● Parameters

---

**message\_tx\_interval**

Specify the message TX interval between consecutive transmissions of LLDP advertisements on any given port.

**<sec 5-32768>**

The range is from 5 to 32768 seconds. The default setting is 30 seconds.

---

**message\_tx\_hold\_multiplier**

Specify the message TX hold multiplier.

**<int 2-10>**

Specify the range is from 2 to 10. The default setting is 4.

---

**tx\_delay** Specify the TX delay time.

**<sec 1-8192>**

Specify the range is from 1 to 8192 seconds. The default setting is 2 seconds.

Note that txDelay should be less than or equal to  $0.25 * \text{msgTxInterval}$ .

---

**reinit\_delay**

Specify the reinit delay time.

**<sec 1-10>**

Specify the range is from 1 to 10 seconds. The default setting is 2 seconds.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To change the packet transmission interval:

```
Zxxx0:admin#config lldp message_tx_interval 30
Command: config lldp message_tx_interval 30

Success.

Zxxx0:admin#
```

To change the multiplier value:

```
Zxxx0:admin#config lldp message_tx_hold_multiplier 3
Command: config lldp message_tx_hold_multiplier 3

Success.

Zxxx0:admin#
```

To configure the delay-interval interval:

```
Zxxx0:admin#config lldp tx_delay 8
Command: config lldp tx_delay 8

Success.

Zxxx0:admin#
```

To change the re-initialization delay interval to five seconds:

```
Zxxx0:admin#config lldp reinit_delay 5
Command: config lldp reinit_delay 5

Success.

Zxxx0:admin#
```

## 46.4. show lldp

---

- **Description**

This command is used to display LLDP.

- **Format**

**show lldp**

- **Parameters**

None.

- **Restrictions**

None.



## 46. LLDP Commands

### ● Example

To display LLDP:

```
Zxxx0:admin#show lldp
Command: show lldp

LLDP System Information
  Chassis ID Subtype      : MAC Address
  Chassis ID              : 00-11-22-33-44-55
  System Name             :
  System Description      : Gigabit Ethernet Switch
  System Capabilities     : Repeater, Bridge

LLDP Configurations
  LLDP Status              : Disabled
  LLDP Forward Status     : Disabled
  Message TX Interval     : 30
  Message TX Hold Multiplier: 4
  ReInit Delay            : 2
  TX Delay                 : 2
  Notification Interval   : 5

Zxxx0:admin#
```

## 46.5. config lldp forward\_message

### ● Description

This command is used to configure LLDP forwarding messages. When LLDP is disabled and LLDP forward message is enabled, the received LLDPDU packet will be forwarded. The default state is disabled.

### ● Format

config lldp forward\_message [enable | disable]

### ● Parameters

|                |                                   |
|----------------|-----------------------------------|
| <b>enable</b>  | Enable LLDP forwarding messages.  |
| <b>disable</b> | Disable LLDP forwarding messages. |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable LLDP forwarding messages:

```
Zxxx0:admin#config lldp forward_message enable
Command: config lldp forward_message enable

Success.

Zxxx0:admin#
```

## 46.6. config lldp notification\_interval

---

### ● Description

This command is used to configure LLDP timer values. This will globally change the interval between successive LLDP change notifications generated by the Switching Hub.

### ● Format

config lldp notification\_interval <sec 5-3600>

### ● Parameters

---

<sec 5-3600>

Specify the notification interval range is from 5 to 3600 seconds. The default setting is 5 seconds.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To change the notification interval to 10 seconds:

```
Zxxx0:admin#config lldp notification_interval 10
Command: config lldp notification_interval 10

Success.

Zxxx0:admin#
```

## 46.7. config lldp ports

---

### ● Description

Use this command to configure LLDP options by port. Enable or disable each port for sending change notification to configured SNMP trap receiver(s) if an LLDP data change is detected in an advertisement received on the port from an LLDP neighbor. The definition of change includes new available information, information timeout, information update. And the changed type includes any data update /insert/remove. The admin status options enable to control which ports participate in LLDP traffic and whether the participating ports allow LLDP traffic in only one direction or in both directions.

The config management address command specifies whether system's IP address needs to be advertised from the specified port. For layer 3 devices, each managed address can be individually specified. The management addresses that are added in the list will be advertised in the LLDP from the specified interface, associated with each management address. The interface for that management address will be also advertised in the if-index form.

An active LLDP port on the Switching Hub always includes the mandatory data in its outbound advertisements. And there are four optional data that can be configured for an individual port or group of ports to exclude one or more of these data types from outbound LLDP advertisements. The mandatory data type include four basic types of information (end of LLDPDU TLV, chassis ID TLV, port ID TLV, and Time to Live TLV). The mandatory type cannot be disabled. There are also four data types which can be optionally selected. They are port\_description, system\_name, system\_description, and system\_capability.

Configure an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally port vlan ID TLV data types from outbound LLDP advertisements.

Configure an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally port and protocol VLAN ID TLV data types from outbound LLDP advertisements.

Configure an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally VLAN name TLV data types from outbound LLDP advertisements.

Configure an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally protocol identity TLV data types from outbound LLDP advertisements. This TLV optional data type indicates whether the corresponding Local System's Protocol Identity instance will be transmitted on the port. The Protocol Identity TLV provides a way for stations to advertise protocols that are important to the operation of the network. Spanning Tree Protocol, the Link Aggregation Control Protocol, and numerous vendor proprietary variations are responsible for maintaining the topology and connectivity of the network. If EAPOL, GVRP, STP (including MSTP), and LACP protocol identity are enabled on this port and it is enabled to be advertised, then this protocol identity will be advertised.

## ● Format

```
config lldp ports [<portlist> | all] [notification [enable | disable] | admin_status
[tx_only | rx_only | tx_and_rx | disable] | mgt_addr [ipv4 <ipaddr> | ipv6 <ipv6addr>]
[enable | disable] | basic_tlvs [{all} | {port_description | system_name |
system_description | system_capabilities}] [enable | disable] | dot1_tlv_pvid [enable |
disable] | dot1_tlv_protocol_vid [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable
| disable] | dot1_tlv_vlan_name [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable
| disable] | dot1_tlv_protocol_identity [all | {eapol | lacp | gvrp | stp}] [enable |
disable] | dot3_tlvs [{all} | {mac_phy_configuration_status | link_aggregation
| maximum_frame_size}] [enable | disable]]
```

## ● Parameters

---

### <portlist>

Specify a range of ports to be configured.

---

### all

Specify to set all the ports on the system.

---

### notification

Enable or disable the SNMP trap notification of LLDP data changes detected on advertisements received from neighbor devices. The default notification state is disabled.

**enable** Enable the SNMP trap notification of LLDP data changes detected on advertisements received from neighbor devices.

**disable** Disable the SNMP trap notification of LLDP data changes detected on advertisements received from neighbor devices.

---

### admin\_status

Select the desired administrative per port state. The default per port state is tx\_and\_rx.

**tx\_only** Configure the specified port(s) to transmit LLDP packets, but block inbound LLDP packets from neighbor devices.

**rx\_only** Configure the specified port(s) to receive LLDP packets from neighbors, but block outbound packets to neighbors.

**tx\_and\_rx** Configure the specified port(s) to both transmit and receive LLDP packets.

**disable** Disable LLDP packet transmit and receive on the specified port(s).

---

### mgt\_address

The port types specified for advertising indicated management address instance.

**ipv4** Specify the IP address of IPv4.

**<ipaddr>** Specify the IP address of IPv4.

**ipv6** Specify the IP address of IPv6.

**<ipv6addr>** Specify the IP address of IPv6.

**enable** Enable port(s) specified for advertising indicated management address instance.

**disable** Disable port(s) specified for advertising indicated management address instance.

---

## 46. LLDP Commands

---

### basic\_tlvs

Configure an individual port or group of ports to exclude one or more of optional TLV data types from outbound LLDP advertisements.

**all** (Optional) Configure all four TLV data types listed below.

**port\_description**

(Optional) This TLV optional data type indicates that LLDP agent should transmit "Port Description TLV" on the port. The default state is disabled.

**system\_name**

(Optional) This TLV optional data type includes indicates that LLDP agent should transmit "System Name TLV." The default state is disabled.

**system\_description**

(Optional) This TLV optional data type includes indicates that LLDP agent should transmit "System Description TLV." The default state is disabled.

**system\_capabilities**

(Optional) This TLV optional data type includes indicates that LLDP agent should transmit "System Capabilities TLV." The system capability will indicate whether the device provides repeater, bridge, or router function, and whether the provided functions are currently enabled. The default state is disabled.

**enable** Enable configuration of an individual port or group of ports to exclude one or more of optional TLV data types from outbound LLDP advertisements.

**disable** Disable configuration of an individual port or group of ports to exclude one or more of optional TLV data types from outbound LLDP advertisements.

---

### dot1\_tlv\_pvid

This TLV optional data type determines whether the IEEE 802.1 organizationally defined port VLAN ID TLV transmission is allowed on a given LLDP transmission capable port. The default state is disabled.

**enable** Enable port VLAN ID TLV transmission on a given LLDP transmission capable port.

**disable** Disable port VLAN ID TLV transmission on a given LLDP transmission capable port.

---

### dot1\_tlv\_protocol\_vid

This TLV optional data type determines whether the IEEE 802.1 organizationally defined port and protocol VLAN ID TLV transmission is allowed on a given LLDP transmission capable port. The default state is disabled.

**vlan** (Optional) Specify a VLAN to be transmitted.

**all** (Optional) Specify that all VLAN names will be transmitted.

**<vlan\_name 32>**

(Optional) Specify a VLAN name to be transmitted.

**vlanid**(Optional) Specify a VLAN ID list to be transmitted.

**<vidlist>** Specify a VLAN ID list to be transmitted.

**enable** Enable configuration of an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally port and protocol VLAN ID TLV data types from outbound LLDP advertisements.

**disable** Disable configuration of an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally port and protocol VLAN ID TLV data types from outbound LLDP advertisements.

---

---

**dot1\_tlv\_vlan\_name**

This TLV optional data type indicates whether the corresponding Local System's VLAN name instance will be transmitted on the port. If a port is associated with multiple VLANs, those enabled VLAN ID will be advertised. The default state is disabled.

**vlan** (Optional) Specify a VLAN to be transmitted.

**all** (Optional) Specify that all VLAN names will be transmitted.

**<vlan\_name 32>**

(Optional) Specify a VLAN name to be transmitted.

**vlanid** (Optional) Specify a VLAN ID list to be transmitted.

**<vidlist>**

Specify a VLAN ID list to be transmitted.

**enable** Enable configuration of an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally VLAN name TLV data types from outbound LLDP advertisements.

**disable** Disable configuration of an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally VLAN name TLV data types from outbound LLDP advertisements.

---

**dot1\_tlv\_protocol\_identity**

This TLV optional data type indicates whether the corresponding Local System's Protocol Identity instance will be transmitted on the port. The Protocol Identity TLV provides a way for stations to advertise protocols that are important to the operation of the network, such as Spanning Tree Protocol, the Link Aggregation Control Protocol, and numerous vendor proprietary variations which are responsible for maintaining the topology and connectivity of the network. If EAPOL, GVRP, STP (including MSTP), and LACP protocol identity are enabled on this port and enabled to be advertised, then the protocol identity will be advertised. The default state is disabled.

**all** Advertise all of the protocols lists below.

**eapol** (Optional) Advertise EAPOL.

**lacp** (Optional) Advertise LACP.

**gvrp** (Optional) Advertise GVRP.

**stp** (Optional) Advertise STP.

**enable** Enable configuration an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally protocol identity TLV data types from outbound LLDP advertisements.

**disable** Disable configuration an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally protocol identity TLV data types from outbound LLDP advertisements.

---

## 46. LLDP Commands

---

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dot3_tlvs</b>                    | An individual port or group of ports to exclude one or more of IEEE 802.3 Organizationally Specific TLV data types from outbound LLDP advertisements.                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>all</b>                          | (Optional) Configure all of the TLV optional data types below.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>mac_phy_configuration_status</b> | (Optional) This TLV optional data type indicates that LLDP agent should transmit "MAC/PHY configuration/status TLV." This type indicates it is possible for two ends of an IEEE 802.3 link to be configured with different duplex and/or speed settings and still establish some limited network connectivity. More precisely, the information includes whether the port supports the auto-negotiation function, whether the function is enabled, the auto-negotiated advertised capability, and the operational MAU type. The default state is disabled. |
| <b>link_aggregation</b>             | (Optional) This TLV optional data type indicates that LLDP agent should transmit "Link Aggregation TLV." This type indicates the current link aggregation status of IEEE 802.3 MACs. More precisely, the information should include whether the port is capable of doing link aggregation, whether the port is aggregated in an aggregated link, and the aggregated port ID. The default state is disabled.                                                                                                                                               |
| <b>maximum_frame_size</b>           | (Optional) This TLV optional data type indicates that LLDP agent should transmit "Maximum-frame-size TLV." The default state is disabled.                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>enable</b>                       | Enable the configuration of an individual port or group of ports to exclude one or more of IEEE 802.3 Organizationally Specific TLV data types from outbound LLDP advertisements.                                                                                                                                                                                                                                                                                                                                                                         |
| <b>disable</b>                      | Disable the configuration of an individual port or group of ports to exclude one or more of IEEE 802.3 Organizationally Specific TLV data types from outbound LLDP advertisements.                                                                                                                                                                                                                                                                                                                                                                        |

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To change the SNMP notification state of ports 1 to 5 to enable:

```
Zxxx0:admin#config lldp ports 1-5 notification enable
Command: config lldp ports 1-5 notification enable

Success.

Zxxx0:admin#
```

To configure the mode of ports 1 to 5 to transmit and receive:

```
Zxxx0:admin#config lldp ports 1-5 admin_status tx_and_rx
Command: config lldp ports 1-5 admin_status tx_and_rx

Success.

Zxxx0:admin#
```

To enable ports 1 to 5 to manage address entries:

```
Zxxx0:admin#config lldp ports 1-5 mgt_addr ipv4 192.168.254.10 enable
Command: config lldp ports 1-5 mgt_addr ipv4 192.168.254.10 enable

Success.

Zxxx0:admin#
```

To exclude the system name TLV from the outbound LLDP advertisements for all ports:

```
Zxxx0:admin#config lldp ports all basic_tlvs system_name enable
Command: config lldp ports all basic_tlvs system_name enable

Success.

Zxxx0:admin#
```

To exclude the VLAN name TLV from the outbound LLDP advertisements for all ports:

```
Zxxx0:admin#config lldp ports all dot1_tlv_pvid enable
Command: config lldp ports all dot1_tlv_pvid enable

Success.

Zxxx0:admin#
```

To exclude the port and protocol VLAN ID TLV from the outbound LLDP advertisements for all ports:

```
Zxxx0:admin#config lldp ports all dot1_tlv_protocol_vid vlanid 1-3 enable
Command: config lldp ports all dot1_tlv_protocol_vid vlanid 1-3 enable

Success.

Zxxx0:admin#
```

To exclude the VLAN name TLV from the outbound LLDP advertisements for all ports:

```
Zxxx0:admin#config lldp ports all dot1_tlv_vlan_name vlanid 1-3 enable
Command: config lldp ports all dot1_tlv_vlan_name vlanid 1-3 enable

Success.

Zxxx0:admin#
```



## 46. LLDP Commands

To exclude the protocol identity TLV from the outbound LLDP advertisements for all ports:

```
Zxxx0:admin#config lldp ports all dot1_tlv_protocol_identity all enable
Command: config lldp ports all dot1_tlv_protocol_identity all enable

Success.

Zxxx0:admin#
```

To exclude the MAC/PHY configuration/status TLV from the outbound LLDP advertisements for all ports:

```
Zxxx0:admin#config lldp ports all dot3_tlvs mac_phy_configuration_status enable
Command: config lldp ports all dot3_tlvs mac_phy_configuration_status enable

Success.

Zxxx0:admin#
```

## 46.8. show lldp ports

---

### ● Description

This command is used to display LLDP per port configuration for advertisement options.

### ● Format

**show lldp ports {<portlist>}**

### ● Parameters

---

**<portlist>**(Optional) Specify the ports to be displayed.

---

---

**NOTE** When a port list is not specified, information for all ports will be displayed.

---

### ● Restrictions

None.

## ● Example

To display LLDP TLV option port 1:

```
Zxxx0:admin#show lldp ports 1
Command: show lldp ports 1

Port ID                : 1
-----
Admin Status           : TX_and_RX
Notification Status     : Disabled
Advertised TLVs Option :
    Port Description      Disabled
    System Name           Disabled
    System Description    Disabled
    System Capabilities   Disabled
    Enabled Management Address
        (None)
    Port VLAN ID          Disabled
Enabled Port_and_Protocol_VLAN_ID
    (None)
Enabled VLAN Name
    (None)
Enabled Protocol Identity
    (None)
    MAC/PHY Configuration/Status Disabled
    Link Aggregation       Disabled
    Maximum Frame Size     Disabled

Zxxx0:admin#
```

## **46.9. config lldp\_med fast\_start repeat\_count**

### ● Description

This command is used to configure the fast start repeat count. When an LLDP-MED Capabilities TLV is detected for an MSAP identifier not associated with an existing LLDP remote system MIB, the application layer shall start the fast start mechanism and set the 'medFastStart' timer to 'medFastStartRepeatCount' times 1. The default value is 4.

### ● Format

**config lldp\_med fast\_start repeat\_count <value 1-10>**

### ● Parameters

**<value 1-10>**

Specify a fast start repeat count value between 1 and 10. The default value is 4.

### ● Restrictions

## 46. LLDP Commands

Only Administrator and Operator-level users can issue this command.

### ● Example

To configure a LLDP-MED fast start repeat count of 5:

```
Zxxx0:admin#config lldp_med fast_start repeat_count 5
Command: config lldp_med fast_start repeat_count 5

Success.

Zxxx0:admin#
```

## 46.10. config lldp\_med log state

---

### ● Description

This command is used to configure the log state of LLDP-MED events.

### ● Format

config lldp\_med log state [enable | disable]

### ● Parameters

|                |                                                                     |
|----------------|---------------------------------------------------------------------|
| <b>enable</b>  | Enable the log state for LLDP-MED events.                           |
| <b>disable</b> | Disable the log state for LLDP-MED events. The default is disabled. |

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To enable the log state of LLDP-MED events:

```
Zxxx0:admin#config lldp_med log state enable
Command: config lldp_med log state enable

Success.

Zxxx0:admin#
```

## 46.11. config lldp\_med notification topo\_change ports

---

### ● Description

This command is used to enable or disable each port for sending topology change notification to configured SNMP trap receiver(s) if an endpoint device is removed or moved to another port. The default state is disabled.

### ● Format

config lldp\_med notification topo\_change ports [<portlist> | all] state [enable | disable]

### ● Parameters

|                                                                                              |                                                                                                             |
|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| <b>&lt;portlist&gt;</b> Specify a range of ports to be configured.                           |                                                                                                             |
| <b>all</b>                                                                                   | Specify to set all ports in the system.                                                                     |
| <b>state</b> Enable or disable the SNMP trap notification of topology change detected state. |                                                                                                             |
| <b>enable</b>                                                                                | Enable the SNMP trap notification of topology change detected.                                              |
| <b>disable</b>                                                                               | Disable the SNMP trap notification of topology change detected. The default notification state is disabled. |

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To enable topology change notification on ports 1 to 2:

```
Zxxx0:admin#config lldp_med notification topo_change ports 1-2 state enable
Command: config lldp_med notification topo_change ports 1-2 state enable

Success.

Zxxx0:admin#
```

## 46.12. config lldp\_med ports

### ● Description

This command is used to enable or disable transmitting LLDP-MED TLVs. It effectively disables LLDP-MED on a per-port basis by disabling transmission of TLV capabilities. In this case, the remote table's objects in the LLDP-MED MIB corresponding to the respective port will not be populated.

### ● Format

**config lldp\_med ports [<portlist> | all] med\_transmit\_capabilities [all | {capabilities | network\_policy | inventory}(1)] state [enable | disable]**

### ● Parameters

|                                 |                                                                                                                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;portlist&gt;</b>         | Specify a range of ports to be configured.                                                                                                                                                                        |
| <b>all</b>                      | Specify to set all ports in the system.                                                                                                                                                                           |
| <b>med_transit_capabilities</b> | Select to send the LLDP-MED TLV capabilities specified.                                                                                                                                                           |
| <b>all</b>                      | Select to send capabilities, network policy, and inventory.                                                                                                                                                       |
| <b>capabilities</b>             | (Optional) Specify that the LLDP agent should transmit "LLDP-MED capabilities TLV." If a user wants to transmit LLDP-MED PDU, this TLV type should be enabled. Otherwise, this port cannot transmit LLDP-MED PDU. |
| <b>network_policy</b>           | (Optional) Specify that the LLDP agent should transmit "LLDP-MED network policy TLV."                                                                                                                             |
| <b>inventory</b>                | (Optional) Specify that the LLDP agent should transmit "LLDP-MED inventory TLV."                                                                                                                                  |
| <b>state</b>                    | Enable or disable the transmitting of LLDP-MED TLVs.                                                                                                                                                              |
| <b>enable</b>                   | Enable the transmitting of LLDP-MED TLVs.                                                                                                                                                                         |
| <b>disable</b>                  | Disable the transmitting of LLDP-MED TLVs.                                                                                                                                                                        |

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To enable transmitting of all capabilities on ports 1 to 2:

```
Zxxx0:admin#config lldp_med ports 1-2 med_transmit_capabilities all state enable
Command: config lldp_med ports 1-2 med_transmit_capabilities all state enable

Success.

Zxxx0:admin#
```

## 46.13. show lldp\_med ports

---

### ● Description

This command is used to display LLDP-MED per port configuration for advertisement options.

### ● Format

show lldp\_med ports {<portlist>}

### ● Parameters

---

<portlist> Specify a range of ports to be displayed.

---



---

**NOTE** When a port list is not specified, information for all ports will be displayed.

---

### ● Restrictions

None.

### ● Example

To display LLDP-MED configuration information for port 1:

```
Zxxx0:admin#show lldp_med ports 1
Command: show lldp_med ports 1

Port ID : 1
-----
Topology Change Notification Status      : Enabled
LLDP-MED Capabilities TLV                : Enabled
LLDP-MED Network Policy TLV              : Enabled
LLDP-MED Inventory TLV                   : Enabled

Zxxx0:admin#
```

## 46.14. show lldp\_med

---

### ● Description

This command is used to display the Switching Hub's general LLDP-MED configuration status.

### ● Format

show lldp\_med

## 46. LLDP Commands

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display the Switching Hub's general LLDP-MED configuration status:

```
Zxxx0:admin#show lldp_med
Command: show lldp_med

LLDP-MED System Information:
  Device Class           : Network Connectivity Device
  Hardware Revision      : A1
  Firmware Revision      : 1.0.0.xx
  Software Revision      : 1.0.0.xx
  Serial Number          :
  Manufacturer Name      : MANAGER
  Model Name             : Zxxx0 Gigabit Ethernet S
  Asset ID               :

LLDP-MED Configuration:
  Fast Start Repeat Count : 4

LLDP-MED Log State:Disabled

Zxxx0:admin#
```

## **46.15. show lldp\_med local\_ports**

### ● Description

This command is used to display the per-port LLDP-MED information currently available for populating outbound LLDP-MED advertisements.

### ● Format

**show lldp\_med local\_ports {<portlist>}**

### ● Parameters

---

**<portlist>**Specify a range of ports to be displayed.

---

---

**NOTE** When a port list is not specified, information for all ports will be displayed.

---

### ● Restrictions

None.

### ● Example

To display LLDP-MED information currently available for populating outbound LLDP-MED advertisements for port 1:

```
Zxxx0:admin#show lldp_med local_ports 1
Command: show lldp_med local_ports 1

Port ID                : 1
-----
LLDP-MED Capabilities Support:
  Capabilities           :Support
  Network Policy         :Support
  Location Identification :Not Support
  Extended Power Via MDI PSE :Not Support
  Extended Power Via MDI PD :Not Support
  Inventory              :Support

Network Policy:
  None

Extended Power Via MDI:
  None

Zxxx0:admin#
```

## 46.16. show lldp\_med remote\_ports

---

### ● Description

This command is used to display LLDP-MED information learned from neighbors.

### ● Format

**show lldp\_med remote\_ports {<portlist>}**

### ● Parameters

---

**<portlist>**(Optional) Specify a range of ports to be displayed.

---



## 46. LLDP Commands

---

**NOTE** When a port list is not specified, information for all ports will be displayed.

---

- **Restrictions**

None.

- **Example**

To display remote entry information:

```

Zxxx0:admin#show lldp_med remote_ports 1
Command: show lldp_med remote_ports 1

Port ID : 1
-----
Remote Entities Count : 1
Entity 1
  Chassis ID Subtype      : MAC Address
  Chassis ID              : 00-01-02-03-04-00
  Port ID Subtype        : Net Address
  Port ID                 : 172.18.10.11

  LLDP-MED capabilities:
    LLDP-MED Device Class: Endpoint Device Class III
    LLDP-MED Capabilities Support:
      Capabilities          : Support
      Network Policy        : Support
      Location Identification : Support
      Extended Power Via MDI : Support
      Inventory             : Support
    LLDP-MED Capabilities Enabled:
      Capabilities          : Enabled
      Network Policy        : Enabled
      Location Identification : Enabled
      Extended Power Via MDI : Enabled
      Inventory             : Enabled

  Network Policy:
    Application Type : Voice
      VLAN ID        :
      Priority        :
      DSCP            :
      Unknown         : True
      Tagged          :
    Application Type : Softphone Voice
      VLAN ID        : 200
      Priority        : 7
      DSCP            : 5
      Unknown         : False
      Tagged          : True

  Location Identification:
    Location Subtype: CoordinateBased
      Location Information :
    Location Subtype: CivicAddress
      Location Information :

  Extended Power Via MDI
    Power Device Type: PD Device
      Power Priority    : High
      Power Source      : From PSE
      Power Request     : 8 Watts

```

## 46. LLDP Commands

```
Inventory Management:
```

```
Hardware Revision      :  
Firmware Revision     :  
Software Revision     :  
Serial Number         :  
Manufacturer Name     :  
Model Name            :  
Asset ID              :
```

```
Zxxx0:admin#
```

### 46.17. show lldp local\_ports

---

#### ● Description

This command is used to display the per-port information currently available for populating outbound LLDP advertisements.

#### ● Format

**show lldp local ports {<portlist>} {mode [brief | normal | detailed]}**

#### ● Parameters

---

**<portlist>** (Optional) Specify the ports to be displayed. When a port list is not specified, information for all ports will be displayed.

---

**mode** (Optional) Select the mode: brief, normal, or detailed.

**brief** Specify to display the information in brief mode.

**normal** Specify to display the information in normal mode. This is the default display mode.

**detailed** Specify to display the information in detailed mode.

---

#### ● Restrictions

None.

## ● Example

To display LLDP local port information for port 1:

```
Zxxx0:admin#show lldp local_ports 1
Command: show lldp local_ports 1

Port ID : 1
-----
Port ID Subtype           : MAC Address
Port ID                   : 00-01-02-03-05-00
Port Description          : Zxxx0 R1.0.0.xx
                          Port 1 on Unit 1
Port PVID                  : 1
Management Address Count  : 1
PPVID Entries Count       : 0
VLAN Name Entries Count   : 1
Protocol Identity Entries Count : 0
MAC/PHY Configuration/Status : (See Detail)
Link Aggregation          : (See Detail)
Maximum Frame Size        : 1536

Zxxx0:admin#
```

## 46.18. show lldp mgt\_addr

### ● Description

This command is used to display the LLDP management address.

### ● Format

**show lldp mgmt\_addr** {[ipv4 <ipaddr> | ipv6 <ipv6addr>]}

### ● Parameters

|             |                                                                                                                                                        |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipv4</b> | (Optional) Specify the IPv4 address of the LLDP management address entry.<br><ipaddr> Specify the IPv4 address of the LLDP management address entry.   |
| <b>ipv6</b> | (Optional) Specify the IPv6 address of the LLDP management address entry.<br><ipv6addr> Specify the IPv6 address of the LLDP management address entry. |

### ● Restrictions

None.

## 46. LLDP Commands

### ● Example

To display the LLDP management address:

```
Zxxx0:admin#show lldp mgt_addr
Command: show lldp mgt_addr

Address 1 :
-----
Subtype                : IPv4
Address                : 10.19.72.38
IF Type                : Unknown
OID                    : 1.3.6.1.4.1.396.5.4.1.xx
Advertising Ports      :
Total Entries : 1

Zxxx0:admin#
```

## 46.19. show lldp remote\_ ports

---

### ● Description

This command is used to display the information learned from the neighbor parameters.

### ● Format

**show lldp remote\_ports {<portlist>} {mode [brief | normal | detailed]}**

### ● Parameters

---

**<portlist>** (Optional) Specify the ports to be displayed. When a port list is not specified, information for all ports will be displayed.

---

**mode** (Optional) Select the mode: brief, normal, or detailed.

**brief** Specify to display the information in brief mode.

**normal** Specify to display the information in normal mode. This is the default display mode.

**detailed** Specify to display the information in detailed mode.

---

### ● Restrictions

None.

- **Example**

To display LLDP information for remote ports 1 and 2:

```
Zxxx0:admin#show lldp remote_ports 1-2
Command: show lldp remote_ports 1-2

Remote Entities Count : 0

Zxxx0:admin#
```

## **46.20. show lldp statistics**

---

- **Description**

This command is used to display an overview of neighbor detection activity on the Switching Hub.

- **Format**

**show lldp statistics**

- **Parameters**

None.

- **Restrictions**

None.

- **Example**

To display LLDP statistics:

```
Zxxx0:admin#show lldp statistics
Command: show lldp statistics

Last Change Time          : 3648
Number of Table Insert    : 0
Number of Table Delete    : 0
Number of Table Drop      : 0
Number of Table Ageout    : 0

Zxxx0:admin#
```

## 46.21. show lldp statistics ports

---

### ● Description

This command is used to display LLDP statistic information for individual ports.

### ● Format

show lldp statistics ports {<portlist>}

### ● Parameters

---

<portlist>(Optional) Specify the ports to be displayed.

---

---

**NOTE** When a port list is not specified, information for all ports will be displayed.

---

### ● Restrictions

None.

### ● Example

To display LLDP statistic information for port 1:

```
Zxxx0:admin#show lldp statistics ports 1
Command: show lldp statistics ports 1

Port ID : 1
-----
LLDPStatsTXPortFramesTotal      : 0
LLDPStatsRXPortFramesDiscardTotal : 0
LLDPStatsRXPortFramesErrors     : 0
LLDPStatsRXPortFramesTotal      : 0
LLDPStatsRXPortTTLVsDiscardedTotal : 0
LLDPStatsRXPortTTLVsUnrecognizedTotal : 0
LLDPStatsRXPortAgeoutsTotal     : 0

Zxxx0:admin#
```

## 47. Loopback Interface Commands

A loopback interface is a virtual interface to set this Switching Hub as an output destination.

Assigning a network address to a loopback interface allows you to configure a virtual network. It is also used in other protocols, such as OSPF and BGP.

In this chapter, you will create and delete a loopback interface.

---

```
create loopback ipif <ipif_name 12> {<network_address>} {state [enable | disable]}
config loopback ipif <ipif_name 12> [{ipaddress <network_address> | state [enable | disable]}](1)
show loopback ipif {<ipif_name 12>}
delete loopback ipif [<ipif_name 12> | all]
```

---

### 47.1. create loopback ipif

#### ● Description

This command is used to create a loopback interface on the Switch.

#### ● Format

```
create loopback ipif <ipif_name 12> {<network_address>} {state [enable | disable]}
```

#### ● Parameters

---

**<ipif\_name 12>**

Enter the IP interface name used for this configuration here. This name can be up to 12 characters long.

---

**<network\_address>**

(Optional) Enter the IPv4 network address of the loopback interface here. It specifies a host address and length of network mask.

---

**state**

(Optional) Specifies the state of the loopback interface.

**enable** Specifies that the loopback interface state will be enabled.

**disable** Specifies that the loopback interface state will be disabled.

---

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.



## 47. Loopback Interface Commands

### ● Example

To create one loopback interface named loopback1 with subnet address 20.1.1.1/8 and enable the admin state:

```
Zxxx0:admin# create loopback ipif loopback1 20.1.1.1/8 state enable
Command: create loopback ipif loopback1 20.1.1.1/8 state enable

Success.

Zxxx0:admin#
```

## 47.2. config loopback ipif

### ● Description

This command is used to configure the loopback interface parameters.

### ● Format

**config loopback ipif <ipif\_name 12> [{ipaddress <network\_address> | state [enable | disable]}](1)**

### ● Parameters

---

**<ipif\_name 12>**

Enter the IP interface name used for this configuration here. This name can be up to 12 characters long.

---

**ipaddress**

(Optional) Specifies the IPv4 network address of the loopback interface.

---

**<network\_address>**

Enter the IPv4 network address of the loopback interface here. It specifies a host address and length of network mask.

---

**state**

(Optional) Specifies the state of the loopback interface.

**enable** Specifies that the loopback interface state will be enabled.

**disable** Specifies that the loopback interface state will be disabled.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the loopback interface named loopback1 with subnet address 10.0.0.1/8:

```
Zxxx0:admin# config loopback ipif loopback1 ipaddress 10.0.0.1/8
Command: config loopback ipif loopback1 ipaddress 10.0.0.1/8

Success.

Zxxx0:admin#
```

## 47.3. show loopback ipif

---

### ● Description

This command is used to display the information of the loopback interface.

### ● Format

**show loopback ipif {<ipif\_name 12>}**

### ● Parameters

---

**<ipif\_name 12>**

(Optional) Enter the IP interface name used for this configuration here. This name can be up to 12 characters long.

---

### ● Restrictions

None.

### ● Example

To show the information of the loopback interface named loopback1:

```
Zxxx0:admin# show loopback ipif loopback1
Command: show loopback ipif loopback1

Loopback Interface      : loopback1
Interface Admin State   : Enabled
IPv4 Address            : 10.0.0.1/8 (MANUAL)

Total Entries:1

Zxxx0:admin#
```

## 47.4. delete loopback ipif

---

### ● Description

This command is used to delete a loopback interface.

### ● Format

delete loopback ipif [<ipif\_name 12> | all]

### ● Parameters

---

<ipif\_name 12>

Enter the IP interface name used for this configuration here. This name can be up to 12 characters long.

---

all

Specifies that all the IP loopback interfaces will be deleted.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete the loopback interface named loopback1:

```
Zxxx0:admin# delete loopback ipif loopback1
Command: delete loopback ipif loopback1

Success.

Zxxx0:admin#
```

## 48. MAC Notification Commands

These commands are used to send a notification to the management server using a SNMP trap when a new entry is registered in the MAC address table of this Switching Hub. It detects access to the network from unauthorized devices.

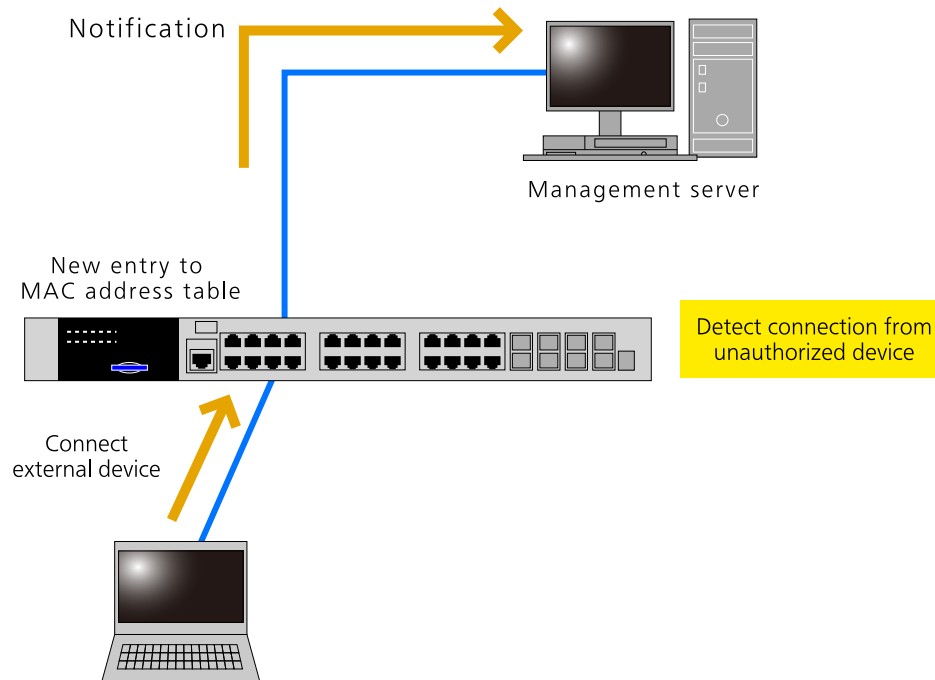


Figure 48-1 MAC Notification overview

```
enable mac_notification
disable mac_notification
config mac_notification {interval <int 1-2147483647> | historysize <int 1-500>}(1)
config mac_notification ports [<portlist> | all] [enable | disable]
show mac_notification
show mac_notification ports [<portlist>]
```

### 48.1. enable mac\_notification

#### ● Description

This command is used to enable the trap notification for new learned MAC addresses on the Switch.

#### ● Format

```
enable mac_notification
```

## 48. MAC Notification Commands

### ● Parameters

None.

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To enable the MAC notification function:

```
Zxxx0:admin#enable mac_notification
Command: enable mac_notification

Success.

Zxxx0:admin#
```

## 48.2. disable mac\_notification

---

### ● Description

This command is used to disable the trap notification for new learned MAC addresses on the Switch.

### ● Format

**disable mac\_notification**

### ● Parameters

None.

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To disable the MAC notification function:

```
Zxxx0:admin#disable mac_notification
Command: disable mac_notification

Success.

Zxxx0:admin#
```

## 48.3. config mac\_notification

---

### ● Description

This command is used to configure the Switching Hub's MAC address table notification global settings.

### ● Format

**config mac\_notification {interval <int 1-2147483647> | historysize <int 1-500>}(1)**

### ● Parameters

---

**interval** Specify the time interval in seconds to trigger the notification.  
 <int 1-2147483647>  
 Specify between 1 second and 2147483647 seconds.

---

**historysize**  
 Specify the entries of new learned MAC to trigger the notification.  
 <int 1-500>  
 Specify up to 500 entries.

---

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To configure the Switching Hub's MAC address table notification global settings:

```
Zxxx0:admin#config mac_notification interval 1 historysize 500
Command: config mac_notification interval 1 historysize 500

Success.

Zxxx0:admin#
```

## 48.4. config mac\_notification ports

---

### ● Description

This command is used to configure the port's MAC address table notification status settings.

### ● Format

**config mac\_notification ports [<portlist> | all] [enable | disable]**

## 48. MAC Notification Commands

### ● Parameters

|                         |                                                               |
|-------------------------|---------------------------------------------------------------|
| <b>&lt;portlist&gt;</b> | Specify a range of ports to be configured.                    |
| <b>all</b>              | Specify to set all ports in the system.                       |
| <b>enable</b>           | Specify to enable the port's MAC address table notification.  |
| <b>disable</b>          | Specify to disable the port's MAC address table notification. |

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To enable MAC address table notification for Port 7:

```
Zxxx0:admin#config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success.

Zxxx0:admin#
```

## 48.5. show mac\_notification

### ● Description

This command is used to display the Switching Hub's MAC address table notification global settings.

### ● Format

**show mac\_notification**

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To show the Switching Hub's MAC address table notification global settings:

```
Zxxx0:admin#show mac_notification
Command: show mac_notification

Global MAC Notification Settings

State      : Enabled
Interval   : 1
History Size : 500

Zxxx0:admin#
```

## 48.6. show mac\_notification ports

### ● Description

This command is used to display the port's MAC address table notification status settings.

### ● Format

`show mac_notification ports {<portlist>}`

### ● Parameters

---

**<portlist>**(Optional) Specify a range of ports to be configured.

---

### ● Restrictions

None.

### ● Example

To display the MAC address table notification status settings of all ports:

```
Zxxx0:admin#show mac_notification ports
Command: show mac_notification ports

Port #  MAC Address Table Notification State
-----  -
1                Disabled
2                Disabled
3                Disabled
4                Disabled
5                Disabled
6                Disabled
7                Disabled
8                Disabled
9                Disabled
10               Disabled

Zxxx0:admin#
```



## 49. MAC-based Access Control Commands

MAC-based Access Control is a function to authorize a device connected to the Switching Hub based on its MAC address to control access to the network.

A RADIUS server or local database in this Switching Hub can be selected for the authentication server. You can configure the access control settings to authorize access to a guest VLAN to permit Internet use only, as well as blocking access, when authorization fails.

---

```

enable mac_based_access_control
disable mac_based_access_control
config mac_based_access_control password <passwd 16>
config mac_based_access_control method [local | radius]
config mac_based_access_control guest_vlan ports <portlist>
config mac_based_access_control ports [<portlist> | all] {state [enable | disable] | aging_time
    [infinite | <min 1-1440>] | block_time <sec 0-300> | max_users [<value 1-4000> |
    no_limit]}(1)
create mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid <vlanid 1-4094>]
delete mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid <vlanid 1-4094>]
clear mac_based_access_control auth_state [ports [all | <portlist>] | mac_addr <macaddr>]
create mac_based_access_control_local mac <macaddr> {[vlan <vlan_name 32> | vlanid <vlanid 1-
4094>]}
config mac_based_access_control_local mac <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-
4094> | clear_vlan]
config mac_based_access_control max_users [<value 1-4000> | no_limit]
config mac_based_access_control authorization attributes {radius [enable | disable] | local [enable
| disable]}(1)
delete mac_based_access_control_local [mac <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-
4094>]
show mac_based_access_control auth_state ports {<portlist>}
show mac_based_access_control {ports {<portlist>}}
show mac_based_access_control_local {[mac <macaddr> | vlan <vlan_name 32> | vlanid <vlanid
1-4094>]}
config mac_based_access_control log state [enable | disable]
config mac_based_access_control trap state [enable | disable]
config mac_based_access_control password_type [manual_string | client_mac_address]

```

---

## 49.1. enable mac\_based\_access\_control

---

- **Description**

This command is used to enable the MAC-based access control function.

- **Format**

enable mac\_based\_access\_control

- **Parameters**

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To enable MAC-based access control:

```
Zxxx0:admin#enable mac_based_access_control
Command: enable mac_based_access_control

Success.

Zxxx0:admin#
```

## 49.2. disable mac\_based\_access\_control

---

- **Description**

This command is used to disable the MAC-based access control function.

- **Format**

disable mac\_based\_access\_control

- **Parameters**

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

## 49. MAC-based Access Control Commands

### ● Example

To disable MAC-based access control:

```
Zxxx0:admin#disable mac_based_access_control
Command: disable mac_based_access_control

Success.

Zxxx0:admin#
```

## 49.3. config mac\_based\_access\_control password

---

### ● Description

This command is used to set the password that will be used for authentication via RADIUS server.

### ● Format

config mac\_based\_access\_control password <passwd 16>

### ● Parameters

---

<passwd 16>

In RADIUS mode, the Switching Hub communicates with the RADIUS server using this password. The maximum length of the key is 16 characters.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the password "rosebud" that will be used for authentication via RADIUS server:

```
Zxxx0:admin#config mac_based_access_control password rosebud
Command: config mac_based_access_control password rosebud

Success.

Zxxx0:admin#
```

## 49.4. config mac\_based\_access\_control method

---

### ● Description

This command is used to authenticate via a local database or a RADIUS server.

### ● Format

config mac\_based\_access\_control method [local | radius]

### ● Parameters

|               |                                             |
|---------------|---------------------------------------------|
| <b>local</b>  | Specify to authenticate via local database. |
| <b>radius</b> | Specify to authenticate via RADIUS server.  |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the MAC-based access control method as local:

```
Zxxx0:admin#config mac_based_access_control method local
Command: config mac_based_access_control method local

Success.

Zxxx0:admin#
```

## 49.5. config mac\_based\_access\_control guest\_vlan ports

---

### ● Description

This command is used to put the specified port in guest VLAN mode. For those ports not contained in the port list, they are in non-guest VLAN mode. For detailed information about the operation of guest VLAN mode, please see the description for configuring the MAC-based access control port command.

### ● Format

config mac\_based\_access\_control guest\_vlan ports <portlist>

## 49. MAC-based Access Control Commands

### ● Parameters

---

**<portlist>** When a port is configured as guest VLAN member port, this port will move to guest VLAN if its MAC-based access control state is enable.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the MAC-based access control guest VLAN membership for port 1 to 8:

```
Zxxx0:admin# config mac_based_access_control guest_vlan ports 1-8
Command: config mac_based_access_control guest_vlan ports 1-8

Success.

Zxxx0:admin#
```

## **49.6. config mac\_based\_access\_control ports**

### ● Description

This command is used to configure the MAC-based access control setting. When the MAC-based access control function is enabled for a port, and the port is not a MAC-based access control guest VLAN member, the user who is attached to this port will not be forwarded unless the user passes the authentication. A user that does not pass the authentication will not be serviced by the Switching Hub. If the user passes the authentication, the user will be able to forward traffic operated under the assigned VLAN.

When the MAC-based access control function is enabled for a port, and the port is a MAC-based access control guest VLAN member, the port(s) will be removed from the original VLAN(s) member ports, and added to MAC-based access control guest VLAN member ports. Before the authentication process starts, the user is able to forward traffic under the guest VLAN. After the authentication process, the user will be able to access the assigned VLAN.

If the port authorize mode is port based mode, when the port has been moved to the authorized VLAN, the subsequent users will not be authenticated again. They will operate in the current authorized VLAN. If the port authorize mode is host based mode, then each user will be authorized individually and be capable of getting its own assigned VLAN.

### ● Format

```
config mac_based_access_control ports [<portlist> | all] {state [enable | disable] |
aging_time [infinite | <min 1-1440>] | block_time <sec 0-300> | max_users [<value 1-
4000> | no_limit]](1)
```

## ● Parameters

|                             |                                                                                                                                                                                           |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;portlist&gt;</b>     | Specify a range of ports to configure the MAC-based access control settings                                                                                                               |
| <b>all</b>                  | Specify to select all the ports.                                                                                                                                                          |
| <b>state</b>                | Specify whether the MAC-based access control function is enabled or disabled.                                                                                                             |
| <b>enable</b>               | Specify to enable the MAC-based access control function.                                                                                                                                  |
| <b>disable</b>              | Specify to disable the MAC-based access control function.                                                                                                                                 |
| <b>aging_time</b>           | Specify a time period during which an authenticated host will be kept in the authenticated state. When the aging time is timed-out, the host will be moved back to unauthenticated state. |
| <b>infinite</b>             | Specify an unlimited aging time.                                                                                                                                                          |
| <b>&lt;min 1-1440&gt;</b>   | Specify the age-out time, in minutes, between 1 and 1440.                                                                                                                                 |
| <b>block_time</b>           | Specify the blocking time, in seconds, between 0 and 300.                                                                                                                                 |
| <b>&lt;second 0-300&gt;</b> | Specify the blocking time. The blocking time value must be between 0 and 300 seconds.                                                                                                     |
| <b>max_users</b>            | Specify the number of maximum users. The default value is 1024 users.                                                                                                                     |
| <b>&lt;value 1-4000&gt;</b> | Specify the maximum number of users between 1 and 4000.                                                                                                                                   |
| <b>no_limit</b>             | Specify unlimitedly until 4000 of a maximum number of users.                                                                                                                              |

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure the port state for ports 1 to 8:

```
Zxxx0:admin# config mac_based_access_control ports 1-8 state enable
Command: config mac_based_access_control ports 1-8 state enable

Success.

Zxxx0:admin#
```

## 49.7. create mac\_based\_access\_control

---

### ● Description

This command is used to create a MAC-based access control guest VLAN.

### ● Format

**create mac\_based\_access\_control [guest\_vlan <vlan\_name 32> | guest\_vlanid <vlanid 1-4094>]**

### ● Parameters

---

#### guest\_vlan

Specify the name of the guest VLAN.

**<vlan\_name 32>**

Specify the name of the guest VLAN. The guest VLAN name can be up to 32 characters long.

---

#### guest\_vlanid

Specify the VLAN ID of the guest VLAN.

**<vlanid 1-4094>**

Specify the VLAN ID of the guest VLAN. The guest VLAN ID must be between 1 and 4094.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create a MAC-based access control guest VLAN:

```
Zxxx0:admin#create mac_based_access_control guest_vlan default
Command: create mac_based_access_control guest_vlan default

Success.

Zxxx0:admin#
```

## 49.8. delete mac\_based\_access\_control

---

### ● Description

This command is used to delete MAC-based access control guest VLANs.

### ● Format

**delete mac\_based\_access\_control [guest\_vlan <vlan\_name 32> | guest\_vlanid <vlanid 1-4094>]**

### ● Parameters

---

#### guest\_vlan

Specify the name of the guest VLAN.

**<vlan\_name 32>**

Specify the name of the guest VLAN. The guest VLAN name can be up to 32 characters long.

---

#### guest\_vlanid

Specify the VLAN ID of the guest VLAN.

**<vlanid 1-4094>**

Specify the VLAN ID of the guest VLAN. The guest VLAN ID must be between 1 and 4094.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete a MAC-based access control guest VLAN:

```
Zxxx0:admin#delete mac_based_access_control guest_vlan default
Command: delete mac_based_access_control guest_vlan default

Success.

Zxxx0:admin#
```



## 49.9. clear mac\_based\_access\_control auth\_state

---

### ● Description

This command is used to clear the authentication state of a user (or port). The port (or the user) will return to un-authenticated state. All the timers associated with the port (or the user) will be reset.

### ● Format

**clear mac\_based\_access\_control auth\_state [ports [all | <portlist>] | mac\_addr <macaddr>]**

### ● Parameters

---

|                         |                                                           |
|-------------------------|-----------------------------------------------------------|
| <b>ports</b>            | Specify the port range to clear the authentication state. |
| <b>all</b>              | Specify all ports.                                        |
| <b>&lt;portlist&gt;</b> | Specify a range of ports.                                 |

---

|                        |                                                         |
|------------------------|---------------------------------------------------------|
| <b>mac_addr</b>        | Specify to clear a specified host authentication state. |
| <b>&lt;macaddr&gt;</b> | Enter the MAC address here.                             |

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To clear the authentication state of all ports:

```
Zxxx0:admin#clear mac_based_access_control auth_state ports all
Command: clear mac_based_access_control auth_state ports all

Success.

Zxxx0:admin#
```

## 49.10. create mac\_based\_access\_control\_local mac

---

### ● Description

This command is used to create a database entry.

### ● Format

**create mac\_based\_access\_control\_local mac <macaddr> {[vlan <vlan\_name 32> |  
vlanid <vlanid 1-4094>]}**

### ● Parameters

---

**<macaddr>**

Specify the MAC address that access accepts by local mode.

---

**vlan** (Optional) If the MAC address is authorized, the port will be assigned to this VLAN.  
**<vlan\_name 32>**

Specify a VLAN name up to 32 characters long.

---

**vlanid** (Optional) If the MAC address is authorized, the port will be assigned to this VLAN ID.  
**<vlanid 1-4094>**

Specify a VLAN ID between 1 and 4094.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create a local database entry:

```
Zxxx0:admin#create mac_based_access_control_local mac 00-00-00-00-00-01 vlan
default
Command: create mac_based_access_control_local mac 00-00-00-00-00-01 vlan default

Success.

Zxxx0:admin#
```

## 49.11. config mac\_based\_access\_control\_local mac

---

### ● Description

This command is used to modify a database entry.

### ● Format

config mac\_based\_access\_control\_local mac <macaddr> [vlan <vlan\_name 32> | vlanid <vlanid 1-4094> | clear\_vlan]

### ● Parameters

---

**<macaddr>**

Specify the MAC address that access is accepted by local mode.

---

**vlan** If the MAC address is authorized, the port will be assigned to this VLAN.

**<vlan\_name 32>**

Specify a VLAN name up to 32 characters long.

---

**vlanid** If the MAC address is authorized, the port will be assigned to this VLAN ID.

**<vlanid 1-4094>**

Specify a VLAN ID between 1 and 4094.

---

**clear\_vlan**

Specify to clear the specified VLAN.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure a local database entry:

```
Zxxx0:admin#config mac_based_access_control_local mac 00-00-00-00-00-01 vlan
default
Command: config mac_based_access_control_local mac 00-00-00-00-00-01 vlan default

Success.

Zxxx0:admin#
```

## 49.12. config mac\_based\_access\_control max\_users

---

### ● Description

This command is used to configure the MAC-based access control maximum number of authorized users.

### ● Format

config mac\_based\_access\_control max\_users [<value 1-4000> | no\_limit]

### ● Parameters

---

<value 1-4000>

Specify the maximum number of authorized users.

---

no\_limit

Specify an unlimited number(4000) of users.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the MAC-based access control maximum number of authorized users:

```
Zxxx0:admin#config mac_based_access_control max_users 2
Command: config mac_based_access_control max_users 2

Success.

Zxxx0:admin#
```

## 49.13. config mac\_based\_access\_control authorization attributes

---

### ● Description

This command is used to enable or disable the acceptance of an authorized configuration. When authorization is enabled for MAC-based access controls with RADIUS authentication, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADIUS server will be accepted if the global authorization status is enabled. When authorization is enabled for MAC-based access controls with local authentication, the authorized attributes assigned by the local database will be accepted.

## 49. MAC-based Access Control Commands

### ● Format

**config mac\_based\_access\_control authorization attributes {radius [enable | disable] | local [enable | disable]}(1)**

### ● Parameters

---

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>radius</b> | Specify to enable or disable the authorized attributes assigned by the RADIUS server that will be accepted.<br><b>enable</b><br>If specified to enable, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADIUS server will be accepted if the global authorization status is enabled. The default state is enabled.<br><b>disable</b><br>If specified to disable, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADIUS server will not be accepted even if the global authorization status is enabled. |
| <b>local</b>  | Specify to enable to disable the authorized attributes assigned by the local database.<br><b>enable</b><br>If specified to enable, the authorized attributes assigned by the local database will be accepted if the global authorization status is enabled. The default state is enabled.<br><b>disable</b><br>If specified to disable, the authorized attributes assigned by the local database will not be accepted even if the global authorization status is enabled.                                                                                                                              |

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To disable the configuration authorized from the local database:

```
Zxxx0:admin#config mac_based_access_control authorization attributes local disable
Command: config mac_based_access_control authorization attributes local disable

Success.

Zxxx0:admin#
```

## 49.14. delete mac\_based\_access\_control\_local

### ● Description

This command is used to delete a database entry

### ● Format

**delete mac\_based\_access\_control\_local [mac <macaddr> | vlan <vlan\_name 32> |  
vlanid <vlanid 1-4094>]**

### ● Parameters

|               |                                                                                                                         |
|---------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>mac</b>    | Delete database by this MAC address.<br><b>&lt;macaddr&gt;</b><br>Enter the MAC address here.                           |
| <b>vlan</b>   | Delete database by this VLAN name.<br><b>&lt;vlan_name 32&gt;</b><br>Specify a VLAN name up to 32 characters long.      |
| <b>vlanid</b> | Delete database by this VLAN ID.<br><b>&lt;vlanid 1-4094&gt;</b><br>Specify a VLAN ID value must be between 1 and 4094. |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete a MAC-based access control local by MAC address:

```
Zxxx0:admin#delete mac_based_access_control_local mac 00-00-00-00-00-01
Command: delete mac_based_access_control_local mac 00-00-00-00-00-01

Success.

Zxxx0:admin#
```

To delete a MAC-based access control local by VLAN name:

```
Zxxx0:admin#delete mac_based_access_control_local vlan default
Command: delete mac_based_access_control_local vlan default

Success.

Zxxx0:admin#
```

## 49.15. show mac\_based\_access\_control auth\_state ports

---

### ● Description

This command is used to display MAC-based access control authentication MAC information.

### ● Format

**show mac\_based\_access\_control auth\_state ports {<portlist>}**

### ● Parameters

---

**<portlist>**(Optional) Specify the ports to display.

---

### ● Restrictions

None.

### ● Example

To display MAC-based access control authentication MAC information:

```
Zxxx0:admin# show mac_based_access_control auth_state ports
Command: show mac_based_access_control auth_state ports

(P): Port-based      Prio: Priority

Port      MAC Address          Original  State      VID  Prio Aging Time/
          RX VID                                     Block Time
-----
1         00-00-00-00-00-01      1         Authenticated -    6    1439
1         00-00-12-00-03-00      1         Blocked    -    -    286
3         00-00-00-00-00-02 (P) 1         Authenticated -    6    1440

Total Authenticating Hosts : 0
Total Authenticated Hosts  : 2
Total Blocked Hosts        : 1

Zxxx0:admin#
```

## 49.16. show mac\_based\_access\_control

---

### ● Description

This command is used to display MAC-based access control information.

### ● Format

**show mac\_based\_access\_control** {ports {<portlist>}}

### ● Parameters

---

|                         |                                                                        |
|-------------------------|------------------------------------------------------------------------|
| <b>ports</b>            | (Optional) Specify to display the MAC-based access control port state. |
| <b>&lt;portlist&gt;</b> | Specify a range of ports to be displayed.                              |

---

### ● Restrictions

None.

### ● Example

To display MAC-based access control information:

```
Zxxx0:admin#show mac_based_access_control
Command: show mac_based_access_control

MAC-based Access Control
-----
State                : Disabled
Method               : Local
Password Type        : Manual String
Password              : default
Max User              : No Limit
Guest VLAN           :
Guest VLAN Member Ports:
RADIUS Authorization : Enabled
Local Authorization  : Enabled
Trap State           : Enabled
Log State             : Enabled

Zxxx0:admin#
```

To display MAC-based access control information for ports 1 to 4:



## 49. MAC-based Access Control Commands

```
Zxxx0:admin#show mac_based_access_control ports 1-4
Command: show mac_based_access_control ports 1-4
```

| Port | State    | Aging Time<br>(min) | Block Time<br>(sec) | Max User |
|------|----------|---------------------|---------------------|----------|
| 1    | Disabled | 1440                | 300                 | 1024     |
| 2    | Disabled | 1440                | 300                 | 1024     |
| 3    | Disabled | 1440                | 300                 | 1024     |
| 4    | Disabled | 1440                | 300                 | 1024     |

```
Zxxx0:admin#
```

### 49.17. show mac\_based\_access\_control\_local

#### ● Description

This command is used to display MAC-based access control local data.

#### ● Format

**show mac\_based\_access\_control\_local** {[mac <macaddr> | vlan <vlan\_name 32> |  
vlanid <vlanid 1-4094>]}

#### ● Parameters

|               |                                                                                                                              |
|---------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>mac</b>    | (Optional) Display MAC-based access control local databases by this MAC address.<br><macaddr><br>Enter the MAC address here. |
| <b>vlan</b>   | (Optional) Specify the VLAN.<br><vlan_name 32><br>Specify the VLAN name up to 32 characters long.                            |
| <b>vlanid</b> | (Optional) Specify the VLAN ID.<br><vlanid 1-4094><br>Specify the VLAN ID value between 1 and 4094.                          |

#### ● Restrictions

None.

#### ● Example

To display MAC-based access control local data:

```
Zxxx0:admin#show mac_based_access_control_local
Command: show mac_based_access_control_local

MAC Address          VID
-----
00-00-00-00-00-01    1

Total Entries:1

Zxxx0:admin#
```

To display MAC-based access control local data by MAC address:

```
Zxxx0:admin#show mac_based_access_control_local mac 00-00-00-00-00-01
Command: show mac_based_access_control_local mac 00-00-00-00-00-01

MAC Address          VID
-----
00-00-00-00-00-01    1

Total Entries:1

Zxxx0:admin#
```

To display MAC-based access control local data by VLAN:

```
Zxxx0:admin#show mac_based_access_control_local vlan default
Command: show mac_based_access_control_local vlan default

MAC Address          VID
-----
00-00-00-00-00-01    1

Total Entries: 1

Zxxx0:admin#
```

## 49.18. config mac\_based\_access\_control log state

---

### ● Description

This command is used to enable or disable the generating of MAC-based Access Control logs.

### ● Format

config mac\_based\_access\_control log state [enable | disable]

## 49. MAC-based Access Control Commands

### ● Parameters

---

|                |                                                                       |
|----------------|-----------------------------------------------------------------------|
| <b>state</b>   | Specifies the log state for MAC-based Access Control.                 |
| <b>enable</b>  | Specifies that the log for MAC-based Access Control will be enabled.  |
| <b>disable</b> | Specifies that the log for MAC-based Access Control will be disabled. |

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To disable the log state for MAC-based Access Control:

```
Zxxx0:admin# config mac_based_access_control log state disable
Command: config mac_based_access_control log state disable

Success.

Zxxx0:admin#
```

## 49.19. config mac\_based\_access\_control trap state

---

### ● Description

This command is used to enable or disable the sending of MAC-based Access Control traps.

### ● Format

**config mac\_based\_access\_control trap state [enable | disable]**

### ● Parameters

---

|                |                                                                              |
|----------------|------------------------------------------------------------------------------|
| <b>state</b>   | Specifies the trap state for MAC-based Access Control.                       |
| <b>enable</b>  | Specifies that the trap state for MAC-based Access Control will be enabled.  |
| <b>disable</b> | Specifies that the trap state for MAC-based Access Control will be disabled. |

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To enable the trap state for MAC-based Access Control:

```
Zxxx0:admin# config mac_based_access_control trap state enable
Command: config mac_based_access_control trap state enable

Success.

Zxxx0:admin#
```

## 49.20. config mac\_based\_access\_control password\_type

---

### ● Description

This command is used to configure the type of RADIUS authentication password for MAC-based Access Control.

### ● Format

```
config mac_based_access_control password_type [manual_string |
client_mac_address]
```

### ● Parameters

---

#### manual\_string

Specifies to use the same string as password for all clients do RADIUS authentication, the string can be configured by using the command "config mac\_based\_access\_control password".

---

#### client\_mac\_address

Specifies to use the client's MAC address as the password for RADIUS authentication. The MAC address format can be configured by using the command "config authentication mac\_format".

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure the MAC-based Access Control using client's MAC address as authentication password:

## 49. MAC-based Access Control Commands

```
Zxxx0:admin# config mac_based_access_control password_type client_mac_address
Command: config mac_based_access_control password_type client_mac_address

Success.

Zxxx0:admin#
```

To configure the MAC-based Access Control using "manual\_string" as authentication password:

```
Zxxx0:admin# config mac_based_access_control password_type manual_string
Command: config mac_based_access_control password_type manual_string

Success.

Zxxx0:admin#
```



---

## 50. MD5 Commands

---

---

```
create md5 key <key_id 1-255> <password 16>
config md5 key <key_id 1-255> <password 16>
delete md5 key <key_id 1-255>
show md5 {key <key_id 1-255>}
```

---

### 50.1. create md5

---

#### ● Description

This command is used to create an MD5 key table.

#### ● Format

```
create md5 key <key_id 1-255> <password 16>
```

#### ● Parameters

---

**<key\_id 1-255>**

Enter the MD5 key to be added. This key must be between 1 and 255.

---

**<password 16>**

Enter an alphanumeric string of between 1 and 16, case-sensitive characters, used to generate the Message Digest which is in turn used to authenticate OSPF packets within the OSPF routing domain.

---

#### ● Restrictions

Only Administrator and Operator-level users can issue this command.

#### ● Example

To create an MD5 key table:

```
Zxxx0:admin#create md5 key 1 zequo
Command: create md5 key 1 zequo

Success.

Zxxx0:admin#
```

## 50.2. config md5

---

### ● Description

This command is used to configure an MD5 key and password. The MD5 Configuration allows for the entry of a 16 character Message Digest - version 5 (MD5) key which can be used to authenticate every packet exchanged between OSPF routers. It is used as a security mechanism to limit the exchange of network topology information to the OSPF routing domain.

### ● Format

**config md5 key <key\_id 1-255> <password 16>**

### ● Parameters

---

**key\_id 1-255>**

Enter the MD5 key to be configured. This key must be between 1 and 255.

---

**<password 16>**

Enter an alphanumeric string of between 1 and 16, case-sensitive characters, used to generate the Message Digest which is in turn used to authenticate OSPF packets within the OSPF routing domain.

---

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To configure an MD5 key and password:

```
Zxxx0:admin#config md5 key 1 zequol
Command: config md5 key 1 zequol

Success.

Zxxx0:admin#
```

## 50.3. delete md5

---

### ● Description

This command is used to delete an MD5 key table.

### ● Format

**delete md5 key <key\_id 1-255>**



## 50. MD5 Commands

### ● Parameters

---

**<key\_id 1-255>**

Enter the MD5 key to be removed. This key must be between 1 and 255.

---

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To delete an MD5 key table:

```
Zxxx0:admin#delete md5 key 1
Command: delete md5 key 1

Success.

Zxxx0:admin#
```

## 50.4. show md5

---

### ● Description

This command is used to display the MD5 key table.

### ● Format

**show md5 {key <key\_id 1-255>}**

### ● Parameters

---

**key** (Optional) Specify that the MD5 key will be displayed.

**<key\_id 1-255>**

Enter the MD5 key used here. This key must be between 1 and 255.

---

If no parameter is specified, the system will display the MD5 key table.

---

### ● Restrictions

None.

### ● Example

To display the MD5 key table:

```
Zxxx0:admin#show md5
Command: show md5

MD5 Key Table Configurations

Key-ID  Key
-----  -----
1       zequol

Total Entries: 1

Zxxx0:admin#
```

## 51. Mirror Commands

The commands are used to mirror (copy) transmit and receive packets on a specified port to other port and monitor packet contents. You can configure the settings, such as mirroring of all transmit and receive packets by setting multiple ports to a mirror group or mirroring of only transmit or receive packets.

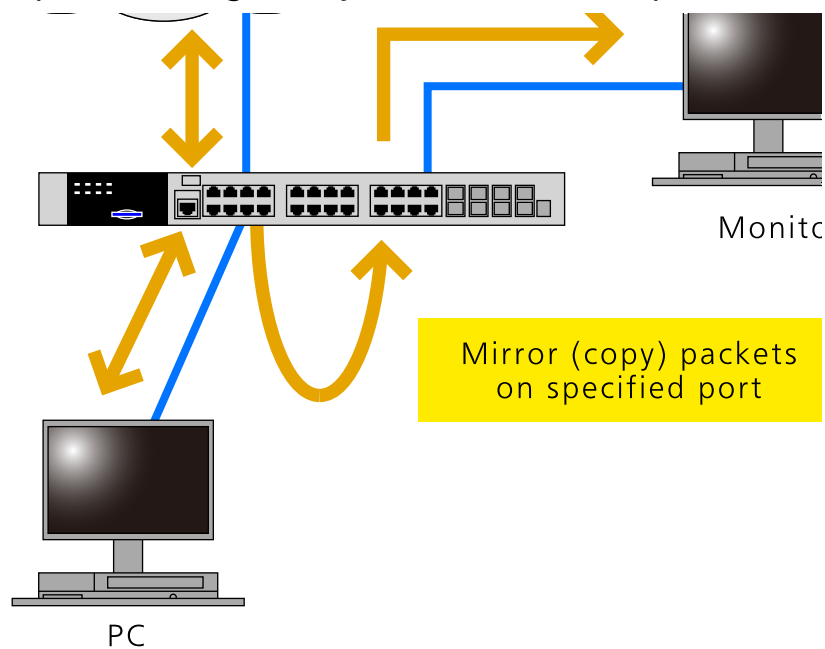


Figure 51-1 Mirroring overview

```
create mirror group_id <value 1-4>
config mirror port <port> {[add | delete] source ports <portlist> [rx | tx | both]}
config mirror group_id <value 1-4> {target_port <port> | [add | delete] source ports <portlist> [rx
| tx | both] | state [enable | disable]}(1)
delete mirror group_id <value 1-4>
enable mirror
disable mirror
show mirror {group_id <value 1-4>}
```

### 51.1. create mirror group\_id

#### ● Description

This command is used to create a mirror group. If the mirror group has existed, do nothing and return success.

#### ● Format

```
create mirror group_id <value 1-4>
```

## ● Parameters

**<value 1-4>**

Enter the mirror group ID used here. This value must be between 1 and 4.

## ● Restrictions

Only Administrator and Operator-level users can issue this command.

## ● Example

Create mirror group 3:

```
Zxxx0:admin# create mirror group_id 3
Command: create mirror group_id 3

Success.

Zxxx0:admin#
```

# 51.2. config mirror port

## ● Description

This command is used to allow a range of ports to have all of their traffic also sent to a designated port where a network sniffer or other device can monitor the network traffic. In addition, you can specify that only traffic received by, sent by or both is mirrored to the target port.

## ● Format

**config mirror port <port> {[add | delete] source ports <portlist> [rx | tx | both]}**

## ● Parameters

**<port>** Specify the port that will receive the packets duplicated at the mirror port.

**add** (Optional) Specify the mirror entry to be added.

**delete** (Optional) Specify the mirror entry to be deleted.

**source ports**

(Optional) Specify the ports that will be mirrored. All packets entering and leaving the source port can be duplicated in the mirror port.

**<portlist>**

Specify a range of ports to be configured.

**rx** (Optional) Allow the mirroring of only packets received (flowing into) the port or ports in the port list.

**tx** (Optional) Allow the mirroring of only packets sent (flowing out of) the port or ports in the port list.

**both** (Optional) Mirror all the packets received or sent by the port or ports in the port list.

## 51. Mirror Commands

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To add mirroring target port 6 and the source ports 1 to 5 rx and tx packets:

```
Zxxx0:admin#config mirror port 6 add source ports 1-5 both
Command: config mirror port 6 add source ports 1-5 both

Success.

Zxxx0:admin#
```

## 51.3. config mirror group\_id

### ● Description

This command used to configure mirror group's parameters. It can configure mirror group's target port, state and source ports. The mirror group target port can't be a member of all mirror groups' source ports. Each mirror group's target port can be the same port. But each mirror group's source ports can't overlap.

### ● Format

**config mirror group\_id** <value 1-4> {**target\_port** <port> | [**add** | **delete**] **source ports** <portlist> [**rx** | **tx** | **both**] | **state** [**enable** | **disable**]}

### ● Parameters

|                                                                                            |                                                                                                                                                 |
|--------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;value 1-4&gt;</b>                                                                   |                                                                                                                                                 |
| Enter the mirror group ID used here. This value must be between 1 and 4.                   |                                                                                                                                                 |
| <b>target_port</b>                                                                         |                                                                                                                                                 |
| (Optional) Specifies the port that will receive the packets duplicated at the mirror port. |                                                                                                                                                 |
| <b>&lt;port&gt;</b>                                                                        |                                                                                                                                                 |
| Enter the target port number used here.                                                    |                                                                                                                                                 |
| <b>add</b>                                                                                 | (Optional) Specifies the mirror source ports to be add.                                                                                         |
| <b>delete</b>                                                                              | (Optional) Specifies the mirror source ports to be delete                                                                                       |
| <b>source</b>                                                                              | (Optional) Specifies the source ports used.                                                                                                     |
| <b>ports</b>                                                                               | (Optional) Specifies the list of ports used as source ports.                                                                                    |
|                                                                                            | <b>&lt;portlist&gt;</b>                                                                                                                         |
| Enter the list of ports to be used as the source ports here.                               |                                                                                                                                                 |
| <b>rx</b>                                                                                  | (Optional) Specifies that only the received packets on the mirror group source ports will be mirrored to the mirror group target port.          |
| <b>tx</b>                                                                                  | (Optional) Specifies that only the sent packets on the mirror group source ports will be mirrored to the mirror group target port.              |
| <b>both</b>                                                                                | (Optional) Specifies that both the received and sent packets on the mirror group source ports will be mirrored to the mirror group target port. |

---

|                |                                                                                             |
|----------------|---------------------------------------------------------------------------------------------|
| <b>state</b>   | (Optional) Specifies the mirror group state to enable or disable the mirror group function. |
| <b>enable</b>  | Specifies that the mirror group state will be enabled.                                      |
| <b>disable</b> | Specifies that the mirror group state will be disabled.                                     |

---

## ● Restrictions

Only Administrator and Operator-level users can issue this command.

## ● Example

Configure mirror group 2 with state enable and add source ports 1:4-1:9:

```
Zxxx0:admin# config mirror group_id 2 state enable add source ports 4-9 both
Command: config mirror group_id 2 state enable add source ports 4-9 both

Success.

Zxxx0:admin#
```

# 51.4. delete mirror group\_id

---

## ● Description

This command is used to delete a mirror group on the Switch.

## ● Format

**delete mirror group\_id <value 1-4>**

## ● Parameters

---

**<value 1-4>**  
Enter the mirror group ID used here. This value must be between 1 and 4.

---

## ● Restrictions

Only Administrator and Operator-level users can issue this command.

## ● Example

To delete mirror group 3:

```
Zxxx0:admin# delete mirror group_id 3
Command: delete mirror group_id 3

Success.

Zxxx0:admin#
```

## 51.5. enable mirror

---

### ● Description

This command, combined with the disable mirror command below, allows you to enable or disable mirror function without having to modify the mirror session configuration.

---

**NOTE** If the target port hasn't been set, enable mirror will not take effect.

---

### ● Format

enable mirrorg

### ● Parameters

None.

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To enable mirroring configurations:

```
Zxxx0:admin#enable mirror
Command: enable mirror

Success.

Zxxx0:admin#
```

## 51.6. disable mirror

---

### ● Description

This command, combined with the enable mirror command above, allows you to enable or disable mirror function without having to modify the mirror session configuration.

### ● Format

disable mirror

### ● Parameters

None.

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To disable mirroring configurations:

```
Zxxx0:admin#disable mirror
Command: disable mirror

Success.

Zxxx0:admin#
```

## 51.7. show mirror

---

### ● Description

This command is used to display the current port mirroring configuration on the Switching Hub.

### ● Format

show mirror {group\_id <value 1-4>}

### ● Parameters

---

**group\_id**(Optional) Specifies the group ID used for this display.  
     <value 1-4>

---

Enter the group ID used for this display here. This value must be between 1 and 4.

---



## 51. Mirror Commands

### ● Restrictions

None.

### ● Example

To display mirroring configuration:

```
Zxxx0:admin#show mirror  
Command: show mirror
```

```
Mirror Global State:   Disabled
```

| Group | State   | Target Port | Source Ports       |
|-------|---------|-------------|--------------------|
| 1     | Enabled | 1           | RX: 2-3<br>TX: 2-3 |

```
Zxxx0:admin#
```

## 52. MLD Proxy Commands

MLD (Multicast Listener Discovery) is a protocol to manage multicast groups in an IPv6 environment. It is a protocol equivalent to IGMP in IPv4. MLD proxy is a function to transfer MLD packets from multicast members to the upstream router. If a multicast transmission route is fixed, this function can transfer multicast packets between routers on the fixed route without using a multicast routing protocol.

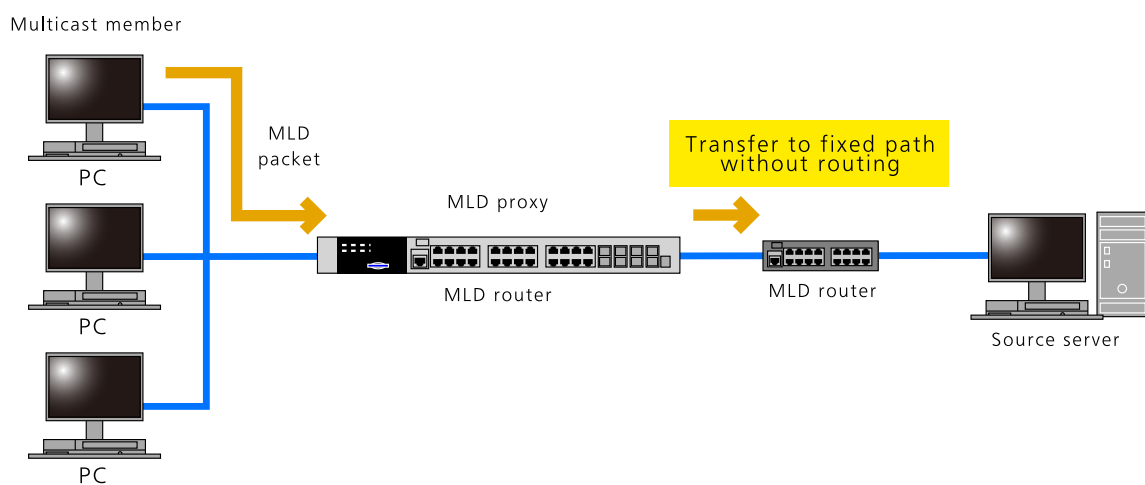


Figure 52-1 MLD proxy overview

```
enable mld_proxy
disable mld_proxy
config mld_proxy downstream_if [add | delete] vlan [<vlan_name 32> | vlanid <vidlist>]
config mld_proxy upstream_if {vlan [<vlan_name 32> | vlanid <vlanid 1-4094>] | router_ports
    [add | delete] <portlist> | source_ip <ipv6addr> | unsolicited_report_interval <sec 0-25>}(1)
show mld_proxy {group}
```

### 52.1. enable mld\_proxy

#### ● Description

This command is used to enable the MLD proxy on the Switching Hub.

#### ● Format

```
enable mld_proxy
```

## 52. MLD Proxy Commands

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable the MLD proxy:

```
Zxxx0:admin#enable mld_proxy
Command: enable mld_proxy

Success.

Zxxx0:admin#
```

## 52.2. disable mld\_proxy

---

### ● Description

This command is used to disable the MLD proxy on the Switching Hub.

### ● Format

**disable mld\_proxy**

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To disable the MLD proxy:

```
Zxxx0:admin#disable mld_proxy
Command: disable mld_proxy

Success.

Zxxx0:admin#
```

## 52.3. config mld\_proxy downstream\_if

### ● Description

This command configures the MLD proxy downstream interfaces. The MLD proxy plays the server role on the downstream interfaces. The downstream interface must be an MLD Snooping enabled VLAN.

### ● Format

**config mld\_proxy downstream\_if** [add | delete] vlan [<vlan\_name 32> | vlanid <vidlist>]

### ● Parameters

|                             |                                                                                                                    |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>add</b>                  | Specify to add a downstream interface.                                                                             |
| <b>delete</b>               | Specify to delete a downstream interface .                                                                         |
| <b>vlan</b>                 | Specify the VLAN by name or ID.                                                                                    |
| <b>&lt;vlan_name 32&gt;</b> | Specify a name of VLAN which belong to the MLD proxy downstream interface.<br>The maximum length is 32 characters. |
| <b>vlanid</b>               | Specify a list of VLAN IDs which belong to the MLD proxy downstream interface.                                     |
| <b>&lt;vidlist&gt;</b>      | Specify a list of VLAN IDs which belong to the MLD proxy downstream interface.                                     |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the MLD Proxy's downstream interface:

```
Zxxx0:admin#config mld_proxy downstream_if add vlan vlanid 2-7
Command: config mld_proxy downstream_if add vlan vlanid 2-7

Success.

Zxxx0:admin#
```

## 52.4. config mld\_proxy upstream\_if

---

### ● Description

This command is used to configure the setting for the MLD proxy's upstream interface. The MLD proxy plays the host role on the upstream interface. It will send MLD report packets to the router port. The source IP address determines the source IP address to be encoded in the MLD protocol packet. If the router port is empty, the upstream will send the MLD protocol packet to all member ports on the upstream interface.

### ● Format

```
config mld_proxy upstream_if {vlan [<vlan_name 32> | vlanid <vlanid 1-4094>] |
router_ports [add | delete] <portlist> | source_ip <ipv6addr> | unsolicited_report_interval
<sec 0-25>}(1)
```

### ● Parameters

|                                    |                                                                                                                                                                                                                                                                             |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan</b>                        | Specify the VLAN for the upstream interface.<br><b>&lt;vlan_name 32&gt;</b><br>Specify a VLAN name between 1 and 32 characters.<br><b>vlanid</b> Specify the VLAN ID for the upstream interface.<br><b>&lt;vlanid 1-4094&gt;</b><br>Specify the VLAN ID between 1 and 4094. |
| <b>router_ports</b>                | Specify a list of ports that are connected to multicast-enabled routers.<br><b>add</b> Specify to add the router ports.<br><b>delete</b> Specify to delete the router ports.<br><b>&lt;portlist&gt;</b><br>Specify a range of ports to be configured.                       |
| <b>source_ip</b>                   | Specify the source IPv6 address of the upstream protocol packet. If it is not specified, zero IP address will be used as the protocol source IP address.<br><b>&lt;ipv6addr&gt;</b><br>Specify the IPv6 address.                                                            |
| <b>unsolicited_report_interval</b> | Specify the time between repetitions of the host's initial report of membership in a group. The default is 10 seconds. If set to 0, only one report packet is sent.<br><b>&lt;sec 0-25&gt;</b><br>Specify the time between 0 and 25 seconds.                                |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the router port of MLD proxy's upstream interface:

```
Zxxx0:admin#config mld_proxy upstream_if vlan default router_ports add 3
Command: config mld_proxy upstream_if vlan default router_ports add 3

Success.

Zxxx0:admin#
```

## 52.5. show mld\_proxy

---

### ● Description

This command is used to display the MLD proxy's configuration or group information. The display status item means group entry is determined by whether or not the chip has been inserted.

### ● Format

`show mld_proxy {group}`

### ● Parameters

---

|              |                                           |
|--------------|-------------------------------------------|
| <b>group</b> | (Optional) Specify the group information. |
|--------------|-------------------------------------------|

---

---

|             |                                                                               |
|-------------|-------------------------------------------------------------------------------|
| <b>NOTE</b> | If the group is not specified, the MLD proxy configuration will be displayed. |
|-------------|-------------------------------------------------------------------------------|

---

### ● Restrictions

None.

### ● Example

To display the MLD proxy's information:

## 52. MLD Proxy Commands

```
Zxxx0:admin#show mld_proxy
Command: show mld_proxy

MLD Proxy Global State      : Enabled

Upstream Interface
  VLAN ID                   : 1
  Dynamic Router Ports      : 1-4
  Static Router Ports       : 5-6
  Unsolicited Report Interval : 10
  Source IP Address         : ::

Downstream Interface
  VLAN List                  : 2-4

Zxxx0:admin#
```

To display the MLD proxy's group information:

```
Zxxx0:admin#show mld_proxy group
Command: show mld_proxy group

Source      : NULL
Group       : FF1E::0202
Downstream VLAN : 4
Member Ports : 3,6
Status      : Active

Source      : FF80::200
Group       : FF1E::0202
Downstream VLAN : 2
Member Ports : 2,5,8
Status      : Inactive

Total Entries: 2

Zxxx0:admin#
```

## 53. MLD Snooping Commands

MLD (Multicast Listener Discovery) is a protocol to manage multicast groups in an IPv6 environment. It is a protocol equivalent to IGMP in IPv4. MLD snooping is a filtering function to monitor MLD packets flowing on ports of the Switching Hub and prevent data from flowing to unnecessary ports. This prevention function allows to efficiently process a large amount of data, such as video distribution.

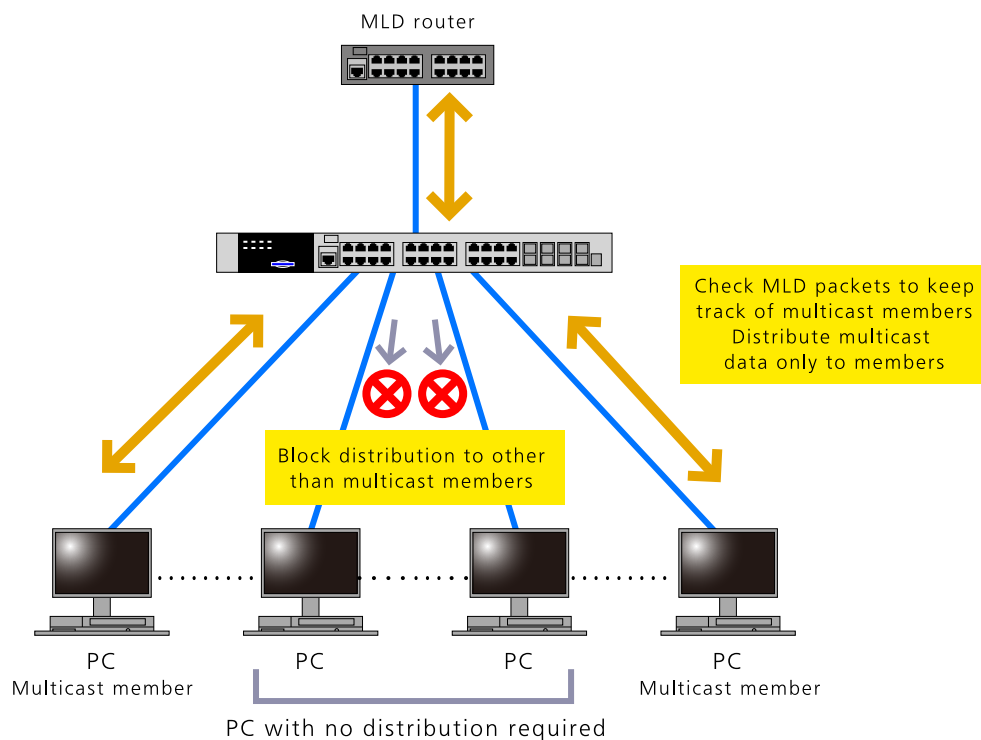


Figure 53-1 MLD Snooping overview

```

config mld_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable |
  disable] | fast_done [enable | disable] | proxy_reporting {state [enable | disable] | source_ip
  <ipv6addr>}(1)}
config mld_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>] [<value 1-1000> | no_limit]
show mld_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>]
create mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>
config mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr> [add |
  delete] <portlist>
delete mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>
show mld_snooping static_group {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>}
show mld_snooping statistic counter [vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>]
clear mld_snooping statistics counter
config mld_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all]
  {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-
  7> | last_listener_query_interval <sec 1-25> | state [enable | disable] | version <value 1-2>}(1)
  
```



## 53. MLD Snooping Commands

---

```
config mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete]
    <portlist>
config mld_snooping mrouter_ports_forbidden [vlan <vlan_name 32> | vlanid <vlanid_list>] [add |
    delete] <portlist>
enable mld_snooping
disable mld_snooping
show mld_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list >]}
show mld_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>]
    {<ipv6addr>}}
show mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static |
    dynamic | forbidden]}
show mld_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}
config mld_snooping unknow_data_learning [all | vlan_name <vlan_name 32> |
    vlanid <vlanid_list>] {state [enable | disable] | aged_out [enable | disable] | expiry_time
    <sec 1-65535>}
config mld_snooping unknow_data_learning max_learned_entry <value 1-1024>
clear mld_snooping data_learning_group [all | [vlan_name <vlan_name 32> | vlanid
    <vlanid_list>][<ipv6addr> | all]
```

---

### 53.1. config mld\_snooping

---

#### ● Description

This command is used to configure MLD snooping on the Switching Hub.

#### ● Format

```
config mld_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable
| disable] | fast_done [enable | disable] | proxy_reporting {state [enable | disable] |
source_ip <ipv6addr>}}(1)}
```

#### ● Parameters

---

|                  |                                                                                                                                                                                 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan_name</b> | Specify the name of the VLAN for which MLD snooping is to be configured.<br><b>&lt;vlan_name 32&gt;</b><br>Specify the VLAN name. The maximum length is 32 characters.          |
| <b>vlanid</b>    | Specify the VLAN ID list.<br><b>&lt;vlanid_list&gt;</b><br>Specify the VLAN ID list.                                                                                            |
| <b>all</b>       | Specify to configure all VLANs.                                                                                                                                                 |
| <b>state</b>     | Enable or disable MLD snooping for the chosen VLAN.<br><b>enable</b><br>Enable MLD snooping for the chosen VLAN.<br><b>disable</b><br>Disable MLD snooping for the chosen VLAN. |

---

**fast\_done**

Enable or disable the MLD snooping fast leave function. If enabled, the membership is immediately removed when the system receive the MLD leave message.

**enable**

Enable the MLD snooping fast leave function.

**disable**

Disable the MLD snooping fast leave function.

**proxy\_reporting**

Specifies that the proxy reporting function will be configured.

**state** Specifies the state of the proxy reporting function.

enable Specifies that the proxy reporting function will be enabled.

disable Specifies that the proxy reporting function will be disabled.

**source\_ip**

Specifies the source IPv6 address used.

**<ipv6addr>**

Enter the source IPv6 address used here.

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure MLD snooping:

```
Zxxx0:admin#config mld_snooping vlan_name default state enable
Command: config mld_snooping vlan_name default state enable

Success.

Zxxx0:admin#
```

## 53.2. config mld\_snooping rate\_limit

### ● Description

This command is used to configure the upper limit per second for ingress MLD control packets.

### ● Format

config mld\_snooping rate\_limit [ports <portlist> | vlanid <vlanid\_list>] [<value 1-1000> | no\_limit]

### ● Parameters

**ports** Specify a range of ports to be configured.

**<portlist>**

Specify a range of ports to be configured.

## 53. MLD Snooping Commands

---

|               |                                            |
|---------------|--------------------------------------------|
| <b>vlanid</b> | Specify a range of VLANs to be configured. |
|---------------|--------------------------------------------|

**<vlanid\_list>**

Specify the VLAN ID list.

---

**<value 1-1000>**

Specify the rate limit of MLD control packet that the Switching Hub can process on a specific port/VLAN. The rate is specified in packet per second. The packet that exceeds the limited rate will be dropped.

---

|                 |                                  |
|-----------------|----------------------------------|
| <b>no_limit</b> | The default setting is no limit. |
|-----------------|----------------------------------|

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the MLD snooping packet rate limit on port 1 for 100pps:

```
Zxxx0:admin#config mld_snooping rate_limit ports 1 100
```

```
Command: config mld_snooping rate_limit ports 1 100
```

```
Success.
```

```
Zxxx0:admin#
```

## 53.3. show mld\_snooping rate\_limit

---

### ● Description

This command is used to display the MLD snooping rate limit setting.

### ● Format

**show mld\_snooping rate\_limit [ports <portlist> | vlanid <vlanid\_list>]**

### ● Parameters

---

|              |                                           |
|--------------|-------------------------------------------|
| <b>ports</b> | Specify a range of ports to be displayed. |
|--------------|-------------------------------------------|

**<portlist>**

Specify a range of ports to be displayed.

---

|               |                                           |
|---------------|-------------------------------------------|
| <b>vlanid</b> | Specify a range of VLANs to be displayed. |
|---------------|-------------------------------------------|

**<vlanid\_list>**

Specify the VLAN ID list.

---

### ● Restrictions

None.

### ● Example

To display the MLD snooping packet rate limit for ports 1 to 2:

```
Zxxx0:admin#show mld_snooping rate_limit ports 1-2
Command: show mld_snooping rate_limit ports 1-2

  Port      Rate Limit
  -----  -
1           No Limit
2           No Limit

Total Entries: 2
Zxxx0:admin#
```

## 53.4. create mld\_snooping static\_group

### ● Description

This command is used to create an MLD snooping multicast static group. Member ports can be added to the static group. The static member and the dynamic member port form the member ports of a group.

The static group will only take effect when MLD snooping is enabled on the VLAN. For those static member ports, the device needs to emulate the MLD protocol operation to the querier, and forward the traffic destined to the multicast group to the member ports. For a layer 3 device, the device is also responsible to route the packet destined for this specific group to static member ports. The static member port will only affect V2 MLD operation. The Reserved IP multicast addresses FF0x::/16 must be excluded from the configured group. The VLAN must be created first before a static group can be created.

### ● Format

**create mld\_snooping static\_group [vlan <vlan\_name 32> | vlanid <vlanid\_list>] <ipv6addr>**

### ● Parameters

|                         |                                                                                                                                                               |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan</b>             | Specify the name of the VLAN on which the static group resides.<br><b>&lt;vlan_name 32&gt;</b><br>Specify the VLAN name. The maximum length is 32 characters. |
| <b>vlanid</b>           | Specify the VLAN ID list.<br><b>&lt;vlanid_list&gt;</b><br>Specify the VLAN ID list.                                                                          |
| <b>&lt;ipv6addr&gt;</b> | Specify the multicast group IPv6 address.                                                                                                                     |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create an MLD snooping static group on vlan1, group FF1E::1:

## 53. MLD Snooping Commands

```
Zxxx0:admin#create mld_snooping static_group vlan vlan1 FF1E::1
Command: create mld_snooping static_group vlan vlan1 FF1E::1

Success.

Zxxx0:admin#
```

### 53.5. config mld\_snooping static\_group

#### ● Description

This command is used to configure an MLD snooping static group on the Switching Hub. When a port is configured as a static member port, the MLD protocol will not operate on this port. Therefore, suppose that a port is a dynamic member port learned by MLD. If this port is configured as a static member later, then the MLD protocol will stop operating on this port. The MLD protocol will resume once this port is removed from static member ports. The static member port will only affect V1 MLD operation.

#### ● Format

**config mld\_snooping static\_group [vlan <vlan\_name 32> | vlanid <vlanid\_list>] <ipv6addr> [add | delete] <portlist>**

#### ● Parameters

|                         |                                                                                                                                                               |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan</b>             | Specify the name of the VLAN on which the static group resides.<br><b>&lt;vlan_name 32&gt;</b><br>Specify the VLAN name. The maximum length is 32 characters. |
| <b>vlanid</b>           | Specify the ID of the VLAN on which the static group resides.<br><b>&lt;vlanid_list&gt;</b><br>Specify the VLAN ID list.                                      |
| <b>&lt;ipv6addr&gt;</b> | Specify the multicast group IPv6 address (for Layer 3 Switching Hub).                                                                                         |
| <b>add</b>              | Specify to add the member ports.                                                                                                                              |
| <b>delete</b>           | Specify to delete the member ports.                                                                                                                           |
| <b>&lt;portlist&gt;</b> | Specify a range of ports to be configured.                                                                                                                    |

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To unset ports 9 to 10 from MLD Snooping static member ports for group FF1E::1 on default VLAN:

```
Zxxx0:admin#config mld_snooping static_group vlan default FF1E::1 delete 9-10
Command: config mld_snooping static_group vlan default FF1E::1 delete 9-10

Success.

Zxxx0:admin#
```

## 53.6. delete mld\_snooping static\_group

### ● Description

This command is used to delete an MLD snooping static group on the Switching Hub. The deletion of an MLD snooping static group will not affect the MLD snooping dynamic member ports for a group.

### ● Format

**delete mld\_snooping static\_group [vlan <vlan\_name 32> | vlanid <vlanid\_list>] <ipv6addr>**

### ● Parameters

|                         |                                                                                                                                                               |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan</b>             | Specify the name of the VLAN on which the static group resides.<br><b>&lt;vlan_name 32&gt;</b><br>Specify the VLAN name. The maximum length is 32 characters. |
| <b>vlanid</b>           | Specify the ID of the VLAN on which the static group resides.<br><b>&lt;vlanid_list&gt;</b><br>Specify the VLAN ID list.                                      |
| <b>&lt;ipv6addr&gt;</b> | Specify the multicast group IPv6 address (for Layer 3 Switching Hub).                                                                                         |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete an MLD snooping static group from the default VLAN, group FF1E::1:

```
Zxxx0:admin#delete mld_snooping static_group vlan default FF1E::1
Command: delete mld_snooping static_group vlan default FF1E::1

Success.

Zxxx0:admin#
```

## 53.7. `show mld_snooping static_group`

### ● Description

This command is used to display the MLD snooping static groups.

### ● Format

`show mld_snooping static_group` {[vlan <vlan\_name 32> | vlanid <vlanid\_list>] <ipv6addr>}

### ● Parameters

|                         |                                                                                                                                                             |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan</b>             | (Optional) Specify the name of the VLAN on which the static group resides.<br><vlan_name 32><br>Specify the VLAN name. The maximum length is 32 characters. |
| <b>vlanid</b>           | (Optional) Specify the ID of the VLAN on which the static group resides.<br><vlanid_list><br>Specify the VLAN ID list.                                      |
| <b>&lt;ipv6addr&gt;</b> | (Optional) Specify the multicast group IPv6 address (for Layer 3 Switching Hub).                                                                            |

### ● Restrictions

None.

### ● Example

To display all the MLD snooping static groups:

```
Zxxx0:admin#show mld_snooping static_group
Command: show mld_snooping static_group

VLAN ID/Name      IP Address      Static Member Ports
-----
1/Default         FF1E::1        9-10

Total Entries : 1

Zxxx0:admin#
```

## 53.8. **show mld\_snooping statistic counter**

### ● Description

This command is used to display the MLD snooping statistics counters for MLD protocol packets that are transmitted or received by the Switching Hub since MLD snooping was enabled.

### ● Format

**show mld\_snooping statistic counter** [**vlan** <vlan\_name 32> | **vlanid** <vlanid\_list> | **ports** <portlist>]

### ● Parameters

|               |                                                                                                                  |
|---------------|------------------------------------------------------------------------------------------------------------------|
| <b>vlan</b>   | Specify a VLAN to be displayed.<br><vlan_name 32><br>Specify the VLAN name. The maximum length is 32 characters. |
| <b>vlanid</b> | Specify a list of VLANs to be displayed.<br><vlanid_list><br>Specify the VLAN ID list.                           |
| <b>ports</b>  | Specify a list of ports to be displayed.<br><portlist><br>Specify a list of ports.                               |

### ● Restrictions

None.

### ● Example

To display the MLD snooping statistics counters on port 1:



## 53. MLD Snooping Commands

```
Zxxx0:admin#show mld_snooping statistic counter ports 1
Command: show mld_snooping statistic counter ports 1
```

```
Port #           : 1
-----
```

```
Group Number     : 0
```

### Receive Statistics

#### Query

|                            |     |
|----------------------------|-----|
| MLD v1 Query               | : 0 |
| MLD v2 Query               | : 0 |
| Total                      | : 0 |
| Dropped By Rate Limitation | : 0 |
| Dropped By Multicast VLAN  | : 0 |

#### Report & Done

|                                 |     |
|---------------------------------|-----|
| MLD v1 Report                   | : 0 |
| MLD v2 Report                   | : 0 |
| MLD v1 Done                     | : 0 |
| Total                           | : 0 |
| Dropped By Rate Limitation      | : 0 |
| Dropped By Max Group Limitation | : 0 |
| Dropped By Group Filter         | : 0 |
| Dropped By Multicast VLAN       | : 0 |

### Transmit Statistics

#### Query

|              |     |
|--------------|-----|
| MLD v1 Query | : 0 |
| MLD v2 Query | : 0 |
| Total        | : 0 |

#### Report & Done

|               |     |
|---------------|-----|
| MLD v1 Report | : 0 |
| MLD v2 Report | : 0 |
| MLD v1 Done   | : 0 |
| Total         | : 0 |

```
Total Entries : 1
```

```
Zxxx0:admin#
```

## 53.9. **clear mld\_snooping statistics counter**

---

- **Description**

This command is used to clear the MLD snooping statistics counters.

- **Format**

**clear mld\_snooping statistics counter**

- **Parameters**

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To clear the MLD snooping statistics counters:

```
Zxxx0:admin#clear mld_snooping statistics counter
Command: clear mld_snooping statistics counter

Success.

Zxxx0:admin#
```

## 53.10. **config mld\_snooping querier**

---

- **Description**

This command is used to configure the time, in seconds, between general query transmissions, the maximum time to wait for reports from listeners, and the permitted packet loss that guarantees MLD snooping.

- **Format**

**config mld\_snooping querier [vlan\_name <vlan\_name 32> | vlanid <vlanid\_list> | all]  
{query\_interval <sec 1-65535> | max\_response\_time <sec 1-25> | robustness\_variable  
<value 1-7> | last\_listener\_query\_interval <sec 1-25> | state [enable | disable] | version  
<value 1-2>} (1)**

## 53. MLD Snooping Commands

### ● Parameters

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan_name</b>                  | Specify the name of the VLAN for which MLD snooping querier is to be configured.<br><b>&lt;vlan_name 32&gt;</b><br>Specify the VLAN name. The maximum length is 32 characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>vlanid</b>                     | Specify the ID of the VLAN for which MLD snooping querier is to be configured.<br><b>&lt;vlanid_list&gt;</b><br>Specify the VLAN ID list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>all</b>                        | Specify all VLANs for which MLD snooping querier is to be configured.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>query_interval</b>             | Specify the amount of time in seconds between general query transmissions.<br><b>&lt;sec 1-65535&gt;</b><br>Specify the amount of time in seconds between general query transmissions. The default setting is 125 seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>max_response_time</b>          | Specify the maximum time in seconds to wait for reports from members.<br><b>&lt;sec 1-25&gt;</b><br>Specify the maximum time in seconds to wait for reports from members. The default setting is 10 seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>robustness_variable</b>        | Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following MLD message intervals: <ul style="list-style-type: none"><li>• Group member interval - Amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows:<br/>(robustness variable x query interval) + (1 x query response interval).</li><li>• Other querier present interval - Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows:<br/>(robustness variable x query interval) + (0.5 x query response interval).</li><li>• Last member query count - Number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable.</li></ul> <b>&lt;value 1-7&gt;</b><br>Specify the value between 1 and 7. Increase the value if you expect a subnet to be lossy. The robustness variable is set to 2 by default. |
| <b>last_member_query_interval</b> | Specify the maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last member of a group.<br><b>&lt;sec 1-25&gt;</b><br>Specify the time between 1 and 25 seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>state</b>                      | This allows the Switching Hub to be specified as an MLD Querier (sends MLD query packets) or a Non-Querier (does not send MLD query packets). Set to enable or disable.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>enable</b>                     | Allows the Switching Hub to be selected as an MLD Querier (sends MLD query packets).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>disable</b>                    | When disabled, the Switching Hub can not play the role as a querier.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

---

|                |                                                                                                                                                                                                                                                                                                 |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>version</b> | Specify the version of MLD packet that will be sent by this port. If a MLD packet received by the interface has a version higher than the specified version, this packet will be forward from router ports or VLAN flooding.<br><b>&lt;value 1-2&gt;</b><br>Specify the values between 1 and 2. |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure the MLD snooping querier:

```
Zxxx0:admin#config mld_snooping querier vlan_name default query_interval 125 state
enable
Command: config mld_snooping querier vlan_name default query_interval 125 state
enable

Success.

Zxxx0:admin#
```

# 53.11. config mld\_snooping mrouter\_ports

---

## ● Description

This command allows users to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router, regardless of protocol.

## ● Format

**config mld\_snooping mrouter\_ports [vlan <vlan\_name 32> | vlanid <vlanid\_list>] [add | delete] <portlist>**

## ● Parameters

---

|                         |                                                                                                                                                                                                      |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan</b>             | Specify the name of the VLAN on which the router port resides.<br><b>&lt;vlan_name 32&gt;</b><br>Specify the name of the VLAN on which the router port resides. The maximum length is 32 characters. |
| <b>vlanid</b>           | Specify the ID of the VLAN on which the router port resides.<br><b>&lt;vlanid_list&gt;</b><br>Specify the VLAN ID list.                                                                              |
| <b>add</b>              | Specify to add router ports.                                                                                                                                                                         |
| <b>delete</b>           | Specify to delete router ports.                                                                                                                                                                      |
| <b>&lt;portlist&gt;</b> | Specify a range of ports to be configured.                                                                                                                                                           |

---

## 53. MLD Snooping Commands

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To set up static router ports:

```
Zxxx0:admin#config mld_snooping mrouter_ports vlan default add 1-10
Command: config mld_snooping mrouter_ports vlan default add 1-10

Success.

Zxxx0:admin#
```

## 53.12. config mld\_snooping mrouter\_ports\_forbidden

---

### ● Description

This command allows you to designate a range of ports as being not connected to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.

### ● Format

**config mld\_snooping mrouter\_ports\_forbidden [vlan <vlan\_name 32> | vlanid <vlanid\_list>]  
[add | delete] <portlist>**

### ● Parameters

|                         |                                                                                                                                                                                                      |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan</b>             | Specify the name of the VLAN on which the router port resides.<br><b>&lt;vlan_name 32&gt;</b><br>Specify the name of the VLAN on which the router port resides. The maximum length is 32 characters. |
| <b>vlanid</b>           | Specify the ID of the VLAN on which the router port resides.<br><b>&lt;vlanid_list&gt;</b><br>Specify the VLAN ID list.                                                                              |
| <b>add</b>              | Specify to add router ports.                                                                                                                                                                         |
| <b>delete</b>           | Specify to delete router ports.                                                                                                                                                                      |
| <b>&lt;portlist&gt;</b> | Specify a range of ports to be configured.                                                                                                                                                           |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To set up ports as forbidden router port:

```
Zxxx0:admin#config mld_snooping mrouter_ports_forbidden vlan default add 1-10
Command: config mld_snooping mrouter_ports_forbidden vlan default add 1-10

Success.

Zxxx0:admin#
```

## **53.13. enable mld\_snooping**

---

- **Description**

This command is used to enable MLD snooping on the Switching Hub.

- **Format**

**enable mld\_snooping**

- **Parameters**

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To enable MLD snooping on the Switching Hub:

```
Zxxx0:admin#enable mld_snooping
Command: enable mld_snooping

Success.

Zxxx0:admin#
```

## 53.14. disable mld\_snooping

---

### ● Description

This command is used to disable MLD snooping on the Switching Hub. MLD snooping can be disabled only if IPv6 multicast routing is not being used. Disabling MLD snooping allows all MLD and IPv6 multicast traffic to flood within a given IPv6 interface.

### ● Format

`disable mld_snooping`

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To disable MLD snooping on the Switching Hub:

```
Zxxx0:admin#disable mld_snooping
Command: disable mld_snooping

Success.

Zxxx0:admin#
```

## 53.15. show mld\_snooping

---

### ● Description

This command is used to display the current MLD snooping configuration on the Switching Hub.

### ● Format

`show mld_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}`

### ● Parameters

|             |                                                                                                                                                                                         |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan</b> | (Optional) Specify the name of the VLAN for which to view the MLD snooping configuration.<br><b>&lt;vlan_name 32&gt;</b><br>Specify the VLAN name. The maximum length is 32 characters. |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

---

**vlanid** (Optional) Specify the ID of the VLAN for which to view the MLD snooping configuration.  
**<vlanid\_list>**  
 Specify the VLAN ID list.

---



---

**NOTE** If no parameter is specified, the system will display all current MLD snooping configurations.

---

## ● Restrictions

None.

## ● Example

To display MLD snooping:

```
Zxxx0:admin#show mld_snooping
Command: show mld_snooping

MLD Snooping Global State           : Disabled
Unknown Data Learning Max Entries    : 50

VLAN Name                           : default
Query Interval                       : 125
Max Response Time                    : 10
Robustness Value                     : 2
Last Listener Query Interval        : 1
Querier State                        : Disable
Querier Role                         : Non-Querier
Querier IP                           : ::
Querier Expiry Time                  : 0 secs
State                               : Disable
Fast Done                           : Disable
Proxy Reporting                      : Enable
Proxy Reporting Source IP            : ::
Rate Limit                           : No Limitation
Version                              : 2
Unknown Data Learning State          : Enabled
Unknown Data Learning Aged Out       : Disabled
Data Learning Group Expiry Time: 260

Total Entries: 1

Zxxx0:admin#
```



## 53.16. show mld\_snooping group

---

### ● Description

This command is used to display the current MLD snooping group information on the Switching Hub.

### ● Format

**show mld\_snooping group** {[vlan <vlan\_name 32> | vlanid <vlanid\_list> | ports <portlist>] {<ipv6addr>}}

### ● Parameters

|                         |                                                                                                                                                                                                                                                                                                                 |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan</b>             | (Optional) Specify the name of the VLAN for which to view MLD snooping group information. If VLAN and ports and IP address are not specified, the system will display all current MLD snooping group information.<br><b>&lt;vlan_name 32&gt;</b><br>Specify the VLAN name. The maximum length is 32 characters. |
| <b>vlanid</b>           | (Optional) Specify the ID of the VLAN for which to view MLD snooping group information.<br><b>&lt;vlanid_list&gt;</b><br>Specify the VLAN ID list.                                                                                                                                                              |
| <b>ports</b>            | (Optional) Specify the list of port for which to view MLD snooping group information.<br><b>&lt;portlist&gt;</b><br>Specify a range of ports to be displayed.                                                                                                                                                   |
| <b>&lt;ipv6addr&gt;</b> | (Optional) Specify the group IPv6 address for which to view MLD snooping group information.                                                                                                                                                                                                                     |

### ● Restrictions

None.

### ● Example

To display the MLD snooping group:

```

Zxxx0:admin#show mld_snooping group
Command: show mld_snooping group
Source/Group      : 2001::1/FE1E::1
VLAN Name/VID     : default/1
Member Ports     : 1-2
UP Time          : 26
Expiry Time      : 258
Filter Mode      : INCLUDE

Source/Group      : 2002::2/FE1E::1
VLAN Name/VID     : default/1
Member Ports     : 3
UP Time          : 29
Expiry Time      : 247
Filter Mode      : EXCLUDE

Source/Group      : NULL/FE1E::2
VLAN Name/VID     : default/1
Member Ports     : 4-5
UP Time          : 40
Expiry Time      : 205
Filter Mode      : EXCLUDE

Total Entries : 3

Zxxx0:admin#

```

## 53.17. show mld\_snooping mrouter\_ports

### ● Description

This command is used to display the router ports on the Switching Hub.

### ● Format

**show mld\_snooping mrouter\_ports** [vlan <vlan\_name 32> | vlanid <vlanid\_list> | all]  
 {[static | dynamic | forbidden]}

### ● Parameters

|                |                                                                                                                                                                                                      |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan</b>    | Specify the name of the VLAN on which the router port resides.<br><b>&lt;vlan_name 32&gt;</b><br>Specify the name of the VLAN on which the router port resides. The maximum length is 32 characters. |
| <b>vlanid</b>  | Specify the ID of the VLAN on which the router port resides.<br><b>&lt;vlanid_list&gt;</b><br>Specify the VLAN ID list.                                                                              |
| <b>all</b>     | Specify all VLANs on which the router port resides.                                                                                                                                                  |
| <b>static</b>  | (Optional) Display router ports that have been statically configured.                                                                                                                                |
| <b>dynamic</b> | (Optional) Display router ports that have been dynamically learned.                                                                                                                                  |

## 53. MLD Snooping Commands

---

### forbidden

(Optional) Display forbidden router ports that have been statically configured.

---

---

**NOTE** If no parameter is specified, the system will display all router ports on the Switch.

---

### ● Restrictions

None.

### ● Example

To display router ports:

```
Zxxx0:admin#show mld_snooping mrouter_ports all
Command: show mld_snooping mrouter_ports all

VLAN Name           : default
Static Router Port   :
Dynamic Router Port  :
Router IP            :
Forbidden Router Port:

Total Entries: 1

Zxxx0:admin#
```

## 53.18. show mld\_snooping forwarding

---

### ● Description

This command is used to display the Switching Hub's current MLD snooping forwarding table. It provides an easy way for users to check the list of ports that the multicast group comes from specific sources will be forwarded to. The packet comes from the source VLAN. They will be forwarded to the forwarding ports.

### ● Format

**show mld\_snooping forwarding** {[vlan <vlan\_name 32> | vlanid <vlanid\_list>]}

### ● Parameters

---

|             |                                                                                                                                                                                                    |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan</b> | (Optional) Specify the name of the VLAN for which to view MLD snooping forwarding table information.<br><b>&lt;vlan_name 32&gt;</b><br>Specify the VLAN name. The maximum length is 32 characters. |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

---

**vlanid** (Optional) Specify the ID of the VLAN for which to view MLD snooping forwarding table information.  
**<vlanid\_list>**  
Specify the VLAN ID list.

---

---

**NOTE** If no parameter is specified, the system will display all currently configured MLD snooping forwarding entries.

---

## ● Restrictions

None.

## ● Example

To display all MLD snooping forwarding entries located on the Switching Hub:

```
Zxxx0:admin#show mld_snooping forwarding
Command: show mld_snooping forwarding

VLAN Name      : default
Source IP      : 2001::1
Multicast Group: FE1E::1
Port Member    : 2,7

VLAN Name      : default
Source IP      : 2001::1
Multicast Group: FE1E::2
Port Member    : 5

Total Entries: 2

Zxxx0:admin#
```

---

## 54. Login Banner and Prompt Commands

---

These commands are used to change the command line interface (CLI) command prompt.

---

**config command\_prompt** [<string 16> | username | default]

---

### 54.1. config command\_prompt

---

#### ● Description

This command is used to modify the command prompt. The current command prompt consists of four parts: "product name" + ":" + "user level" + "#" (e.g. "Zxxx0:admin#"). This command is used to modify the first part (1. "product name") with a string consisting of a maximum of 16 characters, or to be replaced with the users' login user name.

#### ● Format

**config command\_prompt** [<string 16> | username | default]

#### ● Parameters

---

**<string 16>**

Specify the new command prompt string of no more than 16 characters.

---

**username**

Specify the command to set the login username as the command prompt.

---

**default** Specify the command to return the command prompt to its original factory default value.

---

#### ● Restrictions

When users issue the "reset" command, the current command prompt will remain in tact. Issuing the "reset system" will return the command prompt to its original factory default value.

Only Administrator and Operator-level users can issue this command.

#### ● Example

To edit the command prompt:

```
Zxxx0:admin#config command_prompt HQ0001
Command: config command_prompt HQ0001

Success.

HQ0001:admin#
```

## 55. Multicast Listener Discovery (MLD) Commands

In multicast where data is simultaneously sent to multiple destinations, destinations are managed in a unit called "group." Each group has its own unique multicast IP address and multicast MAC address assigned. A client that wants to join multicast can be a member of the group after sending a notification that it joins a specific multicast group to neighbor routers. MLD is a protocol to maintain and manage multicast groups in an IPv6 environment. It is a protocol equivalent to IGMP in IPv4. It is used for clients to join or leave a group or used to exchange group information between routers.

---

```

config mld [ipif <ipif_name 12> | all] {query_interval <sec 1-31744> | max_response_time <sec 1-25> | robustness_variable <value 2-7> | last_listener_query_interval <sec 1-25> | version <value 1-2> | state [enable | disable]}
show mld {ipif <ipif_name 12>}
show mld group {ipif <ipif_name 12> | group <ipv6addr>}

```

---

### 55.1. config mld

#### ● Description

This command is used to configure MLD on the Switch.

#### ● Format

```

config mld [ipif <ipif_name 12> | all] {query_interval <sec 1-31744> | max_response_time <sec 1-25> | robustness_variable <value 2-7> | last_listener_query_interval <sec 1-25> | version <value 1-2> | state [enable | disable]}

```

#### ● Parameters

---

|             |                                                                                                                                                                     |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b> | Specifies the IP interface name used for this configuration.<br><ipif_name 12><br>Enter the IP interface name used here. This name can be up to 12 characters long. |
| <b>all</b>  | Specifies that all the IP interfaces will be used.                                                                                                                  |

---

|                       |                                                                                                                                                                                                                                           |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>query_interval</b> | (Optional) Specifies the time in seconds between the general query transmissions.<br><sec 1-31744><br>Enter the general query interval value used here. This value must be between 1 and 31744 seconds. The default value is 125 seconds. |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

## 55. Multicast Listener Discovery (MLD) Commands

---

### **max\_response\_time**

(Optional) Specifies the maximum time in seconds to wait for reports from listeners.

**<sec 1-25>**

Enter the maximum response time value used here. The value must be between 1 and 25 seconds. The default value is 10 seconds.

---

### **robustness\_variable**

(Optional) Specifies the permitted packet loss that guarantees the MLD.

**<value 2-7>**

Enter the robustness variable value used here. This value must be between 2 and 7. The default value is 2.

---

### **last\_listener\_query\_interval**

(Optional) Specifies the maximum response time inserted into the Multicast address specific query sent in response to 'done group' messages. This is also the amount of time between Multicast address specific query messages.

**<sec 1-25>**

Enter the last listener query interval value used here. This value must be between 1 and 25 seconds. The default value is 1 second.

---

**version** (Optional) Specifies the MLD version number.

**<value 1-2>**

Enter the MLD version number used here. This number must be between 1 and 2. The default value is 2.

---

**state** (Optional) Specifies the MLD state for the specified route interface.

**enable**

Specifies that the MLD state for the specified interface will be enabled.

**disable**

Specifies that the MLD state for the specified interface will be disabled.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure the MLD on the IP interface "System":

```
Zxxx0:admin# config mld ipif System version 1 state enabled
Command: config mld ipif System version 1 state enabled

Success.

Zxxx0:admin#
```

To configure the MLD version to v1 on all IP interfaces:

```
Zxxx0:admin# config mld all version 1
Command: config mld all version 1

Success.

Zxxx0:admin#
```

To configure the MLD last listener query interval to 10 seconds on all interfaces:

```
Zxxx0:admin# config mld all last_listener_query_interval 10
Command: config mld all last_listener_query_interval 10

Success.

Zxxx0:admin#
```

## 55.2. show mld

---

### ● Description

This command is used to display the MLD configurations on the Switch.

### ● Format

**show mld {ipif <ipif\_name 12>}**

### ● Parameters

---

|             |                                                                                                        |
|-------------|--------------------------------------------------------------------------------------------------------|
| <b>ipif</b> | (Optional) Specifies the IP interface name used for this configuration.<br><b>&lt;ipif_name 12&gt;</b> |
|-------------|--------------------------------------------------------------------------------------------------------|

---

Enter the IP interface name used here. This name can be up to 12 characters long.

### ● Restrictions

None.

### ● Example

To display the MLD configurations on all interfaces:



## 55. Multicast Listener Discovery (MLD) Commands

```
Zxxx0:admin# show mld
Command: show mld

MLD Interface Configurations

MRT = Maximum Response Time, LLQI = Last Listener Query Interval

Interface  Version Query  MRT  Robustness LLQI  State
-----
System      2      125   10    2         1   Disabled
n10         2      125   10    2         1   Enabled
n11         2      125   10    2         1   Disabled
n12         2      125   10    2         1   Disabled

Total Entries: 4

Zxxx0:admin#
```

To display the MLD configurations for interface "n10":

```
Zxxx0:admin# show mld ipif n10
Command: show mld ipif n10

MLD Interface Details

Interface                : n10
IPv6 Link-Local Address  : FE80::123D:34AC/128
Querier                   : FE80::1E45:2310
Status                    : Enabled
Version                   : 2
Query Interval            : 125 sec
Max Response Time         : 10 sec
Robustness                 : 2
Last Listener Query Interval : 1 sec
Last Listener Query Count  : 2
Startup Query Count        : 2
Startup Query Interval     : 31 sec

Zxxx0:admin#
```

## 55.3. show mld group

### ● Description

This command is used to display the MLD group member table.

### ● Format

**show mld group** {**ipif** <ipif\_name 12> | **group** <ipv6addr>}

### ● Parameters

|              |                                                                                                                                                                                |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b>  | (Optional) Specifies the IP interface name used for this configuration.<br><ipif_name 12><br>Enter the IP interface name used here. This name can be up to 12 characters long. |
| <b>group</b> | (Optional) Specifies the IPv6 multicast group address used.<br><ipv6addr><br>Enter the IPv6 multicast group address used here.                                                 |

### ● Restrictions

None.

### ● Example

To display all the MLD group member information on the Switching Hub, the "Expiry" uses second as the unit:

```
Zxxx0:admin# show mld group
Command: show mld group

Interface      Multicast Group      Expiry
-----
System         FF1E::100:0:0:20      260
n10            FF1E::1001:1234       255
n20            FF1E::2AC4:0:452      260
n10            FF1E::5A3D:11:23C1    260

Total Entries : 4

Zxxx0:admin#
```

To display all the MLD group member information of interface "n10", the "Expiry" uses second as the unit:

## 55. Multicast Listener Discovery (MLD) Commands

```
Zxxx0:admin# show mld group ipif n10
Command: show mld group ipif n10

Interface      Multicast Group      Expiry
-----
n10            FF1E::1001:1234      255
n10            FF1E::5A3D:11:23C1   260

Total Entries : 2

Zxxx0:admin#
```

To display the group source address list for interface "n10" with the group address "FF1E::100:0:20", the "Expiry" uses second as the unit:

```
Zxxx0:admin# show mld group ipif n10 group FF1E::100:0:20
Command: show mld group ipif n10 group FF1E::100:0:20

MLD Group Details

Interface      : n10
Multicast Group : FF1E::100:0:20
Last Reporter   : FE80::2345:FE39
Up Time        : 00:00:32
Expiry Time     : 00:30:02
Filter Mode     : Exclude
V1 Host Time    : 0 sec

Source List Table:

Source Address      Expiry
-----
2001::1234:EF23     10

Total Source Entries: 1

Total Entries: 1

Zxxx0:admin#
```

To display all the MLD group member information for multicast group "FF1E::1001:1234", the "Expiry" uses second as the unit:

```
Zxxx0:admin# show mld group group FF1E::1001:1234
Command: show mld group group FF1E::1001:1234

Interface      Multicast Group      Expiry
-----
n10            FF1E::1001:1234      215
n11            FF1E::1001:1234      200
n20            FF1E::1001:1234      240

Total Entries : 3

Zxxx0:admin#
```

## 56. Network Load Balancing (NLB) Commands

NLB is a load balancing function in Windows Server. It assigns the same virtual IP address to multiple servers providing the same services and uniformly distributes accesses from the clients.

NLB has the unicast mode and multicast mode. In the multicast mode, if the destination MAC address from the client is a multicast MAC address, data may not be transferred.

In this case, you need to register the actual MAC address of the NLB server in the forwarding table.

---

```
create nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr>
delete nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr>
config nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr> [add | delete] <portlist>
show nlb fdb
```

---

### 56.1. create nlb multicast\_fdb

#### ● Description

This command is used to create the Switch's NLB multicast FDB entry. The network load balancing command set is used to support the Microsoft server load balancing application where multiple servers can share the same IP address and MAC address. The requests from clients will be forwarded to all servers, but will only be processed by one of them. In multicast mode, the client use the multicast MAC address as the destination MAC to reach the server. Regarding of the mode, this destination MAC is the named the shared MAC. The server uses its own MAC address (rather than the shared MAC) as the source MAC address of the reply packet.

#### ● Format

```
create nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr>
```

#### ● Parameters

---

|                             |                                                                                                     |
|-----------------------------|-----------------------------------------------------------------------------------------------------|
| <b>&lt;vlan_name 32&gt;</b> | Enter the VLAN name of the NLB multicast FDB entry here. This name can be up to 32 characters long. |
| <b>vlanid</b>               | Specifies the VLAN ID used.                                                                         |
| <b>&lt;vlanid&gt;</b>       | Enter the VLAN ID used here.                                                                        |

---

## 56. Network Load Balancing (NLB) Commands

---

**<macaddr>**

Specifies the MAC address of the NLB multicast FDB entry to be created.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create a NLB multicast FDB entry:

```
Zxxx0:admin# create nlb multicast_fdb default 03-bf-01-01-01-01
Command: create nlb multicast_fdb default 03-bf-01-01-01-01

Success.

Zxxx0:admin#
```

## 56.2. delete nlb multicast\_fdb

---

### ● Description

This command is used to delete the Switch's NLB multicast FDB entry.

### ● Format

**delete nlb multicast\_fdb [<vlan\_name 32> | vlanid <vlanid>] <macaddr>**

### ● Parameters

---

**<vlan\_name 32>**

Enter the VLAN name of the NLB multicast FDB entry here. This name can be up to 32 characters long.

---

**vlanid** Specifies the VLAN ID used.

**<vlanid>**

Enter the VLAN ID used here.

---

**<macaddr>**

Specifies the MAC address of the NLB multicast FDB entry to be deleted.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete NLB multicast FDB entry:

```
Zxxx0:admin# delete nlb multicast_fdb default 03-bf-01-01-01-01
Command: delete nlb multicast_fdb default 03-bf-01-01-01-01

Success.

Zxxx0:admin#
```

## 56.3. config nlb multicast\_fdb

### ● Description

This command is used to configure the Switch's NLB multicast FDB entry.

### ● Format

**config nlb multicast\_fdb** [<vlan\_name 32> | vlanid <vlanid>] <macaddr> [add | delete] <portlist>

### ● Parameters

**<vlan\_name 32>**

Enter the VLAN name of the NLB multicast FDB entry here. This name can be up to 32 characters long.

**vlanid** Specifies the VLAN ID used.

**<vlanid>**

Enter the VLAN ID used here.

**<macaddr>**

Specifies the MAC address of the NLB multicast FDB entry to be configured.

**add** Specifies a list of forwarding ports to be added.

**delete** Specifies a list of forwarding ports to be deleted.

**<portlist>** Specifies a list of forwarding ports to be added or deleted.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure NLB multicast MAC forwarding database:

```
Zxxx0:admin# config nlb multicast_fdb default 03-bf-01-01-01-01 add 1:1-1:5
Command: config nlb multicast_fdb default 03-bf-01-01-01-01 add 1:1-1:5

Success.

Zxxx0:admin#
```

### 56.4. show nlb fdb

---

#### ● Description

This command is used to show the NLB configured entry.

#### ● Format

show nlb fdb

#### ● Parameters

None.

#### ● Restrictions

None.

#### ● Example

To display the NLB forwarding table:

```
Zxxx0:admin# show nlb fdb
```

```
Command: show nlb fdb
```

| MAC Address       | VLAN ID | Egress Ports      |
|-------------------|---------|-------------------|
| 02-bf-01-01-01-01 | -       | 1:1-1:5,1:26,2:26 |
| 02-bf-01-01-01-02 | -       | 1:1-1:5,1:26,2:26 |
| 03-bf-01-01-01-01 | 100     | 1:1-1:5,1:26,2:26 |
| 03-bf-01-01-01-01 | 1       | 1:1-1:5,1:26,2:26 |

```
Total Entries : 4
```

```
Zxxx0:admin#
```

## 57. Network Management Commands

SNMP (Simple Network Management Protocol) is a protocol to monitor and manage network-connected devices via network. Target devices have a management information database called MIB (Management Information Base). SNMP monitors and controls them through access to their MIBs using an external management manager.

---

```

enable snmp
disable snmp
create trusted_host [<ipaddr> | <ipv6addr> | network <network_address> | ipv6_prefix
    <ipv6networkaddr>] {snmp | telnet | ssh | http | https | ping}
config trusted_host [<ipaddr> | <ipv6addr> | network <network_address> | ipv6_prefix
    <ipv6networkaddr>] [add | delete] {snmp | telnet | ssh | http | https | ping | all}
delete trusted_host [ipaddr <ipaddr> | ipv6address <ipv6addr> | network <network_address> |
    ipv6_prefix <ipv6networkaddr> | all]
show trusted_host
config snmp system_name <sw_name>
config snmp system_location <sw_location>
config snmp system_contact <sw_contact>
enable snmp traps
disable snmp traps
enable snmp authenticate_traps
disable snmp authenticate_traps
enable snmp linkchange_traps
disable snmp linkchange_traps
show snmp traps {linkchange_traps {ports <portlist>}}
config snmp linkchange_traps ports [all | <portlist>] [enable | disable]
config snmp coldstart_traps [enable | disable]
config snmp warmstart_traps [enable | disable]
config trap source_ipif [<ipif_name 12> {<ipaddr> | <ipv6addr>} | none]
show trap source_ipif
config rmon trap {rising_alarm [enable | disable] | falling_alarm [enable | disable]}
show rmon

```

---

### 57.1. enable snmp

#### ● Description

This command is used to enable the SNMP function. When SNMP function is disabled, the network manager will not be able to access SNMP MIB objects. The device will not send traps or notification to network manager either.



## 57. Network Management Commands

### ● Format

`enable snmp`

### ● Parameters

None.

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To enable SNMP:

```
Zxxx0:admin#enable snmp
Command: enable snmp

Success.

Zxxx0:admin#
```

## 57.2. disable snmp

---

### ● Description

This command is used to disable the SNMP function. When SNMP function is disabled, the network manager will not be able to access SNMP MIB objects. The device will not send traps or notification to network manager either.

### ● Format

`disable snmp`

### ● Parameters

None. By default, SNMP is disabled.

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To disable SNMP:

```
Zxxx0:admin#disable snmp
Command: disable snmp

Success.

Zxxx0:admin#
```

## 57.3. create trusted\_host

### ● Description

This command is used to create the trusted host. The Switching Hub allows you to specify up to twenty IP addresses (or IP ranges) that are allowed to manage the Switching Hub via in-band SNMP or Telnet based management software. These IP addresses must be members of the Management VLAN. If no IP addresses are specified, then there is nothing to prevent any IP address from accessing the Switching Hub, provided the user knows the Username and Password.

### ● Format

**create trusted\_host** [<ipaddr> | <ipv6addr> | network <network\_address> | ipv6\_prefix <ipv6networkaddr>] {snmp | telnet | ssh | http | https | ping}

### ● Parameters

|                   |                                                                                                       |
|-------------------|-------------------------------------------------------------------------------------------------------|
| <ipaddr>          | Specify the IP address of the trusted host.                                                           |
| <ipv6addr>        | Specify the IPv6 address of the trusted host.                                                         |
| network           | Specify the network address of the trusted network. The form of network address is xxx.xxx.xxx.xxx/y. |
| <network_address> | Specify the network address of the trusted network. The form of network address is xxx.xxx.xxx.xxx/y. |
| ipv6_prefix       | Specify the IPv6 network address of the trusted network.                                              |
| <ipv6networkaddr> | Specify the IPv6 network address of the trusted network.                                              |
| snmp              | (Optional) Specify the trusted host for SNMP.                                                         |
| telnet            | (Optional) Specify the trusted host for Telnet.                                                       |
| ssh               | (Optional) Specify the trusted host for SSH.                                                          |
| http              | (Optional) Specify the trusted host for HTTP.                                                         |
| https             | (Optional) Specify the trusted host for HTTPs.                                                        |
| ping              | (Optional) Specify the trusted host for Ping.                                                         |

**NOTE** If no management method is specified, the IP (range) can access the Switch through any method.

## 57. Network Management Commands

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To create a trusted host:

```
Zxxx0:admin#create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121

Success.

Zxxx0:admin#
```

## 57.4. config trusted\_host

### ● Description

This command is used to configure the access interfaces for the trusted host.

### ● Format

**config trusted\_host** [<ipaddr> | <ipv6addr> | network <network\_address> | ipv6\_prefix <ipv6networkaddr>] [add | delete] {snmp | telnet | ssh | http | https | ping | all}

### ● Parameters

---

**<ipaddr>** Specify the IP address of the trusted host.

---

**<ipv6addr>**  
Specify the IPv6 address of the trusted host.

---

**network** Specify the network address of the trusted network. The form of network address is xxx.xxx.xxx.xxx/y.

**<network\_address>**  
Specify the network address of the trusted network. The form of network address is xxx.xxx.xxx.xxx/y.

---

**ipv6\_prefix**  
Specify the IPv6 network address of the trusted network.

**<ipv6networkaddr>**  
Specify the IPv6 network address of the trusted network.

---

**add** Allow to manage applications for a trusted host.

---

**delete** Prevent from managing applications for a trusted host.

---

**snmp** (Optional) Specify the trusted host for SNMP.

---

**telnet** (Optional) Specify the trusted host for Telnet.

---

**ssh** (Optional) Specify the trusted host for SSH.

---

**http** (Optional) Specify the trusted host for HTTP.

---

**https** (Optional) Specify the trusted host for HTTPs.

---

**ping** (Optional) Specify the trusted host for Ping.

---

**all** Specify the trusted host for all applications.

---

● **Restrictions**

Only Administrator and Operator-level users can issue this command.

● **Example**

To configure the trusted host:

```
Zxxx0:admin#config trusted_host 10.48.74.121 add ssh telnet
Command: config trusted_host 10.48.74.121 add ssh telnet

Success.

Zxxx0:admin#
```

# 57.5. delete trusted\_host

● **Description**

This command is used to delete a trusted host entry.

● **Format**

delete trusted\_host [ipaddr <ipaddr> | ipv6address <ipv6addr> | network <network\_address> | ipv6\_prefix <ipv6networkaddr> | all]

● **Parameters**

|             |                                                                                                                                                                                                                                     |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ipaddr      | Specify the IP address of the trusted host.<br><ipaddr><br>Specify the IP address of the trusted host.                                                                                                                              |
| ipv6address | Specify the IPv6 address of the trusted host.<br><ipv6addr><br>Specify the IPv6 address of the trusted host.                                                                                                                        |
| network     | Specify the network address of the trusted network. The form of network address is xxx.xxx.xxx.xxx/y.<br><network_address><br>Specify the network address of the trusted network. The form of network address is xxx.xxx.xxx.xxx/y. |
| ipv6_prefix | Specify the IPv6 network address of the trusted network.<br><ipv6networkaddr><br>Specify the IPv6 network address of the trusted network.                                                                                           |
| all         | Specify that all trusted hosts will be deleted.                                                                                                                                                                                     |

● **Restrictions**

Only Administrator and Operator-level users can issue this command.

## 57. Network Management Commands

### ● Example

To delete a trusted host:

```
Zxxx0:admin#delete trusted_host ipaddr 10.48.74.121
Command: delete trusted_host ipaddr 10.48.74.121

Success.

Zxxx0:admin#
```

## 57.6. show trusted\_host

---

### ● Description

This command is used to display the trusted hosts.

### ● Format

**show trusted\_host**

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display trusted hosts:

```
Zxxx0:admin#show trusted_host
Command: show trusted_host

Management Stations

IP Address                               Access Interface
-----
10.48.93.100
10.51.17.1
10.50.95.90

Total Entries : 3

Zxxx0:admin#
```

## 57.7. config snmp system\_name

---

### ● Description

This command is used to configure the SNMP system name of the Switching Hub.

### ● Format

config snmp system\_name <sw\_name>

### ● Parameters

---

<sw\_name>

Specify an SNMP system name for the Switching Hub. A maximum of 255 characters is allowed.

---

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To configure the Switching Hub SNMP name for "Zxxx0 Gigabit Ethernet Switch":

```
Zxxx0:admin# config snmp system_name Zxxx0 Gigabit Ethernet Switch
Command: config snmp system_name Zxxx0 Gigabit Ethernet Switch

Success.

Zxxx0:admin#
```

## 57.8. config snmp system\_location

---

### ● Description

This command is used to enter a description of the SNMP system location of the Switching Hub. A maximum of 255 characters can be used.

### ● Format

config snmp system\_location <sw\_location>

### ● Parameters

---

<sw\_location>

Specify an SNMP system location for the Switching Hub. A maximum of 255 characters is allowed.

---

## 57. Network Management Commands

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To configure the Switching Hub location for "7F Server Room":

```
Zxxx0:admin#config snmp system_location 7F Server Room
Command: config snmp system_location 7F Server Room

Success.

Zxxx0:admin#
```

## 57.9. config snmp system\_contact

---

### ● Description

This command is used to enter the name and/or other information to identify an SNMP system contact person who is responsible for the Switching Hub. A maximum of 255 characters can be used.

### ● Format

`config snmp system_contact <sw_contact>`

### ● Parameters

---

`<sw_contact>`

Specify an SNMP system contact person. A maximum of 255 characters is allowed.

---

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To configure the Switching Hub contact to "Network Manager":

```
Zxxx0:admin#config snmp system_contact "Network Manager"
Command: config snmp system_contact "Network Manager"

Success.

Zxxx0:admin#
```

## 57.10. enable snmp traps

---

- **Description**

This command is used to enable SNMP trap support on the Switching Hub.

- **Format**

`enable snmp traps`

- **Parameters**

None.

- **Restrictions**

Only Administrator and Operator-level users can issue this command.

- **Example**

To enable SNMP trap support:

```
Zxxx0:admin#enable snmp traps
Command: enable snmp traps

Success.

Zxxx0:admin#
```

## 57.11. disable snmp traps

---

- **Description**

This command is used to disable SNMP trap support on the Switching Hub.

- **Format**

`disable snmp traps`

- **Parameters**

None.

- **Restrictions**

Only Administrator and Operator-level users can issue this command.



## 57. Network Management Commands

### ● Example

To prevent SNMP traps from being sent from the Switching Hub:

```
Zxxx0:admin#disable snmp traps
Command: disable snmp traps

Success.

Zxxx0:admin#
```

## **57.12. enable snmp authenticate\_traps**

### ● Description

This command is used to enable SNMP authentication failure trap support.

### ● Format

**enable snmp authenticate\_traps**

### ● Parameters

None.

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To enable SNMP authentication trap support:

```
Zxxx0:admin#enable snmp authenticate_traps
Command: enable snmp authenticate_traps

Success.

Zxxx0:admin#
```

## 57.13. disable snmp authenticate\_traps

---

- **Description**

This command is used to disable SNMP authentication failure trap support.

- **Format**

`disable snmp authenticate_traps`

- **Parameters**

None.

- **Restrictions**

Only Administrator and Operator-level users can issue this command.

- **Example**

To disable SNMP authentication trap support:

```
Zxxx0:admin#disable snmp authenticate_traps
Command: disable snmp authenticate_traps

Success.

Zxxx0:admin#
```

## 57.14. enable snmp linkchange\_traps

---

- **Description**

This command is used to enable SNMP linkchange trap support.

- **Format**

`enable snmp linkchange_traps`

- **Parameters**

None.

- **Restrictions**

Only Administrator and Operator-level users can issue this command.

## 57. Network Management Commands

### ● Example

To enable SNMP linkchange trap support:

```
Zxxx0:admin#enable snmp linkchange_traps
Command: enable snmp linkchange_traps

Success.

Zxxx0:admin#
```

## **57.15. disable snmp linkchange\_traps**

### ● Description

This command is used to disable SNMP linkchange trap support.

### ● Format

**disable snmp linkchange\_traps**

### ● Parameters

None.

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To disable SNMP linkchange trap support:

```
Zxxx0:admin#disable snmp linkchange_traps
Command: disable snmp linkchange_traps

Success.

Zxxx0:admin#
```

## 57.16. config snmp linkchange\_traps ports

### ● Description

This command is used to configure the sending of linkchange traps and per port control for sending of change traps.

### ● Format

**config snmp linkchange\_traps ports [all | <portlist>] [enable | disable]**

### ● Parameters

|                         |                                                        |
|-------------------------|--------------------------------------------------------|
| <b>all</b>              | Specify all ports.                                     |
| <b>&lt;portlist&gt;</b> | Specify a port or range of ports.                      |
| <b>enable</b>           | Enable sending of the link change trap for this port.  |
| <b>disable</b>          | Disable sending of the link change trap for this port. |

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To enable SNMP linkchange traps for ports 1 to 4:

```
Zxxx0:admin#config snmp linkchange_traps ports 1-4 enable
Command: config snmp linkchange_traps ports 1-4 enable

Success.

Zxxx0:admin#
```

## 57.17. show snmp traps

### ● Description

This command is used to display the SNMP trap state.

### ● Format

**show snmp traps {linkchange\_traps {ports <portlist>}}**

### ● Parameters

|                         |                                                               |
|-------------------------|---------------------------------------------------------------|
| <b>linkchange_traps</b> | (Optional) Specify to display the status of linkchange traps. |
|-------------------------|---------------------------------------------------------------|

## 57. Network Management Commands

---

**ports** (Optional) Specify a port or port range.  
**<portlist>**  
Specify a port or port range.

---

### ● Restrictions

None.

### ● Example

To display SNMP traps:

```
Zxxx0:admin#show snmp traps
Command: show snmp traps

SNMP Traps           : Enabled
Authenticate Trap    : Enabled
Linkchange Traps     : Enabled
Coldstart Traps      : Enabled
Warmstart Traps      : Enabled

Zxxx0:admin#
```

To display SNMP linkchange traps:

```
Zxxx0:admin#show snmp traps linkchange_traps
Command: show snmp traps linkchange_traps

Linkchange Traps     : Enabled
  Port 1 : Enabled
  Port 2 : Enabled
  Port 3 : Enabled
  Port 4 : Enabled
  Port 5 : Enabled
  Port 6 : Enabled
  Port 7 : Enabled
  Port 8 : Enabled
  Port 9 : Enabled
  Port 10: Enabled
  Port 11: Enabled
  Port 12: Enabled
  Port 13: Enabled
  Port 14: Enabled
  Port 15: Enabled
  Port 16: Enabled
  Port 17: Enabled
  Port 18: Enabled
  Port 19: Enabled
  Port 20: Enabled

CTRL+C  ESC  q  Quit  SPACE  n  Next Page  ENTER  Next Entry  a  All
```

## 57.18. config snmp coldstart\_traps

---

### ● Description

This command is used to configure the trap state for coldstart events.

### ● Format

config snmp coldstart\_traps [enable | disable]

### ● Parameters

|                |                                                                  |
|----------------|------------------------------------------------------------------|
| <b>enable</b>  | Enable traps for coldstart events. The default state is enabled. |
| <b>disable</b> | Disable traps for coldstart events.                              |

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To enable traps for coldstart events:

```
Zxxx0:admin#config snmp coldstart_traps enable
Command: config snmp coldstart_traps enable

Success.

Zxxx0:admin#
```

## 57.19. config snmp warmstart\_traps

---

### ● Description

This command is used to configure the trap state for warmstart events.

### ● Format

config snmp warmstart\_traps [enable | disable]

### ● Parameters

|                |                                                                  |
|----------------|------------------------------------------------------------------|
| <b>enable</b>  | Enable traps for warmstart events. The default state is enabled. |
| <b>disable</b> | Disable traps for warmstart events.                              |

## 57. Network Management Commands

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To enable traps for warmstart events:

```
Zxxx0:admin#config snmp warmstart_traps enable
Command: config snmp warmstart_traps enable

Success.

Zxxx0:admin#
```

## 57.20. config trap source\_ipif

### ● Description

This command is used to force change the ipif information in trap messages. By default, trap messages will carry the information of the ipif they belong to.

### ● Format

config trap source\_ipif [<ipif\_name 12> {<ipaddr> | <ipv6addr>} | none]

### ● Parameters

---

<ipif\_name 12>

Specify the IP interface name. If only this parameter is specified, the IPv4 address and the smallest IPv6 address of ipif\_name will be used as source IP addresses.

---

<ipaddr> (Optional) Specify the IPv4 address.

---

<ipv6addr>

(Optional) Specify the IPv6 address.

---

none Specify to clear the configured source IP interface.

---

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To configure the trap source IP interface:

```
Zxxx0:admin#config trap source_ipif inter4
Command: config trap source_ipif inter4

Success.

Zxxx0:admin#
```

To clear the configured trap source IP interface:

```
Zxxx0:admin#config trap source_ipif none
Command: config trap source_ipif none

Success.

Zxxx0:admin#
```

## 57.21. show trap source\_ipif

---

### ● Description

This command is used to display the trap source IP interface.

### ● Format

**show trap source\_ipif**

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display the trap source IP interface:

```
Zxxx0:admin#show trap source_ipif
Command: show trap source_ipif

Trap Source IP Interface Configuration:

IP Interface      : ipif4
IPv4 Address      : None
IPv6 Address      : 3000::52

Zxxx0:admin#
```



## 57.22. config rmon trap

---

### ● Description

This command is used to configure the trap state for RMON events.

### ● Format

**config rmon trap {rising\_alarm [enable | disable] | falling\_alarm [enable | disable]}**

### ● Parameters

---

#### **rising\_alarm**

(Optional) Specify the trap state for rising alarm. The default state is enabled.

**enable**

Enable the trap state for rising alarm.

**disable**

Disable the trap state for rising alarm.

---

#### **falling\_alarm**

(Optional) Specify the trap state for falling alarm. The default state is enabled.

**enable**

Enable the trap state for falling alarm.

**disable**

Disable the trap state for falling alarm.

---

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To disable the trap state for RMON:

```
Zxxx0:admin#config rmon trap rising_alarm disable
Command: config rmon trap rising_alarm disable

Success.

Zxxx0:admin#
```

## 57.23. show rmon

---

- **Description**

This command is used to display RMON related settings.

- **Format**

show rmon

- **Parameters**

None.

- **Restrictions**

None.

- **Example**

To display current RMON settings:

```
Zxxx0:admin#show rmon
Command: show rmon

RMON Rising Alarm Trap    : Enabled
RMON Falling Alarm Trap   : Enabled

Zxxx0:admin#
```

## 58. Network Monitoring Commands

The commands are used to display the following data for this Switching Hub's operation status.

- Counting the amount of transmission packets and error information for each port
- Displaying the current port usage, CPU usage, DRAM usage, and flash usage

In addition, the following functions can be executed.

- Clearing the summary counter for each port
- Displaying and configuring history log, system log and error log

---

```

show packet ports <portlist>
show error ports <portlist>
show utilization [ports | cpu]
show utilization dram {unit <unit_id>}
show utilization flash {unit <unit_id>}
clear counters {ports <portlist>}
clear log
show log {[index <value_list> | severity {module <module_list>} {emergency | alert | critical |
error | warning | notice | informational | debug | <level_list 0-7>} | module <module_list>}]
show log_save_timing
show log_software_module
config log_save_timing [time_interval <min 1-65535> | on_demand | log_trigger]
enable syslog
disable syslog
show syslog
config syslog host [<index> | all] {severity [emergency | alert | critical | error | warning | notice |
informational | debug | <level 0-7>] | facility [local0 | local1 | local2 | local3 | local4 | local5
| local6 | local7] | udp_port <udp_port_number> | ipaddress [<ipaddr> | <ipv6addr>] | state
[enable | disable]](1)
create syslog host <index 1-4> ipaddress [<ipaddr> | <ipv6addr>] {severity [emergency | alert |
critical | error | warning | notice | informational | debug | <level 0-7>] | facility [local0 |
local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> |
state [enable | disable]}
delete syslog host [<index 1-4> | all]
show syslog host {<index 1-4>}
config syslog source_ipif [<ipif_name 12> {<ipaddr> | <ipv6addr>} | none]
show syslog source_ipif
show attack_log {index <value_list>}
clear attack_log

```

---

## 58.1. show packet ports

---

- **Description**

This command is used to display statistics about the packets sent and received by the Switching Hub.

- **Format**

show packet ports <portlist>

- **Parameters**

---

<portlist>Specify a port or range of ports to be displayed.

---

- **Restrictions**

None.

- **Example**

To display the packets analysis for port 7:

## 58. Network Monitoring Commands

```
Zxxx0:admin#show packet ports 7
```

```
Command: show packet ports 7
```

```
Port number : 7
```

| Frame Size/Type | Frame Counts | Frames/sec |
|-----------------|--------------|------------|
| -----           | -----        | -----      |
| 64              | 0            | 0          |
| 65-127          | 0            | 0          |
| 128-255         | 0            | 0          |
| 256-511         | 0            | 0          |
| 512-1023        | 0            | 0          |
| 1024-1518       | 0            | 0          |
| 1519-1522       | 0            | 0          |
| 1519-2047       | 0            | 0          |
| 2048-4095       | 0            | 0          |
| 4096-9216       | 0            | 0          |
| Unicast RX      | 0            | 0          |
| Multicast RX    | 0            | 0          |
| Broadcast RX    | 0            | 0          |

```
Quit
```

```
Next Page
```

```
Previous Page
```

```
Refresh
```

```
Port number : 7
```

| Frame Type | Total | Total/sec |
|------------|-------|-----------|
| -----      | ----- | -----     |
| RX Bytes   | 0     | 0         |
| RX Frames  | 0     | 0         |
| TX Bytes   | 0     | 0         |
| TX Frames  | 0     | 0         |

```
CTRL+C  ESC  q  Quit  SPACE  n  Next Page  p  Previous Page  r  Refresh
```

### 58.2. show error ports

#### ● Description

This command is used to display error statistics for a range of ports.

#### ● Format

```
show errors ports <portlist>
```

#### ● Parameters

---

<portlist>Specify a port or range of ports to be displayed.

---

#### ● Restrictions

None.

● Example

To display the errors of port 3:

```
Zxxx0:admin#show error ports 3
Command: show error ports 3

Port Number : 3

          RX Frames                                TX Frames
          -----                                -----
CRC Error      0                                Excessive Deferral  0
Undersize      0                                CRC Error           0
Oversize       0                                Late Collision      0
Fragment       0                                Excessive Collision  0
Jabber         0                                Single Collision    0
Drop Pkts      0                                Collision           0
Symbol Error   0

CTRL+C  ESC  q  Quit  SPACE  n  Next Page  p  Previous Page  r  Refresh
```

# 58.3. show utilization

● Description

This command is used to display real-time port utilization or CPU statistics.

● Format

show utilization [ports | cpu]

● Parameters

|       |                                               |
|-------|-----------------------------------------------|
| ports | Specify to display real-time port statistics. |
| cpu   | Specify to display real-time CPU statistics.  |

● Restrictions

None.

● Example

To display port utilization:

## 58. Network Monitoring Commands

```
Zxxx0:admin#show utilization ports
```

```
Command: show utilization ports
```

| Port | TX/sec | RX/sec | Util | Port | TX/sec | RX/sec | Util |
|------|--------|--------|------|------|--------|--------|------|
| 1    | 0      | 0      | 0    | 21   | 0      | 0      | 0    |
| 2    | 0      | 0      | 0    | 22   | 0      | 0      | 0    |
| 3    | 0      | 0      | 0    | 23   | 0      | 0      | 0    |
| 4    | 0      | 0      | 0    | 24   | 0      | 0      | 0    |
| 5    | 0      | 0      | 0    | 25   | 0      | 0      | 0    |
| 6    | 0      | 0      | 0    | 26   | 0      | 0      | 0    |
| 7    | 0      | 0      | 0    | 27   | 0      | 0      | 0    |
| 8    | 0      | 0      | 0    | 28   | 0      | 0      | 0    |
| 9    | 0      | 0      | 0    |      |        |        |      |
| 10   | 0      | 0      | 0    |      |        |        |      |
| 11   | 0      | 0      | 0    |      |        |        |      |
| 12   | 0      | 0      | 0    |      |        |        |      |
| 13   | 0      | 0      | 0    |      |        |        |      |
| 14   | 0      | 0      | 0    |      |        |        |      |
| 15   | 0      | 0      | 0    |      |        |        |      |
| 16   | 0      | 0      | 0    |      |        |        |      |
| 17   | 0      | 0      | 0    |      |        |        |      |
| 18   | 0      | 0      | 0    |      |        |        |      |
| 19   | 0      | 0      | 0    |      |        |        |      |
| 20   | 0      | 0      | 0    |      |        |        |      |

```
CTRL+C  ESC  q  Quit  SPACE  n  Next Page  p  Previous Page  r  Refresh
```

To display CPU utilization:

```
Zxxx0:admin# show utilization cpu
```

```
Command: show utilization cpu
```

```
CPU utilization :
```

```
-----  
Five seconds - 20%          One minute - 10%          Five minutes - 70%
```

```
CTRL+C  ESC  q  Quit  SPACE  n  Next Page  p  Previous Page  r  Refresh
```

### 58.4. show utilization dram

#### ● Description

This command is used to display real-time DRAM utilization statistics.

#### ● Format

**show utilization dram {unit <unit\_id>}**

## ● Parameters

---

|             |                                                                                                                                                              |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>unit</b> | Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.<br><b>&lt;unit_id&gt;</b><br>Enter the unit ID used here. |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

## ● Restrictions

None.

## ● Example

To display DRAM utilization:

```
Zxxx0:admin# show utilization dram
Command: show utilization dram

DRAM utilization :
    Total DRAM      : 262144    KB
    Used DRAM       : 119586    KB
    Utilization      : 45%

[CTRL+C] [ESC] [q] Quit [SPACE] [n] Next Page [p] Previous Page [r] Refresh
```

# 58.5. show utilization flash

---

## ● Description

This command is used to display real-time Flash utilization statistics.

## ● Format

**show utilization flash {unit <unit\_id>}**

## ● Parameters

---

|             |                                                                                                                                                              |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>unit</b> | Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.<br><b>&lt;unit_id&gt;</b><br>Enter the unit ID used here. |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

## ● Restrictions

None.

## ● Example

To display Flash utilization:



## 58. Network Monitoring Commands

```
Zxxx0:admin# show utilization flash
```

```
Command: show utilization flash
```

```
FLASH Memory Utilization :
```

```
    Total FLASH      : 30608    KB
```

```
    Used FLASH       :  4786    KB
```

```
    Utilization      :   15%
```

```
CTRL+C  ESC  q  Quit  SPACE  n  Next Page  p  Previous Page  r  Refresh
```

### 58.6. clear counters

---

#### ● Description

This command is used to clear the Switching Hub's statistics counters.

#### ● Format

**clear counters {ports <portlist>}**

#### ● Parameters

---

|              |                                                                                                                  |
|--------------|------------------------------------------------------------------------------------------------------------------|
| <b>ports</b> | Specify a range of ports to be configured. The beginning and end of the port list range are separated by a dash. |
|--------------|------------------------------------------------------------------------------------------------------------------|

**<portlist>**

Specify a range of ports to be configured.

---

---

|             |                                                                       |
|-------------|-----------------------------------------------------------------------|
| <b>NOTE</b> | If no parameter is specified, the system will count all of the ports. |
|-------------|-----------------------------------------------------------------------|

---

#### ● Restrictions

Only Administrator and Operator-level users can issue this command.

#### ● Example

To clear the Switching Hub's statistics counters for ports 7 to 9:

```
Zxxx0:admin#clear counters ports 7-9
```

```
Command: clear counters ports 7-9
```

```
Success.
```

```
Zxxx0:admin#
```

## 58.7. clear log

---

### ● Description

This command is used to clear the Switching Hub's history log.

### ● Format

clear log

### ● Parameters

None.

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To clear the Switching Hub's history log:

```
Zxxx0:admin#clear log
Command: clear log

Success

Zxxx0:admin#
```

## 58.8. show log

---

### ● Description

This command is used to display the Switching Hub history log.

### ● Format

show log {[index <value\_list> | severity {module <module\_list>} {emergency | alert | critical | error | warning | notice | informational | debug | <level\_list 0-7>} | module <module\_list>]}

### ● Parameters

---

|              |                                                                                                                                                                                                                       |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>index</b> | (Optional) Specify to display the history log between two values.<br><value_list><br>Specify to display the history log between two values. For example, show log index 1-5 will display the history log from 1 to 5. |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

## 58. Network Monitoring Commands

**severity** (Optional) Specify the severity level: emergency, alert, critical, error, warning, notice, informational, or debug.

**module**

(Optional) Specify the modules to be displayed. The module can be obtained by the show log\_software\_module command. Use commas to separate multiple modules.

**<module\_list>**

Specify the modules to be displayed.

**emergency**

(Optional) Specify severity level 0.

**alert** (Optional) Specify severity level 1.

**critical** (Optional) Specify severity level 2.

**error** (Optional) Specify severity level 3.

**warning** (Optional) Specify severity level 4.

**notice** (Optional) Specify severity level 5.

**informational**

(Optional) Specify severity level 6.

**debug** (Optional) Specify severity level 7.

**<level\_list 0-7>**

(Optional) Specify a list of severity levels to be displayed. If more than one severity level, separate them by comma. The level numbers are from 0 to 7.

**module** Specify the modules to be displayed. The module can be obtained by the show log\_software\_module command. Use commas to separate multiple modules.

**<module\_list>**

Specify the modules to be displayed.

**NOTE** If no parameter is specified, all history log entries will be displayed.

### ● Restrictions

None.

### ● Example

To display the Switching Hub history log:

```
Zxxx0:admin#show log index 1-5
Command: show log index 1-5

Index Date          Time          Level   Log Text
-----
3      2000-03-01 00:26:51 INFO(6) Successful login through Console (Username:
Anonymous)
2      2000-03-01 00:26:49 CRIT(2) System started up
1      2000-03-01 00:26:49 CRIT(2) System warm start

Zxxx0:admin#
```

## 58.9. show log\_save\_timing

---

- **Description**

This command is used to display the method to save log.

- **Format**

show log\_save\_log\_timing

- **Parameters**

None.

- **Restrictions**

None.

- **Example**

To display the method to save log:

```
Zxxx0:admin#show log_save_timing
Command: show log_save_timing

Saving Log Method:  On_demand

Zxxx0:admin#
```

## 58.10. show log\_software\_module

---

- **Description**

This command is used to display the protocols or applications that support the enhanced log.

- **Format**

show log\_software\_module

- **Parameters**

None.

- **Restrictions**

None.

## 58. Network Monitoring Commands

### ● Example

To display the the protocols or applications that support the enhanced log:

```
Zxxx0:admin#show log_software_module
Command: show log_software_module

ERROR_LOG          DHCPv6_CLIENT      DHCPv6_RELAY      DHCPv6_SERVER
                   MSTP          OSPFV2            VRRP

Zxxx0:admin#
```

## 58.11. config log\_save\_timing

### ● Description

This command is used to set the method to save log.

### ● Format

config log\_save\_timing [time\_interval <min 1-65535> | on\_demand | log\_trigger]

### ● Parameters

---

#### time\_interval

Specify to save log to Flash every xxx minutes. If no log occurs in this period, nothing will be saved.

<min 1-65535>

Specify the time between 1 and 65535 minutes.

---

#### on\_demand

Specify to save log to Flash whenever the user types "save log" or "save all". This is the default.

---

#### log\_trigger

Specify to save log to Flash whenever log arrives.

---

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To configure method to save log as on demand:

```
Zxxx0:admin# config log_save_timing on_demand
Command: config log_save_timing on_demand

Success.

Zxxx0:admin#
```

## 58.12. enable syslog

---

- **Description**

This command is used to globally enable syslog to send log messages to a remote server.

- **Format**

enable syslog

- **Parameters**

None.

- **Restrictions**

Only Administrator and Operator-level users can issue this command.

- **Example**

To enable syslog to send a message:

```
Zxxx0:admin#enable syslog
Command: enable syslog

Success

Zxxx0:admin#
```

## 58.13. disable syslog

---

- **Description**

This command is used to disable syslog from sending a message.

- **Format**

disable syslog

- **Parameters**

None.

- **Restrictions**

Only Administrator and Operator-level users can issue this command.

## 58. Network Monitoring Commands

### ● Example

To disable syslog sending a message:

```
Zxxx0:admin#disable syslog
Command: disable syslog

Success

Zxxx0:admin#
```

## 58.14. show syslog

---

### ● Description

This command is used to display the syslog protocol global state.

### ● Format

**show syslog**

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display the syslog protocol global state:

```
Zxxx0:admin#show syslog
Command: show syslog

Syslog Global State: Enabled

Zxxx0:admin#
```

# 58.15. config syslog host

## ● Description

This command is used to configure the syslog host configuration.

## ● Format

config syslog host [<index> | all] {severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp\_port <udp\_port\_number> | ipaddress[ <ipaddr> | <ipv6addr>] | state [enable | disable]} (1)

## ● Parameters

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <index>  | Specify the host index.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| all      | Specify all hosts.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| severity | (Optional) Specify the severity level supported: emergency, alert, critical, error, warning, notice, informational, or debug.<br>emergency<br>Specify emergency messages.<br>alert<br>Specify alert messages.<br>critical<br>Specify critical messages.<br>error<br>Specify error messages.<br>warning<br>Specify warning messages.<br>noticeSpecify notice messages.<br>informational<br>Specify informational messages.<br>debugSpecify debug messages.<br><level 0-7><br>Specify a level between 0 and 7.                                                                               |
| facility | Some of the operating system daemons and processes have been assigned facility values. Processes and daemons that have not been explicitly assigned a facility may use any of the "local use" facilities or they may use the "user-level" facility. Those facilities that have been designated are shown in the following:<br>local0User-defined facility.<br>local1User-defined facility.<br>local2User-defined facility.<br>local3User-defined facility.<br>local4User-defined facility.<br>local5User-defined facility.<br>local6User-defined facility.<br>local7User-defined facility. |
| udp_port | Specify the UDP port number.<br><udp_port_number><br>Specify the UDP port number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |



## 58. Network Monitoring Commands

---

### ipaddress

Specify the IPv4 address or IPv6 address of the host.

**<ipaddr>**

Specify the IPv4 address of the host.

**<ipv6addr>**

Specify the IPv6 address of the host.

---

**state** The syslog protocol has been used for the transmission of event notification messages across networks to host. This option enables or disables the host to receive such messages.

**enable**

Enable the host to receive messages.

**disable**

Disable the host to receive messages.

---

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To configure the syslog host configuration:

```
Zxxx0:admin# config syslog host all severity informational facility local0
Command: config syslog host all severity informational facility local0
```

```
Success.
```

```
Zxxx0:admin#
```

## 58.16. create syslog host

---

### ● Description

This command is used to create a new syslog host.

### ● Format

**create syslog host <index 1-4> ipaddress [<ipaddr> | <ipv6addr>] {severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp\_port <udp\_port\_number> | state [enable | disable]}**

### ● Parameters

---

**<index 1-4>**

Specify the host index.

---

---

**ipaddress**

Specify the IPv4 address or IPv6 address of the host.

**<ipaddr>**

Specify the IPv4 address of the host.

**<ipv6addr>**

Specify the IPv6 address of the host.

---

**severity** (Optional) Specify the severity level supported: emergency, alert, critical, error, warning, notice, informational, or debug.

**emergency**

Specify emergency messages.

**alert** Specify alert messages.

**critical**

Specify critical messages.

**error** Specify error messages.

**warning**

Specify warning messages.

**notice** Specify notice messages.

**informational**

Specify informational messages.

**debug** Specify debug messages.

**<level 0-7>**

Specify a level between 0 and 7.

---

**facility** Some of the operating system daemons and processes have been assigned facility values. Processes and daemons that have not been explicitly assigned a facility may use any of the "local use" facilities or they may use the "user-level" facility. Those facilities that have been designated are shown in the following:

**local0** User-defined facility.

**local1** User-defined facility.

**local2** User-defined facility.

**local3** User-defined facility.

**local4** User-defined facility.

**local5** User-defined facility.

**local6** User-defined facility.

**local7** User-defined facility.

---

**udp\_port**

Specify the UDP port number.

**<udp\_port\_number>**

Specify the UDP port number.

---

**state** The syslog protocol has been used for the transmission of event notification messages across networks to host. This option enables or disables the host to receive such messages.

**enable**

Enable the host to receive messages.

**disable**

Disable the host to receive messages.

---

## ● Restrictions

Only Administrator and Operator-level users can issue this command.

## ● Example

To create a new syslog host:

## 58. Network Monitoring Commands

```
Zxxx0:admin# create syslog host 1 ipaddress 10.1.1.1
Command: create syslog host 1 ipaddress 10.1.1.1

Success.

Zxxx0:admin#
```

### 58.17. delete syslog host

---

#### ● Description

This command is used to delete syslog host(s).

#### ● Format

delete syslog host [<index 1-4> | all]

#### ● Parameters

|            |                         |
|------------|-------------------------|
| <inex 1-4> | Specify the host index. |
| all        | Specify all hosts.      |

#### ● Restrictions

Only Administrator and Operator-level users can issue this command.

#### ● Example

To delete a syslog host:

```
Zxxx0:admin#delete syslog host 4
Command: delete syslog host 4

Success

Zxxx0:admin#
```

## 58.18. show syslog host

---

### ● Description

This command is used to display syslog host configurations.

### ● Format

show syslog host {<index 1-4>}

### ● Parameters

---

<index 1-4>

(Optional) Specify the host index.

---

---

**NOTE** If no parameter is specified, all hosts will be displayed.

---

### ● Restrictions

None.

### ● Example

To display syslog host configurations:

```
Zxxx0:admin#show syslog host
Command: show syslog host

Syslog Global State: Disabled

Host 1
  IP Address      : 10.1.1.2
  Severity        : Warning
  Facility        : Local10
  UDP port        : 514
  Status          : Disabled

Host 2
  IP Address      : 3000:501:100:ffff:101:202:303:1
  Severity        : Emergency
  Facility        : Local10
  UDP port        : 514
  Status          : Disabled

Total Entries : 2

Zxxx0:admin#
```

## 58.19. config syslog source\_ipif

### ● Description

This command is used to force change the ipif information in syslogs. By default, syslogs will carry the information of the ipif they belong to.

### ● Format

config syslog source\_ipif [<ipif\_name 12> {<ipaddr> | <ipv6addr>} | none]

### ● Parameters

---

<ipif\_name 12>

Specify the IP interface name. If only this parameter is specified, the IPv4 address and the smallest IPv6 address of ipif\_name will be used as source IP addresses.

---

<ipaddr> (Optional) Specify the IP4 address.

---

<ipv6addr>

(Optional) Specify the IPv6 global address.

---

none Specify to clear the configured source IP interface.

---

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To configure the syslog source IP interface:

```
Zxxx0:admin#config syslog source_ipif Sysetm
Command: config syslog source_ipif System

Success.

Zxxx0:admin#
```

To clear the configured source IP interface for syslog:

```
Zxxx0:admin#config syslog source_ipif none
Command: config syslog source_ipif none

Success.

Zxxx0:admin#
```

## 58.20. show syslog source\_ipif

---

### ● Description

This command is used to display the syslog source IP interface.

### ● Format

show syslog source\_ipif

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display the syslog source interface:

```
Zxxx0:admin#show syslog source_ipif
Command: show syslog source_ipif

Syslog Source IP Interface Configuration:

IP Interface           : System
IPv4 Address           : None
IPv6 Address           : None

Zxxx0:admin#
```

## 58.21. show attack\_log

---

### ● Description

This command is used to display the Switching Hub's attack log.

### ● Format

show attack\_log {index <value\_list>}

### ● Parameters

---

**index** (Optional) Specify the list of index of the entries that need to be displayed.  
<value\_list>

Specify the list of index of the entries that need to be displayed. For example, show attack\_log index 1-5 will display the attack log messages from 1 to 5.

---

## 58. Network Monitoring Commands

---

**NOTE** If no parameter is specified, all entries in the attack log will be displayed.

---

### ● Restrictions

None.

### ● Example

To display the Switching Hub's attack log:

```
Zxxx0:admin#show attack_log index 1-3
Command: show attack_log index 1-3

Index Date          Time          Level         Log Text
-----
3      2009-12-26 14:15:45  WARN(4)  Port security violation mac addrss 00-18-F3-10-94-89 on locking address full port 28
2      2009-12-26 14:15:45  WARN(4)  Port security violation mac addrss 00-18-F3-10-94-89 on locking address full port 28
1      2009-12-26 14:15:45  WARN(4)  Port security violation mac addrss 00-18-F3-10-94-89 on locking address full port 28

Zxxx0:admin#
```

## 58.22. clear attack\_log

---

### ● Description

This command is used to clear the Switching Hub's attack log.

### ● Format

clear attack\_log

### ● Parameters

None.

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To clear the Switching Hub's attack log:

```
Zxxx0:admin#clear attack_log  
Command: clear attack_log
```

```
Success.
```

```
Zxxx0:admin#
```



## 59. Open Shortest Path First (OSPF) Command List

OSPF is a function to determine packet destinations dynamically. While RIP decides a route based on the number of routers passed through, OSPF determines an optimum route from the total number of cost values based on the route bandwidth. This allows for efficient routing even in a large-size network.

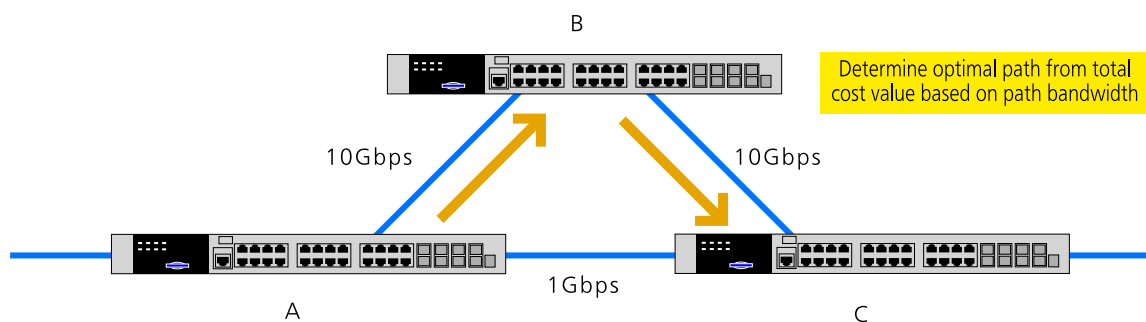


Figure 59-1 OSPF overview

You need to configure the cost value for each output port of a L3 Switching Hub or router. It can be configured manually, as well as automatically based on bandwidth. Manual configuration allows you to set up distributing traffic to multiple routes according to the conditions.

The cost value is calculated based on a network configuration created by exchanging route information (LSA) with neighbor Switching Hubs. The larger a configuration becomes, the higher a calculation load becomes. If a configuration is too large, configure "areas" - multiple regions into which the network is divided.

```

config ospf [ipif <ipif_name 12> | all] {area <area_id> | priority <value> | hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | authentication [none | simple <password 8>] | metric <value 1-65535> | state [enable | disable] | passive [enable | disable]}(1)
create ospf aggregation <area_id> <network_address> lsdb_type [summary {advertise [enable | disable]} | nssa_ext {advertise [enable | disable]}]
config ospf aggregation <area_id> <network_address> lsdb_type [summary {advertise [enable | disable]} | nssa_ext {advertise [enable | disable]}]
delete ospf aggregation <area_id> <network_address> lsdb_type [summary | nssa_ext]
show ospf aggregation {<area_id>}
create ospf area <area_id> type [normal | [stub | nssa {translate [enable | disable]}] {stub_summary [enable | disable] | metric <value 0-65535>}]
config ospf area <area_id> type [normal | [stub | nssa {translate [enable | disable]}] {stub_summary [enable | disable] | metric <value 0-65535>}]
delete ospf area <area_id>
  
```

---

```

show ospf area {<area_id>}
create ospf host_route <ipaddr> {area <area_id> | metric <value 1-65535>}
config ospf host_route <ipaddr> {area <area_id> | metric <value 1-65535>}(1)
delete ospf host_route <ipaddr>
show ospf host_route {<ipaddr>}
config ospf router_id <ipaddr>
create ospf virtual_link <area_id> <neighbor_id> {hello_interval <sec 1-65535> | dead_interval
    <sec 1-65535> | authentication [none | simple <password 8>]}
config ospf virtual_link <area_id> <neighbor_id> {hello_interval <sec 1-65535> | dead_interval
    <sec 1-65535> | authentication [none | simple <password 8>]}(1)
delete ospf virtual_link <area_id> <neighbor_id>
show ospf virtual_link {<area_id> <neighbor_id>}
enable ospf
show ospf {[ipif <ipif_name 12> | all]}
disable ospf
show ospf lsdb {area <area_id> | advertise_router <ipaddr> | type [rtrlink | netlink | summary |
    assummary | asextlink | nssa_ext | stub]}
show ospf neighbor {<ipaddr>}
show ospf virtual_neighbor {<area_id> <neighbor_id>}

```

---

## 59.1. config ospf

---

### ● Description

This command is used to configure the OSPF interface settings.

### ● Format

```

config ospf [ipif <ipif_name 12> | all] {area <area_id> | priority <value> | hello_interval <sec
1-65535> | dead_interval <sec 1-65535> | authentication [none | simple <password 8>] |
metric <value 1-65535> | state [enable | disable] | passive [enable | disable]}(1)

```

### ● Parameters

---

|                 |                                                                                                                                                                                                                                                                     |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b>     | Specifies the name of the IP interface.<br><b>&lt;ipif_name 12&gt;</b><br>Enter the IP interface name here. This name can be up to 12 characters long.                                                                                                              |
| <b>all</b>      | Specifies that all the IP interfaces will be used.                                                                                                                                                                                                                  |
| <b>area</b>     | (Optional) Specifies the area to which the interface is assigned. An Area ID is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.<br><b>&lt;area_id&gt;</b><br>Enter the area ID used here. |
| <b>priority</b> | (Optional) Specifies the priority value for the Designated Router election. If a Router Priority of 0 is set, the Switch cannot be elected as the DR for the network.<br><b>&lt;value&gt;</b><br>Enter the priority value used here.                                |

---

## 59. Open Shortest Path First (OSPF) Command List

---

### hello\_interval

(Optional) Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. Between 1 and 65535 seconds can be specified. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.

**<sec 1-65535>**

Enter the hello packet interval value here. This value must be between 1 and 65535 seconds.

---

### dead\_interval

(Optional) Allows the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 1 and 65535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval.

**<sec 1-65535>**

Enter the dead packet interval value here. This value must be between 1 and 65535 seconds.

---

### authentication

(Optional) Specifies that authentication value.

**none**

Specifies that the authentication value will be set to none.

**simple**

Specifies that a simple text password must be specified.

**<password 8>**

Enter the simple text password value here.

---

**metric** (Optional) Specifies the interface metric used.

**<value 1-65535>**

Enter the metric value here. This value must be between 1 and 65535.

---

**state** (Optional) Specifies the OSPF interface state here.

**enable**

Specifies that the state will be set to enabled.

**disable**

Specifies that the state will be set to disabled.

---

**passive** (Optional) Specifies whether the designated entry to be a passive interface or not. When the interface is specified to be passive, OSPF protocol packets will neither be sent out or received.

**enable**

Specifies that the passive interface will be enabled.

**disable**

Specifies that the passive interface will be disabled.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure OSPF interface settings:

```
Zxxx0:admin# config ospf ipif System priority 2 hello_interval 20 metric 2 state
enabled
Command: config ospf ipif System priority 2 hello_interval 20 metric 2 state
enabled

Success.

Zxxx0:admin#
```

## 59.2. create ospf aggregation

### ● Description

This command is used to create an OSPF area aggregation entry.

### ● Format

**create ospf aggregation** <area\_id> <network\_address> lsdb\_type [summary {advertise [enable | disable]} | nssa\_ext {advertise [enable | disable]}]

### ● Parameters

#### <area\_id>

A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

#### <network\_address>

The IP address that uniquely identifies the network that corresponds to the OSPF Area. The network address format is 'IP address/prefix length'.

#### lsdb\_type

Specifies the Link-State Database (LSDB) type of address aggregation.

##### summary

Specifies the LSDB type as summary.

##### advertise

(Optional) Allows for the advertisement of the summary LSDB.

##### enable

Specifies that the advertisement trigger will be enabled.

##### disable

Specifies that the advertisement trigger will be disabled.

##### nssa\_ext

Specifies the the LSDB type as a Not-So-Stub Area External Route (NSSA EXT).

##### advertise

(Optional) Allows for the advertisement of aggregated NSSA external route.

##### enable

Specifies that the advertisement trigger will be enabled.

##### disable

Specifies that the advertisement trigger will be disabled.

## 59. Open Shortest Path First (OSPF) Command List

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create OSPF area aggregation settings:

```
Zxxx0:admin# create ospf aggregation 10.1.1.1 192.168.0.0/16 lsdb_type summary
Command: create ospf aggregation 10.1.1.1 192.168.0.0/16 lsdb_type summary

Success.

Zxxx0:admin#
```

## 59.3. config ospf aggregation

---

### ● Description

This command is used to configure the OSPF area aggregation settings.

### ● Format

**config ospf aggregation <area\_id> <network\_address> lsdb\_type [summary {advertise [enable | disable]} | nssa\_ext {advertise [enable | disable]}]**

### ● Parameters

---

**<area\_id>**

A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

---

**<network\_address>**

The IP address that uniquely identifies the network that corresponds to the OSPF Area. The network address format is 'IP address/prefix length'.

---

**lsdb\_type**

Specifies the Link-State Database (LSDB) type of address aggregation.

**summary**

Specifies the LSDB type as summary.

**advertise**

(Optional) Allows for the advertisement of the summary LSDB.

**enable**

Specifies that the advertisement trigger will be enabled.

**disable**

Specifies that the advertisement trigger will be disabled.

**nssa\_ext**

Specifies the the LSDB type as a Not-So-Stub Area External Route (NSSA EXT).

**advertise**

(Optional) Allows for the advertisement of aggregated NSSA external route.

**enable**

Specifies that the advertisement trigger will be enabled.

**disable**

Specifies that the advertisement trigger will be disabled.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure the OSPF area aggregation settings:

```
Zxxx0:admin# config ospf aggregation 10.1.1.1 10.48.76.122/16 lsdb_type summary
advertise enabled
Command: config ospf aggregation 10.1.1.1 10.48.76.122/16 lsdb_type summary
advertise enabled

Success.

Zxxx0:admin#
```

# 59.4. delete ospf aggregation

## ● Description

This command is used to delete an OSPF area aggregation configuration.

## ● Format

**delete ospf aggregation <area\_id> <network\_address> lsdb\_type [summary | nssa\_ext]**

## ● Parameters

**<area\_id>**A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

**<network\_address>**  
The IP address that uniquely identifies the network that corresponds to the OSPF Area.  
The network address format is 'IP address/prefix length'.

**lsdb\_type**  
Specifies the LSDB type.  
**summary**  
Specifies the type of address aggregation.  
**nssa\_ext**  
Specifies the NSSA EXT type.

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## 59. Open Shortest Path First (OSPF) Command List

### ● Example

To delete an OSPF area aggregation settings:

```
Zxxx0:admin# delete ospf aggregation 10.1.1.1 10.48.76.122/16 lsdb_type summary
Command: delete ospf aggregation 10.1.1.1 10.48.76.122/16 lsdb_type summary

Success.

Zxxx0:admin#
```

## 59.5. show ospf aggregation

### ● Description

This command is used to display the current OSPF host route table.

### ● Format

**show ospf aggregation {<area\_id>}**

### ● Parameters

---

**<area\_id>**(Optional) Enter the area ID used here.

---

### ● Restrictions

None.

### ● Example

To display OSPF host route settings:

```
Zxxx0:admin#show ospf aggregation
Command: show ospf aggregation

OSPF Area Aggregation Settings

Area ID          Aggregated      LSDB      Advertise
                  Network Address  Type
-----
0.0.0.0          10.90.0.0/16     Summary   Enabled
0.0.0.0          10.90.0.0/17     Summary   Enabled
0.0.0.0          10.90.64.0/18    Summary   Enabled

Total Entries : 3

Zxxx0:admin#
```

## 59.6. create ospf area

---

### ● Description

This command is used to create an OSPF area. OSPF allows collections of contiguous networks and hosts to be grouped together. Such a group, together with the routers having interfaces to any one of the included networks, is called an area.

### ● Format

```
create ospf area <area_id> type [normal | [stub | nssa {translate [enable | disable]}]
{stub_summary [enable | disable] | metric <value 0-65535>}]
```

### ● Parameters

---

**<area\_id>** Enter the OSPF area ID used here.

---

**type** Specifies the OSPF area operation type. In some Autonomous Systems, the majority of the topological database may consist of AS external advertisements. An OSPF AS external advertisement is usually flooded throughout the entire AS. However, OSPF allows certain areas to be configured as "stub areas". AS external advertisements are not flooded into/throughout stub areas; routing to AS external destinations in these areas is based on a (per-area) default only. This reduces the topological database size, and therefore the memory requirements, for a stub area's internal routers.

**normal**

Specifies that the OSPF area type will be set to normal.

**stub** Specifies that the OSPF area type will be set to STUB.

**nssa** Specifies that the OSPF area type will be set to NSSA.

**translate**

(Optional) Specifies if translation will be enabled or disabled.

**enable**

Specifies that the translate option will be enabled.

**disable**

Specifies that the translate option will be disabled.

---

**stub\_summary**

(Optional) Specifies whether the summary LSA is effective for this area.

**enable**

Specifies that the STUB summary option will be enabled.

**disable**

Specifies that the STUB summary option will be disabled.

---

**metric** (Optional) Specifies the metric (1 - 65535; 0 for auto cost) of this area.

**<value 0-65535>**

Enter the metric value used here. This value must be between 0 and 65535.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.



## 59. Open Shortest Path First (OSPF) Command List

### ● Example

To create an OSPF area:

```
Zxxx0:admin# create ospf area 10.48.74.122 type stub stub_summary enabled metric 1
Command: create ospf area 10.48.74.122 type stub stub_summary enabled metric 1

Success.

Zxxx0:admin#
```

## 59.7. config ospf area

---

### ● Description

This command is used to configure an OSPF area's settings.

### ● Format

**config ospf area <area\_id> type [normal | [stub | nssa {translate [enable | disable]}] {stub\_summary [enable | disable] | metric <value 0-65535>}]**

### ● Parameters

---

**<area\_id>**Enter the OSPF area ID used here.

**type** Specifies the OSPF area operation type. In some Autonomous Systems, the majority of the topological database may consist of AS external advertisements. An OSPF AS external advertisement is usually flooded throughout the entire AS. However, OSPF allows certain areas to be configured as "stub areas". AS external advertisements are not flooded into/throughout stub areas; routing to AS external destinations in these areas is based on a (per-area) default only. This reduces the topological database size, and therefore the memory requirements, for a stub area's internal routers.

**normal**

Specifies that the OSPF area type will be set to normal.

**stub** Specifies that the OSPF area type will be set to STUB.

**nssa** Specifies that the OSPF area type will be set to NSSA.

**translate**

(Optional) Specifies if translation will be enabled or disabled.

**enable**

Specifies that the translate option will be enabled.

**disable**

Specifies that the translate option will be disabled.

---

**stub\_summary**

(Optional) Specifies whether the summary LSA is effective for this area.

**enable**

Specifies that the STUB summary option will be enabled.

**disable**

Specifies that the STUB summary option will be disabled.

---

---

**metric** (Optional) Specifies the metric (1 - 65535; 0 for auto cost) of this area.  
**<value 0-65535>**

Enter the metric value used here. This value must be between 0 and 65535.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure an OSPF area's settings:

```
Zxxx0:admin# config ospf area 10.48.74.122 type stub stub_summary enabled metric 1
Command: config ospf area 10.48.74.122 type stub stub_summary enabled metric 1

Success.

Zxxx0:admin#
```

## 59.8. delete ospf area

---

### ● Description

This command is used to delete an OSPF area.

### ● Format

**delete ospf area <area\_id>**

### ● Parameters

---

**<area\_id>**Enter the OSPF area ID used here.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete an OSPF area:

```
Zxxx0:admin# delete ospf area 10.48.74.122
Command: delete ospf area 10.48.74.122

Success.

Zxxx0:admin#
```

## 59.9. show ospf area

---

### ● Description

This command is used to display an OSPF area's configuration.

### ● Format

`show ospf area {<area_id>}`

### ● Parameters

---

`<area_id>`(Optional) Enter the OSPF area ID used here.

---

### ● Restrictions

None.

### ● Example

To display OSPF area's configuration:

```
Zxxx0:admin# show ospf area
Command: show ospf area

OSPF Area Settings

Area ID          Type    Stub Import Summary LSA Stub Default Cost Translate
-----
0.0.0.0          Normal None                    None          None
1.1.1.1          Normal None                    None          None
4.4.4.4          Normal None                    None          None
5.5.5.5          Stub   Enabled                 1             None

Total Entries : 4

Zxxx0:admin#
```

## 59.10. create ospf host\_route

---

### ● Description

This command is used to create an OSPF host route.

### ● Format

**create ospf host\_route <ipaddr> {area <area\_id> | metric <value 1-65535>}**

### ● Parameters

---

**<ipaddr>** Enter the host's IP address used here.

**area** (Optional) Specifies a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

**<area\_id>**

Enter the area ID value here.

---

**metric** (Optional) Specifies a metric that will be advertised.

**<value 1-65535>**

Enter the metric value used here. This value must be between 1 and 65535.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create an OSPF host route:

```
Zxxx0:admin# create ospf host_route 10.48.74.122 area 10.1.1.1 metric 2
Command: create ospf host_route 10.48.74.122 area 10.1.1.1 metric 2

Success.

Zxxx0:admin#
```

## 59.11. config ospf host\_route

---

### ● Description

This command is used to configure an OSPF host route.

### ● Format

**config ospf host\_route <ipaddr> {area <area\_id> | metric <value 1-65535>}(1)**

## 59. Open Shortest Path First (OSPF) Command List

### ● Parameters

---

**<ipaddr>** Enter the host's IP address used here.

---

**area** (Optional) Specifies a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

**<area\_id>**

Enter the area ID value here.

---

**metric** (Optional) Specifies a metric that will be advertised.

**<value 1-65535>**

Enter the metric value used here. This value must be between 1 and 65535.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure an OSPF host route:

```
Zxxx0:admin# config ospf host_route 10.48.74.122 area 10.1.1.1 metric 2
```

```
Command: config ospf host_route 10.48.74.122 area 10.1.1.1 metric 2
```

```
Success.
```

```
Zxxx0:admin#
```

## 59.12. delete ospf host\_route

---

### ● Description

This command is used to delete an OSPF host route.

### ● Format

**delete ospf host\_route <ipaddr>**

### ● Parameters

---

**<ipaddr>** Enter the host's IP address used here.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To delete an OSPF host route:

```
Zxxx0:admin# delete ospf host_route 10.48.74.122
Command: delete ospf host_route 10.48.74.122

Success.

Zxxx0:admin#
```

## 59.13. show ospf host\_route

---

### ● Description

This command is used to display the current OSPF host route table.

### ● Format

**show ospf host\_route {<ipaddr>}**

### ● Parameters

---

**<ipaddr>**(Optional) Enter the host's IP address used here.

---

### ● Restrictions

None.

## ● Example

To display the OSPF host route settings:

```
Zxxx0:admin# show ospf host_route
Command: show ospf host_route

OSPF Host Route Settings

Host Address      Metric Area ID
-----
10.48.73.21       2    10.1.1.1
10.48.74.122     1    10.1.1.1

Total Entries : 2

Zxxx0:admin#
```

## 59.14. config ospf router\_id

---

### ● Description

The command is used to configure the router ID for the Switching Hub. Each Switching Hub that is configured to run OSPF must have a unique router ID.

### ● Format

**config ospf router\_id <ipaddr>**

### ● Parameters

---

**<ipaddr>**Enter the router's IP address here.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the router ID for the Switching Hub:

```
Zxxx0:admin# config ospf router_id 10.48.74.122
Command: config ospf router_id 10.48.74.122

Success.

Zxxx0:admin#
```

## 59.15. create ospf virtual\_link

---

### ● Description

This command is used to create an OSPF virtual link.

### ● Format

**create ospf virtual\_link <area\_id> <neighbor\_id> {hello\_interval <sec 1-65535> | dead\_interval <sec 1-65535> | authentication [none | simple <password 8>]}(1)**

### ● Parameters

---

**<area\_id>**Specifies a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

---

## 59. Open Shortest Path First (OSPF) Command List

---

### <neighbor\_id>

Specifies the OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. This is the router ID of the neighbor router.

---

### hello\_interval

(Optional) Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.

#### <sec 1-65535>

Enter the hello packet interval used here. This value must be between 1 and 65535.

---

### dead\_interval

(Optional) Allows the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 1 and 65535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval.

#### <sec 1-65535>

Enter the dead packet interval used here. This value must be between 1 and 65535.

---

### authentication

(Optional) Specifies the authentication type used.

**none** Specifies that the authentication type will be set to none.

**simple** Specifies that a simple text password will be used in the authentication.

#### <password 8>

Enter the simple text password value here. This value can be up to 8 characters long.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To create a virtual link to another ABR:

```
Zxxx0:admin# create ospf virtual_link 10.1.1.12 20.1.1.1 hello_interval 10
Command: create ospf virtual_link 10.1.1.12 20.1.1.1 hello_interval 10

Success.

Zxxx0:admin#
```



## 59.16. config ospf virtual\_link

---

### ● Description

This command is used to configure the OSPF virtual link.

### ● Format

```
config ospf virtual_link <area_id> <neighbor_id> {hello_interval <sec 1-65535> |  
dead_interval <sec 1-65535> | authentication [none | simple <password 8>]}
```

### ● Parameters

---

**<area\_id>** Specifies a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

---

**<neighbor\_id>**

Specifies the OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. This is the router ID of the neighbor router.

---

**hello\_interval**

(Optional) Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.

**<sec 1-65535>**

Enter the hello packet interval used here. This value must be between 1 and 65535.

---

**dead\_interval**

(Optional) Allows the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 1 and 65535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval.

**<sec 1-65535>**

Enter the dead packet interval used here. This value must be between 1 and 65535.

---

**authentication**

(Optional) Specifies the authentication type used.

**none** Specifies that the authentication type will be set to none.

**simple** Specifies that a simple text password will be used in the authentication.

**<password 8>**

Enter the simple text password value here. This value can be up to 8 characters long.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure the OSPF virtual link:

```
Zxxx0:admin# config ospf virtual_link 10.1.1.2 20.1.1.1 hello_interval 10
Command: config ospf virtual_link 10.1.1.2 20.1.1.1 hello_interval 10

Success.

Zxxx0:admin#
```

## 59.17. delete ospf virtual\_link

---

### ● Description

This command is used to delete an OSPF virtual link.

### ● Format

**delete ospf virtual\_link <area\_id> <neighbor\_id>**

### ● Parameters

---

**<area\_id>** Specifies a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

---

**<neighbor\_id>**

Specifies the OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. This is the router ID of the neighbor router.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To delete an OSPF virtual link:

```
Zxxx0:admin# delete ospf virtual_link 10.1.1.12 20.1.1.1
Command: delete ospf virtual_link 10.1.1.12 20.1.1.1

Success.

Zxxx0:admin#
```

## 59.18. show ospf virtual\_link

### ● Description

This command is used to display the current OSPF virtual interface configuration.

### ● Format

**show ospf virtual\_link {<area\_id> <neighbor\_id>}**

### ● Parameters

**<area\_id>**(Optional) Specifies a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

**<neighbor\_id>**

(Optional) The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. This is the router ID of the neighbor router.

If no parameter is specified, the system will display the all current OSPF virtual interface configuration.

### ● Restrictions

None.

### ● Example

To display the current OSPF virtual interface configuration:

```
Zxxx0:admin#show ospf virtual_link
```

```
Command: show ospf virtual_link
```

```
Virtual Interface Configuration
```

| Transit<br>Area ID | Virtual<br>Neighbor Router | Hello<br>Interval | Dead<br>Interval | Authentication | Link<br>Status |
|--------------------|----------------------------|-------------------|------------------|----------------|----------------|
| 4.4.4.4            | 1.1.1.1                    | 10                | 60               |                | Up             |
| 4.4.4.4            | 6.6.6.6                    | 10                | 250              | Simple         | Down           |

```
Total Entries : 2
```

```
Zxxx0:admin#
```

## 59.19. enable ospf

---

### ● Description

This command is used to enable OSPF on the Switching Hub.

### ● Format

enable ospf

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable OSPF on the Switching Hub:

```
Zxxx0:admin# enable ospf
Command: enable ospf

Success.

Zxxx0:admin#
```

## 59.20. show ospf

---

### ● Description

This command is used to display the current OSPF state on the Switching Hub.

### ● Format

show ospf {[ipif <ipif\_name 12> | all]}

### ● Parameters

|             |                                                                                                                                                      |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b> | (Optional) Specifies the name of the IP interface.<br><ipif_name 12><br>Enter the IP interface name here. This name can be up to 12 characters long. |
| <b>all</b>  | Specifies that all the IP interfaces will be displayed.                                                                                              |

If no parameter is specified, the system will display the current OSPF state.

## 59. Open Shortest Path First (OSPF) Command List

### ● Restrictions

None.

### ● Example

To display the current OSPF state:

```
Zxxx0:admin# show ospf
Command: show ospf

OSPF Router ID : 10.90.90.90 (Auto selected)
State          : Enabled

OSPF Interface Settings

Interface      IP Address      Area ID      State      Link      Metric
-----
System        10.90.90.90/8   0.0.0.0      Disabled   Link Down 1

Total Entries : 1

OSPF Area Settings

Area ID      Type      Stub Import Summary LSA Stub Default Cost Translate
-----
0.0.0.0      Normal    None                                None              None
10.0.0.0     Normal    None                                None              None
10.0.0.1     NSSA      Enabled          1              Disabled
10.0.0.2     Stub      Enabled          1              None

Total Entries : 4

Virtual Interface Configuration

Transit      Virtual      Hello      Dead      Authentication Link
Area ID      Neighbor Router Interval Interval          Status
-----
10.0.0.0     10.0.0.1     10         60         None           Down

Total Entries : 1
```

```

OSPF Area Aggregation Settings

Area ID          Aggregated      LSDB      Advertise
                  Network Address  Type
-----
10.0.0.2         10.0.0.0/8      Summary  Enabled

Total Entries : 1

OSPF Host Route Settings

Host Address      Metric Area ID
-----
10.90.91.90      1          0.0.0.0

Total Entries : 1

Zxxx0:admin#

```

## 59.21. disable ospf

### ● Description

This command is used to disable OSPF on the Switching Hub.

### ● Format

**disable ospf**

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To disable OSPF on the Switching Hub:

```

Zxxx0:admin# disable ospf
Command: disable ospf

Success.

Zxxx0:admin#

```

## 59.22. show ospf lsdb

---

### ● Description

This command is used to display the OSPF Link State Database (LSDB).

### ● Format

**show ospf lsdb {area <area\_id> | advertise\_router <ipaddr> | type [rtrlink | netlink | summary | assummary | asexmlink | nssa\_ext | stub]}**

### ● Parameters

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>area</b>             | (Optional) Specifies a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.<br><b>&lt;area_id&gt;</b><br>Enter the area ID used here.                                                                                                                                                                                                                                                                                                                                                                         |
| <b>advertise_router</b> | (Optional) Specifies the IP address of the advertising router.<br><b>&lt;ipaddr&gt;</b><br>Enter the advertising router's IP address here.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>type</b>             | (Optional) Specifies the type of link displayed.<br><b>rtrlink</b> Specifies the type to be displayed as router link.<br><b>netlink</b><br>Specifies the type to be displayed as network link.<br><b>summary</b><br>Specifies the type to be displayed as summary.<br><b>assummary</b><br>Specifies the type to be displayed as AS summary.<br><b>asemlink</b><br>Specifies the type to be displayed as AS external link.<br><b>nssa_ext</b><br>Specifies the type to be displayed as NSSA external information.<br><b>stub</b> Specifies the type to be displayed as STUB link. |

### ● Restrictions

None.

## ● Example

To display the link state database of OSPF:

```
Zxxx0:admin# show ospf lsdb
```

```
Command: show ospf lsdb
```

| Area ID | LSDB<br>Type | Advertising<br>Router ID | Link State<br>ID | Cost | Sequence<br>Number |
|---------|--------------|--------------------------|------------------|------|--------------------|
| 0.0.0.0 | RTRLINK      | 50.48.75.73              | 50.48.75.73      | *    | 0x80000002         |
| 0.0.0.0 | Summary      | 50.48.75.73              | 10.0.0.0/8       | 1    | 0x80000001         |
| 1.0.0.0 | RTRLINK      | 50.48.75.73              | 50.48.75.73      | *    | 0x80000001         |
| 1.0.0.0 | Summary      | 50.48.75.73              | 40.0.0.0/8       | 1    | 0x80000001         |
| 1.0.0.0 | Summary      | 50.48.75.73              | 50.0.0.0/8       | 1    | 0x80000001         |
| 0.0.0.0 | ASExtLink    | 50.48.75.73              | 1.2.0.0/16       | 20   | 0x80000001         |

```
Total Entries : 6
```

```
Zxxx0:admin#
```

## 59.23. show ospf neighbor

### ● Description

This command is used to display the OSPF-neighbor information on a per-interface basis.

### ● Format

**show ospf neighbor {<ipaddr>}**

### ● Parameters

---

**<ipaddr>**(Optional) Specifies the IP address of the neighbor router.

---

If no parameter is specified, the system will display all OSPF neighbor information.

### ● Restrictions

None.



## 59. Open Shortest Path First (OSPF) Command List

### ● Example

To display OSPF neighbor information:

```
Zxxx0:admin# show ospf neighbor
Command: show ospf neighbor

IP Address of   Router ID of   Neighbor Neighbor
Neighbor       Neighbor       Priority State
-----
10.48.74.122    10.2.2.2        1         Initial

Total Entries : 1

Zxxx0:admin#
```

## 59.24. show ospf virtual\_neighbor

### ● Description

This command is used to display the OSPF-neighbor information of OSPF virtual links.

### ● Format

**show ospf virtual\_neighbor {<area\_id> <neighbor\_id>}**

### ● Parameters

---

**<area\_id>**(Optional) Specifies a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

---

**<neighbor\_id>**  
(Optional) Specifies the OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router.

---

If no parameter is specified, the system will display all OSPF virtual-link neighbor information.

### ● Restrictions

None.

## ● Example

To display OSPF virtual-link neighbor information:

```
Zxxx0:admin# show ospf virtual_neighbor
```

```
Command: show ospf virtual_neighbor
```

| Transit<br>Area ID | Router ID of<br>Virtual Neighbor | IP Address of<br>Virtual Neighbor | Virtual Neighbor<br>State |
|--------------------|----------------------------------|-----------------------------------|---------------------------|
| -----              | -----                            | -----                             | -----                     |
| 10.1.1.1           | 10.2.3.4                         | 10.48.74.111                      | Exchange                  |

```
Total Entries : 1
```

```
Zxxx0:admin#
```

## 60. OSPFv3 Commands

OSPFv3 is an OSPF protocol for IPv6. It has almost the same functions as OSPF for IPv4 does.

OSPF and OSPFv3 can be used simultaneously.

---

```

enable ospfv3
disable ospfv3
show ospfv3 {[ipif <ipif_name 12> | all]}
config ospfv3 router_id <ipaddr>
create ospfv3 area <area_id> type [normal | stub {stub_summary [enable | disable] | metric
    <value 0-65535>}]
delete ospfv3 area <area_id>
config ospfv3 area <area_id> type [normal | stub {stub_summary [enable | disable] | metric
    <value 0-65535>}]
show ospfv3 area {<area_id>}
create ospfv3 aggregation <area_id> <ipv6networkaddr> advertise [enable | disable]
delete ospfv3 aggregation <area_id> <ipv6networkaddr>
config ospfv3 aggregation <area_id> <ipv6networkaddr> advertise [enable | disable]
show ospfv3 aggregation {<area_id>}
show ospfv3 lsdb {area <area_id> | type [rtrlink | netlink | inter_area_prefix | inter_area_router |
    asexthlink | link_lsa | intra_area_prefix]}
show ospfv3 neighbor {<neighbor_id> ipif <ipif_name 12>}
show ospfv3 virtual_neighbor {<area_id> <neighbor_id>}
config ospfv3 [ipif <ipif_name 12> | all] {area <area_id> | priority <value 0-255> | hello_interval
    <sec 1-65535> | dead_interval <sec 1-65535> | instance <value 0-255> | metric <value 1-
    65535> | state [enable | disable] | passive [enable | disable]}
create ospfv3 virtual_link <area_id> <neighbor_id> {hello_interval <sec 1-65535> | dead_interval
    <sec 1-65535> | instance <value 0-255>}
config ospfv3 virtual_link <area_id> <neighbor_id> {hello_interval <sec 1-65535> | dead_interval
    <sec 1-65535> | instance <value 0-255>}
delete ospfv3 virtual_link <area_id> <neighbor_id>
show ospfv3 virtual_link {<area_id> <neighbor_id>}

```

---

### 60.1. enable ospfv3

#### ● Description

This command is used to enable OSPFv3 on the Switch.

#### ● Format

```
enable ospfv3
```

#### ● Parameters

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To enable OSPFv3:

```
Zxxx0:admin# enable ospfv3
Command: enable ospfv3

Success.

Zxxx0:admin#
```

## 60.2. **disable ospfv3**

---

- **Description**

This command is used to disable OSPFv3 on the Switch.

- **Format**

**disable ospfv3**

- **Parameters**

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To disable OSPFv3:

```
Zxxx0:admin# disable ospfv3
Command: disable ospfv3

Success.

Zxxx0:admin#
```

## 60.3. show ospfv3

---

### ● Description

This command is used to display the OSPFv3 configurations or OSPFv3 interfaces information.

### ● Format

**show ospfv3** {[ipif <ipif\_name 12> | all]}

### ● Parameters

---

|             |                                                                                                                                                                                    |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b> | (Optional) Specifies the OSPFv3 IP interface name used.<br><b>&lt;ipif_name 12&gt;</b><br>Enter the OSPFv3 IP interface name used here. This name can be up to 12 characters long. |
| <b>all</b>  | Specifies that all the OSPFv3 IP interfaces will be used.                                                                                                                          |

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To display OSPFv3 configurations or interfaces information:

```
Zxxx0:admin# show ospfv3
```

```
Command: show ospfv3
```

```
OSPFv3 Router ID: 1.1.1.1
```

```
State           : Enabled
```

```
OSPFv3 Interface Settings
```

| Interface | Area ID | State    | Link<br>Status | Metric | Instance ID |
|-----------|---------|----------|----------------|--------|-------------|
| -----     | -----   | -----    | -----          | -----  | -----       |
| System    | 0.0.0.0 | Disabled | Link Up        | 10     | 0           |

```
Total Entries: 1
```

```
OSPFv3 Area Settings
```

| Area ID | Type   | Stub Import | Summary LSA | Stub Default | Cost  |
|---------|--------|-------------|-------------|--------------|-------|
| -----   | -----  | -----       | -----       | -----        | ----- |
| 0.0.0.0 | Normal | None        |             | None         |       |

```
Total Entries: 1
```

```
Virtual Interface Configuration
```

| Transit<br>Area ID | Virtual<br>Neighbor | Hello<br>Router | Dead<br>Interval | Instance ID | Link<br>Status |
|--------------------|---------------------|-----------------|------------------|-------------|----------------|
| -----              | -----               | -----           | -----            | -----       | -----          |

```
Total Entries: 0
```

```
OSPFv3 Area Aggregation Settings
```

| Area ID | Aggregated<br>Network Address | LSDB<br>Type | Advertise |
|---------|-------------------------------|--------------|-----------|
| -----   | -----                         | -----        | -----     |

```
Total Entries: 0
```

## 60. OSPFv3 Commands

```
Zxxx0:admin# show ospfv3 all
Command: show ospfv3 all

Interface Name: System                               Link Local Address: FE80::201:2FF:FE03:400
(Link Up)
Network Medium Type: BROADCAST                       Metric: 10
Area ID: 0.0.0.0                                     Administrative State: Disabled
Priority: 1                                           DR State: DOWN
DR ID: None                                          Backup DR ID: None
Hello Interval: 10                                  Dead Interval: 40
Transmit Delay: 1                                   Retransmit Time: 5
Passive Mode: Disabled                             Instance ID: 0

Total Entries: 1

Zxxx0:admin# show ospfv3 ipif System
Command: show ospfv3 ipif System

Interface Name: System                               Link Local Address: FE80::201:2FF:FE03:400
(Link Up)
Network Medium Type: BROADCAST                       Metric: 10
Area ID: 0.0.0.0                                     Administrative State: Disabled
Priority: 1                                           DR State: DOWN
DR ID: None                                          Backup DR ID: None
Hello Interval: 10                                  Dead Interval: 40
Transmit Delay: 1                                   Retransmit Time: 5
Passive Mode: Disabled                             Instance ID: 0

Total Entries: 1

Zxxx0:admin#
```

### 60.4. config ospfv3 router\_id

---

#### ● Description

This command is used to configure the OSPFv3 router ID.

#### ● Format

**config ospfv3 router\_id <ipaddr>**

#### ● Parameters

---

**<ipaddr>** Specifies that the user may enter a 32-bit number in the form of an IPv4 address that uniquely identifies the router in the OSPFv3 domain. Setting it to be 0.0.0.0 means auto-selected. The Switch will select the largest IPv4 address among the IP interfaces to be the router ID. The default for the OSPFv3 router ID is 0.0.0.0 (auto-selected). Only by executing this command, can the OSPFv3 router ID be changed.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To set OSPFv3 router ID:

```
Zxxx0:admin# config ospfv3 router_id 1.1.1.1
Command: config ospfv3 router_id 1.1.1.1

Success.

Zxxx0:admin#
```

# 60.5. create ospfv3 area

## ● Description

This command is used to create an OSPFv3 area.

## ● Format

**create ospfv3 area <area\_id> type [normal | stub {stub\_summary [enable | disable] | metric <value 0-65535>}]**

## ● Parameters

|                              |                                                                                                                                                     |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;area_id&gt;</b>       | Specifies the OSPFv3 area's ID. It is a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain. |
| <b>type</b>                  | Specifies the OSPFv3 area mode of operation. There are two types:                                                                                   |
| <b>normal</b>                | Specifies that the OSPFv3 area will be created as a normal area.                                                                                    |
| <b>stub</b>                  | Specifies that the OSPFv3 area will be created as a stub area.                                                                                      |
| <b>stub_summary</b>          | (Optional) Specifies the OSPFv3 stub area to import inter-area prefix LSA advertisements or not.                                                    |
| <b>enable</b>                | Import inter-area prefix LSA into this stub area.                                                                                                   |
| <b>disable</b>               | Do not import inter-area prefix LSA into this stub area.                                                                                            |
| <b>metric</b>                | (Optional) Specifies the default cost of OSPFv3 stub area.                                                                                          |
| <b>&lt;value 0-65535&gt;</b> | Enter the metric value used here. This value must be between 0 and 65535. The default value is 1.                                                   |

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.



## 60. OSPFv3 Commands

### ● Example

To create OSPFv3 areas:

```
Zxxx0:admin# create ospfv3 area 1.1.1.1 type normal
Command: create ospfv3 area 1.1.1.1 type normal

Success.

Zxxx0:admin# create ospfv3 area 2.2.2.2 type stub stub_summary enable
Command: create ospfv3 area 2.2.2.2 type stub stub_summary enable

Success.

Zxxx0:admin#
```

## 60.6. delete ospfv3 area

---

### ● Description

This command is used to delete an OSPFv3 area. The backbone area (0.0.0.0) can not be deleted.

### ● Format

**delete ospfv3 area <area\_id>**

### ● Parameters

---

**<area\_id>**Enter the OSPFv3 area's ID here. It is a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete an OSPFv3 area:

```
Zxxx0:admin# delete ospfv3 area 1.1.1.1
Command: delete ospfv3 area 1.1.1.1

Success.

Zxxx0:admin#
```

## 60.7. config ospfv3 area

---

### ● Description

This command is used to configure an OSPFv3 area. The backbone area (0.0.0.0) can not be configured to be stub area.

### ● Format

**config ospfv3 area <area\_id> type [normal | stub {stub\_summary [enable | disable] | metric <value 0-65535>}]**

### ● Parameters

---

|                              |                                                                                                                                                     |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;area_id&gt;</b>       | Specifies the OSPFv3 area's ID. It is a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain. |
| <b>type</b>                  | Specifies the OSPFv3 area mode of operation. There are two types:                                                                                   |
| <b>normal</b>                | Specifies that the OSPFv3 area will be configured as a normal area.                                                                                 |
| <b>stub</b>                  | Specifies that the OSPFv3 area will be configured as a stub area.                                                                                   |
| <b>stub_summary</b>          | (Optional) Specifies the OSPFv3 stub area to import inter-area prefix LSA advertisements or not.                                                    |
| <b>enable</b>                | Import inter-area prefix LSA into this stub area.                                                                                                   |
| <b>disable</b>               | Do not import inter-area prefix LSA into this stub area.                                                                                            |
| <b>metric</b>                | (Optional) Specifies the default cost of OSPFv3 stub area.                                                                                          |
| <b>&lt;value 0-65535&gt;</b> | Enter the metric value used here. This value must be between 0 and 65535. The default value is 1.                                                   |

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create OSPFv3 areas:

```
Zxxx0:admin# config ospfv3 area 2.2.2.2 type normal
Command: config ospfv3 area 2.2.2.2 type normal

Success.

Zxxx0:admin#
```

## 60.8. show ospfv3 area

---

### ● Description

This command is used to display OSPFv3 area configurations or information.

### ● Format

**show ospfv3 area {<area\_id>}**

### ● Parameters

---

**<area\_id>**(Optional) Specifies the OSPFv3 area's ID. It is a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain.

---

### ● Restrictions

None.

### ● Example

To display OSPFv3 areas:

```
Zxxx0:admin# show ospfv3 area
Command: show ospfv3 area

OSPFv3 Area Settings

Area ID          Type    Stub Import Summary LSA Stub Default Cost
-----
0.0.0.0          Normal None                               None
2.2.2.2          Normal None                               None

Total Entries: 2

Zxxx0:admin# show ospfv3 area 0.0.0.0
Command: show ospfv3 area 0.0.0.0

Area ID: 0.0.0.0          Area Type: Normal

SPF Algorithm Runs For Area 0.0.0.0: 1 time
Number Of LSA In This Area: 2          Checksum Sum: 0x0
Number Of ABR In This Area: 0          Number Of ASBR In This Area: 0

Total Entries: 1

Zxxx0:admin#
```

## 60.9. create ospfv3 aggregation

---

### ● Description

This command is used to create an OSPFv3 area aggregation.

### ● Format

**create ospfv3 aggregation** <area\_id> <ipv6networkaddr> advertise [enable | disable]

### ● Parameters

---

**<area\_id>** Specifies the OSPFv3 area's ID. It is a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain.

---

**<ipv6networkaddr>**

Specifies the IPv6 network address of the aggregation.

---

**advertise** Specifies whether the OSPFv3 ABR will use this aggregation to aggregate the intra-area routes or not.

**enable**

Specifies that the OSPFv3 ABR will use this aggregation to aggregate the intra-area routes when it advertises these routes to another area.

**disable**

Specifies that the OSPFv3 ABR will not use this aggregation to aggregate the intra-area routes when it advertises these routes to another area.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create an OSPFv3 area aggregation:

```
Zxxx0:admin# create ospfv3 aggregation 2.2.2.2 2000::/16 advertise enable
Command: create ospfv3 aggregation 2.2.2.2 2000::/16 advertise enable

Success.

Zxxx0:admin#
```

## 60.10. delete ospfv3 aggregation

---

### ● Description

This command is used to delete an OSPFv3 area aggregation.

### ● Format

**delete ospfv3 aggregation <area\_id> <ipv6networkaddr>**

### ● Parameters

---

**<area\_id>** Specifies the OSPFv3 area's ID. It is a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain.

---

**<ipv6networkaddr>**  
Specifies the IPv6 network address of the aggregation.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete an OSPFv3 area aggregation:

```
Zxxx0:admin# delete ospfv3 aggregation 2.2.2.2 2000::/16
Command: delete ospfv3 aggregation 2.2.2.2 2000::/16

Success.

Zxxx0:admin#
```

## 60.11. config ospfv3 aggregation

---

### ● Description

This command is used to configure an OSPFv3 area aggregation.

### ● Format

**config ospfv3 aggregation <area\_id> <ipv6networkaddr> advertise [enable | disable]**

### ● Parameters

---

**<area\_id>** Specifies the OSPFv3 area's ID. It is a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain.

---

**<ipv6networkaddr>**  
Specifies the IPv6 network address of the aggregation.

---

---

**advertise** Specifies whether the OSPFv3 ABR will use this aggregation to aggregate the intra-area routes or not.

**enable**

Specifies that the OSPFv3 ABR will use this aggregation to aggregate the intra-area routes when it advertises these routes to another area.

**disable**

Specifies that the OSPFv3 ABR will not use this aggregation to aggregate the intra-area routes when it advertises these routes to another area.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure an OSPFv3 area aggregation:

```
Zxxx0:admin# config ospfv3 aggregation 2.2.2.2 2000::/16 advertise disable
Command: config ospfv3 aggregation 2.2.2.2 2000::/16 advertise disable

Success.

Zxxx0:admin#
```

# 60.12. show ospfv3 aggregation

---

## ● Description

This command is used to display OSPFv3 area aggregation configurations.

## ● Format

**show ospfv3 aggregation {<area\_id>}**

## ● Parameters

---

**<area\_id>** (Optional) Specifies the OSPFv3 area's ID. It is a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain.

---

## ● Restrictions

None.

## ● Example

To display OSPFv3 area aggregations:

## 60. OSPFv3 Commands

```
Zxxx0:admin# show ospfv3 aggregation
Command: show ospfv3 aggregation

OSPFv3 Area Aggregation Settings

Area ID          Aggregated          LSDB      Advertise
                  Network Address   Type
-----
1.1.1.1          1000::/16            Summary   Disabled
2.2.2.2          2000::/16            Summary   Disabled

Total Entries: 2

Zxxx0:admin# show ospfv3 aggregation 2.2.2.2
Command: show ospfv3 aggregation 2.2.2.2

OSPFv3 Area Aggregation Settings

Area ID          Aggregated          LSDB      Advertise
                  Network Address   Type
-----
2.2.2.2          2000::/16            Summary   Disabled

Total Entries: 1

Zxxx0:admin#
```

### 60.13. show ospfv3 lsdb

#### ● Description

This command is used to display OSPFv3 Link-State Database.

#### ● Format

**show ospfv3 lsdb {area <area\_id> | type [rtrlink | netlink | inter\_area\_prefix | inter\_area\_router | asexmlink | link\_lsa | intra\_area\_prefix]}**

#### ● Parameters

---

|             |                                                                                                                                               |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>area</b> | (Optional) Specifies that only the LSAs that belong to this area will be displayed.<br><b>&lt;area_id&gt;</b><br>Enter the area ID used here. |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------|

---

---

|                          |                                                                                                                                              |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>type</b>              | (Optional) Specifies that only this type of LSAs will be displayed and detail information for these LSAs will be displayed at the same time. |
| <b>rtrlink</b>           | Specifies that the Router LSA will be displayed.                                                                                             |
| <b>netlink</b>           | Specifies that the Network LSA will be displayed.                                                                                            |
| <b>inter_area_prefix</b> | Specifies that the Inter-Area-Prefix LSA will be displayed.                                                                                  |
| <b>inter_area_router</b> | Specifies that the Inter-Area-Router LSA will be displayed.                                                                                  |
| <b>asextlink</b>         | Specifies that the AS external LSA will be displayed.                                                                                        |
| <b>link_lsa</b>          | Specifies that the Link LSA will be displayed.                                                                                               |
| <b>intra_area_prefix</b> | Specifies that the Intra-Area-Prefix LSA will be displayed.                                                                                  |

---

## ● Restrictions

None.

## ● Example

To display OSPFv3 Link-State Database:



## 60. OSPFv3 Commands

```
Zxxx0:admin# show ospfv3 lsdb
Command: show ospfv3 lsdb

Router LSA (Area 0.0.0.0)
Link State ID  ADV Router      Age  Seq#      Link
0.0.0.0         2.2.2.2        696  0x80000003  0

Link LSA (Interface System)
Link State ID  ADV Router      Age  Seq#      Prefix
0.0.0.1        2.2.2.2        696  0x80000003  1

Intra-Area-Prefix LSA (Area 0.0.0.0)
Link State ID  ADV Router      Age  Seq#      Ref LSA Type
0.0.0.1        2.2.2.2        684  0x80000004  0x2001

Total Entries: 3

Zxxx0:admin# show ospfv3 lsdb type rtrlink
Command: show ospfv3 lsdb type rtrlink

LS Age: 782
LS Type: Router-LSA
Link State ID: 0.0.0.0
Advertising Router: 2.2.2.2
LS Seq Number: 0x80000003
Checksum: 0xED3A
Length: 24
Flags: 0x0: - - - -
Options: 0x13: - R - - E V6

Total Entries: 1

Zxxx0:admin#
```

## 60.14. show ospfv3 neighbor

### ● Description

This command is used to display OSPFv3 neighbor information.

### ● Format

**show ospfv3 neighbor {<neighbor\_id> ipif <ipif\_name 12>}**

### ● Parameters

|                             |                                                                                   |
|-----------------------------|-----------------------------------------------------------------------------------|
| <b>&lt;neighbor_id&gt;</b>  | (Optional) Specifies the ID of the neighbor.                                      |
| <b>ipif</b>                 | (Optional) Specifies the IP interface where the neighbor is built.                |
| <b>&lt;ipif_name 12&gt;</b> | Enter the IP interface name used here. This name can be up to 12 characters long. |

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To display OSPFv3 neighbor:

```
Zxxx0:admin# show ospfv3 neighbor
Command: show ospfv3 neighbor

Router ID of      Interface      Neighbor Neighbor
Neighbor          Name          Priority State
-----
10.10.10.10       System        1         Full
20.20.20.20       ip1           10        Full

Total Entries: 2

Zxxx0:admin# show ospfv3 neighbor 10.10.10.10 ipif System
Command: show ospfv3 neighbor 10.10.10.10 ipif System

Neighbor ID: 10.10.10.10          Interface Name: System
Neighbor Options: 19              Neighbor Priority: 255
Neighbor State: Full              State Changes: 6 times
Interface ID: 1

Zxxx0:admin#
```

## 60.15. show ospfv3 virtual\_neighbor

---

### ● Description

This command is used to display OSPFv3 virtual neighbor information.

### ● Format

**show ospfv3 virtual\_neighbor {<area\_id> <neighbor\_id>}**

### ● Parameters

---

**<area\_id>**

(Optional) Specifies the transit area where the virtual neighbor is built.

---

**<neighbor\_id>**

(Optional) Specifies the ID of the virtual neighbor. If none of the parameters are set, all the virtual neighbors will be displayed.

---

### ● Restrictions

None.

### ● Example

To display OSPFv3 virtual neighbor:

```
Zxxx0:admin# show ospfv3 virtual_neighbor
Command: show ospfv3 virtual_neighbor

Transit      Router ID Of      Virtual Neighbor
Area ID      Virtual Neighbor  State
-----
1.1.1.1      30.30.30.30      Full

Total Entries: 1

Zxxx0:admin# show ospfv3 virtual_neighbor 6.6.6.6 20.20.20.20
Command: show ospfv3 virtual_neighbor 6.6.6.6 20.20.20.20

Transit Area ID: 6.6.6.6
Virtual Neighbor ID: 20.20.20.20
Virtual Neighbor Options: 19
Virtual Neighbor State: Full           State Changes: 9 times

Total Entries: 1

Zxxx0:admin#
```

## 60.16. config ospfv3

---

### ● Description

This command is used to configure an OSPFv3 interface.

### ● Format

**config ospfv3** [**ipif** <ipif\_name 12> | **all**] {**area** <area\_id> | **priority** <value 0-255> | **hello\_interval** <sec 1-65535> | **dead\_interval** <sec 1-65535> | **instance** <value 0-255> | **metric** <value 1-65535> | **state** [enable | disable] | **passive** [enable | disable]}

### ● Parameters

|                       |                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b>           | Specifies the OSPFv3 IP interface name used.<br><ipif_name 12><br>Enter the OSPFv3 IP interface name used here. This name can be up to 12 characters long.                                                                                                                                                                                                                                            |
| <b>all</b>            | Specifies that all the OSPFv3 IP interfaces will be used.                                                                                                                                                                                                                                                                                                                                             |
| <b>area</b>           | (Optional) Specifies a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain.<br><area_id><br>Enter the area ID used here.                                                                                                                                                                                                                       |
| <b>priority</b>       | (Optional) Specifies the priority used in the election of the Designated Router (DR).<br><value 0-255><br>Enter the priority value used here. This value must be between 0 and 255. The default value is 1.                                                                                                                                                                                           |
| <b>hello_interval</b> | (Optional) Specifies to allow the specification of the interval between the transmission of OSPFv3 Hello packets, in seconds. The Hello Interval and Dead Interval should be the same for all routers on the same link.<br><sec 1-65535><br>Enter the hello interval value here. This value must be between 1 and 65535 seconds. The default value is 10 seconds.                                     |
| <b>dead_interval</b>  | (Optional) Specifies to allow the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. The Dead Interval must be evenly divisible by the Hello Interval.<br><sec 1-65535><br>Enter the dead interval value used here. This value must be between 1 and 65535 seconds. The default value is 40 seconds. |
| <b>instance</b>       | (Optional) Specifies the instance ID of the interface.<br><value 0-255><br>Enter the instance ID used here. This value must be between 0 and 255. The default value is 0.                                                                                                                                                                                                                             |
| <b>metric</b>         | (Optional) Specifies the field that allows the entry that is the representative of the OSPFv3 cost of reaching the selected OSPFv3 interface.<br><value 1-65535><br>Enter the metric value used here. This value must be between 1 and 65535. The default value is 1.                                                                                                                                 |

## 60. OSPFv3 Commands

---

|                |                                                                         |
|----------------|-------------------------------------------------------------------------|
| <b>state</b>   | (Optional) Specifies to enable or disable this interface to run OSPFv3. |
| <b>enable</b>  | Specifies that the OSPFv3 state, for this interface, will be enabled.   |
| <b>disable</b> | Specifies that the OSPFv3 state, for this interface, will be disabled.  |

---

|                |                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>passive</b> | (Optional) Specifies that the user may select Active or Passive for this OSPFv3 interface. Active interfaces actively advertise OSPFv3 to routers on other Intranets that are not part of this specific OSPFv3 group. Passive interfaces will not advertise to any other routers than those within its OSPFv3 intranet. When this field is disabled, it denotes an active interface. |
| <b>enable</b>  | Specifies that the passive state will be enabled.                                                                                                                                                                                                                                                                                                                                    |
| <b>disable</b> | Specifies that the passive state will be disabled.                                                                                                                                                                                                                                                                                                                                   |

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure an OSPFv3 interface:

```
Zxxx0:admin# config ospfv3 ipif System area 0.0.0.0 priority 100 hello_interval 20
dead_interval 60 instance 1 metric 20 state enable passive disable
Command: config ospfv3 ipif System area 0.0.0.0 priority 100 hello_interval 20
dead_interval 60 instance 1 metric 20 state enable passive disable

Success.

Zxxx0:admin#
```

## 60.17. create ospfv3 virtual\_link

---

### ● Description

This command is used to create an OSPFv3 virtual link.

### ● Format

**create ospfv3 virtual\_link** <area\_id> <neighbor\_id> {hello\_interval <sec 1-65535> | dead\_interval <sec 1-65535> | instance <value 0-255>}

### ● Parameters

---

**<area\_id>** Specifies a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain. This area is the transit area where the virtual link is built.

---

**<neighbor\_id>**  
Specifies a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 virtual neighbor in the OSPFv3 domain.

---

**hello\_interval**  
(Optional) Specifies to allow the specification of the interval between the transmission of OSPFv3 Hello packets. The Hello Interval and Dead Interval should be the same for all routers on the same link.

**<sec 1-65535>**

Enter the hello interval value used here. This value must be between 1 and 65535 seconds. The default value is 10 seconds.

---

**dead\_interval**  
(Optional) Specifies to allow the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. The Dead Interval must be evenly divisible by the Hello Interval

**<sec 1-65535>**

Enter the dead interval value used here. This value must be between 1 and 65535 seconds. The default value is 60 seconds.

---

**instance** (Optional) Specifies the instance ID on the virtual link.

**<value 0-255>**

Enter the instance ID value here. This value must be between 0 and 255. The default value is 0.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create OSPFv3 virtual link:

```
Zxxx0:admin# create ospfv3 virtual_link 1.1.1.1 60.60.60.60
Command: create ospfv3 virtual_link 1.1.1.1 60.60.60.60

Success.

Zxxx0:admin#
```

### 60.18. config ospfv3 virtual\_link

---

#### ● Description

This command is used to configure an OSPFv3 virtual link.

#### ● Format

**config ospfv3 virtual\_link <area\_id> <neighbor\_id> {hello\_interval <sec 1-65535> | dead\_interval <sec 1-65535> | instance <value 0-255>}**

#### ● Parameters

---

**<area\_id>** Specifies a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain. This area is the transit area where the virtual link is built.

---

**<neighbor\_id>**  
Specifies a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 virtual neighbor in the OSPFv3 domain.

---

**hello\_interval**  
(Optional) Specifies to allow the specification of the interval between the transmission of OSPFv3 Hello packets. The Hello Interval and Dead Interval should be the same for all routers on the same link.  
**<sec 1-65535>**  
Enter the hello interval value used here. This value must be between 1 and 65535 seconds. The default value is 10 seconds.

---

**dead\_interval**  
(Optional) Specifies to allow the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. The Dead Interval must be evenly divisible by the Hello Interval  
**<sec 1-65535>**  
Enter the dead interval value used here. This value must be between 1 and 65535 seconds. The default value is 60 seconds.

---

**instance** (Optional) Specifies the instance ID on the virtual link.  
**<value 0-255>**  
Enter the instance ID value here. This value must be between 0 and 255. The default value is 0.

---

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure an OSPFv3 virtual link:

```
Zxxx0:admin# config ospfv3 virtual_link 1.1.1.1 60.60.60.60 hello_interval 20
dead_interval 80 instance 1
Command: config ospfv3 virtual_link 1.1.1.1 60.60.60.60 hello_interval 20
dead_interval 80 instance 1

Success.

Zxxx0:admin#
```

## 60.19. delete ospfv3 virtual\_link

### ● Description

This command is used to delete an OSPFv3 virtual link.

### ● Format

**delete ospfv3 virtual\_link <area\_id> <neighbor\_id>**

### ● Parameters

---

**<area\_id>** Specifies a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain. This area is the transit area where the virtual link is built.

---

**<neighbor\_id>**  
Specifies a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 virtual neighbor in the OSPFv3 domain.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete an OSPFv3 virtual link:

```
Zxxx0:admin# delete ospfv3 virtual_link 1.1.1.1 60.60.60.60
Command: delete ospfv3 virtual_link 1.1.1.1 60.60.60.60

Success.

Zxxx0:admin#
```



## 60.20. show ospfv3 virtual\_link

---

### ● Description

This command is used to display OSPFv3 virtual link configurations. If no parameters are set, all the virtual links will be displayed.

### ● Format

**show ospfv3 virtual\_link {<area\_id> <neighbor\_id>}**

### ● Parameters

---

**<area\_id>**(Optional) Specifies a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain. This area is the transit area where the virtual link is built.

---

**<neighbor\_id>**  
(Optional) Specifies a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 virtual neighbor in the OSPFv3 domain.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To display an OSPFv3 virtual link:

```
Zxxx0:admin# show ospfv3 virtual_link
```

```
Command: show ospfv3 virtual_link
```

Virtual Interface Configuration

| Transit<br>Area ID | Virtual<br>Neighbor Router | Hello<br>Interval | Dead<br>Interval | Instance ID | Link<br>Status |
|--------------------|----------------------------|-------------------|------------------|-------------|----------------|
| 1.1.1.1            | 60.60.60.60                | 10                | 60               | 0           | DOWN           |
| 1.1.1.1            | 70.70.70.70                | 10                | 60               | 0           | DOWN           |

Total Entries: 2

```
Zxxx0:admin# show ospfv3 virtual_link 1.1.1.1 60.60.60.60
```

```
Command: show ospfv3 virtual_link 1.1.1.1 60.60.60.60
```

|                           |                                         |
|---------------------------|-----------------------------------------|
| Transit Area ID: 1.1.1.1  | Virtual Neighbor Router ID: 60.60.60.60 |
| Hello Interval: 10        | Dead Interval: 60                       |
| Transmit Delay: 1         | Retransmit Time: 5                      |
| Instance ID: 0            |                                         |
| Virtual Link Status: DOWN |                                         |

Total Entries: 1

```
Zxxx0:admin#
```

## 61. Packet Storm Commands

A packet storm is a phenomenon where packets overflow on the network. It occurs when a large amount of broadcast or multicast data is sent simultaneously or a network device fails. A packet storm decreases network efficiency, interfering with normal communications. This Switching Hub allows you to monitor and control a packet storm on a specified port with the following methods.

- drop: Discard exceeded packets if the number of packets exceeds a set threshold.
- shutdown: Stop transferring packets if the number of packets exceeds a set threshold. If a packet storm does not stop within a specified time, the port is kept isolated until it is recovered manually.

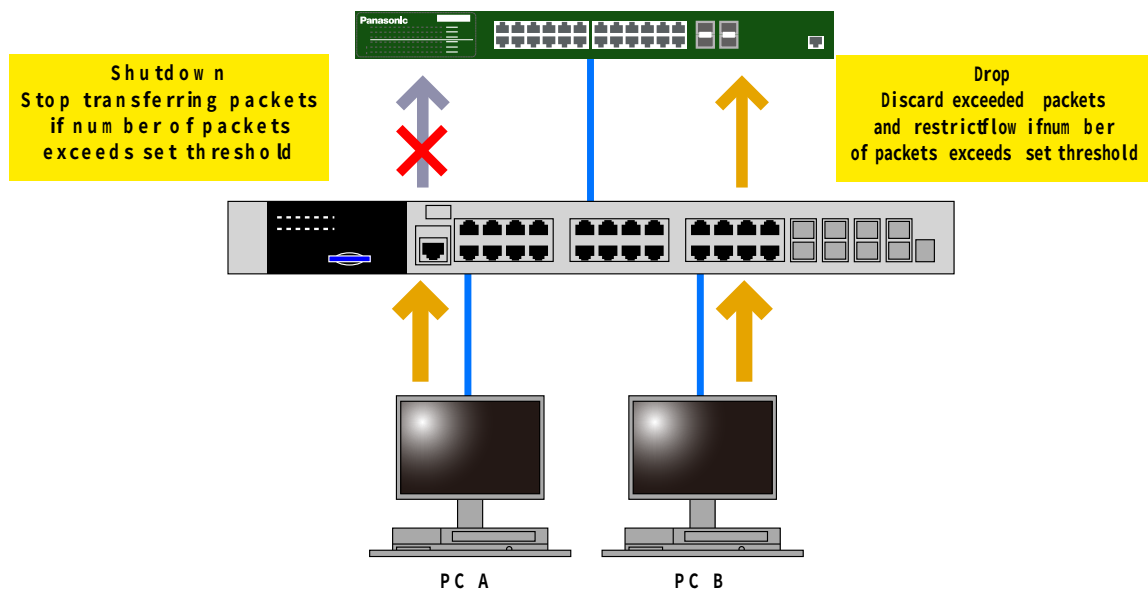


Figure 61-1 Packet storm control

```
config traffic control [<portlist> | all] {broadcast [enable | disable] | multicast [enable | disable] |
    unicast [enable | disable] | action [drop | shutdown] | threshold <value 0-255000> |
    countdown [<min 0> | <min 3-30> | disable] | time_interval <sec 5-600>}(1)
config traffic control auto_recover_time [<min 0> | <min 1-65535>]
config traffic control log state [enable | disable]
config traffic trap [none | storm_occurred | storm_cleared | both]
show traffic control {<portlist>}
```

## 61.1. config traffic control

---

### ● Description

This command is used to configure broadcast/multicast/unicast storm control. The broadcast storm control commands provide a hardware storm control mechanism only. These packet storm control commands include hardware and software mechanisms to provide shutdown, recovery, and trap notification functions.

### ● Format

**config traffic control** [<portlist> | all] {broadcast [enable | disable] | multicast [enable | disable] | unicast [enable | disable] | action [drop | shutdown] | threshold <value 0-255000> | countdown [<min 0> | <min 3-30> | disable] | time\_interval <sec 5-600>}(1)

### ● Parameters

|                         |                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;portlist&gt;</b> | Specify a range of ports to be configured.                                                                                                                                                                                                                                                                                                            |
| <b>all</b>              | Specify all ports are to be configured.                                                                                                                                                                                                                                                                                                               |
| <b>broadcast</b>        | Specify the broadcast storm status.                                                                                                                                                                                                                                                                                                                   |
| <b>enable</b>           | Enable broadcast storm control.                                                                                                                                                                                                                                                                                                                       |
| <b>disable</b>          | Disable broadcast storm control.                                                                                                                                                                                                                                                                                                                      |
| <b>multicast</b>        | Specify the multicast storm status.                                                                                                                                                                                                                                                                                                                   |
| <b>enable</b>           | Enable multicast storm control.                                                                                                                                                                                                                                                                                                                       |
| <b>disable</b>          | Disable multicast storm control.                                                                                                                                                                                                                                                                                                                      |
| <b>unicast</b>          | Specify the unknown unicast packet storm status.                                                                                                                                                                                                                                                                                                      |
| <b>enable</b>           | Enable unknown unicast packet storm control (only support drop action).                                                                                                                                                                                                                                                                               |
| <b>disable</b>          | Disable unknown unicast packet storm control.                                                                                                                                                                                                                                                                                                         |
| <b>action</b>           | Specify the action.                                                                                                                                                                                                                                                                                                                                   |
| <b>drop</b>             | Drop the packet by hardware when it is detected threshold.                                                                                                                                                                                                                                                                                            |
| <b>shutdown</b>         | Shutdown the port by software when it is detected threshold. If this is chosen, threshold, countdown, and time_interval also need to be configured.                                                                                                                                                                                                   |
| <b>threshold</b>        | The upper threshold at which the specified storm control will turn on.<br>This is the number of broadcast/multicast/unknown unicast packets per second received by the Switching Hub that will trigger the storm traffic control measure. It must be an unsigned integer.<br><b>&lt;value 0-255000&gt;</b><br>Specify the value between 0 and 255000. |

## 61. Packet Storm Commands

---

### countdown

The timer for shutdown mode. When a port enters a shutdown RX state, and if this times out, the port will shut down the port forever. The default is 0 minutes.

**<min 0>**

Zero is the disable forever state.

**<min 3-30>**

Enter a value between 3 and 30 minutes.

### disable

Specifies that when the action is shutdown and the countdown is disabled, when the Switch detects a storm, it will shutdown the port directly.

---

### time\_interval

The sampling interval of received packet counts. This parameter is meaningless for dropping packets is selected as action.

**<value 5-600>**

Specify the value between 5 and 600.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure traffic control and state:

```
Zxxx0:admin#config traffic control 1-10 broadcast enable action shutdown threshold 640 time_interval 10
Command: config traffic control 1-10 broadcast enable action shutdown threshold 640 time_interval 10

Success.

Zxxx0:admin#
```

## 61.2. config traffic control auto\_recover\_time

## ● Description

This command is used to configure the traffic auto recover time that allowed for a port to recover from shutdown forever status. The time allowed for auto recovery from shutdown for a port. The default value is 0, so no auto recovery is possible; the port remains in shutdown forever mode. This requires manual entry of the CLI command "**config ports [ <portlist> | all ] state enable**" to return the port to a forwarding state. The default value is 0, which means disable auto recover mode, shutdown forever.

## ● Format

**config traffic control auto\_recover\_time [ <min 0> | <min 1-65535> ]**

## ● Parameters

---

**<min 0>** Enter the automatic recovery time used here. This value will specifies the time to be 0 otherwise known as 'no recovery mode'.

---

**<min 1-65535>**

Enter the automatic recovery time used here. This value must be between 1 and 65535 minutes.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure the auto recover time to 5 minutes:

```
Zxxx0:admin# config traffic control auto_recover_time 5
Command: config traffic control auto_recover_time 5

Success.

Zxxx0:admin#
```

# 61.3. config traffic control log state

---

## ● Description

This command is used to configure the traffic control log state. When the log state is enabled, traffic control states are logged when a storm occurs and when a storm is cleared. If the log state is disabled, traffic control events are not logged.

The log state is only applicable for shutdown mode. Since shutdown mode only support broadcast and multicast storm control, doesn't support unicast storm control. The log only generate for broadcast and multicast storm control.

## ● Format

**config traffic control log state [enable | disable]**

## ● Parameters

---

|                |                                                                          |
|----------------|--------------------------------------------------------------------------|
| <b>state</b>   | Specifies the traffic control log state.                                 |
| <b>enable</b>  | Specifies that traffic control state will be logged when a storm occurs. |
| <b>disable</b> | Specifies that the traffic control state will be disabled.               |

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## 61. Packet Storm Commands

### ● Example

To configure the traffic log state on the Switch:

```
Zxxx0:admin# config traffic control log state enable
Command: config traffic control log state enable

Success.

Zxxx0:admin#
```

## 61.4. config traffic trap

### ● Description

This command is used to configure whether storm control notification will be generated or not while traffic storm events are detected by a SW traffic storm control mechanism.

#### NOTE

A traffic control trap is active only when the control action is configured as shutdown. If the control action is drop there will no traps issue while storm event is detected.

### ● Format

**config traffic trap [none | storm\_occurred | storm\_cleared | both]**

### ● Parameters

|             |                                                                                   |
|-------------|-----------------------------------------------------------------------------------|
| <b>none</b> | none - No notification will be generated when storm event is detected or cleared. |
|-------------|-----------------------------------------------------------------------------------|

|                       |
|-----------------------|
| <b>storm_occurred</b> |
|-----------------------|

|                                                                  |
|------------------------------------------------------------------|
| A notification will be generated when a storm event is detected. |
|------------------------------------------------------------------|

|                      |
|----------------------|
| <b>storm_cleared</b> |
|----------------------|

|                                                                 |
|-----------------------------------------------------------------|
| A notification will be generated when a storm event is cleared. |
|-----------------------------------------------------------------|

|             |                                                                                   |
|-------------|-----------------------------------------------------------------------------------|
| <b>both</b> | A notification will be generated both when a storm event is detected and cleared. |
|-------------|-----------------------------------------------------------------------------------|

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure a traffic control trap:

```
Zxxx0:admin#config traffic trap both
Command: config traffic trap both

Success.

Zxxx0:admin#
```

## 61.5. show traffic control

### ● Description

This command is used to display current traffic control settings.

### ● Format

show traffic control {<portlist>}

### ● Parameters

---

<portlist>(Optional) Specify a range of ports to be shown.

---



---

**NOTE** If no parameter is specified, the system will display all port packet storm control configurations.

---

### ● Restrictions

None.

### ● Example

To display the packet storm control setting for ports 1 to 3:

```
Zxxx0:admin#show traffic control 1-3
Command: show traffic control 1-3

Traffic Control Trap           : [None]
Traffic Control Log            : Enabled
Traffic Control Auto Recover Time: 0 Minutes

Port Thres  Broadcast Multicast Unicast  Action  Count  Time  Shutdown
  hold  Storm   Storm   Storm              down  down  Interval Forever
-----
1   640   Enabled  Disabled Disabled shutdown 0    10
2   640   Enabled  Disabled Disabled shutdown 0    10
3   640   Enabled  Disabled Disabled shutdown 0    10

Zxxx0:admin#
```



## 62. Protocol Independent Multicast (PIM) Commands

Sending data simultaneously to multiple destinations is called "multicast" and used for music and video distribution.

PIM (Protocol Independent Multicast routing) is one of multicast routing protocols. It uses unicast routing such as existing RIP or OSPF to control multicast route selection.

This Switching Hub supports the following four PIM types.

### ● PIM-DM (Dense Mode)

It identifies adjacent routers by flooding multicast packets in a VLAN. This is effective when clients are packed in one VLAN.

### ● PIM-SM (Sparse Mode)

It uses a distribution tree combining source and shared trees. A router that is a contact between source and shared trees is called RP (Rendezvous Point). It can learn client locations and distribute multicast packets only to routes on which clients exist.

RP is normally configured manually but can also be configured automatically using a BSR (Bootstrap Router).

### ● PIM-SM-DM (Sparse-Dense Mode)

It is a distribution method combining PIM-DM and PIM-SM. Use PIM-SM if the RP address is configured and use PIM-DM if the RP address is unknown in a multicast group.

### ● PIM-SSM (PIM Source Specific multicast)

It is an advanced PIM-SM function. This provides more efficient distribution by bypassing RP when distributing to IGMPv3 (INCLUDE mode) clients.

---

```

config pim [[ipif <ipif_name 12> | all] {hello <sec 1-18724> | jp_interval <sec 1-18724> | state
    [enable | disable] | mode [dm | sm | sm-dm] | dr_priority <uint 0-4294967294>} |
    register_probe_time <value 1-127> | register_suppression_time <value 3-255>]
enable pim
disable pim
show pim neighbor {ipif <ipif_name 12> | ipaddress <network_address>}
show pim {ipif <ipif_name 12>}
config pim cbsr [ipif <ipif_name 12> {priority [-1 | <value 0-255>]} | hash_masklen <value 0-32> |
    bootstrap_period <value 1-255>]
show pim cbsr {ipif <ipif_name 12>}
  
```

---

---

```

config pim crp {holdtime <value 0-255> | priority <value 0-255> | wildcard_prefix_cnt [0 | 1]}
create pim crp group <network_address> rp <ipif_name 12>
delete pim crp group <network_address>
show pim crp
config pim last_hop_spt_switchover [never | immediately]
show pim ipmroute
create pim static_rp group <network_address> rp <ipaddr>
delete pim static_rp group <network_address>
show pim static_rp
show pim rpset
create pim register_checksum_include_data rp_address <ipaddr>
delete pim register_checksum_include_data rp_address <ipaddr>
show pim register_checksum_include_data_rp_list
config pim-ssm {state [enable | disable] | group_range [default | <network_address>]}
show pim-ssm

```

---

## 62.1. config pim

---

### ● Description

This command is used to configure the PIM settings.

### ● Format

```

config pim [[ipif <ipif_name 12> | all] {hello <sec 1-18724> | jp_interval <sec 1-18724> |
state [enable | disable] | mode [dm | sm | sm-dm] | dr_priority <uint 0-4294967294>} |
register_probe_time <value 1-127> | register_suppression_time <value 3-255>]

```

### ● Parameters

---

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b>        | Specifies the IP interface name.<br><b>&lt;ipif_name 12&gt;</b><br>Enter the IP interface name used here. This name can be up to 12 characters long.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>all</b>         | Specifies that all the IP interfaces will be used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>hello</b>       | (Optional) Specifies the time between issuing hello packets to find neighboring routers.<br><b>&lt;sec 1-18724&gt;</b><br>Enter the hello time value here. This value must be between 1 and 18724 seconds.<br>The default value is 30 seconds.                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>jp_interval</b> | (Optional) Specifies the interval between transmitting (flooding to all interfaces) multicast messages to downstream routers, and automatically 'pruning' a branch from the multicast delivery tree. This interval also determines the time interval the router uses to automatically remove prune information from a branch of a multicast delivery tree and begin to flood multicast messages to all branches of that delivery tree. These two actions are equivalent. The default is 60 seconds.<br><b>&lt;sec 1-18724&gt;</b><br>Enter the join/prune interval value here. This value must be between 1 and 18724 seconds. |

---

## 62. Protocol Independent Multicast (PIM) Commands

|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>state</b>                     | (Optional) Specifies to allow the PIM function to be disabled or enabled for the above IP interface. The default is disabled.<br><b>enable</b><br>Specifies that the PIM function will be enabled.<br><b>disable</b><br>Specifies that the PIM function will be disabled.                                                                                                                                           |
| <b>mode</b>                      | (Optional) Specifies the multicast protocol mode used. - dense mode or sparse mode, or sm-dm mode. The default value is dense mode.<br><b>dm</b> Specifies that the multicast protocol mode will be set to dense mode.<br><b>sm</b> Specifies that the multicast protocol mode will be set to sparse mode.<br><b>sm-dm</b><br>Specifies that the multicast protocol mode will be set to both dense and sparse mode. |
| <b>dr_priority</b>               | (Optional) Specifies the priority for DR election.<br><uint 0-4294967294><br>Enter the DR priority value used here. This value must be between 0 and 4294967294.                                                                                                                                                                                                                                                    |
| <b>register_probe_time</b>       | Specifies the register probe time. The default value is 5 sec.<br><value 1-127><br>Enter the register probe time value here. This value must be between 1 and 127.                                                                                                                                                                                                                                                  |
| <b>register_suppression_time</b> | Specifies the register suppression time. The default value is 60 sec.<br><value 3-255><br>Enter the register suppression time value here. This value must be between 3 and 255.                                                                                                                                                                                                                                     |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure PIM configurations of IP interface System:

```
Zxxx0:admin# config pim ipif System hello 35 jp_interval 70 state enable
Command: config pim ipif System hello 35 jp_interval 70 state enable

Success.

Zxxx0:admin#
```

## 62.2. enable pim

---

- **Description**

This command is used to enable PIM on the Switching Hub.

- **Format**

enable pim

- **Parameters**

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To enable PIM:

```
Zxxx0:admin# enable pim
Command: enable pim

Success.

Zxxx0:admin#
```

## 62.3. disable pim

---

- **Description**

This command is used to disable PIM on the Switching Hub.

- **Format**

disable pim

- **Parameters**

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

## 62. Protocol Independent Multicast (PIM) Commands

### ● Example

To disable PIM:

```
Zxxx0:admin# disable pim
Command: disable pim

Success.

Zxxx0:admin#
```

## 62.4. show pim neighbor

---

### ● Description

This command is used to display the current PIM neighbor router table.

### ● Format

**show pim neighbor {ipif <ipif\_name 12> | ipaddress <network\_address>}**

### ● Parameters

---

|             |                                                                                                                                                                                                                                            |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b> | (Optional) Specifies the name of the IP interface for which you want to display the current PIM neighbor router table.<br><b>&lt;ipif_name 12&gt;</b><br>Enter the IP interface name used here. This name can be up to 12 characters long. |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

|                  |                                                                                                                                                      |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipaddress</b> | (Optional) Specifies the IP address and netmask of the destination.<br><b>&lt;network_address&gt;</b><br>Enter the destination IP address used here. |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|

---

If no parameter is specified, the system will display all the PIM neighbor addresses in the table.

### ● Restrictions

None.

### ● Example

To display PIM neighbor address table:

```

Zxxx0:admin# show pim neighbor
Command: show pim neighbor

PIM Neighbor Address Table
Interface Name   Neighbor Address   Expire Time
-----
System          10.48.74.122      5

Total Entries : 1

Zxxx0:admin#

```

## 62.5. show pim

---

### ● Description

This command is used to display the current PIM configuration.

### ● Format

**show pim {ipif <ipif\_name 12>}**

### ● Parameters

---

|             |                                                                                                                         |
|-------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b> | (Optional) Specifies the name of the IP interface used to display the PIM configuration.<br><b>&lt;ipif_name 12&gt;</b> |
|-------------|-------------------------------------------------------------------------------------------------------------------------|

---

Enter the IP interface name used here. This name can be up to 12 characters long.

---

If no parameter is specified, the system will display all the PIM configurations of all IP interfaces.

### ● Restrictions

None.

### ● Example

To display PIM configurations of IP interface System:

## 62. Protocol Independent Multicast (PIM) Commands

```
Zxxx0:admin# show pim
```

```
Command: show pim
```

```
PIM Global State      : Enabled
```

```
Last Hop SPT Switchover : Never
```

```
Register Probe Time    : 5
```

```
Register Suppression Time : 60
```

```
PIM Interface Table
```

| Interface | IP Address     | Designated<br>Router | Hello<br>Interval | J/P<br>Interval | Mode | State   |
|-----------|----------------|----------------------|-------------------|-----------------|------|---------|
| System    | 10.90.90.101/8 | 10.90.90.101         | 35                | 70              | DM   | Enabled |

```
Total Entries : 1
```

```
Zxxx0:admin#
```

## 62.6. config pim cbsr

---

### ● Description

This command is used to set the priority, hash mask length, and bootstrap period of the candidate bootstrap (C-BSR) router per interface.

### ● Format

**config pim cbsr** [**ipif** <ipif\_name 12> {**priority** [-1 | <value 0-255>]} | **hash\_masklen** <value 0-32> | **bootstrap\_period** <value 1-255>]

### ● Parameters

|                         |                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b>             | Specifies the IP interface used for this configuration.<br><ipif_name 12><br>Enter the IP interface name used here. This name can be up to 12 characters long.                                                                                                                                                                                                                |
| <b>priority</b>         | (Optional) Specifies to set the C-BSR priority. The lower value indicates lower priority. The default value is -1. Note that only one interface can be the C-BSR in one device.<br>-1 Specifies that the interface will be disable to be the BSR.<br><value 0-255><br>Enter the C-BSR priority value used here. This value must be between 0 and 255.                         |
| <b>hash_masklen</b>     | Enter a hash mask length, which will be used with the IP address of the candidate RP and the multicast group address, to calculate the hash algorithm used by the router to determine which CRP on the PIM-SM enabled network will be the RP.<br><value 0-32><br>Enter the hash mask lenght value here. This value must be between 0 and 32. The default value is 30 seconds. |
| <b>bootstrap_period</b> | Specifies the interval between originating Bootstrap message.<br><value 1-255><br>Enter the bootstrap period value used here. This value must be between 1 and 255. The default value is 60 seconds.                                                                                                                                                                          |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the C-BSR for the System interface :

```
Zxxx0:admin# config pim cbsr ipif System priority 255 hash_mask length 30
bootstrap_period 60
Command: config pim cbsr ipif System priority 255 hash_mask length 30
bootstrap_period 60

Success.

Zxxx0:admin#
```



## 62.7. show pim cbsr

---

### ● Description

This command is used to list the candidate bootstrap router related information.

### ● Format

show pim cbsr {ipif <ipif\_name 12>}

### ● Parameters

---

|      |                                                                           |
|------|---------------------------------------------------------------------------|
| ipif | Specifies the IP interface used for this configuration.<br><ipif_name 12> |
|------|---------------------------------------------------------------------------|

---

Enter the IP interface name used here. This name can be up to 12 characters long.  
If no parameter is specified, the system will display all C-BSR configurations.

---

### ● Restrictions

None.

### ● Example

To display the C-BSR settings:

```
Zxxx0:admin# show pim cbsr
Command: show pim cbsr

PIM Candidate-BSR Table

C-BSR Hash Mask Len      : 30
C-BSR Bootstrap Period   : 60

Interface    IP Address      Priority
-----
System       11.52.33.3/8    -1 (disabled)

Total Entries: 1

Zxxx0:admin#
```

## 62.8. config pim crp

---

### ● Description

This command is used to set the candidate rendezvous point (RP) related parameters.

### ● Format

**config pim crp {holdtime <value 0-255> | priority <value 0-255> | wildcard\_prefix\_cnt [0 | 1]}**

### ● Parameters

---

**holdtime**(Optional) This field is used to set the time Candidate RP (CRP) advertisements are valid on the PIM-SM enabled network. If CRP advertisements are not received by the BSR within this time frame, the CRP is removed from the list of candidates. An entry of 0 will send out one advertisement that states to the BSR that it should be immediately removed from CRP status on the PIM-SM network.

**<value 0-255>**

Enter the hold time for the RP here. This value must be between 0 and 255. The default value is 150 seconds.

---

**priority** (Optional) Specifies the priority used for RP election. This priority value will be included in the router's CRP advertisements. A lower value means a higher priority, yet, if there is a tie for the highest priority, the router having the higher IP address will become the RP.

**<value 0-255>**

Enter the priority value used here. This value must be between 0 and 255. The default value is 192.

---

**wildcard\_prefix\_cnt**

(Optional) Specifies the Prefix Count value of the wildcard address (224.0.0.0/24) to be chosen. The default value is 0.

**0** Specifies that the wildcard prefix count value will be set to 0.

**1** Specifies that the wildcard prefix count value will be set to 1.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the candidate rendezvous point (RP) holdtime, priority and wildcard prefix count:

```
Zxxx0:admin# config pim crp holdtime 150 priority 192 wildcard_prefix_cnt 0
Command: config pim crp holdtime 150 priority 192 wildcard_prefix_cnt 0

Success.

Zxxx0:admin#
```

## 62.9. create pim crp group

---

### ● Description

This command is used to add a multicast group range into a C-RP serve list for PIM-SM.

### ● Format

**create pim crp group <network\_address> rp <ipif\_name 12>**

### ● Parameters

|              |                                                                                                                                                                                                         |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>group</b> | Specifies the multicast group address for this Switch to become a Candidate RP. This address must be a class D address.<br><b>&lt;network_address&gt;</b><br>Enter the group network address used here. |
| <b>rp</b>    | Specifies that the interface will act as C-RP for the group.<br><b>&lt;ipif_name 12&gt;</b><br>Enter the IP interface name used here. This name can be up to 12 characters long.                        |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To add a multicast group range into a C-RP server list:

```
Zxxx0:admin# create pim crp group 224.1.2.3/32 rp System
Command: create pim crp group 224.1.2.3/32 rp System

Success.

Zxxx0:admin#
```

## 62.10. delete pim crp group

---

### ● Description

This command is used to delete a multicast group range from the C-RP server list.

### ● Format

delete pim crp group <network\_address>

### ● Parameters

---

|              |                                                                                                                                                                                                                            |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>group</b> | Specifies the multicast group address for this Switching Hub to be removed from being a Candidate RP. This address must be a class D address.<br><network_address><br>Enter the multicast group network address used here. |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete a multicast group range from the C-RP server list:

```
Zxxx0:admin# delete pim crp group 224.1.2.3/32
Command: delete pim crp group 224.1.2.3/32

Success.

Zxxx0:admin#
```

## 62.11. show pim crp

---

### ● Description

This command is used to list all the candidate rendezvous point (C-RP) related information.

### ● Format

show pim crp

### ● Parameters

None.

## 62. Protocol Independent Multicast (PIM) Commands

### ● Restrictions

None.

### ● Example

To list all the candidate rendezvous point (C-RP) related information:

```
Zxxx0:admin# show pim crp
Command: show pim crp

PIM Candidate-RP Table

C-RP Holdtime           : 150
C-RP Priority            : 192
C-RP wildcard prefix count : 0

Group                Interface
-----
224.0.0.0/4          System

Total Entries: 1

Zxxx0:admin#
```

## **62.12. config pim last\_hop\_spt\_switchover**

### ● Description

This command is used by the last hop router to decide whether to receive the multicast data from the shared tree or switch over to the shortest path tree. When the switchover mode is set to be never, the last hop router will always receive the multicast data from the shared tree. When the mode is set to immediately, the last hop router will always receive the multicast data from the shortest path tree.

### ● Format

**config pim last\_hop\_spt\_switchover [never | immediately]**

### ● Parameters

|                    |                                                                                       |
|--------------------|---------------------------------------------------------------------------------------|
| <b>never</b>       | Specifies that the router will always receive multicast data from the shared tree.    |
| <b>immediately</b> | Specifies that the router will always receive multicast data from shortest path tree. |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

Set the SPT-switchover mode to never:

```
Zxxx0:admin# config pim last_hop_spt_switchover never
Command: config pim last_hop_spt_switchover never

Success.

Zxxx0:admin#
```

## 62.13. show pim ipmroute

---

### ● Description

This command is used to list all the entries of multicast routing, includes (\*,G), (S,G) and (S,G,rpt).

### ● Format

show pim ipmroute

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To list all the entries of multicast routing:

## 62. Protocol Independent Multicast (PIM) Commands

```
Zxxx0:admin# show pim ipmroute
Command: show pim ipmroute

PIM IP Multicast Route Table

UA = Upstream AssertTimer
AM = Assert Metric
AMPref = Assert MetricPref
ARB = Assert RPTBit

Group Address      Source Address      UA   AM   AMPref ARB   Flag Type      Mode
-----
225.0.0.0          12.90.90.90/32      0    0    0       0    RPT  (*.G)    ASM
225.0.0.1          12.90.90.90/32      0    0    0       0    RPT  (*.G)    ASM
225.0.0.5          12.90.90.90/32      0    0    0       0    RPT  (*.G)    ASM
225.7.7.5          12.90.90.90/32      0    0    0       0    RPT  (*.G)    ASM
226.0.0.0          12.90.90.90/32      0    0    0       0    RPT  (*.G)    ASM
227.0.0.3          12.90.90.90/32      0    0    0       0    RPT  (*.G)    ASM
232.0.0.0          12.90.90.114/32     0    0    0       0    SPT  (S.G)    SSM
239.255.255.250    12.90.90.90/32      0    0    0       0    RPT  (*.G)    ASM

Total Entries: 8

Zxxx0:admin#
```

### 62.14. create pim static\_rp group

#### ● Description

This command is used to create a static RP.

#### ● Format

**create pim static\_rp group <network\_address> rp <ipaddr>**

#### ● Parameters

|              |                                                                                                                                                       |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>group</b> | Specifies to assign the multicast group address for this static RP.<br><b>&lt;network_address&gt;</b><br>Enter the multicast group address used here. |
| <b>rp</b>    | Specifies the IP address used by this static RP.<br><b>&lt;ipaddr&gt;</b><br>Enter the IP address used here.                                          |

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create a static RP:

```
Zxxx0:admin# create pim static_rp group 239.1.1.0/24 rp 10.52.33.18
Command: create pim static_rp group 239.1.1.0/24 rp 10.52.33.18

Success.

Zxxx0:admin#
```

## 62.15. delete pim static\_rp group

---

### ● Description

This command is used to delete a static RP.

### ● Format

**delete pim static\_rp group <network\_address>**

### ● Parameters

---

|              |                                                                                                                                                               |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>group</b> | Specifies the multicast group address that will removed from the static RP.<br><b>&lt;network_address&gt;</b><br>Enter the multicast group address used here. |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete a static RP:

```
Zxxx0:admin# delete pim static_rp group 224.1.2.0/24
Command: delete pim static_rp group 224.1.2.0/24

Success.

Zxxx0:admin#
```



## 62.16. show pim static\_rp

---

- **Description**

This command is used to list all the static RP settings.

- **Format**

show pim static\_rp

- **Parameters**

None.

- **Restrictions**

None.

- **Example**

To list all the static RP settings:

```
Zxxx0:admin# show pim static_rp
Command: show pim static_rp

PIM Static RP Table

Group                RP Address
-----
224.1.2.0/24         10.52.33.4
239.1.1.0/24         10.52.33.18

Total Entries: 2

Zxxx0:admin#
```

## 62.17. show pim rpset

---

- **Description**

This command is used to list all the RPset information.

- **Format**

show pim rpset

- **Parameters**

None.

## ● Restrictions

None.

## ● Example

To list all the RPset information:

```
Zxxx0:admin# show pim rpset
Command: show pim rpset
```

PIM RP-Set Table

Bootstrap Router: 10.54.71.9

| RP-Set Group | RP-Set Address | Holdtime | Expired Time | Type   |
|--------------|----------------|----------|--------------|--------|
| 224.0.0.0/4  | 10.20.6.36     | 210      | 196          |        |
| 224.0.0.0/4  | 10.54.71.9     | 0        | 0            | static |

Total Entries: 2

```
Zxxx0:admin#
```

## 62.18. create pim register\_checksum\_include\_data rp\_address

---

### ● Description

This command is used to decide the checksum in register packet will include the data portion or not. As defined in RFC 4601, the checksum for Registers is done only on the first 8 bytes of the packet, including the PIM header and the next 4 bytes, excluding the data packet portion. Some earlier PIM-SM routers will calculate checksum for register packet including data portion. This configuration makes our routers communicate with those earlier routers smoothly. The default set is not including data portion.

### ● Format

**create pim register\_checksum\_include\_data rp\_address <ipaddr>**

### ● Parameters

**rp\_address**

Specifies that the RP will expect to receive a register packet in which the checksum will be included in the data portion .

**<ipaddr>**

Enter the IP address used here.

## 62. Protocol Independent Multicast (PIM) Commands

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create an entry for a specific RP in which the checksum in the registered packet will include the data portion:

```
Zxxx0:admin# create pim register_checksum_include_data rp_address 24.1.2.3
Command: create pim register_checksum_include_data rp_address 24.1.2.3

Success.

Zxxx0:admin#
```

## 62.19. delete pim register\_checksum\_include\_data rp\_address

---

### ● Description

This command is used to delete the register checksum including the data for the specific RP address.

### ● Format

**delete pim register\_checksum\_include\_data rp\_address <ipaddr>**

### ● Parameters

---

**rp\_address**

Specifies the RP address that will be removed from the checksum, including the data portion list.

**<ipaddr>**

Enter the RP address used here.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete the register checksum including the data for the specific RP address:

```
Zxxx0:admin# delete pim register_checksum_include_data rp_address 10.54.71.9
Command: delete pim register_checksum_include_data rp_address 10.54.71.9

Success.

Zxxx0:admin#
```

### 62.20. show pim register\_checksum\_include\_data\_rp\_list

---

#### ● Description

This command is used to list all the RPs of the registered checksum, including the data.

#### ● Format

**show pim register\_checksum\_include\_data\_rp\_list**

#### ● Parameters

None.

#### ● Restrictions

None.

#### ● Example

To list all the RPs of the registered checksum, including the data:

```
Zxxx0:admin# show pim register_checksum_include_data_rp_list
Command: show pim register_checksum_include_data_rp_list

PIM Register Full Table

RP addresss
-----
24.0.0.0
24.1.2.3

Total Entries: 2

Zxxx0:admin#
```

## 62.21. config pim-ssm

---

### ● Description

This command is used to enable the SSM (Source-Specific Multicast) service model in PIM-SM on the Switching Hub. The PIM-SSM function will take active only when SSM service model and PIM-SM state both enabled.

### ● Format

**config pim-ssm {state [enable | disable] | group\_range [default | <network\_address>]}**

### ● Parameters

---

|              |                                                                               |
|--------------|-------------------------------------------------------------------------------|
| <b>state</b> | (Optional) Specifies to enable or disable the SSM service model on the Switch |
|--------------|-------------------------------------------------------------------------------|

|               |
|---------------|
| <b>enable</b> |
|---------------|

|                                                       |
|-------------------------------------------------------|
| Specifies that the SSM service model will be enabled. |
|-------------------------------------------------------|

|                |
|----------------|
| <b>disable</b> |
|----------------|

|                                                        |
|--------------------------------------------------------|
| Specifies that the SSM service model will be disabled. |
|--------------------------------------------------------|

---

|                    |
|--------------------|
| <b>group_range</b> |
|--------------------|

|                                                                           |
|---------------------------------------------------------------------------|
| (Optional) Specifies the group address range for the SSM service in IPv4. |
|---------------------------------------------------------------------------|

|                |
|----------------|
| <b>default</b> |
|----------------|

|                                                                    |
|--------------------------------------------------------------------|
| The default indicates that the group address range is 232.0.0.0/8. |
|--------------------------------------------------------------------|

|                                |
|--------------------------------|
| <b>&lt;network_address&gt;</b> |
|--------------------------------|

|                                                         |
|---------------------------------------------------------|
| Enter the group address range for the SSM service here. |
|---------------------------------------------------------|

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure PIM-SSM state and group range:

```
Zxxx0:admin# config pim-ssm state enable group_range default
Command: config pim-ssm state enable group_range default
```

```
Success.
```

```
Zxxx0:admin#
```

## 62.22. show pim-ssm

---

- **Description**

This command is used to list all PIM-SSM protocol related information.

- **Format**

show pim-ssm

- **Parameters**

None.

- **Restrictions**

None.

- **Example**

To display PIM-SSM state and group range:

```
Zxxx0:admin# show pim-ssm
Command: show pim-ssm

SSM Service Model State      : Enabled
SSM Group                    : 232.0.0.0/8

Zxxx0:admin#
```

## 63. PIM for IPv6 Command List

---

```

config pim6 [ipif <ipif_name 12> | all] {hello_interval <sec 0-18000> | triggered_hello_delay <sec 0-60> | propagation_delay <sec 0-32> | override_interval <sec 0-65> | jp_interval <sec 0-18000> | dr_priority <uint 0-4294967294> | bsr_border [disable | enable] | stub_interface [disable | enable] | state [enable | disable]}}(1)
show pim6 {ipif <ipif_name 12>}
config pim6 cbsr {ipif <ipif_name 12> state [enable | disable] | priority <value 0-255> | hash_masklen <value 0-128>}}(1)
show pim6 cbsr
config pim6 crp [rp <ipif_name 12> | all] {priority <value 0-255> | interval <sec 1-16383>}}(1)
create pim6 crp group <ipv6networkaddr> rp <ipif_name 12>
delete pim6 crp group <ipv6networkaddr>
enable pim6
disable pim6
config pim6 last_hop_spt_switchover [never | immediately]
show pim6 neighbor {ipif <ipif_name 12>}
show pim6 mroute {group <ipv6addr> {source <ipv6addr>}}
show pim6 mroute star_g {group <ipv6addr> {ipif <ipif_name 12>}}
show pim6 mroute s_g {rpt} {group <ipv6addr> source <ipv6addr> {ipif <ipif_name 12>}}
create pim6 static_rp group <ipv6networkaddr> rp <ipv6addr> {override_dynamic}
delete pim6 static_rp group <ipv6networkaddr>
config pim6 embedded_rp state [enable | disable]
show pim6 crp
show pim6 static_rp
show pim6 rpset
config pim6 register_checksum_calculate [include_data | not_include_data]
config pim6 register_probe_time <sec 1-127>
config pim6 register_suppression_time <sec 3-65535>
config pim6 keepalive_period <sec 120-65535>

```

---

### 63.1. config pim6

#### ● Description

This command is used to set the PIM6 multicast protocol state and some related parameters in the protocol on some interfaces.

#### ● Format

```

config pim6 [ipif <ipif_name 12> | all] {hello_interval <sec 0-18000> | triggered_hello_delay <sec 0-60> | propagation_delay <sec 0-32> | override_interval <sec 0-65> | jp_interval <sec 0-18000> | dr_priority <uint 0-4294967294> | bsr_border [disable | enable] | stub_interface [disable | enable] | state [enable | disable]}}(1)

```

## ● Parameters

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b>                  | Specify to apply the configurations to this specific IP interface.<br><b>&lt;ipif_name 12&gt;</b><br>Enter the IP interface name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>all</b>                   | Specify to apply the configurations to all IP interfaces.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>hello_interval</b>        | Specify the interval of issuing hello packets to find neighboring routers.<br><b>&lt;sec 0-18000&gt;</b><br>Enter the time between 0 and 18000 seconds. The default value is 30.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>triggered_hello_delay</b> | Specify the maximum time, in seconds, before the router sends a triggered PIM Hello message on the specified interface. A value of zero indicates that triggered PIM6 Hello message should always be sent immediately.<br><b>&lt;sec 0-60&gt;</b><br>Enter the time between 0 and 60 seconds. The default value is 5.                                                                                                                                                                                                                                                                                                                                                      |
| <b>propagation_delay</b>     | Specify the expected propagation delay between the PIM6 routers on this network or link, in seconds.<br><b>&lt;sec 0-32&gt;</b><br>Enter the time between 0 and 32 seconds. The default value is 1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>override_interval</b>     | Specify the value for the router to insert into the Override_Interval field of the LAN Prune Delay option in the PIM6 Hello messages it sends on this interface. When overriding a prune, PIM6 routers pick random time duration up to the value of this object. The more PIM6 routers that are active on a network, the more likely it is that the prune will be overridden after a small proportion of this time has elapsed. The more PIM6 routers are active on this network, the larger this object should be to obtain an optimal spread of prune override latencies.<br><b>&lt;sec 0-65&gt;</b><br>Enter the time between 0 and 65 seconds. The default value is 3. |
| <b>jp_interval</b>           | Specify the frequency at which this router sends PIM6 Join/Prune messages on this PIM6 interface. A value of zero represents not to send PIM Join/Prune message on this interface.<br><b>&lt;sec 0-18000&gt;</b><br>Enter the time between 0 and 18000 seconds. The default value is 60.                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>dr_priority</b>           | Specify the Designated Router Priority value inserted into the DR Priority option in PIM6 Hello message transmitted on this interface. Numerically higher values for this parameter indicate higher priorities.<br><b>&lt;uint 0-4294967294&gt;</b><br>Enter the value between 0 and 4294967294. The default value is 1.                                                                                                                                                                                                                                                                                                                                                   |
| <b>bsr_border</b>            | Specify to determine whether this interface is a PIM6 domain border. If this interface is a domain border, it prevents bootstrap router (BSR) messages from being sent or received through it.<br><b>disable</b><br>Specify that the interface is not a PIM6 domain border. This is the default.<br><b>enable</b><br>Specify that the interface is a PIM6 domain border.                                                                                                                                                                                                                                                                                                   |



## 63. PIM for IPv6 Command List

---

### stub\_interface

Specify whether this interface is a stub interface. If this interface is a stub interface, no PIM6 packets are sent out to this interface, and any received PIM6 packets are ignored.

#### disable

Specify that the interface is not a stub interface. This is the default.

#### enable

Specify that the interface is a stub interface.

---

### state

Specify to allow the PIM6 to be disabled or enabled for the IPv6 interface.

#### enable

Enable PIM6 for the IPv6 interface.

#### disable

Disable PIM6 for the IPv6 interface.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To set the jp\_interval to 60 seconds, the hello\_interval to 60 seconds, and enable the PIM6 state for interface "System":

```
Zxxx0:admin#config pim6 ipif System jp_interval 60 hello_interval 60 state enable
Command: config pim6 ipif System jp_interval 60 hello_interval 60 state enable

Success.

Zxxx0:admin#
```

## 63.2. show pim6

---

## ● Description

This command is used to display the PIM6 configurations.

## ● Format

show pim6 {ipif <ipif\_name 12>}

## ● Parameters

---

**ipif** (Optional) Specify to the IP interface name to be displayed.  
**<ipif\_name 12>**  
Enter the IP interface name.

---

## ● Restrictions

None.

## ● Example

To show brief information for the PIM6 protocol related parameters on all interfaces:

```
Zxxx0:admin#show pim6
Command: show pim6

PIM6 Global State           : Disabled
Last Hop SPT Switchover     : Never
Register Probe Interval     : 5 sec
Register Suppression Timeout : 60 sec
Keepalive Period            : 210 sec
Register Checksum Calculate  : Not Include Data
Embedded RP State           : Disabled

PIM6-SM Interface Table

Interface      DR      Hello   J/P      State      BSR
Priority       Interval Interval Interval
-----
System        1         60      60      Enabled    Disabled

Total Entries : 1

Zxxx0:admin#
```

To show detailed information for PIM6 protocol related parameters on the interface "System":

## 63. PIM for IPv6 Command List

```
Zxxx0:admin#show pim6 ipif System
Command: show pim6 ipif System

Interface name           : System
Interface Link-Local Address : -
Interface Global Address  : -
PIM6 Mode                : SM
State                    : Enabled
Designated Router        : -
Designated Router Priority : 1
Designated Router Priority Enabled : True
Hello Interval           : 60 sec
Triggered Hello Interval : 5 sec
Hello Holdtime           : 210 sec
Join Prune Interval      : 60 sec
Join Prune Holdtime      : 210 sec
LAN Delay Enabled        : True
Propagation Delay         : 1 sec
Override Interval        : 3 sec
Effective Propagation Delay : 1 sec
Effective Override Interval : 3 sec
Join Suppression Enabled : False
Bidirectional Capable    : False
BSR Domain Border        : Disabled
Stub interface           : Disabled

Zxxx0:admin#
```

### 63.3. config pim6 cbsr

#### ● Description

This command is used to set the C-BSR state, the priority and the hash mask length of the candidate bootstrap router on an interface.

#### ● Format

```
config pim6 cbsr {ipif <ipif_name 12> state [enable | disable] | priority <value 0-255> |
hash_masklen <value 0-128>}(1)
```

#### ● Parameters

---

**ipif** Specify the IP interface.

**<ipif\_name 12>**

Enter the IP interface name. This name can be up to 12 characters long.

---

**state** Specify to determine whether the input interface can be a C-BSR.

**enable**

Specify that the interface is a C-BSR.

**disable**

Specify that the interface is not a C-BSR. This is the default.

---

---

**priority** (Optional) Specify to set the C-BSR priority.

**<value 0-255>**

Enter the value between 0 and 255. The default value is 64.

---

**hash\_masklen**

Specify the length in bits of the mask. This makes use of a hash function for the case where a group range has multiple RPs with the same priority.

**<value 0-128>**

Enter the value must be between 0 and 128. The default value is 126 seconds.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure the C-BSR on the interface "System":

```
Zxxx0:admin#config pim6 cbsr ipif System state enable priority 64 hash_masklen 126
Command: config pim6 cbsr ipif System state enable priority 64 hash_masklen 126

Success.

Zxxx0:admin#
```

## 63.4. show pim6 cbsr

---

### ● Description

This command is used to display the candidate bootstrap router related information.

### ● Format

show pim6 cbsr

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To show C-BSR settings on the Switch:

## 63. PIM for IPv6 Command List

```
Zxxx0:admin#show pim6 cbsr
Command: show pim6 cbsr

PIM6 Candidate-BSR Information
-----
C-BSR Interface Name : System
C-BSR Priority       : 64
C-BSR Hash Mask Len : 126

Zxxx0:admin#
```

### 63.5. config pim6 crp

---

#### ● Description

This command is used to configure the PIM6 C-RP related parameters.

#### ● Format

**config pim6 crp [rp <ipif\_name 12> | all] {priority <value 0-255> | interval <sec 1-16383>}(1)**

#### ● Parameters

|                             |                                                                                                                  |
|-----------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b>                 | Specify to apply the configurations to this specific IP interface.                                               |
| <b>&lt;ipif_name 12&gt;</b> | Enter the IP interface name.                                                                                     |
| <b>all</b>                  | Specify to apply the configurations to all IP interfaces.                                                        |
| <b>priority</b>             | Specify for RP election.                                                                                         |
| <b>&lt;value 0-255&gt;</b>  | Enter the value between 0 and 255. The lower the value is, the higher the priority is. The default value is 192. |
| <b>interval</b>             | Specify the C-RP advertisement interval in seconds.                                                              |
| <b>&lt;sec 1-16383&gt;</b>  | Enter the interval between 1 and 16383 seconds. The default value is 60.                                         |

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To set the C-RP priority and the interval on the interface "System":

```
Zxxx0:admin#config pim6 crp rp System priority 60 interval 60
Command: config pim6 crp rp System priority 60 interval 60

Success.

Zxxx0:admin#
```

## 63.6. create pim6 crp group

### ● Description

This command is used to add a multicast group range into a C-RP serve list.

### ● Format

**create pim6 crp group <ipv6networkaddr> rp <ipif\_name 12>**

### ● Parameters

|                                |                                                        |
|--------------------------------|--------------------------------------------------------|
| <b>&lt;ipv6networkaddr&gt;</b> | Specify the IPv6 group address range served by the RP. |
| <b>rp</b>                      | Specify the interface act as a C-RP.                   |
| <b>&lt;ipif_name 12&gt;</b>    | Enter the IP interface name.                           |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To add a multicast group range "FF1E::12EF:1023/64" into the serve list of the C-RP "System":

```
Zxxx0:admin#create pim6 crp group FF1E::12EF:1023/64 rp System
Command: create pim6 crp group FF1E::12EF:1023/64 rp System

Success.

Zxxx0:admin#
```

## 63.7. delete pim6 crp group

---

### ● Description

This command is used to delete a multicast group range from the C-RP serve list.

### ● Format

delete pim6 crp group <ipv6networkaddr>

### ● Parameters

---

<ipv6networkaddr>

Specify the multicast group address range of the C-RP entry to be removed from C-RP serve list.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete a multicast group range "FF1E::12EF:1023/64" from the C-RP serve list:

```
Zxxx0:admin#delete pim6 crp group FF1E::12EF:1023/64
Command: delete pim6 crp group FF1E::12EF:1023/64

Success.

Zxxx0:admin#
```

## 63.8. enable pim6

---

### ● Description

This command is used to enable the PIM global state for an IPv6 network.

### ● Format

enable pim6

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To enable the PIM global state for an IPv6 network:

```
Zxxx0:admin#enable pim6
Command: enable pim6

Success.

Zxxx0:admin#
```

## 63.9. disable pim6

---

- **Description**

This command is used to disable the PIM global state for an IPv6 network.

- **Format**

**disable pim6**

- **Parameters**

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To disable PIM-SM for an IPv6 network:

```
Zxxx0:admin#disable pim6
Command: disable pim6

Success.

Zxxx0:admin#
```



## 63.10. config pim6 last\_hop\_spt\_switchover

### ● Description

This command is used to make the last hop router to decide whether to receive the multicast data from the shared tree or switch over to the shortest path tree (SPT).

### ● Format

config pim6 last\_hop\_spt\_switchover [never | immediately]

### ● Parameters

---

|              |                                                                                                                                   |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <b>never</b> | Specify to never switch to SPT. The last hop router always receives the multicast data from the shared tree. This is the default. |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------|

---

|                    |                                                                                                                                                |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>immediately</b> | Specify to immediately switch to SPT. The last hop router switches from shared tree to shortest path tree on the first multicast data arrived. |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------|

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To set the SPT-switchover mode to never:

```
Zxxx0:admin#config pim6 last_hop_spt_switchover never
Command: config pim6 last_hop_spt_switchover never

Success.

Zxxx0:admin#
```

## 63.11. show pim6 neighbor

### ● Description

This command is used to display all neighbors learned by PIM6 on the Switching Hub.

### ● Format

show pim6 neighbor {ipif <ipif\_name 12>}

## ● Parameters

---

**ipif** (Optional) Specify to the IPv6 interface name to be displayed.  
**<ipif\_name 12>**  
 Enter the IPv6 interface name.

---

## ● Restrictions

None.

## ● Example

To show the PIM6 neighbors:

```
Zxxx0:admin#show pim6 neighbor
Command: show pim6 neighbor

PIM6 Neighbor Address Table

Interface      Neighbor Address
-----
System        FE80::200:FF:FE26:66D0
n1             FE80::200:FF:FE26:66D1

Total Entries : 2

Zxxx0:admin#
```

To show the PIM6 neighbors of interface "n20":

```
Zxxx0:admin# show pim6 neighbor ipif n20
Command: show pim6 neighbor ipif n20

Neighbor Info on Interface n20
-----
Neighbor Address           : FE80::11FF:4CD8
Neighbor Up Time           : 00:00:50
Neighbor Expiry Time       : 00:01:50
Neighbor DR Priority Present : True
Neighbor DR Priority        : 1

Total Entries : 1

Zxxx0:admin#
```

# 63.12. show pim6 mroute

---

## ● Description

This command is used to display the multicast routing information generated by PIM6.

## 63. PIM for IPv6 Command List

### ● Format

**show pim6 mroute {group <ipv6addr> {source <ipv6addr>}}**

### ● Parameters

---

**group** (Optional) Specify the IPv6 multicast group address to be displayed.  
**<ipv6addr>**  
Enter the IPv6 address.

---

**source** (Optional) Specify the IPv6 source address to be displayed.  
**<ipv6addr>**  
Enter the IPv6 address.

---

### ● Restrictions

None.

### ● Example

To show the whole IPv6 multicast routing table generated on the Switch:

```
Zxxx0:admin#show pim6 mroute
Command: show pim6 mroute

Total (*,*,RP) Entries : 0
Total (*,G) Entries    : 1
Total (S,G) Entries    : 2
Total (S,G,rpt) Entries : 1

Group      : FF13::100
Source     : *                               Upstream: n1
Outgoing   : n10 n30

Group      : FF13::100
Source     : 2001::1111                       Upstream: n2
Outgoing   : n10

Group      : FF13::102
Source     : 2001::3F6D                       Upstream: n2
Outgoing   : n20

Group      : FF13::100
Source     : 2001::1111       rpt, Upstream: n1
RP Address : 3FFE:10:10::153
Outgoing   : -

Total Entries: 4

Zxxx0:admin#
```

## 63.13. show pim6 mroute star\_g

### ● Description

This command is used to display the multicast routing information for (\*, G) entries generated by PIM6.

### ● Format

**show pim6 mroute star\_g {group <ipv6addr> {ipif <ipif\_name 12>}}**

### ● Parameters

---

**group** (Optional) Specify the IPv6 multicast group address to be displayed.  
**<ipv6addr>**  
 Enter the IPv6 address.

---

**ipif** (Optional) Specify the IPv6 interface to be displayed.  
**<ipif\_name 12>**  
 Enter the IPv6 interface name.

---

### ● Restrictions

None.

### ● Example

To show the whole IPv6 multicast routing table of (\*, G) generated on the Switching Hub:

```
Zxxx0:admin#show pim6 mroute star_g
Command: show pim6 mroute star_g

(*, G) Entry Table
-----
Group       : FF13::100
Upstream    : n2
RP Address  : 3FFE:10:10::153

Group       : FF13::101
Upstream    : n2
RP Address  : 3FFE:10:10::153

Group       : FF13::102
Upstream    : n2
RP Address  : 3FFE:10:10::153

Total Entries: 3

Zxxx0:admin#
```

## 63.14. show pim6 mroute s\_g

### ● Description

This command is used to display the multicast routing information for (S, G) or (S, G, rpt) entries generated by PIM6.

### ● Format

**show pim6 mroute s\_g {rpt} {group <ipv6addr> source <ipv6addr> {ipif <ipif\_name 12>}}**

### ● Parameters

|                                            |                                                                                                 |
|--------------------------------------------|-------------------------------------------------------------------------------------------------|
| <b>rpt</b>                                 | (Optional) Specify the (S, G, rpt) entry.                                                       |
| <b>group</b><br><b>&lt;ipv6addr&gt;</b>    | (Optional) Specify the IPv6 multicast group address to be displayed.<br>Enter the IPv6 address. |
| <b>source</b><br><b>&lt;ipv6addr&gt;</b>   | (Optional) Specify the IPv6 source address to be displayed.<br>Enter the IPv6 address.          |
| <b>ipif</b><br><b>&lt;ipif_name 12&gt;</b> | (Optional) Specify the IPv6 interface name to be displayed.<br>Enter the IPv6 interface name.   |

### ● Restrictions

None.

### ● Example

To show all (S, G) route entries generated on the Switch:

```
Zxxx0:admin#show pim6 mroute s_g
Command: show pim6 mroute s_g

(S, G) Entry Table
-----
Group      : FF13::100
Source     : 2001::1111

Group      : FF13::100
Source     : 2001::2222

Group      : FF13::200
Source     : 2001::1111

Group      : FF13::300
Source     : 2001::1111

Total Entries: 4

Zxxx0:admin#
```

## 63.15. create pim6 static\_rp group

### ● Description

This command is used to create a static RP. In general, a static RP cannot override a dynamic RP. If `override_dynamic` is configured, the static RP will override any dynamically learned RP.

### ● Format

`create pim6 static_rp group <ipv6networkaddr> rp <ipv6addr> {override_dynamic}`

### ● Parameters

---

**<ipv6networkaddr>**

Specify the multicast group network address for this static RP.

---

**rp** Specify the IPv6 address to this static RP.

**<ipv6addr>**

Enter the IPv6 address.

---

**override\_dynamic**

(Optional) Specify to enable static RP to override dynamically learned RP.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create a static RP:

```
Zxxx0:admin#create pim6 static_rp group FF02::11/64 rp 3000::12
Command: create pim6 static_rp group FF02::11/64 rp 3000::12

Success.

Zxxx0:admin#
```

## 63.16. delete pim6 static\_rp group

### ● Description

This command is used to delete a static RP.

### ● Format

`delete pim6 static_rp group <ipv6networkaddr>`

## 63. PIM for IPv6 Command List

### ● Parameters

---

**<ipv6networkaddr>**

Specify the multicast group network address for this static RP.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete a static RP:

```
Zxxx0:admin#delete pim6 static_rp group FF02::11/64
Command: delete pim6 static_rp group FF02::11/64

Success.

Zxxx0:admin#
```

## **63.17. config pim6 embedded\_rp state**

---

### ● Description

This command is used to configure the state of the embedded RP.

### ● Format

**config pim6 embedded\_rp state [enable | disable]**

### ● Parameters

---

**enable** Specify to enable embedded RP support in PIM6.

---

**disable** Specify to disable embedded RP support in PIM6.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable the embedded RP state:

```
Zxxx0:admin#config pim6 embedded_rp state enable
Command: config pim6 embedded_rp state enable

Success.

Zxxx0:admin#
```

## 63.18. show pim6 crp

---

### ● Description

This command is used to display all candidate rendezvous point (C-RP) related information.

### ● Format

show pim6 crp

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To show C-RP information:

```
Zxxx0:admin#show pim6 crp
Command: show pim6 crp

PIM6 Candidate-RP Table

Group                                     Interface    Priority  Interval
-----
ffle::/64                               System      192      60

Total Entries : 1

Zxxx0:admin#
```

## 63.19. show pim6 static\_rp

---

### ● Description

This command is used to display all static RP settings.

### ● Format

show pim6 static\_rp

### ● Parameters

None.



## 63. PIM for IPv6 Command List

### ● Restrictions

None.

### ● Example

To show the static RP:

```
Zxxx0:admin#show pim6 static_rp
Command: show pim6 static_rp

PIM6 Static RP Table
-----
Group           : FF02::/64
RP Address      : 3000::12
Override Dynamic : False

Total Entries: 1

Zxxx0:admin#
```

## 63.20. show pim6 rpset

---

### ● Description

This command is used to display all the active RP information.

### ● Format

**show pim6 rpset**

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To show all the active RP information:

```
Zxxx0:admin#show pim6 rpset
Command: show pim6 rpset
```

```
Bootstrap Router: 3120::110
```

```
PIM6 RP-Set Table
```

```
-----
Group           : FF3D::/64
RP Address      : 3121::110
Hold Time       : 210 sec
Expired Time    : 196 sec
Type            : Dynamic
```

```
Group           : FF3E::/64
RP Address      : 3127::111
Override Dynamic : False
Type            : Static
```

```
Total Entries: 2
```

```
Zxxx0:admin#
```

## 63.21. config pim6 register\_checksum\_calculate

---

### ● Description

This command is used to decide whether the checksum in register packet will include the data portion.

### ● Format

```
config pim6 register_checksum_calculate [include_data | not_include_data]
```

### ● Parameters

#### include\_data

When specified to calculate the checksum in IPv6 PIM register packets, the data portion is included.

#### not\_include\_data

When specified to calculate the checksum in IPv6 PIM register packets, the data portion is excluded.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## 63. PIM for IPv6 Command List

### ● Example

To specify the Switching Hub calculates the register packet checksum including the data portion:

```
Zxxx0:admin#config pim6 register_checksum_calculate include_data
Command: config pim6 register_checksum_calculate include_data

Success.

Zxxx0:admin#
```

## **63.22. config pim6 register\_probe\_time**

### ● Description

This command is used to configure the PIM6-SM register probe time.

### ● Format

**config pim6 register\_probe\_time <sec 1-127>**

### ● Parameters

---

**<sec 1-127>**

Enter the time before the Register-Stop Timer (RST) expires when a DR may send a Null-Register to the RP to cause it to resend a Register-Stop message. The default value is 5.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the register probe time to be 20 seconds:

```
Zxxx0:admin#config pim6 register_probe_time 20
Command: config pim6 register_probe_time 20

Success.

Zxxx0:admin#
```

## 63.23. config pim6 register\_suppression\_time

### ● Description

This command is used to configure the PIM6-SM register suppression time.

### ● Format

config pim6 register\_suppression\_time <sec 3-65535>

### ● Parameters

<sec 3-65535>

Enter the period during which a PIM DR stops sending Register-encapsulated data to the RP after receiving a Register-Stop message. The default value is 60.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the PIM6-SM register suppression time to be 120 seconds:

```
Zxxx0:admin#config pim6 register_suppression_time 120
Command: config pim6 register_suppression_time 120

Success.

Zxxx0:admin#
```

## 63.24. config pim6 keepalive\_period

### ● Description

This command is used to configure the PIM6-SM multicast routing entry Keepalive Timer.

### ● Format

config pim6 keepalive\_period <sec 120-65535>

### ● Parameters

<sec 120-65535>

Enter the period during which the PIM router will maintain the (S, G) state in the absence of explicit (S, G) local membership or (S, G) join messages received to maintain it. The default value is 210.

## 63. PIM for IPv6 Command List

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the multicast routing keepalive period to be 220 seconds:

```
Zxxx0:admin#config pim6 keepalive_period 220  
Command: config pim6 keepalive_period 220
```

```
Success.
```

```
Zxxx0:admin#
```

## 64. Policy Route Commands

The commands are used to configure policy-based routing. In general routing, a route is selected according to metrics such as the number of routers passed through and the bandwidth. Meanwhile, policy-based routing allows to create an access profile and select a route for each access profile.

---

```
create policy_route name <policyroute_name 32>
delete policy_route name <policyroute_name 32>
config policy_route name <policyroute_name 32> acl profile_id <value 1-6> access_id <value 1-256> nexthop <ipaddr> state [enable | disable]
show policy_route
```

---

### 64.1. create policy\_route name

#### ● Description

This command is used to create a policy route and define the rule's name.

#### ● Format

```
create policy_route name <policyroute_name 32>
```

#### ● Parameters

---

```
<policyroute_name 32>
```

The policy route name. The maximum length is 32 characters.

---

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To create a policy route named "Danilo":

```
Zxxx0:admin#create policy_route name danilo
Command: create policy_route name danilo

Success.

Zxxx0:admin#
```

## 64.2. delete policy\_route name

---

### ● Description

This command is used to delete a policy route.

### ● Format

delete policy\_route name <policyroute\_name 32>

### ● Parameters

---

<policyroute\_name 32>

The policy route name. The maximum length is 32 characters.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete an IP route entry in the Switching Hub's IP routing table named "Duhon":

```
Zxxx0:admin#delete policy_route name duhon
Command: delete policy_route name duhon

Success.

Zxxx0:admin#
```

## 64.3. config policy\_route name

---

### ● Description

This command allows users to configure the different fields for a policy route entry. Users can set the state of a policy route to enable or disable.

- The user must create an ACL rule. If the ACL rule does not exist, the system will display an error message.
- If the ACL rule action is drop, these packets will not forward and the policy route will not be implemented.
- When a packet passes from the policy route, its TTL will decrease by 1.
- If a user deletes an ACL rule that is linked to a policy rule, the system will display an error message.

## ● Format

**config policy\_route name** <policyroute\_name 32> **acl profile\_id** <value 1-6> **access\_id** <value 1-256> **nexthop** <ipaddr> **state** [enable | disable]

## ● Parameters

---

**<policyroute\_name 32>**

The policy route name. The maximum length is 32 characters.

---

**acl profile\_id**

The ACL profile ID.

**<value 1-6>**

Specify the value between 1 and 6.

---

**access\_id**

The ACL access ID.

**<value 1-256>**

Specify the value between 1 and 256.

---

**nexthop** The next hop IP address.

**<ipaddr>**

Specifiy the IP address.

---

**state** Activate or deactivate this rule.

**enable**

Activate this rule.

**disable**

Deactivate this rule.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure all packets which match ACL rule profile ID=1 and access ID=1, and then route to 20.1.1.100:

```
Zxxx0:admin#config policy_route name danillo acl profile_id 1 access_id 1 nexthop
20.1.1.100 state enable
Command: config policy_route name danillo acl profile_id 1 access_id 1 nexthop
20.1.1.100 state enable

Success.

Zxxx0:admin#
```



## 64.4. show policy\_route

---

### ● Description

This command is used to display the Switching Hub's current policy route rules.

### ● Format

show policy\_route

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display the Switching Hub's current policy route rules:

```
Zxxx0:admin#show policy_route
```

```
Command: show policy_route
```

```
Policy Routing Table
```

```
-----
```

| Name  | Profile ID | Access ID | Next Hop     | State   |
|-------|------------|-----------|--------------|---------|
| ----- | -----      | -----     | -----        | -----   |
| rname | 1          | 1         | 192.168.69.1 | Enabled |

```
Total Entries: 1
```

```
Zxxx0:admin#
```

## 65. Port Security Commands

Port security is used to limit the number of MAC addresses learned in this Switching Hub to limit the number of terminals to be accessed. If the specified number of terminals to be accessed is exceeded, exceeded accesses are discarded.

You can configure the number of terminals based on the following four levels.

- Entire system
- For a port
- For a VLAN
- For a port within a specific VLAN

---

```

config port_security ports [<portlist> | all] [{admin_state [enable | disable] | max_learning_addr
  <max_lock_no 0-3328> | lock_address_mode [permanent | deleteontimeout |
  deleteonreset]](1) | {vlan [<vlan_name 32> | vlanid <vidlist>] max_learning_addr
  [<max_lock_no 0-3328> | no_limit]}}]
config port_security system max_learning_addr [<max_lock_no 1-3328> | no_limit]
config port_security vlan [<vlan_name 32> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-
  3328> | no_limit]
delete port_security_entry [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] mac_address
  <macaddr>
clear port_security_entry {ports [<portlist> | all] | {[vlan <vlan_name 32> | vlanid <vidlist>]}}
show port_security_entry {ports {<portlist>} {[vlan <vlan_name 32> | vlanid <vidlist>]}}
show port_security {ports {<portlist>} {[vlan <vlan_name 32> | vlanid <vidlist>]}}
enable port_security trap_log
disable port_security trap_log

```

---

### 65.1. config port\_security ports

#### • Description

This command is used to set the port's state, maximum supported MAC address entries, the default entry type, and set the maximum port-security entries that can be learned with a specific VLAN on a specific port. There are four levels of limitations on the learned entry number, for the entire system, for a port, for a VLAN, and for specific VLAN on a port. If any limitation is exceeded, the new entry will be discarded.

## 65. Port Security Commands

### ● Format

```
config port_security ports [<portlist> | all] [{admin_state [enable | disable] |  
max_learning_addr <max_lock_no 0-3328> | lock_address_mode [permanent |  
deleteontimeout | deleteonreset]}(1) | {vlan [<vlan_name 32> | vlanid <vidlist>]  
max_learning_addr [<max_lock_no 0-3328> | no_limit]}]
```

### ● Parameters

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;portlist&gt;</b>  | Specify a range of ports to be configured.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>all</b>               | Specify that all ports will be configured.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>admin_state</b>       | Allow the port security to be enabled or disabled for the ports specified in the port list. The default setting is disabled.<br><b>enable</b><br>Enable port security for the ports specified in the port list.<br><b>disable</b><br>Disable port security for the ports specified in the port list.                                                                                                                                                                                                                                                                                                         |
| <b>max_learning_addr</b> | Specify the maximum of MAC address entries that can be learned on this port. If the value is set to 0, it means that no user can get authorized by the port security function on this port. If the setting is smaller than the number of current learned entries on the port, the command will be rejected. The default value is 32.<br><b>&lt;max_lock_no 0-3328&gt;</b><br>Specify the value between 0 and 3328.                                                                                                                                                                                           |
| <b>lock_address_mode</b> | Indicate locking address mode. The default mode is deleteonreset.<br><b>permanent</b><br>The address will never be deleted unless the user removes it manually or the VLAN of the entry is removed or the port are removed from the VLAN, or port security is disabled on the port where the address resides.<br><b>deleteontimeout</b><br>The locked addresses can be aged out after aging timer expires.<br><b>deleteonreset</b><br>This address will be removed if the Switching Hub is reset or reboots. The cases under which the permanent entries are deleted also apply to the deleteonreset entries |
| <b>vlan</b>              | (Optional) Specify the VLAN to limit the address learning.<br><b>&lt;vlan_name 32&gt;</b><br>Specify the name of the VLAN. The maximum length is 32 characters.<br><b>vlanid</b> Specify a list of VLANs by VLAN ID to limit the address learning.<br><b>&lt;vidlist&gt;</b><br>Specify a list of VLAN ID.                                                                                                                                                                                                                                                                                                   |
| <b>max_learning_addr</b> | (Optional) Specify the maximum of MAC address entries that can be learned on this port. If the value is set to 0, it means that no user can get authorized by the port security function on this port. If the setting is smaller than the number of current learned entries on the port, the command will be rejected. The default value is 32.<br><b>&lt;max_lock_no 0-3328&gt;</b><br>Specify the value between 0 and 3328.<br><b>no_limit</b><br>Specify no limitation on the number of entries.                                                                                                          |

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure port security:

```
Zxxx0:admin#config port_security ports 6 admin_state enable max_learning_addr 10
lock_address_mode permanent
Command: config port_security ports 6 admin_state enable max_learning_addr 10
lock_address_mode permanent

Success.

Zxxx0:admin#
```

To configure a port security setting:

```
Zxxx0:admin#config port_security ports 1 vlan vlanid 1 max_learning_addr 16
Command: config port_security ports 1 vlan vlanid 1 max_learning_addr 16

Success.

Zxxx0:admin#
```

## 65.2. config port\_security system max\_learning\_addr

---

### ● Description

This command is used to set the maximum number of MAC address entries that can be authorized system wide. There are four levels of limitations on the learned entry number, for the entire system, for a port, for a VLAN, and for specific VLAN on a port. If any limitation is exceeded, the new entry will be discarded. The setting for system level max learned users must be greater than the total of the max learned users allowed on all ports.

### ● Format

config port\_security system max\_learning\_addr [<max\_lock\_no 1-3328> | no\_limit]

## 65. Port Security Commands

### ● Parameters

---

**<max\_lock\_no 1-3328>**

Specify the maximum number of MAC address entries that can be learned by the system. If the setting is smaller than the number of current learned entries on all enabled ports, the command will be rejected.

---

**no\_limit** By default, the number above is set to no limit.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the maximum number of port security entries to 256:

```
Zxxx0:admin# config port_security system max_learning_addr 256
Command: config port_security system max_learning_addr 256

Success.

Zxxx0:admin#
```

## 65.3. config port\_security vlan

---

### ● Description

This command sets the maximum number of MAC address entries that can be learned on a specific VLAN. There are four levels of limitations on the learned entry number, for the entire system, for a port, for a VLAN, and for specific VLAN on a port. If any limitation is exceeded, the new entry will be discarded.

### ● Format

**config port\_security vlan [<vlan\_name 32> | vlanid <vidlist>] max\_learning\_addr [<max\_lock\_no 0-3328> | no\_limit]**

### ● Parameters

---

**<vlan\_name 32>**

Specify the VLAN by name. The maximum length is 32 characters.

---

**vlanid** Specify a list of VLANs by VLAN ID.

**<vidlist>**

Specifies a VLAN ID.

---

**max\_learning\_addr**

Specify the maximum number of MAC address entries that can be learned with this VLAN. If this parameter is set to 0, it means that no user can get authorization on this VLAN. If the setting is smaller than the number of current learned entries on the VLAN, the command will be rejected.

**<max\_lock\_no 0-3328>**

Specify the value between 0 and 3328.

**no\_limit**

Specify the default value is no limit.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure the maximum number of entries that can be learned at 64:

```
Zxxx0:admin#config port_security vlan vlanid 1 max_learning_addr 64
Command: config port_security vlan vlanid 1 max_learning_addr 64

Success.

Zxxx0:admin#
```

# 65.4. delete port\_security\_entry

---

## ● Description

This command is used to delete a port security entry by VLAN, VLAN ID, and MAC address.

## ● Format

**delete port\_security\_entry [vlan <vlan\_name 32> | vlanid <vlanid 1-4094>]  
mac\_address <macaddr>**

## ● Parameters

---

**vlan** Specify the VLAN by name.

**<vlan\_name 32>**

Specify the VLAN name. The maximum length is 32 characters.

---

**vlanid** Specify a list of VLANs by VLAN ID.

**<vlanid 1-4094>**

Specify the VLAN ID. This value must be between 1 and 4094.

---

**mac\_address**

Specify the MAC address of the entry.

**<macaddr>**

Specify the MAC address of the entry.

---

## 65. Port Security Commands

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete the port security entry with a MAC address of 00-01-30-10-2c-c7 on the default VLAN:

```
Zxxx0:admin#delete port_security_entry vlan default mac_address 00-01-30-10-2C-C7
Command: delete port_security_entry vlan default mac_address 00-01-30-10-2C-C7

Success.

Zxxx0:admin#
```

## 65.5. clear port\_security\_entry

### ● Description

This command is used to clear the MAC entries learned from the specified port(s) or VLAN(s) for the port security function.

### ● Format

**clear port\_security\_entry {ports [<portlist> | all] | {[vlan <vlan\_name 32> | vlanid <vidlist>]}}**

### ● Parameters

|               |                                                                                                                                                                                    |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ports</b>  | (Optional) The port-security entries learned on the specified port will be cleared.<br><b>&lt;portlist&gt;</b><br>Specify a range of ports to be configured.                       |
| <b>all</b>    | All the port-security entries learned by the system will be cleared.                                                                                                               |
| <b>vlan</b>   | (Optional) The port-security entries learned on the specified VLANs will be cleared.<br><b>&lt;vlan_name 32&gt;</b><br>Specify the VLAN name. The maximum length is 32 characters. |
| <b>vlanid</b> | (Optional) Specify a list of VLANs by VLAN ID.<br><b>&lt;vidlist&gt;</b><br>Specify a list of VLAN ID.                                                                             |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

● Example

To clear port security entry for port 6:

```
Zxxx0:admin#clear port_security_entry port 6
Command: clear port_security_entry port 6

Success.

Zxxx0:admin#
```

## 65.6. show port\_security\_entry

● Description

This command is used to display a port security entry.

● Format

show port\_security\_entry {ports {<portlist>} {[vlan <vlan\_name 32> | vlanid <vidlist>]}}

● Parameters

|        |                                                                                                                                  |
|--------|----------------------------------------------------------------------------------------------------------------------------------|
| ports  | (Optional) Specify a range of ports to be displayed.<br><portlist><br>Specify a range of ports to be displayed.                  |
| vlan   | (Optional) Specify a VLAN to display its entry.<br><vlan_name 32><br>Specify the VLAN name. The maximum length is 32 characters. |
| vlanid | (Optional) Specify a VLAN list to display its entry.<br><vidlist><br>Specify a list of VLAN ID.                                  |

● Restrictions

None.



## 65. Port Security Commands

### ● Example

To display a port security entry:

```
Zxxx0:admin#show port_security_entry
Command: show port_security_entry

MAC Address          VID    Port    Lock Mode
-----
00-00-00-00-00-01    1      25      DeleteOnTimeout

Total Entry Number: 1

Zxxx0:admin#
```

## 65.7. show port\_security

### ● Description

This command is used to display the port security related information of the Switching Hub ports including the port security admin state, the maximum number of learning addresses, and the lock mode.

### ● Format

**show port\_security {ports {<portlist>} [[vlan <vlan\_name 32> | vlanid <vidlist>]]}**

### ● Parameters

|               |                                                                                                                                                       |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ports</b>  | (Optional) Specify a range of ports to be displayed.<br><b>&lt;portlist&gt;</b><br>Specify a range of ports to be displayed.                          |
| <b>vlan</b>   | (Optional) Specify a VLAN to display its configuration.<br><b>&lt;vlan_name 32&gt;</b><br>Specify the VLAN name. The maximum length is 32 characters. |
| <b>vlanid</b> | (Optional) Specify a VLAN list to display the configuration.<br><b>&lt;vidlist&gt;</b><br>Specify a list of VLAN ID.                                  |

### ● Restrictions

None.

## ● Example

To display the global configuration of port security:

```
Zxxx0:admin# show port_security
Command: show port_security

Port Security Trap/Log      : Disabled
System Maximum Address     : 512

VLAN Configuration (Only VLANs with limitation are displayed)
VID   VLAN Name              Max. Learning Addr.
----  -
1     default                 64
2     TstVLAN                 8

Zxxx0:admin#
```

To display the port security information of Switching Hub ports 1 to 6:

```
Zxxx0:admin#show port_security ports 1-6
Command: show port_security ports 1-6

Port   State   Lock Address Mode   Max. Learning Addr.
-----
1      Disabled DeleteOnReset      32
2      Disabled DeleteOnReset      32
3      Disabled DeleteOnReset      32
4      Disabled DeleteOnReset      32
5      Disabled DeleteOnReset      32
6      Disabled DeleteOnReset      32

Zxxx0:admin#
```

## 65.8. enable port\_security trap\_log

### ● Description

This command is used to enable port security traps/logs. When this command is enabled, if there's a new MAC that violates the pre-defined port security configuration, a trap will be sent out with the MAC and port information and the relevant information will be logged.

### ● Format

**enable port\_security trap\_log**

### ● Parameters

None.

## 65. Port Security Commands

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable a port security trap:

```
Zxxx0:admin#enable port_security trap_log
Command: enable port_security trap_log

Success.

Zxxx0:admin#
```

## **65.9. disable port\_security trap\_log**

---

### ● Description

This command is used to disable a port security trap/log. If the port security trap is disabled, no trap will be sent out for MAC violations, and no log will be recorded.

### ● Format

**disable port\_security trap\_log**

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To prevent a port security trap from being sent from the Switching Hub:

```
Zxxx0:admin#disable port_security trap_log
Command: disable port_security trap_log

Success.

Zxxx0:admin#
```

---

## 66. Power Saving Commands

---

The commands are used to configure the power saving mode.

If a port is not link up, the mode periodically repeats turning ON/OFF the power feed to the port to save more power consumption than when the power feed is always ON.

It also detects the length of a cable connected to the port and adjusts the power according to the length.

---

```
config power_saving {state [enable | disable] | length_detection [enable | disable]}  
show power_saving
```

---

### 66.1. config power\_saving

---

#### ● Description

This command is used to configure the power saving for the system. By default, the power saving mode is enabled and the length detection mode is disabled. The power saving length detection function applies to the Gigabit ports with copper media.

The power is saved by the following mechanisms. When the port has no link partner, the port automatically turns off and wakes up once a second to send a single link pulse. When the port is turned off, a simple receive energy-detect circuit is continuously monitoring energy on the cable. At the moment when energy is detected, the port turns on fully per IEEE specification requirements. The power saving function is performed while no link is detected and it will not affect the port capabilities while it is link up.

When the port is link up, for shorter cable, the power consumption can be reduced by lowering the signal amplitude since the signal attenuation is proportional to the cable length. The port will adjust the power based on cable length and still maintain error free applications from both sides of the link. This mechanism will only be supported when the hardware supports the cable diagnostics function.

#### ● Format

```
config power_saving {state [enable | disable] | length_detection [enable | disable]}
```

## 66. Power Saving Commands

### ● Parameters

---

|                |                                                                                                |
|----------------|------------------------------------------------------------------------------------------------|
| <b>state</b>   | (Optional) Configure the power saving state to enable or disable. The default value is enable. |
| <b>enable</b>  | Enable the power saving feature.                                                               |
| <b>disable</b> | Disable the power saving feature.                                                              |

---

|                         |                                                                                          |
|-------------------------|------------------------------------------------------------------------------------------|
| <b>length_detection</b> | Configure the length detection state to enable or disable. The default value is disable. |
| <b>enable</b>           | Enable the length detection feature.                                                     |
| <b>disable</b>          | Disable the length detection feature.                                                    |

---

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To configure power saving:

```
Zxxx0:admin# config power_saving state enable
Command: config power_saving state enable

Success

Zxxx0:admin#
```

## 66.2. show power\_saving

### ● Description

This command is used to display power saving information.

### ● Format

**show power\_saving**

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display power saving information:

```
Zxxx0:admin#show power_saving
Command: show power_saving

Power Saving State: Enabled

Length Detection State: Enabled

Zxxx0:admin#
```

## 67. Precision Time Protocol (PTP) Commands

PTP (Precision Time Protocol) is a technology to enable the time synchronization at an accuracy of 1  $\mu$ s or less. It allows for more highly accurate time synchronization than NTP (Network Time Protocol) on multicast network.

PTP establishes a master-slave relationship between the grand master clock and devices on the network and performs time synchronization through PTP packet exchanges.

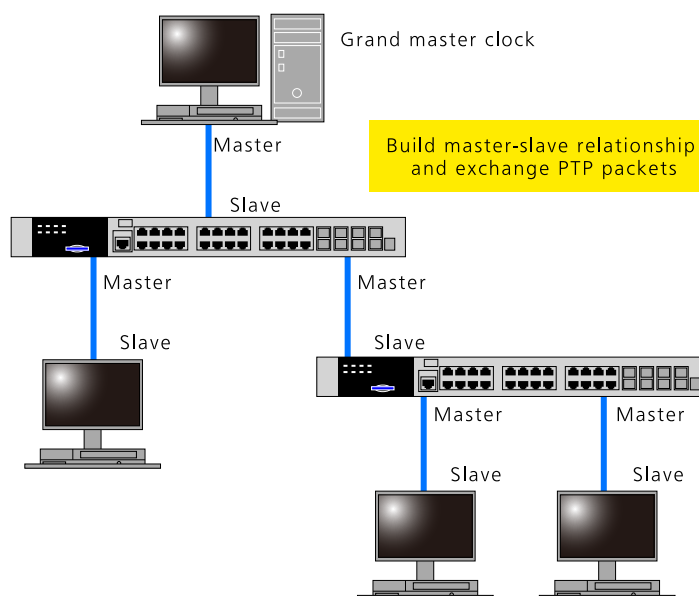


Figure 67-1 PTP overview

```
enable ptp
disable ptp
config ptp mode [boundary | p2p_transparent | e2e_transparent]
config ptp transport protocol [ethernet | udp]
config ptp clock domain_number <value 0-127> {unit <unit_id 1-3>} {domain_name <string 1-32>}
config ptp boundary {priority1 <value 0-255> | priority2 <value 0-255>}(1)
config ptp ports [<portlist> | all] state [enable | disable]
config ptp boundary ports [<portlist> | all] {announce [interval <sec 1-16> | timeout <value 2-10>]
| sync_interval [half_second | <sec 1-2>] | delay_req_interval <value 0-5> |
pdelay_req_interval <sec 1-32> | delay_mechanism [e2e | p2p]}(1)
config ptp p2p_transparent ports [<portlist> | all] pdelay_req_interval <sec 1-32>
show ptp
show ptp clock
show ptp clock parent
show ptp ports [<portlist> | all]
```

---

```
show ptp boundary {ports [<portlist> | all]}  
show ptp p2p_transparent ports [<portlist> | all]  
show ptp foreign_master_records ports [<portlist> | all]
```

---

## 67.1. enable ptp

---

### ● Description

This command is used to enable the PTP function globally. The device will enter the P2P-transparent clock mode when the PTP global state is enabled. The PTP function can only work when both the global PTP state and the per port PTP state are enabled.

### ● Format

**enable ptp**

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable the PTP function globally:

```
Zxxx0:admin# enable ptp  
Command: enable ptp  
  
Success.  
  
Zxxx0:admin#
```

## 67.2. disable ptp

---

### ● Description

This command is used to disable the PTP function globally. When the PTP function is disabled, all Switching Hub ports will forward the PTP packets according to the multicast filtering configuration.

### ● Format

**disable ptp**



## 67. Precision Time Protocol (PTP) Commands

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To disable the PTP function globally:

```
Zxxx0:admin# disable ptp
Command: disable ptp

Success.

Zxxx0:admin#
```

## 67.3. config ptp mode

---

### ● Description

This command is used to configure the PTP device type of the Switching Hub. The Switching Hub supports three PTP device types, which the user can set globally.

A Boundary Clock:

- Has multiple Precision Time Protocol (PTP) ports in a domain and maintains the timescale used in the domain.
- Can serve as the time source and can synchronize with another clock.
- Device type can choose to use the delay request-response mechanism or the peer delay mechanism to measure the propagation delay between the PTP ports.

A clock that provides Precision Time Protocol (PTP) event transit time information also provides corrections for the propagation delay of the link. The link, in this case, is connected to the port that is receiving the PTP event messages. Ports on peer-to-peer transparent clocks use the peer delay mechanism to calculate the propagation delay between PTP ports.

An End-to-End Transparent Clock supports the use of an end-to-end delay measurement mechanism between the slave clock and the master clock. Ports on end-to-end transparent clocks are independent of propagation delay mechanisms.

### ● Format

**config ptp mode [boundary | p2p\_transparent | e2e\_transparent]**

### ● Parameters

---

**boundary**

Specifies the Switch as a Boundary Clock.

---

**p2p\_transparent**

Specifies the Switch as a Peer-to-Peer Transparent Clock.

**e2e\_transparent**

Specifies the Switch as an End-to-End Transparent Clock.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To specify the Switching Hub as a peer-to-peer transparent clock:

```
Zxxx0:admin# config ptp mode p2p_transparent
Command: config ptp mode p2p_transparent

Success.

Zxxx0:admin#
```

## 67.4. config ptp transport protocol

- **Description**

This command is used to specify the transport protocol that will be used for the communication path.

- **Format**

config ptp transport protocol [ethernet | udp]

- **Parameters**

|                 |                                                                |
|-----------------|----------------------------------------------------------------|
| <b>ethernet</b> | Specifies the transport protocol of PTP as IEEE802.3 Ethernet. |
| <b>udp</b>      | Specifies the transport protocol of PTP as UDP over IPv4.      |

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To specify the transport protocol of PTP as IEEE802.3 Ethernet frames:

```
Zxxx0:admin# config ptp transport protocol ethernet
Command: config ptp transport protocol ethernet

Success.

Zxxx0:admin#
```

## 67.5. config ptp clock domain\_number

---

### ● Description

This command is used to configure the PTP clock common attribute of the domain number. The domain number is used to identify the PTP domain that the PTP clock is working on. If the domain number of the received PTP message is not identical to the domain number of the local device, the PTP message shall be forwarded according to the multicast filtering configuration.

### ● Format

**config ptp clock domain\_number** <value 0-127> {unit <unit\_id 1-3>} {domain\_name <string 1-32>}

### ● Parameters

---

#### domain\_number

Specifies the domain attribute of the local clock. All PTP messages, data sets, state machines, and all other PTP entities are always associated with a particular domain number.

**<value 0-127>**

Enter the domain number used here. This value must be between 0 and 127. The default value is 0.

---

#### unit

(Optional) specifies the domain number for a specified unit. If not specified, the domain configurations applies to the local unit. If the unit is not present, the configuration is ignored.

**<unit\_id 1-3>**

Enter the unit ID used here. This value must be between 1 and 3.

---

#### domain\_name

(Optional) Specifies the domain name for a specified domain number.

**<string 1-32>**

Enter the domain name used here. This name can be up to 32 characters long.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the domain number of the PTP clock as 1 and assign a domain name of internal\_domain on the local unit, when the stacking mode is disabled:

```
Zxxx0:admin# config ptp clock domain_number 1 domain_name internal_domain
Command: config ptp clock domain_number 1 domain_name internal_domain

Success.

Zxxx0:admin#
```

To configure the domain number of the PTP clock as 1 and assign a domain name of `internal_domain` for the unit 1, when the stacking mode is enabled.

```
Zxxx0:admin#config ptp clock domain_number 1 unit 1 domain_name internal_domain
Command: config ptp clock domain_number 1 unit 1 domain_name internal_domain

Success.

Zxxx0:admin#
```

## 67.6. config ptp boundary

### ● Description

This command is used to configure the PTP boundary clock attributes and requires at least one parameter to execute.

### ● Format

**config ptp boundary {priority1 <value 0-255> | priority2 <value 0-255>}(1)**

### ● Parameters

**priority1** (Optional) Specifies that the priority 1 attribute is used in the execution of the best master clock algorithm. Lower values take precedence.

**<value 0-255>**

Enter the priority 1 value used here. This value must be between 0 and 255.

**priority2** (Optional) Specifies that the priority 2 attribute is used in the execution of the best master clock algorithm. Lower values take precedence. In the event that the operation of the BMC algorithm fails to order the clocks based on the values of priority1, the clock's class, and the clock's accuracy; the priority2 attribute will allow the creation of lower values compared to the other devices.

**<value 0-255>**

Enter the priority 2 value used here. This value must be between 0 and 255.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the priority1 value of the boundary clock as 127:

```
Zxxx0:admin# config ptp boundary priority1 127
Command: config ptp boundary priority1 127

Success.

Zxxx0:admin#
```

## 67.7. config ptp ports

---

### ● Description

This command is used to configure the per port state of the PTP clock.

PTP port active state should meet the following three conditions:

- The global PTP state is enabled.
- The port PTP state is enabled.
- The port is not blocked, if the stp state is enabled.

### ● Format

**config ptp ports [<portlist> | all] state [enable | disable]**

### ● Parameters

|                |                                                                                                                                                |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ports</b>   | Specifies the list of port used for this configuration.<br><b>&lt;portlist&gt;</b><br>Enter the list of port used for this configuration here. |
| <b>all</b>     | Specifies that all the ports will be used for this configuration.                                                                              |
| <b>state</b>   | Specifies the port state of the PTP clock function.                                                                                            |
| <b>enable</b>  | Specifies that the port state of the PTP clock function will be enabled.                                                                       |
| <b>disable</b> | Specifies that the port state of the PTP clock function will be disabled.                                                                      |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable PTP on ports 1:1-1:4:

```
Zxxx0:admin# config ptp ports 1:1-1:4 state enable
Command: config ptp ports 1:1-1:4 state enable

Success.

Zxxx0:admin#
```

## 67.8. config ptp boundary ports

---

### ● Description

This command is used to configure the attributes of the PTP boundary clock. The configuration takes effect when the PTP device is a boundary type.

### ● Format

config ptp boundary ports [<portlist> | all] {announce [interval <sec 1-16> | timeout <value 2-10>] | sync\_interval [half\_second | <sec 1-2>] | delay\_req\_interval <value 0-5> | pdelay\_req\_interval <sec 1-32> | delay\_mechanism [e2e | p2p]](1)

### ● Parameters

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ports</b>           | Specifies the list of port used for this configuration.<br><portlist><br>Enter the list of port used for this configuration here.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>all</b>             | Specifies that all the ports will be used for this configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>announce</b>        | (Optional) Specifies that the announce options will be configured.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>interval</b>        | Specifies the mean time interval between successive announce messages. In line with the IEEE 1588 protocol, the value of the announce interval is represented as the logarithm to the base 2 of this time measured in seconds. If the input is not allowed, then the input is automatically adjusted to allow the bigger and closest value. The value of the announce interval should be uniform throughout a domain. If the announce interval of one port changes, the announce interval of all the ports must be changed automatically to be consistent.<br><sec 1-16><br>Enter the interval value used here. This value must be between 1 and 16 seconds. |
| <b>timeout</b>         | Specifies the announce interval number that has to pass without receiving an Announce message before the occurrence of the ANNOUNCE_RECEIPT_TIMEOUT_EXPIRES event. This value multiplied by the announce interval value is equal to the interval time of the announce receipt timeout. The value of the interval time of the announce receipt timeout should be uniform throughout a domain. If the value of one port is changed, the value of all ports must be changed automatically to be consistent.<br><value 2-10><br>Enter the timeout value used here. This value must be between 2 and 10 seconds.                                                  |
| <b>sync_interval</b>   | (Optional) Specifies the mean time interval between successive Sync messages.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>half_second</b>     | Specifies that the synchronization interval will be set to half a second.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>&lt;sec 1-2&gt;</b> | Enter the synchronization interval value used here. This value must be between 1 and 2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## 67. Precision Time Protocol (PTP) Commands

---

### **delay\_req\_interval**

(Optional) Specifies the permitted mean time interval between successive delay request messages which are sent by a slave to a specific port on the master. This mean time interval value is determined and advertised by a master.

**<value 0-5>**

Enter the delay required interval value used here. This value must be between 0 and 5.

---

### **pdelay\_req\_interval**

(Optional) Specifies the permitted mean time interval between successive pdelay\_request messages.

**<sec 1-32>**

Enter the permitted mean time interval value used here. This value must be between 1 and 32 seconds.

---

### **delay\_mechanism**

(Optional) Specifies the mechanism for measuring the propagation delay time of an event message.

**e2e** E2E indicates that the port is configured to use the delay request-response mechanism.

**p2p** P2P indicates that the port is configured to use the peer delay mechanism.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure the announce interval attribute of ports 1-4 to 3 seconds:

```
Zxxx0:admin# config ptp boundary ports 1:1-1:4 announce interval 3
Command: config ptp boundary ports 1:1-1:4 announce interval 3

The announce interval is automatically adjusted to 4.

Success.

Zxxx0:admin#
```

To configure the announce timeout attribute of ports 1-4 to 4 seconds, which is about 4\*Announce interval:

```
Zxxx0:admin# config ptp boundary ports 1:1-1:4 announce timeout 4
Command: config ptp boundary ports 1:1-1:4 announce timeout 4

Success.

Zxxx0:admin#
```

To configure the sync\_interval attribute of the all the PTP ports to 2 seconds:

## 67. Precision Time Protocol (PTP) Commands

```
Zxxx0:admin# config ptp boundary ports all sync_interval 2
Command: config ptp boundary ports all sync_interval 2

Success.

Zxxx0:admin#
```

If the sync\_interval is 0.5 seconds, then the delay\_req\_interval attribute of the all PTP ports is configured as 0.

```
Zxxx0:admin# config ptp boundary ports all delay_req_interval 0
Command: config ptp boundary ports all delay_req_interval 0

Success.

Zxxx0:admin#
```

To configure the pdelay\_req\_interval attribute of the all PTP ports as 5 seconds:

```
Zxxx0:admin# config ptp boundary ports all pdelay_req_interval 5
Command: config ptp boundary ports all pdelay_req_interval 5

The pdelay_req interval is automatically adjusted to 8.

Success.

Zxxx0:admin#
```

To configure the delay\_mechanism attribute of the all the PTP ports as P2P:

```
Zxxx0:admin# config ptp boundary ports all delay_mechanism p2p
Command: config ptp boundary ports all delay_mechanism p2p

Success.

Zxxx0:admin#
```



## 67.9. config ptp p2p\_transparent ports

---

### ● Description

This command is used to configure the pdelay\_request message attribute for the message interval of the P2P transparent clock.

### ● Format

**config ptp p2p\_transparent ports [<portlist> | all] pdelay\_req\_interval <sec 1-32>**

### ● Parameters

---

|                            |                                                                                                                                                                                                               |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ports</b>               | Specifies the list of port used for this configuration.<br><portlist>Enter the list of port used for this configuration here.<br><b>all</b> Specifies that all the ports will be used for this configuration. |
| <b>pdelay_req_interval</b> | Specifies the permitted mean time interval between successive messages.<br><sec 1-32><br>Enter the permitted mean time interval value used here. This value must be between 1 and 32.                         |

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the pdelay\_req\_interval attribute of all the PTP ports to 4 seconds:

```
Zxxx0:admin# config ptp p2p_transparent ports all pdelay_req_interval 4
Command: config ptp p2p_transparent ports all pdelay_req_interval 4

Success.

Zxxx0:admin#
```

## 67.10. show ptp

---

### ● Description

This command is used to display the configured attributes of PTP on the Switching Hub.

### ● Format

**show ptp**

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To show the global PTP configuration:

```
Zxxx0:admin# show ptp
Command: show ptp

PTP State Setting           : Enabled
PTP Mode Setting            : Boundary Clock
PTP Transport Protocol Setting : UDP
PTP Clock Domain Number Setting : 0
PTP Clock Domain Name Setting : Internal Domain

Zxxx0:admin#
```

## 67.11. show ptp clock

---

### ● Description

This command is used to display the active attributes of the PTP clock.

### ● Format

**show ptp clock**

### ● Parameters

None.

## 67. Precision Time Protocol (PTP) Commands

### ● Restrictions

None.

### ● Example

To show the active attributes of the boundary clock:

```
Zxxx0:admin# show ptp clock
Command: show ptp clock

PTP State                : Enabled
PTP Clock Mode           : Boundary Clock
PTP Transport Protocol   : UDP
PTP Clock Domain Number  : 1
PTP Clock Domain Name    : internal_domain
PTP Clock Identity       : ACDE48FFFE6789AB
PTP Priority 1           : 128
PTP Priority 2           : 128
PTP Clock Class          : 187
PTP Steps Removed       : 2
PTP Last Offset          : +130ns
PTP Mean Path Delay      : 1 second
PTP Enabled Ports        : 1:1-1:4, 2:1-2:4

Zxxx0:admin#
```

To show the properties of the Peer-to-Peer transparent clock:

```
Zxxx0:admin# show ptp clock
Command: show ptp clock

PTP State                : Enabled
PTP Clock Mode           : Peer-to-Peer Transparent Clock
PTP Transport Protocol   : UDP
PTP Clock Domain Number  : 1
PTP Clock Domain Name    : internal_domain
PTP Clock Delay Mechanism : P2P
PTP Clock Identity       : ACDE48FFFE6789AC
PTP Enabled Ports        : 1:1-1:4, 2:1-2:4

Zxxx0:admin#
```

To show the properties of the boundary clock of all stacking devices, when the stacking mode is enabled:

```

Zxxx0:admin# show ptp clock
Command: show ptp clock

Box ID: 1

PTP State           : Enabled
PTP Clock Mode      : Boundary Clock
PTP Transport Protocol : UDP
PTP Clock Domain Number : 1
PTP Clock Domain Name : internal_domain
PTP Clock Identity   : ACDE4823456789AB
PTP Priority 1       : 128
PTP Priority 2       : 128
PTP Clock Class      : 187
PTP Steps Removed    : 2
PTP Last Offset      : +110 ns
PTP Mean Path Delay  : 120 second
PTP Enabled Ports    : 1:1-1:4,

Box ID: 2

PTP State           : Enabled
PTP Clock Mode      : Boundary Clock
PTP Transport Protocol : UDP
PTP Clock Domain Number : 1
PTP Clock Domain Name : internal_domain
PTP Clock Identity   : ACDE482345678910
PTP Priority 1       : 128
PTP Priority 2       : 128
PTP Clock Class      : 187
PTP Steps Removed    : 3
PTP Last Offset      : +130ns
PTP Mean Path Delay  : 140 second
PTP Enabled Ports    : 2:1-2:4

Zxxx0:admin#

```

## 67.12. show ptp clock parent

---

### ● Description

This command is used to display the active attributes of the PTP parent clock.

### ● Format

**show ptp clock parent**

### ● Parameters

None.

## 67. Precision Time Protocol (PTP) Commands

### ● Restrictions

None.

### ● Example

To show the active attributes of the boundary clock parent:

```
Zxxx0:admin# show ptp clock parent
Command: show ptp clock parent

PTP Parent Port Identity      : ACDE48FFFE6789AB
PTP Parent Port Number       : 3
PTP Grandmaster Identity     : ACDE48FFFE9789AD
PTP Grandmaster Clock Class  : 13
PTP Grandmaster Clock Accuracy : 100ns
PTP Grandmaster Priority 1    : 120
PTP Grandmaster Priority 2    : 127

Zxxx0:admin#
```

The display of the active attributes of the boundary clock parent when the synchronization does not complete:

```
Zxxx0:admin# show ptp clock parent
Command: show ptp clock parent

The boundary clock has not completed synchronization.

Zxxx0:admin#
```

The display of the active attributes of the boundary clock parent when the boundary clock is the grandmaster clock:

```
Zxxx0:admin# show ptp clock parent
Command: show ptp clock parent

The grandmaster clock does not have this attribute.

Zxxx0:admin#
```

To show the parent and grandmaster properties of the transparent clock:

```
Zxxx0:admin# show ptp clock parent
Command: show ptp clock parent

The transparent clock does not have this attribute.

Zxxx0:admin#
```

To show the active attributes of the boundary clock parent of all stacking devices, when the stacking mode is enabled.

```

Zxxx0:admin# show ptp clock parent
Command: show ptp clock parent

Box ID: 1

PTP Parent Port Identity      : ACDE4823456789AB
PTP Parent Port Number       : 3
PTP Grandmaster Identity     : ACDE4823659789AD
PTP Grandmaster Clock Class  : 13
PTP Grandmaster Clock Accuracy : 100ns
PTP Grandmaster Priority 1    : 120
PTP Grandmaster Priority 2    : 127

Box ID: 2

PTP Parent Port Identity      : ACDE482345678910
PTP Parent Port Number       : 5
PTP Grandmaster Identity     : ACDE4823659789AD
PTP Grandmaster Clock Class  : 13
PTP Grandmaster Clock Accuracy : 100ns
PTP Grandmaster Priority 1    : 120
PTP Grandmaster Priority 2    : 127

Zxxx0:admin#

```

## 67.13. show ptp ports

### ● Description

This command is used to display the active attributes of the special PTP ports on the Switching Hub.

### ● Format

show ptp ports [<portlist> | all]

### ● Parameters

---

|                         |                                                             |
|-------------------------|-------------------------------------------------------------|
| <b>ports</b>            | Specifies the list of port used for this display.           |
| <b>&lt;portlist&gt;</b> | Enter the list of port used for this display here.          |
| <b>all</b>              | Specifies that all the ports will be used for this display. |

---

### ● Restrictions

None.

### ● Example

To show the active attributes for special ports 1:1-1:4 of the boundary clock:

## 67. Precision Time Protocol (PTP) Commands

```
Zxxx0:admin# show ptp ports 1:1-1:4
Command: show ptp ports 1:1-1:4
```

The active attributes:

DM : Delay Mechanism  
AI : Announce Interval  
ART : Announce Receipt Timeout  
SI : Synchronization Interval  
DRIM: Delay\_Request Interval-Master  
DRIS: Delay\_Request Interval-Slave  
PDRI: Pdelay\_Request Interval  
PMPD: Peer Mean Path Delay

| Port | Role   | DM  | AI | ART | SI  | DRIM | DRIS | PDRI | PMPD | State   |
|------|--------|-----|----|-----|-----|------|------|------|------|---------|
| 1:1  | Master | P2P | 2  | 8   | 1   | 1    | 2    | 4    | 1    | Enabled |
| 1:2  | Slave  | E2E | 1  | 8   | 0.5 | 2    | 8    | 8    | 0    | Enabled |
| 1:3  | Master | P2P | 2  | 8   | 1   | 8    | 4    | 8    | 1    | Enabled |
| 1:4  | Master | P2P | 2  | 8   | 1   | 32   | 16   | 16   | 0    | Enabled |

```
Zxxx0:admin#
```

To show the active attributes for special ports 1:1-1:4 of the p2p-transparent clock:

```
Zxxx0:admin# show ptp ports 1:1-1:4
Command: show ptp ports 1:1-1:4
```

The active attributes:

PDRI : Pdelay\_Request Interval  
PMPD : Peer Mean Path Delay

| Port | PDRI | PMPD | State    |
|------|------|------|----------|
| 1:1  | 4    | 1    | Enabled  |
| 1:2  | 8    | 0    | Disabled |
| 1:3  | 8    | 1    | Enabled  |
| 1:4  | 16   | 1    | Enabled  |

```
Zxxx0:admin#
```

## 67.14. show ptp boundary

---

### ● Description

This command is used to display the configured attributes of the boundary clock or the configured attributes of the boundary clock's special ports.

### ● Format

**show ptp boundary {ports [<portlist> | all]}**

### ● Parameters

---

|              |                                                                                                                                               |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ports</b> | (Optional) Specifies the list of port used for this display.<br><b>&lt;portlist&gt;</b><br>Enter the list of port used for this display here. |
| <b>all</b>   | Specifies that all the ports will be used for this display.                                                                                   |

---

### ● Restrictions

None.

### ● Example

To show the configured attributes of the boundary clock:

```
Zxxx0:admin# show ptp boundary
Command: show ptp boundary

PTP Priority1 Setting      : 128
PTP Priority2 Setting      : 127

Zxxx0:admin#
```

To show the configured attributes of special ports 1:1-1:4 of the boundary clock:



## 67. Precision Time Protocol (PTP) Commands

```
Zxxx0:admin# show ptp boundary ports 1:1-1:4
Command: show ptp boundary ports 1:1-1:4

The attribute configurations of the ports of boundary:

DM   : Delay Mechanism
AI   : Announce Interval
CART : The Coefficient of Announce Receipt Timeout
SI   : Synchronization Interval
EDRI : The Exponent of Delay_Request Interval
PDRI : Pdelay_Request Interval

Port    DM    AI    CART    SI    EDRI    PDRI    State
1:1     P2P    2     3       1     1       8     Enabled
1:2     E2E    1     2       0.5   0      16     Enabled
1:3     P2P    2     5       1     2       8     Enabled
1:4     P2P    2     6       1     4       4     Enabled

Zxxx0:admin#
```

### 67.15. show ptp p2p\_transparent ports

#### ● Description

This command is used to display the configured attributes of the P2P transparent clock's special ports.

#### ● Format

**show ptp p2p\_transparent ports [<portlist> | all]**

#### ● Parameters

|              |                                                                                                                                    |
|--------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>ports</b> | Specifies the list of port used for this display.<br><b>&lt;portlist&gt;</b><br>Enter the list of port used for this display here. |
| <b>all</b>   | Specifies that all the ports will be used for this display.                                                                        |

#### ● Restrictions

None.

#### ● Example

To show the configured attributes of special ports 1:1-1:4 of the p2p\_transparent clock:

```

Zxxx0:admin# show ptp p2p_transparent ports 1:1-1:4
Command: show ptp p2p_transparent ports 1:1-1:4

The attribute configuration of the p2p_transparent ports:

PDRI : Pdelay_Request Interval

Port      PDRI      State
1:1       8         Enabled
1:2       16        Enabled
1:3       8         Enabled
1:4       4         Disabled

Zxxx0:admin#

```

## **67.16. show ptp foreign\_master\_records ports**

### ● Description

This command is used to display the current foreign master data set records of the boundary clock's special ports.

### ● Format

**show ptp foreign\_master\_records ports [<portlist> | all]**

### ● Parameters

---

|              |                                                                 |
|--------------|-----------------------------------------------------------------|
| <b>ports</b> | Specifies the list of port used for this display.<br><portlist> |
|              | Enter the list of port used for this display here.              |
| <b>all</b>   | Specifies that all the ports will be used for this display.     |

---

### ● Restrictions

None.

### ● Example

To show the current records of the foreign master data set for special ports 1:1-1:3 of the boundary clock:

## 67. Precision Time Protocol (PTP) Commands

```
Zxxx0:admin#show ptp foreign_master_records ports all  
Command: show ptp foreign_master_records ports all
```

FM Port Identity : The clock identity of the Foreign Master Port  
FM Port Number : The port number of the Foreign Master Port  
FM Announce Messages : The numbers of Foreign Master announce messages

| Port | FM Port Identity  | FM Port Number | FM Announce Messages |
|------|-------------------|----------------|----------------------|
| 1:1  | 001655ffffe200000 | 1:7            | 4                    |
| 2:1  | 001655ffffe200000 | 1:8            | 4                    |

```
Zxxx0:admin#
```

## 68. Protocol VLAN Commands

Protocol VLAN is a function to determine a VLAN to which a port belongs based on protocol information written in the header of a receive packet.

You can specify the frame type of Ethernet ver2, Sub Network Access Protocol (SNAP), or Link Logical Control (LLC) and map it to a VLAN.

```
create dot1v_protocol_group group_id <id> group_name <name 32>
config dot1v_protocol_group [group_id <id> | group_name <name 32>] [add protocol
    [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value> | delete protocol
    [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value>]
delete dot1v_protocol_group [group_id <id> | group_name <name 32> | all]
show dot1v_protocol_group {group_id <id> | group_name <name 32>}
config port dot1v ports [<portlist> | all] [add protocol_group [group_id <id> | group_name <name
    32>] [vlan <vlan_name 32> | vlanid <id>] {priority <value 0-7>} | delete protocol_group
    [group_id <id> | all]]
show port dot1v {ports <portlist>}
```

### 68.1. create dot1v\_protocol\_group

#### ● Description

This command is used to create a protocol group for the protocol VLAN function.

#### ● Format

**create dot1v\_protocol\_group group\_id <id> group\_name <name 32>**

#### ● Parameters

**group\_id** Specify the ID of the protocol group which is used to identify a set of protocols.  
**<id>** The ID range is between 1 and 16.

**group\_name**  
 Specify the name of the protocol group.  
**<name 32>**  
 Specify the name of the protocol group. The maximum length is 32 characters.

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To create a protocol group:

```
Zxxx0:admin#create dot1v_protocol_group group_id 4 group_name General_Group
Command: create dot1v_protocol_group group_id 4 group_name General_Group

Success.
Zxxx0:admin#
```

### 68.2. config dot1v\_protocol\_group

---

#### ● Description

This command is used to add a protocol to a protocol group. The selection of a protocol can be a pre-defined protocol type or a user defined protocol.

#### ● Format

```
config dot1v_protocol_group [group_id <id> | group_name <name 32>] [add protocol
[ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value> | delete protocol
[ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value>]
```

#### ● Parameters

---

**group\_id** Specify the ID of the protocol group which is used to identify a set of protocols.

**<id>** The ID range is between 1 and 16.

---

**group\_name**

Specify the name of the protocol group.

**<name 32>**

Specify the name of the protocol group. The maximum length is 32 characters.

---

**add protocol**

Specify the protocol to be added. Depending on the frame type, the octet string will have one of the following values below. The form of the input is 0x0 to 0xffff.

**ethernet\_2**

This is a 16-bit (2-octet) hex value. Example: IPv4 is 800, IPv6 is 86dd, ARP is 806, etc.

**ieee802.3\_snap**

This is a 16-bit (2-octet) hex value. Example: IPv4 is 800, IPv6 is 86dd, ARP is 806, etc.

**ieee802.3\_llc**

This is the 2-octet IEEE 802.2 Link Service Access Point (LSAP) pair: first octet for Destination Service Access Point (DSAP) and second octet for Source.

---

**<protocol\_value>**

Specify the protocol value used to identify a protocol of the frame type. The form of the input is 0x0 to 0xffff. Depending on the frame type, the octet string will have one of the following values: For Ethernet II, this is a 16-bit (2-octet) hex value. For example, IPv4 is 800, IPv6 is 86dd, ARP is 806, etc. For IEEE802.3 SNAP, this is this is a 16-bit (2-octet) hex value. For IEEE802.3 LLC, this is the 2-octet IEEE 802.2 Link Service Access Point (LSAP) pair. The first octet is for Destination Service Access Point (DSAP) and the second octet is for Source.

---

**delete protocol**

Specify the protocol to be deleted. Depending on the frame type, the octet string will have one of the following values below. The form of the input is 0x0 to 0xffff.

**ethernet\_2**

This is a 16-bit (2-octet) hex value. Example: IPv4 is 800, IPv6 is 86dd, ARP is 806, etc.

**ieee802.3\_snap**

This is a 16-bit (2-octet) hex value. Example: IPv4 is 800, IPv6 is 86dd, ARP is 806, etc.

**ieee802.3\_llc**

This is the 2-octet IEEE 802.2 Link Service Access Point (LSAP) pair: first octet for Destination Service Access Point (DSAP) and second octet for Source.

**<protocol\_value>**

Specify the protocol value used to identify a protocol of the frame type. The form of the input is 0x0 to 0xffff. Depending on the frame type, the octet string will have one of the following values: For Ethernet II, this is a 16-bit (2-octet) hex value. For example, IPv4 is 800, IPv6 is 86dd, ARP is 806, etc. For IEEE802.3 SNAP, this is this is a 16-bit (2-octet) hex value. For IEEE802.3 LLC, this is the 2-octet IEEE 802.2 Link Service Access Point (LSAP) pair. The first octet is for Destination Service Access Point (DSAP) and the second octet is for Source.

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To add a protocol IPv6 to protocol group 4:

```
Zxxx0:admin# config dotlv_protocol_group group_id 4 add protocol ethernet_2 86dd
Command: config dotlv_protocol_group group_id 4 add protocol ethernet_2 86dd

Success.
Zxxx0:admin#
```

To delete a protocol IPv6 from protocol group ID 4:

```
Zxxx0:admin# config dotlv_protocol_group_group_id 4 delete protocol ethernet_2
86dd
Command: config dotlv_protocol_group group_id 4 delete protocol ethernet_2 86dd

Success.
Zxxx0:admin#
```

## 68.3. delete dot1v\_protocol\_group

---

### ● Description

This command is used to delete a protocol group.

### ● Format

**delete dot1v\_protocol\_group** [group\_id <id> | group\_name <name 32> | all]

### ● Parameters

---

**group\_id** Specify the group ID to be deleted.

    <id> Specify the group ID to be deleted.

---

**group\_name**

    Specify the name of the protocol group to be deleted.

    <name 32>

        Specify the name of the protocol group to be deleted. The maximum length is 32 characters.

---

**all** Specify to delete all protocol groups.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete protocol group ID 4:

```
Zxxx0:admin# delete dot1v_protocol_group group_id 4
Command: delete dot1v_protocol_group group_id 4

Success.
Zxxx0:admin#
```

## 68.4. show dot1v\_protocol\_group

---

### ● Description

This command is used to display the protocols defined in protocol groups.

### ● Format

**show dot1v\_protocol\_group** {group\_id <id> | group\_name <name 32>}

## ● Parameters

**group\_id**(Optional) Specify the group ID to be displayed.

**<id>** Specify the group ID to be displayed.

**group\_name**

(Optional) Specify the name of the protocol group.

**<name 32>**

Specify the name of the protocol group. The maximum length is 32 characters.

**NOTE** If no parameter is specified, all configured protocol groups will be displayed.

## ● Restrictions

None.

## ● Example

To display protocol group ID 4:

```
Zxxx0:admin# show dot1v_protocol_group group_id 4
Command: show dot1v_protocol_group group_id 4

Protocol          Protocol          Frame Type          Protocol
Group ID         Group Name                               Value
-----
4                General Group      EthernetII           86dd

Total Entries: 1

Zxxx0:admin#
```

## 68.5. config port dot1v ports

### ● Description

This command is used to assign the VLAN for untagged packets ingress from the portlist based on the protocol group configured. This assignment can be removed by using the **delete protocol\_group** option.

When priority is not specified in the command, the port default priority will be the priority for those untagged packets classified by the protocol VLAN.

### ● Format

```
config port dot1v ports [<portlist> | all] [add protocol_group [group_id <id>|
group_name <name 32>] [vlan <vlan_name 32> | vlanid <id>] {priority <value 0-7>} |
delete protocol_group [group_id <id> | all]]
```



## 68. Protocol VLAN Commands

### ● Parameters

|                              |                                                                                                                        |
|------------------------------|------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;portlist&gt;</b>      | Specify a range of ports to apply this command.                                                                        |
| <b>all</b>                   | Specify all ports.                                                                                                     |
| <b>add protocol_group</b>    | Specify to add a protocol group.                                                                                       |
| <b>group_id</b>              | Specify the group ID of the protocol group.                                                                            |
| <b>&lt;id&gt;</b>            | Specify the group ID of the protocol group.                                                                            |
| <b>group_name</b>            | Specify the name of the protocol group.                                                                                |
| <b>&lt;name 32&gt;</b>       | Specify the name of the protocol group. The maximum length is 32 characters.                                           |
| <b>vlan</b>                  | Specify the VLAN that is to be associated with this protocol group on this port.                                       |
| <b>&lt;vlan_name 32&gt;</b>  | Specify the VLAN that is to be associated with this protocol group on this port. The maximum length is 32 characters.  |
| <b>vlanid</b>                | Specify the VLAN ID.                                                                                                   |
| <b>&lt;id&gt;</b>            | Specify the VLAN ID.                                                                                                   |
| <b>priority</b>              | Specify the priority to be associated with the packet which has been classified to the specified VLAN by the protocol. |
| <b>&lt;value 0-7&gt;</b>     | Specify a value between 0 and 7.                                                                                       |
| <b>delete protocol_group</b> | Specify to delete a protocol group.                                                                                    |
| <b>group_id</b>              | Specify the group ID to be deleted.                                                                                    |
| <b>&lt;id&gt;</b>            | Specify the group ID.                                                                                                  |
| <b>all</b>                   | Specify all groups.                                                                                                    |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the group ID 4 on port 3 to be associated with VLAN 2:

```
Zxxx0:admin# config port dotlv ports 3 add protocol_group group_id 4 vlan VLAN2
Command: config port dotlv ports 3 add protocol_group group_id 4 vlan VLAN2

Success.
Zxxx0:admin#
```

## 68.6. show port dot1v

### ● Description

This command is used to display the VLAN to be associated with untagged packets ingress from a port based on the protocol group.

### ● Format

**show port dot1v {ports <portlist>}**

### ● Parameters

|              |                                                                                                                              |
|--------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>ports</b> | (Optional) Specify a range of ports to be displayed.<br><b>&lt;portlist&gt;</b><br>Specify a range of ports to be displayed. |
|--------------|------------------------------------------------------------------------------------------------------------------------------|

**NOTE** If no parameter is specified, information for all ports will be displayed.

### ● Restrictions

None.

### ● Example

To display the protocol VLAN information for ports 1 to 2:

```
Zxxx0:admin# show port dot1v ports 1-2
Command: show port dot1v ports 1-2

Port: 1
Protocol Group ID      VLAN Name              Protocol Priority
-----
1                      default                -

Port: 2
Protocol Group ID      VLAN Name              Protocol Priority
-----
1                      default                1

Total Entries   :   2

Zxxx0:admin#
```

## 69. QoS Commands

QoS (Quality of Service) is a function to allocate the optimum bandwidth according to the communication purpose to secure response time and throughput required for each communication.

It performs communication priority control based on the priority tag (priority information) added to the header of a receive packet.

It also allows to restrict bandwidth according to the priority tag for each port.

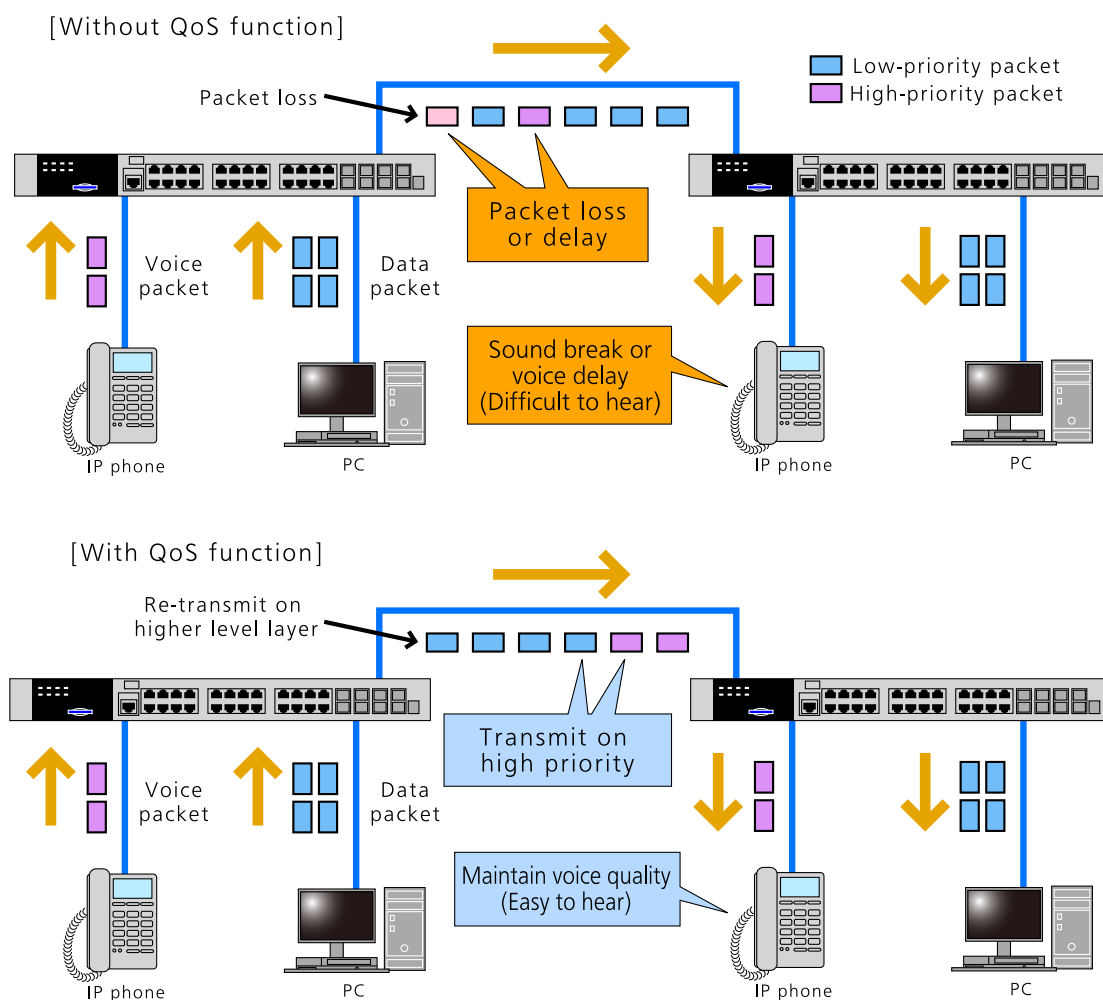


Figure 69-1 QoS overview

```

config bandwidth_control [<portlist> | all] {rx_rate [no_limit | <value 64-10240000>] | tx_rate
    [no_limit | <value 64-10240000>]](1)
show bandwidth_control {<portlist>}
config per_queue bandwidth_control {ports [<portlist> | all]} <cos_id_list 0-7> {{min_rate
    [no_limit | <value 64-10240000>]] max_rate [no_limit | <value 64-10240000>]](1)
show per_queue bandwidth_control {<portlist>}
config scheduling {ports [<portlist> | all]} <class_id 0-7> [strict | weight <value 1-127>]
config scheduling_mechanism {ports [<portlist> | all]} [strict | wrr]
show scheduling {<portlist>}
show scheduling_mechanism {<portlist>}
config 802.1p user_priority {ports [<portlist> | all]} <priority 0-7> <class_id 0-7>
show 802.1p user_priority {<portlist>}
config 802.1p default_priority [<portlist> | all] <priority 0-7>
show 802.1p default_priority {<portlist>}
enable hol_prevention
disable hol_prevention
show hol_prevention
config dscp_map {{<portlist> | all}} [dscp_priority <dscp_list> to <priority 0-7> | dscp_dscp
    <dscp_list> to <dscp 0-63>]
config dscp_trust [<portlist> | all] state [enable | disable]
show dscp_map {<portlist>} [dscp_priority | dscp_dscp] {dscp <dscp_list>}
show dscp_trust {<portlist>}

```

## 69.1. config bandwidth\_control

### ● Description

This command is used to set the maximum limit for port bandwidth.

### ● Format

```

config bandwidth_control [<portlist> | all] {rx_rate [no_limit | <value 64-10240000>] |
tx_rate [no_limit | <value 64-10240000>]](1)

```

### ● Parameters

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <portlist>          | Specify a range of ports to be configured.                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| all                 | Specify all ports.                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| rx_rate             | (Optional) Specify the limitation of receive data rate.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| no_limit            | Specify to indicate there is no limit on port rx bandwidth.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <value 64-10240000> | Specify an integer value from 64 to 10240000 to set a maximum limit in Kbits/sec. The specified bandwidth limit may be equaled but not exceeded. This exact logical limit or token value is hardware determined. Note: 1 Kbit = 1000 bits, 1 Gigabit = 1000*1000 Kbits.<br>The displayed value calculates value using as following the calculation formula. The decimal point is suppressed. So, The set range is just keep on the multiple of 64. Actual rate = (inputted rate/ 64) * 64. |

## 69. QoS Commands

---

**tx\_rate** (Optional) Specify the limitation of transmit data rate.

**no\_limit**

Specify to indicate there is no limit on port tx bandwidth.

**<value 64-10240000>**

Specify an integer value from 64 to 10240000 to set a maximum limit in Kbits/sec. The specified bandwidth limit may be equaled but not exceeded. This exact logical limit or token value is hardware determined.

The displayed value calculates value using as following the calculation formula. The decimal point is suppressed. So, The set range is just keep on the multiple of 64. Actual rate = (inputted rate/ 64) \* 64.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure port bandwidth:

```
Zxxx0:admin#config bandwidth_control 1-10 tx_rate 1024
Command: config bandwidth_control 1-10 tx_rate 1024

Success.

Zxxx0:admin#
```

## 69.2. show bandwidth\_control

---

### ● Description

This command is used to display the port bandwidth configurations. The bandwidth can also be assigned by the RADIUS server through the authentication process. If the RADIUS server has assigned the bandwidth, then the RADIUS-assigned bandwidth will be the effective bandwidth.

### ● Format

**show bandwidth\_control {<portlist>}**

### ● Parameters

---

**<portlist>**(Optional) Specify a range of ports to be displayed.

---

---

**NOTE** If no parameter is specified, the system will display all port bandwidth configurations.

---

### ● Restrictions

None.

## ● Example

To display the port bandwidth control table for ports 1 to 2:

```
Zxxx0:admin#show bandwidth_control 1-2
```

```
Command: show bandwidth_control 1-2
```

```
Bandwidth Control Table
```

| Port | RX Rate<br>(Kbit/sec) | TX Rate<br>(Kbit/sec) | Effective RX<br>(Kbit/sec) | Effective TX<br>(Kbit/sec) |
|------|-----------------------|-----------------------|----------------------------|----------------------------|
| ---- | -----                 | -----                 | -----                      | -----                      |
| 1    | No Limit              | No Limit              | No Limit                   | No Limit                   |
| 2    | No Limit              | No Limit              | No Limit                   | No Limit                   |

```
Zxxx0:admin#
```

## 69.3. config per\_queue bandwidth\_control

### ● Description

This command is used to set the bandwidth control for each specific egress queue on specified ports. The maximum rate limits the bandwidth. When specified, packets transmitted from the queue will not exceed the specified limit even if extra bandwidth is available. The specification of maximum rate is effective regardless of whether the queue is operating in strict or Shaped Deficit Weighted Round Robin (SDWRR) mode.

### ● Format

```
config per_queue bandwidth_control {ports [<portlist> | all]} <cos_id_list 0-7>
[{min_rate [no_limit | <value 64-10240000>]} max_rate [no_limit | <value 64-10240000>]}(1)
```

### ● Parameters

|                                |                                                                                                                   |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>ports</b>                   | (Optional) Specify a range of ports to be configured.<br><portlist><br>Specify a range of ports to be configured. |
| <b>all</b>                     | Specify to set all ports in the system. If no parameter is specified, the system will set all the ports.          |
| <b>&lt;cos_id_list 0-7&gt;</b> | Specify a list of priority queues. The priority queue number ranges from 0 to 7.                                  |

## 69. QoS Commands

---

**min\_rate** Specify that one of the parameters below will be applied to the minimum rate that the class specified above will be allowed to transmit packets at.

**no\_limit**

Indicates there is no limit on egress queue of specified port bandwidth.

**<value 64-10240000>**

Specify an integer value from 64 to 10240000 to set a minimum limit in Kbits/sec. The specified bandwidth limit may be equaled but not exceeded. The exact logical limit or token value is hardware determined. Note: 1 Kbit = 1000 bits, 1 Gigabit = 1000\*1000 Kbits. Actual rate = (inputted rate/ 64) \* 64.

---

**max\_rate** Specify one of the parameters below will be applied to the maximum rate that the class specified above will be allowed to transmit packets at.

**no\_limit**

Indicates there is no limit on egress queue of specified port bandwidth.

**<value 64-10240000>**

Specify an integer value from 64 to 10240000 to set a maximum limit in Kbits/sec. The specified bandwidth limit may be equaled but not exceeded. The exact logical limit or token value is hardware determined. Note: 1 Kbit = 1000 bits, 1 Gigabit = 1000\*1000 Kbits. Actual rate = (inputted rate/ 64) \* 64.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the maximum rate to be 100 on queue 1 for ports 1 to 10:

```
Zxxx0:admin#config per_queue bandwidth_control ports 1-10 1 max_rate 100
Command: config per_queue bandwidth_control ports 1-10 1 max_rate 100
```

```
Granularity: TX: 64. Actual Rate: MAX: 64.
```

```
Success.
```

```
Zxxx0:admin#
```

## **69.4. show per\_queue bandwidth\_control**

---

### ● Description

This command is used to display the bandwidth control setting of per egress queue for each port.

### ● Format

**show per\_queue bandwidth\_control {<portlist>}**

### ● Parameters

---

**<portlist>**(Optional) Specify a range of ports to be displayed.

---

## ● Restrictions

None.

## ● Example

To display the port bandwidth control table for port 1:

```
Zxxx0:admin#show per_queue bandwidth_control 1
Command: show per_queue bandwidth_control 1

Queue Bandwidth Control Table On Port: 1

Queue      Min Rate(Kbit/sec)    Max Rate(Kbit/sec)
0          No Limit          No Limit
1          No Limit          No Limit
2          64              1024
3          64              No Limit
4          No Limit          No Limit
5          No Limit          No Limit
6          No Limit          No Limit
7          No Limit          No Limit

Zxxx0:admin#
```

## 69.5. config scheduling

### ● Description

This command is used to configure the traffic scheduling mechanism for each CoS queue.

### ● Format

config scheduling {ports [<portlist> | all]} <class\_id 0-7> [strict | weight <value 1-127>]

### ● Parameters

---

|                         |                                                       |
|-------------------------|-------------------------------------------------------|
| <b>ports</b>            | (Optional) Specify a range of ports to be configured. |
| <b>&lt;portlist&gt;</b> | Enter the list of ports here.                         |
| <b>all</b>              | Specifies that all the ports will be used.            |

---

|                             |                                                                                                                                                                                                                  |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;class_id 0-7&gt;</b> | Specifies the 8 hardware priority queues that the config scheduling command will apply to. The eight hardware priority queues are identified by a number from 0 to 7 with the 0 queue being the lowest priority. |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

|               |                                                       |
|---------------|-------------------------------------------------------|
| <b>strict</b> | Specifies that the queue will operate in strict mode. |
|---------------|-------------------------------------------------------|

---



## 69. QoS Commands

---

|               |                                                                                                                                                                                                                                                                                 |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>weight</b> | Specifies the weight value for weighted round robin. The queue will operate in WRR mode if the port mode is WRR. It will operate in strict mode if the port mode is strict.<br><b>&lt;value 1-127&gt;</b><br>Enter the weight value here. This value must be between 1 and 127. |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the traffic scheduling on CoS queue 0 with a maximum packet value of 10:

```
Zxxx0:admin#config scheduling 0 weight 10
Command: config scheduling 0 weight 10

Success.

Zxxx0:admin#
```

To configure the traffic scheduling on CoS queue 1, with a weight value of 25, on port 1:10:

```
Zxxx0:admin# config scheduling ports 1:10 1 weight 25
Command: config scheduling ports 1:10 1 weight 25

Success.

Zxxx0:admin#
```

## **69.6. config scheduling\_mechanism**

---

### ● Description

This command is used to configure the traffic scheduling mechanism for each CoS queue.

### ● Format

**config scheduling\_mechanism {ports [<portlist> | all]} [strict | wrr]**

### ● Parameters

---

|              |                                                                                                                   |
|--------------|-------------------------------------------------------------------------------------------------------------------|
| <b>ports</b> | (Optional) Specify a range of ports to be configured.<br><b>&lt;portlist&gt;</b><br>Enter the list of ports here. |
| <b>all</b>   | Specifies that all the ports will be used.                                                                        |

---

|               |                                                                        |
|---------------|------------------------------------------------------------------------|
| <b>strict</b> | Specifies that all the queues will operate in strict mode.             |
| <b>wrr</b>    | Specifies that each queue will operate based on their weight settings. |

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure the traffic scheduling mechanism for each CoS queue:

```
Zxxx0:admin# config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Success.

Zxxx0:admin#
```

To configure the traffic scheduling mechanism for the CoS queue on port 1:1:

```
Zxxx0:admin# config scheduling_mechanism ports 1:1 strict
Command: config scheduling_mechanism ports 1:1 strict

Success.

Zxxx0:admin#
```

# 69.7. show scheduling

---

## ● Description

This command is used to display the current traffic scheduling parameters.

## ● Format

**show scheduling {<portlist>}**

## ● Parameters

---

**<portlist>**(Optional) Specifies the range of ports to be displayed.

---

## ● Restrictions

None.

## ● Example

To display the traffic scheduling parameters for each CoS queue:

## 69. QoS Commands

```
Zxxx0:admin#show scheduling
Command: show scheduling

QOS Output Scheduling On Port: 1
Class ID  Weight
-----  -
Class-0   1
Class-1   2
Class-2   3
Class-3   4
Class-4   5
Class-5   6
Class-6   7
Class-7   8

QOS Output Scheduling On Port: 2
Class ID  Weight
-----  -
Class-0   1
Class-1   2
Class-2   3
Class-3   4
Class-4   5
Class-5   6
CTRL+C  ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

To display the traffic scheduling parameters for each CoS queue on port 1:1.

```
Zxxx0:admin#show scheduling 1
Command: show scheduling 1

QOS Output Scheduling On Port: 1
Class ID  Weight
-----  -
Class-0   1
Class-1   2
Class-2   3
Class-3   4
Class-4   5
Class-5   6
Class-6   7
Class-7   8

Zxxx0:admin#
```

## 69.8. show scheduling\_mechanism

---

### ● Description

This command is used to display the traffic scheduling mechanism.

### ● Format

`show scheduling_mechanism {<portlist>}`

### ● Parameters

---

**<portlist>**(Optional) Specifies a range of ports to be displayed.

---

### ● Restrictions

None.

### ● Example

To display the scheduling mechanism for all ports:

```
Zxxx0:admin#show scheduling_mechanism
Command: show scheduling_mechanism

Port      Mode
-----  -
1         Strict
2         Strict
3         Strict
4         Strict
5         Strict
6         Strict
7         Strict
8         Strict
9         Strict
10        Strict

CTRL+C  ESC  q  Quit  SPACE  n  Next Page  ENTER  Next Entry  a  All
```

To show the scheduling mechanism on ports 1-10:

## 69. QoS Commands

```
Zxxx0:admin#show scheduling_mechanism 1-10
Command: show scheduling_mechanism 1-10
```

```
Port      Mode
-----  -
1         Strict
2         Strict
3         Strict
4         Strict
5         Strict
6         Strict
7         Strict
8         Strict
9         Strict
10        Strict
```

```
Zxxx0:admin#
```

### 69.9. config 802.1p user\_priority

#### ● Description

This command is used to configure the way by which the Switching Hub will map an incoming packet, based on its 802.1p user priority, to one of the eight available hardware priority queues on the Switching Hub. The Switching Hub's default is to map the following incoming 802.1p user priority values to the eight hardware priority queues. The suggested mapping is shown in the following table. Users can change this mapping by specifying the 802.1p user priority to assign to the <class\_id>.

| Priority in Frames | Priority Queue of ASIC | Remark   |
|--------------------|------------------------|----------|
| 0                  | 2                      | Mid-Low  |
| 1                  | 0                      | Lowest   |
| 2                  | 1                      | Lowest   |
| 3                  | 3                      | Mid-Low  |
| 4                  | 4                      | Mid-High |
| 5                  | 5                      | Mid-High |
| 6                  | 6                      | Highest  |
| 7                  | 7                      | Highest  |

#### ● Format

```
config 802.1p user_priority {ports [<portlist> | all]} <priority 0-7> <class_id 0-7>
```

## ● Parameters

|                             |                                                                                                                                                                                                                    |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ports</b>                | (Optional) Specifies that port used for this configuration.                                                                                                                                                        |
| <b>portlist</b>             | Specifies the range of ports to be configured.                                                                                                                                                                     |
| <b>all</b>                  | Specifies that all the ports will be used for this configuration.                                                                                                                                                  |
| <b>&lt;priority 0-7&gt;</b> | Specify the 802.1p user priority to associate with the <class_id> (the number of the hardware queue).                                                                                                              |
| <b>&lt;class_id 0-7&gt;</b> | Specify the number of the Switching Hub's hardware priority queue. The Switching Hub has eight hardware priority queues available. They are numbered between 0 (the lowest priority) and 7 (the highest priority). |

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure an 802.1p user priority of 1 map to class ID of 3:

```
Zxxx0:admin#config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

Success.

Zxxx0:admin#
```

# 69.10. show 802.1p user\_priority

## ● Description

This command is used to display 802.1p user priority.

## ● Format

**show 802.1p user\_priority {<portlist>}**

## ● Parameters

|                         |                                                       |
|-------------------------|-------------------------------------------------------|
| <b>&lt;portlist&gt;</b> | (Optional) Specify a range of ports to be configured. |
|-------------------------|-------------------------------------------------------|

## ● Restrictions

None.

## 69. QoS Commands

### ● Example

To display the 802.1p user priority:

```
Zxxx0:admin#show 802.1p user_priority
Command: show 802.1p user_priority

QoS Class of Traffic

Port 1
  Priority-0 -> <Class-2>
  Priority-1 -> <Class-0>
  Priority-2 -> <Class-1>
  Priority-3 -> <Class-3>
  Priority-4 -> <Class-4>
  Priority-5 -> <Class-5>
  Priority-6 -> <Class-6>
  Priority-7 -> <Class-7>

Port 2
  Priority-0 -> <Class-2>
  Priority-1 -> <Class-0>
  Priority-2 -> <Class-1>
  Priority-3 -> <Class-3>
  Priority-4 -> <Class-4>
  Priority-5 -> <Class-5>
  Priority-6 -> <Class-6>
  Priority-7 -> <Class-7>

Zxxx0:admin#
```

## 69.11. config 802.1p default\_priority

### ● Description

This command is used to specify default priority for untagged packets received on a port of the Switching Hub.

### ● Format

config 802.1p default\_priority [<portlist> | all ] <priority 0-7>

### ● Parameters

---

#### <portlist>

Specify a range of ports for which the default priority is to be configured. That is, a range of ports for which all untagged packets received will be assigned the priority specified below. The beginning and end of the port list range are separated by a dash.

---

#### all

Specify that the command applies to all ports on the Switching Hub.

---

#### <priority 0-7>

Specify a priority value (0 to 7) to assign to untagged packets received by the Switching Hub or a range of ports on the Switching Hub.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure an 802.1p default priority settings of 5 on all Switch ports:

```
Zxxx0:admin#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

Zxxx0:admin#
```

# 69.12. show 802.1p default\_priority

## ● Description

This command is used to display the current default priority settings on the Switching Hub. The default priority can also be assigned by the RADIUS server through the authentication process. Authentication with the RADIUS server can be either per port or per user. For per port authentication, the priority assigned by the RADIUS server will be the default priority of the effective port. For per user authentication, the priority assigned by RADIUS will not be the effective port default priority, as the will priority associated with MAC address will be assigned. Note that only devices supporting MAC-based VLANs can provide per user authentication.

## ● Format

**show 802.1p default\_priority {<portlist>}**

## ● Parameters

---

**<portlist>**(Optional) Specify a range of ports to be displayed.

---

### NOTE

If no parameter is specified, the system will display all ports with 802.1p default priority.

---

## ● Restrictions

None.

## ● Example

To display 802.1p default priority for ports 1 to 4:



## 69. QoS Commands

```
Zxxx0:admin#show 802.1p default_priority 1-4
Command: show 802.1p default_priority 1-4

Port          Priority      Effective Priority
----          -
1             0            0
2             0            0
3             0            0
4             0            0

Zxxx0:admin#
```

### 69.13. enable hol\_prevention

---

- **Description**

This command is used to enable head of line prevention on the Switching Hub.

- **Format**

**enable hol\_prevention**

- **Parameters**

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To enable HOL prevention on the Switching Hub:

```
Zxxx0:admin#enable hol_prevention
Command: enable hol_prevention

Success.

Zxxx0:admin#
```

## 69.14. disable hol\_prevention

---

### ● Description

This command is used to disable head of line prevention on the Switching Hub.

### ● Format

disable hol\_prevention

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To disable HOL prevention on the Switching Hub:

```
Zxxx0:admin#disable hol_prevention
Command: disable hol_prevention

Success.

Zxxx0:admin#
```

## 69.15. show hol\_prevention

---

### ● Description

This command is used to display the head of line prevention state on the Switching Hub.

### ● Format

show hol\_prevention

### ● Parameters

None.

### ● Restrictions

None.

## 69. QoS Commands

### ● Example

To display HOL prevention state on the Switching Hub:

```
Zxxx0:admin#show hol_prevention
Command: show hol_prevention

Device HOL Prevention State: Enabled

Zxxx0:admin#
```

## 69.16. config dscp map

---

### ● Description

This command is used to configure DSCP mapping. The mapping of DSCP to priority will be used to determine the priority of the packet (which will be then used to determine the scheduling queue) when the port is in DSCP trust state.

The mapping of DSCP to color will be used to determine the initial color of the packet when the policing function of the packet is color aware and the packet is DSCP-trusted.

The DSCP-to-DSCP mapping is used in the swap of DSCP of the packet when the packet is ingresses to the port. The remaining processing of the packet will base on the new DSCP. By default, the DSCP is mapped to the same DSCP.

These DSCP mapping will take effect at the same time when IP packet ingress from a DSCP-trusted port.

### ● Format

**config dscp map** {[<portlist> | all]} [**dscp\_priority** <dscp\_list> to <priority 0-7> | **dscp\_dscp** <dscp\_list> to <dscp 0-63>]

### ● Parameters

---

**<portlist>**

(Optional) Enter the list of port used for this configuration here.

---

**all**

(Optional) Specify that all the ports will be included in this configuration.

---

**dscp\_priority**

Specify a list of DSCP value to be mapped to a specific priority.

**<dscp\_list>**

Enter the DSCP priority list here.

**<priority 0-7>**

Specify the result priority of mapping.

---

**dscp\_dscp**

Specify a list of DSCP value to be mapped to a specific DSCP.

**<dscp\_list>**

Enter the DSCP to DSCP list here.

**<dscp 0-63>**

Specify the result DSCP of mapping.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the mapping of the DSCP priority to priority 1 on port 1:1 -1:8 :

```
Zxxx0:admin#config dscp map 1-8 dscp_priority 1 to 1
Command: config dscp map 1-8 dscp_priority 1 to 1

Success.

Zxxx0:admin#
```

## 69.17. config dscp trust

### ● Description

This command is used to configure the state of DSCP trust per port. When DSCP is not trusted, 802.1p is trusted.

### ● Format

**config dscp trust [<portlist> | all] state [enable | disable]**

### ● Parameters

|                         |                                                                      |
|-------------------------|----------------------------------------------------------------------|
| <b>&lt;portlist&gt;</b> | Enter the list of port used for this configuration here.             |
| <b>all</b>              | Specify that the command apply to all ports on the Switch.           |
| <b>state</b>            | Enable or disable to trust DSCP. By default, DSCP trust is disabled. |
| <b>enable</b>           | Specify that the DSCP trust state will be enabled.                   |
| <b>disable</b>          | Specify that the DSCP trust state will be disabled.                  |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

Enable DSCP trust on ports 1:1-1:8.

## 69. QoS Commands

```
Zxxx0:admin#config dscp trust 1-8 state enable
Command: config dscp trust 1-8 state enable

Success.

Zxxx0:admin#
```

### 69.18. show dscp map

---

#### ● Description

This command is used to show DSCP trusted port list and mapped color, priority and DSCP.

#### ● Format

**show dscp map {<portlist>} [dscp\_priority | dscp\_dscp] {dscp <dscp\_list>}**

#### ● Parameters

---

**<portlist>**

(Optional) A range of ports to show. If no parameter is specified, all ports' dscp mapping will be displayed.

---

**dscp\_priority**

Specify a list of DSCP value to be mapped to a specific priority.

---

**dscp\_dscp**

Specify a list of DSCP value to be mapped to a specific DSCP.

---

**dscp**

(Optional) This specifies DSCP value that will be mapped.

**<dscp\_list>**

Enter the DSCP list here.

---

#### ● Restrictions

None.

#### ● Example

In case of project support per port configure, show DSCP map configuration on port 1:1.

```
Zxxx0:admin# show dscp map 1 dscp_priority
Command: show dscp map 1 dscp_priority

DSCP to 802.1p Priority Mapping:

Port 1
DSCP 0,2-7 is mapped to 0
DSCP 1,8-15 is mapped to 1
DSCP 16-23 is mapped to 2
DSCP 24-31 is mapped to 3
DSCP 32-39 is mapped to 4
DSCP 40-47 is mapped to 5
DSCP 48-55 is mapped to 6
DSCP 56-63 is mapped to 7

Zxxx0:admin#
```

To configure the global mapping of the DSCP priority to priority 1:

```
Zxxx0:admin# show dscp map 1 dscp_dscp
Command: show dscp map 1 dscp_dscp

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

Zxxx0:admin#
```

## 69.19. show dscp trust

### ● Description

This command is used to display DSCP trust state for the specified ports on the Switch.

### ● Format

**show dscp trust {<portlist>}**

### ● Parameters

**<portlist>**

(Optional) A range of ports to display.

## 69. QoS Commands

### ● Restrictions

None.

### ● Example

Display DSCP trust status on ports 1:1-1:8.

```
Zxxx0:admin# show dscp trust 1-8  
Command: show dscp trust 1-8
```

```
Port DSCP-Trust  
----
```

```
1      Enabled  
2      Enabled  
3      Enabled  
4      Enabled  
5      Enabled  
6      Enabled  
7      Enabled  
8      Enabled
```

```
Zxxx0:admin#
```





## 70. Ring Redundant Protocol (RRP) Commands

Ring Redundant Protocol (RRP) realizes to make a redundant network via ring topology to recover the communication failure quickly, when the device or link failure is happened.

One ring topology unit is called “domain”, RRP controller is called “Master node”, and the other RRP members are called “Transit node”. “Master node” must be existed only one node in domain.

Each domain require two VLANs: “Control VLAN” for RRP control, and “Data VLAN” for actual data communication networks.

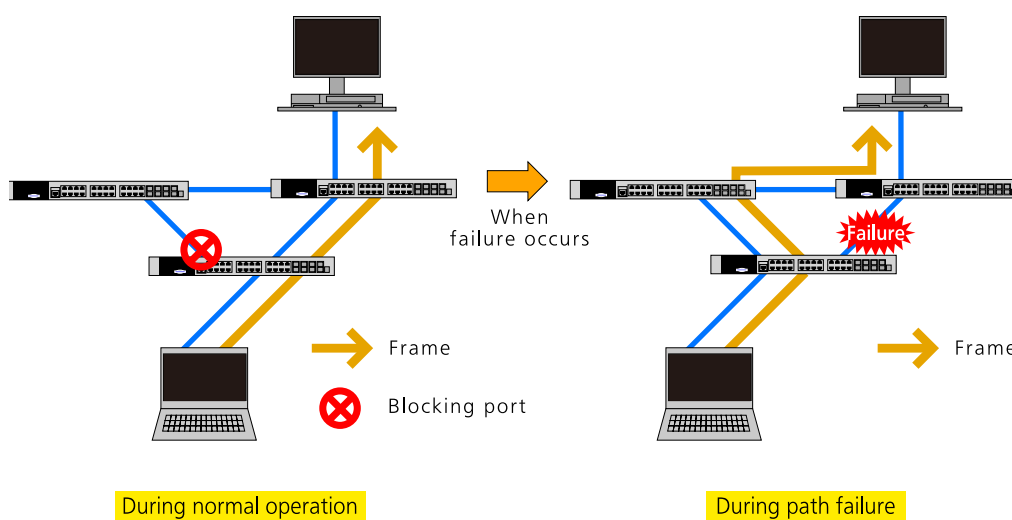


Figure 70-1 RRP overview

```

config rrp domain <domain name> [type {master|transit}] [control_vlan_id <vid>] [data_vlan_id
  <vid list>] [primary_port <port num>] [secondary_port <port num>] [polling_interval <1-2sec>]
  [fail_period <2-5sec>] [ring_guard_port {primary|secondary|both|disable}]
create rrp domain <domain name> type {master|transit} control_vlan_id <vid> data_vlan_id <vid
  list> primary_port <port num> secondary_port <port num> [polling_interval <1-2sec>]
  [fail_period <2-5sec>] [ring_guard_port {primary|secondary|both|disable}]
delete rrp domain <domain name>
disable rrp
disable rrp domain <domain name>
enable rrp
enable rrp domain <domain name>
show rrp
show rrp status
  
```

## 70.1. config rrp domain

---

### ● Description

This command is used to configure the RRP domain.

### ● Format

```
config rrp domain <domain name> [type {master|transit}] [control_vlan_id <vid>]
[data_vlan_id <vid list>] [primary_port <port num>] [secondary_port <port num>]
[polling_interval <1-2sec>] [fail_period <2-5sec>] [ring_guard_port
{primary|secondary|both|disable}]
```

### ● Parameters

---

**<domain name>**

Specify the domain name of the RRP domain with 1-25 characters.

---

**type**

Specify the RRP node type.

**master**

Specify the RRP node as Master. The Master node must be existed only one in domain.

**transit**

Specify the RRP node as Transit.

---

**control\_vlan\_id**

Specify the control VLAN ID.

**<vid>**

Specify the control VLAN ID between 2-4094. The existed VLAN ID is not allowed to use.

---

**data\_vlan\_id**

Specify the data VLAN ID.

**<vid list>**

Specify the data VLAN ID(s) between 1-4094. You can use a comma (,) or hyphen (-) for multiple assignment.

---

**primary\_port**

Specify the primary port to connect with other nodes.

**<port num>**

Specify the port number.

---

**secondary\_port**

Specify the secondary port to connect with other nodes.

**<port num>**

Specify the port number.

---

**polling\_interval**

Specify the polling interval time to send RRP control frame to next node. The factory default is 1 sec.

**<1-2 sec>**

Specify the time between 1 and 2 seconds.

polling\_interval and fail\_period are not allowed to set the same value.

---

## 70. Ring Redundant Protocol (RRP) Commands

---

### **fail\_period**

Specify the fail period time to detect communication failure. The factory default is 2 sec.

**<2-5 sec>**

Specify the time between 2 and 5 seconds.

polling\_interval and fail\_period are not allowed to set the same value.

---

### **ring\_guard\_port**

(Option) Specify the ring guard function state. The factory default is “disable” .

#### **primary**

Specify to enable the ring guard and set the target port to primary port.

#### **secondary**

Specify to enable the ring guard and set the target port to secondary port.

#### **both**

Specify to enable the ring guard and set the target port to primary and secondary port.

#### **disable**

Specify to disable the ring guard.

---

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To change the “pc-ring” domain settings to node type=Transit, control VLAN=30, primary port=9, secondary port=10, data VLAN=1, polling interval=1, and fail period=2:

```
Zxxx0:admin# config rrp domain pc-ring type transit control_vlan_id 30 primary_port 9 secondary_port 10 data_vlan_id 1 polling_interval 1 fail_period 2
Command: config rrp domain pc-ring type transit control_vlan_id 30 primary_port 9 secondary_port 10 data_vlan_id 1 polling_interval 1 fail_period 2
```

```
Success.
```

```
Zxxx0:admin#
```

## 70.2. create rrp domain

---

### ● Description

This command is used to create the RRP domain.

### ● Format

**create rrp domain <domain name> type {master|transit} control\_vlan\_id <vlanid> data\_vlan\_id <vid list> primary\_port <port> secondary\_port <port num> [polling\_interval <1-2sec>] [fail\_period <2-5sec>] [ring\_guard\_port {primary|secondary|both|disable}]**

## ● Parameters

|                            |                                                                                                                      |
|----------------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>&lt;domain name&gt;</b> | Specify the domain name of the RRP domain with 1-25 characters.                                                      |
| <b>type</b>                | Specify the RRP node type.                                                                                           |
| <b>master</b>              | Specify the RRP node as Master. The Master node must be existed only one in domain.                                  |
| <b>transit</b>             | Specify the RRP node as Transit.                                                                                     |
| <b>control_vlan_id</b>     | Specify the control VLAN ID.                                                                                         |
| <b>&lt;vid&gt;</b>         | Specify the control VLAN ID between 2-4094. The existed VLAN ID is not allowed to use.                               |
| <b>data_vlan_id</b>        | Specify the data VLAN ID.                                                                                            |
| <b>&lt;vid list&gt;</b>    | Specify the data VLAN ID(s) between 1-4094. You can use a comma (,) or hyphen (-) for multiple assignment.           |
| <b>primary_port</b>        | Specify the primary port to connect with other nodes.                                                                |
| <b>&lt;port num&gt;</b>    | Specify the port number.                                                                                             |
| <b>secondary_port</b>      | Specify the secondary port to connect with other nodes.                                                              |
| <b>&lt;port num&gt;</b>    | Specify the port number.                                                                                             |
| <b>polling_interval</b>    | Specify the polling interval time to send RRP control frame to next node. The factory default is 1 sec.              |
| <b>&lt;1-2 sec&gt;</b>     | Specify the time between 1 and 2 seconds.<br>polling_interval and fail_period are not allowed to set the same value. |
| <b>fail_period</b>         | Specify the fail period time to detect communication failure. The factory default is 2 sec.                          |
| <b>&lt;2-5 sec&gt;</b>     | Specify the time between 2 and 5 seconds.<br>polling_interval and fail_period are not allowed to set the same value. |
| <b>ring_guard_port</b>     | (Option) Specify the ring guard function state. The factory default is "disable".                                    |
| <b>primary</b>             | Specify to enable the ring guard and set the target port to primary port.                                            |
| <b>secondary</b>           | Specify to enable the ring guard and set the target port to secondary port.                                          |
| <b>both</b>                | Specify to enable the ring guard and set the target port to primary and secondary port.                              |
| <b>disable</b>             | Specify to disable the ring guard.                                                                                   |

## 70. Ring Redundant Protocol (RRP) Commands

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To create the “pc-ring” domain settings to node type=Transit, control VLAN=30, primary port=9, secondary port=10, data VLAN=1, polling interval=1, and fail period=2:

```
Zxxx0:admin# create rrp domain pc-ring type transit control_vlan_id 30 primary_port 9 secondary_port 10 data_vlan_id 1 polling_interval 1 fail_period 2
Command: create rrp domain pc-ring type transit control_vlan_id 30 primary_port 9 secondary_port 10 data_vlan_id 1 polling_interval 1 fail_period 2

Success.

Zxxx0:admin#
```

## 70.3. delete rrp domain

---

### ● Description

This command is used to delete the RRP domain.

### ● Format

delete rrp domain <domain name>

### ● Parameters

---

<domain name>  
Specify the RRP domain name to delete.

---

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To delete the “pc-ring” domain:

```
Zxxx0:admin# delete rrp domain pc-ring
Command: delete rrp domain pc-ring

Success.

Zxxx0:admin#
```

## 70.4. disable rrp

---

- **Description**

This command used to disable the global RRP function state. The factory default is disable.

- **Format**

disable rrp

- **Parameters**

None.

- **Restrictions**

Only Administrator and Operator-level users can issue this command.

- **Example**

To disable RRP function:

```
Zxxx0:admin# disable rrp
Command: disable rrp

Success.

Zxxx0:admin#
```

## 70.5. disable rrp domain

---

- **Description**

This command used to disable the specific RRP domain state.

- **Format**

disable rrp domain <domain name>

- **Parameters**

---

<domain name>  
Specify the RRP domain name to disable.

---

- **Restrictions**

Only Administrator and Operator-level users can issue this command.

## 70. Ring Redundant Protocol (RRP) Commands

### ● Example

To disable “pc-ring” domain state:

```
Zxxx0:admin# disable rrp domain pc-ring
Command: disable rrp domain pc-ring

Success.

Zxxx0:admin#
```

## 70.6. enable rrp

---

### ● Description

This command used to enable the global RRP function state. The factory default is disable.

### ● Format

enable rrp

### ● Parameters

None.

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To enable RRP function:

```
Zxxx0:admin# enable rrp
Command: enable rrp

Success.

Zxxx0:admin#
```

## 70.7. enable rrp domain

---

### ● Description

This command used to enable the specific RRP domain state.

### ● Format

enable rrp domain <domain name>

### ● Parameters

---

**<domain name>**

Specify the RRP domain name to enable.

---

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To enable the “pc-ring” domain state:

```
Zxxx0:admin# enable rrp domain pc-ring
Command: enable rrp domain pc-ring

Success.

Zxxx0:admin#
```

## 70.8. show rrp

---

### ● Description

This command is used to display the RRP settings.

### ● Format

show rrp

### ● Parameters

None.

### ● Restrictions

None.



## 70. Ring Redundant Protocol (RRP) Commands

### ● Example

To display the RRP settings:

```
Zxxx0:admin# show rrp
Command: show rrp

RRP Status : Enabled
Total Domain Number(s) : 1

Domain Name  Ctrl VLAN  Data VLAN(s)  Ring Status
-----
pc-ring      30          1             Link-Up

Zxxx0:admin#
```

## 70.9. show rrp status

---

### ● Description

This command is used to display the specific RRP domain settings.

### ● Format

**show rrp status <domain name>**

### ● Parameters

---

**<domain name>**  
Specify the RRP domain name to display.

---

### ● Restrictions

None.

## ● Example

To display “pc-ring” domain settings:

```
Zxxx0:admin# show rrp status pc-ring
Command: show rrp status pc-ring

RRP Domain Name      : pc-ring
RRP Domain Status    : Enabled
RRP Node Type        : Transit
RRP Ring Status      : Link-Up

Primary Port         : 10
Primary Port Status   : Forwarding
Primary Port Role     : Upstream

Secondary Port        : 11
Secondary Port Status : Forwarding
Secondary Port Role   : Downstream

Polling Interval     : 1
Fail Period          : 2

Ring Guard Port      : Disable

Control VLAN         : 30
Data VLAN(s)         : 1

Zxxx0:admin#
```

## 71. Routing Information Protocol (RIP) Command List

RIP is a function to determine packet destinations dynamically.

RIP exchanges routing tables with adjacent routers and determines a route based on the number of routers (hops) passed through to reach the destination.

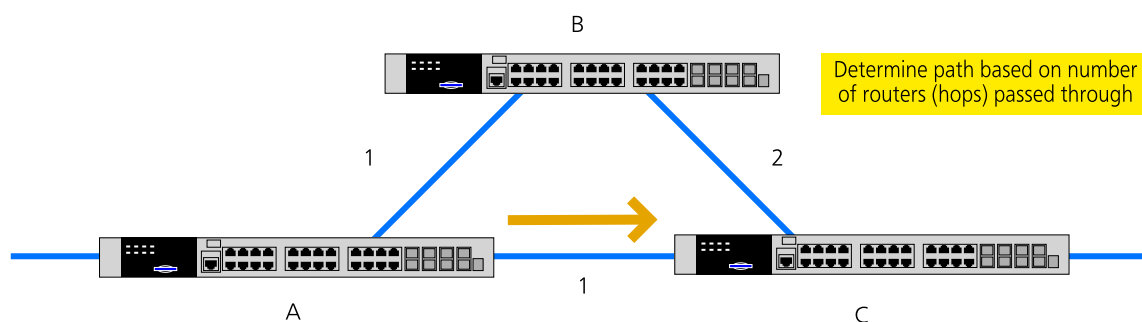


Figure 71-1 RIP overview

The maximum number of hops is approximately 15, and this function is useful in a relatively small-size network. In a large-size network, use a routing protocol such as OSPF (Open Shortest Path First).

```
enable rip
config rip [ipif <ipif_name 12> | all] {authentication [enable <password 16> | disable] | tx_mode
    [disable | v1_only | v1_compatible | v2_only] | rx_mode [v1_only | v2_only | v1_or_v2 |
    disable] | state [enable | disable]}(1)
config rip timers {update <sec 5-65535> | timeout <sec 5-65535> | garbage_collection <sec 5-
    65535>}
disable rip
show rip {ipif <ipif_name 12>}
```

### 71.1. enable rip

#### ● Description

This command is used to enable RIP for the Switching Hub. The default setting is disabled.

#### ● Format

```
enable rip
```

## ● Parameters

None.

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To enable RIP:

```
Zxxx0:admin# enable rip
Command: enable rip

Success.

Zxxx0:admin#
```

# 71.2. config rip

---

## ● Description

This command is used to configure the RIP settings for one or more IP interfaces.

## ● Format

**config rip [ipif <ipif\_name 12> | all] {authentication [enable <password 16> | disable] | tx\_mode [disable | v1\_only | v1\_compatible | v2\_only] | rx\_mode [v1\_only | v2\_only | v1\_or\_v2 | disable] | state [enable | disable]}(1)**

## ● Parameters

---

### ipif\_name

Specifies the IP interface name used for this configuration.

#### <ipif\_name 12>

Enter the IP interface name used here. This name can be up to 12 characters long.

**all** Specifies that all the IP interfaces will be used in this configuration.

---

### authentication

(Optional) Specifies to set the state of authentication.

#### enable

Specifies that the authentication state will be enabled.

#### <password 16>

When the authentication state is enabled, enter the password used here.  
This value can be up to 16 characters long.

#### disable

Specifies that the authentication state will be disabled.

---

## 71. Routing Information Protocol (RIP) Command List

---

**tx\_mode**(Optional) Specifies the RIP transmission mode.

**disable**

Specifies to prevent the transmission of RIP packets.

**v1\_only**

Specifies that only RIP version 1 format packets will be transmitted.

**v1\_compatible**

Specifies to transmit RIP version 2 format packets to the broadcast address.

**v2\_only**

Specifies that only RIP version 2 format packets will be transmitted.

---

**rx\_mode**(Optional) Specifies the RIP receive mode.

**v1\_only**

Specifies to receive RIP version 1 format packets to the RIP multicast address.

**v2\_only**

Specifies to receive RIP version 2 format packets to the RIP multicast address.

**v1\_or\_v2**

Specifies to receive both v1 and v2 packet.

**disable**

Specifies that the receiving of RIP packets will be prevented.

---

**state** (Optional) Specifies that the RIP state will be enabled or disabled. If the state is disabled, then RIP packets will not be either transmitted or received by the interface. The network configured on this interface will not be in the RIP database.

**enable**

Specifies that the RIP state will be enabled

**disable**

Specifies that the RIP state will be disabled.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To change the RIP receive mode for the IP interface System:

```
Zxxx0:admin# config rip ipif System rx_mode v1_only
Command: config rip ipif System rx_mode v1_only

Success.

Zxxx0:admin#
```

## 71.3. config rip timers

---

### ● Description

This command is used to configure RIP timers.

### ● Format

**config rip timers {update <sec 5-65535> | timeout <sec 5-65535> | garbage\_collection <sec 5-65535>}**

### ● Parameters

---

**update** (Optional) Specifies the value of the rate at which RIP updates are sent.  
**<sec 5-65535>**

Enter the update value used here. This value must be between 5 and 65535 seconds.

---

**timeout** (Optional) Specifies the value of the time after which a RIP route is declared to be invalid.  
**<sec 5-65535>**

Enter the timeout value used here. This value must be between 5 and 65535 seconds.

---

**garbage\_collection**

(Optional) Specifies the value of the time for which a RIP route will be kept before it is removed from routing table.

**<sec 5-65535>**

Enter the garbage collection value used here. This value must be between 5 and 65535 seconds.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the RIP timers on "System" interface:

```
Zxxx0:admin# config rip timers update 60 timeout 360 garbage_collection 240
Command: config rip timers update 60 timeout 360 garbage_collection 240

Success.

Zxxx0:admin#
```

## 71.4. disable rip

---

### ● Description

This command is used to disable RIP for the Switching Hub.

### ● Format

disable rip

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To disable RIP:

```
Zxxx0:admin# disable rip
Command: disable rip

Success.

Zxxx0:admin#
```

## 71.5. show rip

---

### ● Description

This command is used to display the RIP configuration for one or all the IP interfaces.

### ● Format

show rip {ipif <ipif\_name 12>}

### ● Parameters

---

|                |                                                                         |
|----------------|-------------------------------------------------------------------------|
| ipif           | (Optional) Specifies the IP interface name used for this configuration. |
| <ipif_name 12> |                                                                         |

---

Enter the IP interface name used here. This name can be up to 12 characters long.

If no parameter is specified, the system will display RIP configuration and statistics for all the IP interface.

## ● Restrictions

None.

## ● Example

To display RIP configuration and statistics for all IP interface.

```
Zxxx0:admin#show rip
Command: show rip

RIP Global State           : Enabled
Update Time                : 120 seconds
Timeout Time               : 300 seconds
Garbage Collection Time    : 150 seconds

RIP Interface Settings

Interface      IP Address      TX Mode    RX Mode      Authen-      State
-----
System        2.2.2.2/8        V1 Comp.   V1 or V2     Enabled      Disabled
n40           40.0.0.2/16      V1 Comp.   V1 or V2     Enabled      Enabled
n90           90.0.0.2/16      V1 Comp.   V1 or V2     Enabled      Enabled
n100          100.0.0.2/16     V1 Comp.   V1 or V2     Enabled      Enabled

Total Entries : 4

Zxxx0:admin#
```



## 72.RSPAN Commands

RSPAN (Remote Switched Port Analyzer) is a function to mirror receive packets to other Switching Hubs.

You need to configure the RSPAN VLAN source setting on the packet source (source Switching Hub) and the RSPAN VLAN redirect setting on a Switching Hub which relays mirror packets.

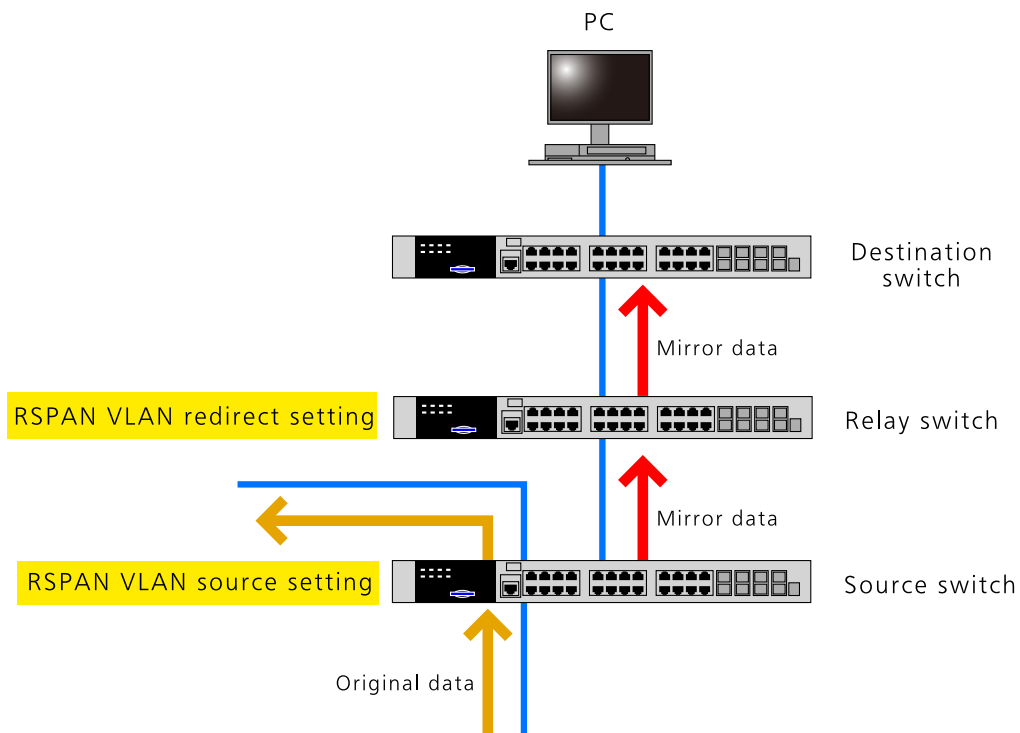


Figure 72-1 RSPAN overview

```
enable rspan
disable rspan
create rspan vlan [vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]
delete rspan vlan [vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]
config rspan vlan [vlan_name <vlan_name> | vlan_id <vlanid 1-4094>] [redirect [add | delete]
    ports <portlist> | source {[mirror_group_id <value 1-4> | [add | delete] ports <portlist> [rx |
    tx | both]]}]
show rspan {[vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]}
```

## 72.1. enable rspan

---

- **Description**

This command is used to enable RSPAN globally.

- **Format**

enable rspan

- **Parameters**

None.

- **Restrictions**

Only Administrator and Operator-level users can issue this command.

- **Example**

To enable RSPAN globally:

```
Zxxx0:admin#enable rspan
Command: enable rspan

Success.

Zxxx0:admin#
```

## 72.2. disable rspan

---

- **Description**

This command is used to disable RSPAN globally.

- **Format**

disable rspan

- **Parameters**

None.

- **Restrictions**

Only Administrator and Operator-level users can issue this command.

## 72. RSPAN Commands

### ● Example

To disable the RSPAN globally:

```
Zxxx0:admin#disable rspan
Command: disable rspan

Success.

Zxxx0:admin#
```

## 72.3. create rspan vlan

---

### ● Description

This command is used to create an RSPAN VLAN. Up to 16 RSPAN VLANs can be created.

### ● Format

**create rspan vlan [vlan\_name <vlan\_name> | vlan\_id <vlanid 1-4094>]**

### ● Parameters

---

**vlan\_name**

Create the RSPAN VLAN by VLAN name.

**<vlan\_name>**

Specify the VLAN name.

---

**vlan\_id** Create the RSPAN VLAN by VLAN ID.

**<vlanid 1-4094>**

Specify the VLAN ID between 1 and 4094.

---

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To create an RSPAN VLAN entry by VLAN name "v2":

```
Zxxx0:admin#create rspan vlan vlan_name v2
Command: create rspan vlan vlan_name v2

Success.

Zxxx0:admin#
```

To create an RSPAN VLAN entry by VLAN ID "3":

```
Zxxx0:admin#create rspan vlan vlan_id 3
Command: create rspan vlan vlan_id 3

Success.

Zxxx0:admin#
```

## 72.4. delete rspan vlan

---

### ● Description

This command is used to delete an RSPAN VLAN.

### ● Format

**delete rspan vlan [vlan\_name <vlan\_name> | vlan\_id <vlanid 1-4094>]**

### ● Parameters

---

#### **vlan\_name**

Specify the RSPAN VLAN by VLAN name.

**<vlan\_name>**

Specify the VLAN name.

---

#### **vlan\_id**

Specify the RSPAN VLAN by VLAN ID.

**<vlanid 1-4094>**

Specify the VLAN ID between 1 and 4094.

---

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To delete an RSPAN VLAN entry by VLAN name "v2":

```
Zxxx0:admin#delete rspan vlan vlan_name v2
Command: delete rspan vlan vlan_name v2

Success.

Zxxx0:admin#
```

To delete an RSPAN VLAN entry by VLAN ID "3":

## 72. RSPAN Commands

```
Zxxx0:admin#delete rspan vlan vlan_id 3
Command: delete rspan vlan vlan_id 3

Success.

Zxxx0:admin#
```

### 72.5. config rspan vlan

---

#### ● Description

This command is used by the source Switching Hub to configure the source setting for the RSPAN VLAN. The redirect command is used by the intermediate or last Switching Hub to configure the output port of the RSPAN VLAN packets, and makes sure that the RSPAN VLAN packets can egress to the redirect ports. In addition, the VLAN setting must be correctly configured to make the RSPAN VLAN work correctly. That is, for the intermediate Switching Hub, the redirect port must be a tagged member port of the RSPAN VLAN. For the last Switching Hub, the redirect port must be either a tagged member port or an untagged member port of the RSPAN VLAN based on the users' requirements. If untagged membership is specified, the RSPAN VLAN tag will be removed. The redirect function will only work when RSPAN is enabled. Multiple RSPAN VLANs can be configured with the redirect setting at the same time.

A RSPAN VLAN can be configured with the source setting and the redirect setting at the same time.

#### ● Format

**config rspan vlan** [**vlan\_name** <vlan\_name> | **vlan\_id** <vlanid 1-4094>] [**redirect** [add | delete] **ports** <portlist> | **source** {[**mirror\_group\_id** <value 1-4> | [add | delete] **ports** <portlist> [rx | tx | both]]}]

#### ● Parameters

|                  |                                                                                                                                                                                                                                                                            |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan_name</b> | Specify the RSPAN VLAN by VLAN name.<br><b>&lt;vlan_name&gt;</b><br>Specify the VLAN name.                                                                                                                                                                                 |
| <b>vlan_id</b>   | Specify the RSPAN VLAN by VLAN ID.<br><b>&lt;vlanid 1-4094&gt;</b><br>Specify the VLAN ID between 1 and 4094.                                                                                                                                                              |
| <b>redirect</b>  | Specify output port list for the RSPAN VLAN packets. If the redirect port is a Link Aggregation port, the Link Aggregation behavior will apply to the RSPAN packets.<br><b>add</b> Specify to add the redirect port.<br><b>delete</b> Specify to delete the redirect port. |
| <b>ports</b>     | Specify the output port list to add to or delete from the RSPAN packets.<br><b>&lt;portlist&gt;</b><br>Specify a range of ports to be configured.                                                                                                                          |

|                        |                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>source</b>          | If the ports are not specified by this command, the source of RSPAN will come from the source specified by the mirror command or the flow-based source specified by an ACL. If no parameter is specified for source, it deletes the configured source parameters.                                                                                                      |
| <b>mirror_group_id</b> | The mirror group identify that specify which mirror session used for RSPAN source function. If the mirror group is not specified when configuring the mirror ports, the mirror group 1 will be the default group.<br><b>&lt;value 1-4&gt;</b><br>Enter the mirror group ID value here. This value must be between 1 and 4.                                             |
| <b>add</b>             | (Optional) Specify to add source ports.                                                                                                                                                                                                                                                                                                                                |
| <b>delete</b>          | (Optional) Specify to delete source ports.                                                                                                                                                                                                                                                                                                                             |
| <b>ports</b>           | (Optional) Specify source port list to add to or delete from the RSPAN source.<br><b>&lt;portlist&gt;</b><br>Specify a range of ports to be configured.<br><b>rx</b> (Optional) Specify to only monitor ingress packets.<br><b>tx</b> (Optional) Specify to only monitor egress packets.<br><b>both</b> (Optional) Specify to monitor both ingress and egress packets. |

## ● Restrictions

Only Administrator and Operator-level users can issue this command.

## ● Example

To configure an RSPAN source entry without source target port:

```
Zxxx0:admin#config rspan vlan vlan_name vlan2 source add ports 2-5 rx
Command: config rspan vlan vlan_name vlan2 source add ports 2-5 rx

Success.

Zxxx0:admin#
```

To configure an RSPAN source entry for per flow RSPAN, without any source ports:

```
Zxxx0:admin#config rspan vlan vlan_id 2 source
Command: config rspan vlan vlan_id 2 source

Success.

Zxxx0:admin#
```

To configure RSPAN redirect for "VLAN 2" to ports 18 and 19:

```
Zxxx0:admin#config rspan vlan vlan_name vlan2 redirect add ports 18-19
Command: config rspan vlan vlan_name vlan2 redirect add ports 18-19

Success.

Zxxx0:admin#
```

## 72.6. show rspan

---

### ● Description

This command is used to display RSPAN configuration.

### ● Format

**show rspan** {[vlan\_name <vlan\_name> | vlan\_id <vlanid 1-4094>]}

### ● Parameters

---

**vlan\_name**

Specify the RSPAN VLAN by VLAN name.

**<vlan\_name>**

Specify the VLAN name.

---

**vlan\_id** Specify the RSPAN VLAN by VLAN ID.

**<vlanid 1-4094>**

Specify the VLAN ID between 1 and 4094.

---

### ● Restrictions

None.

### ● Example

To display specific RSPAN settings:

```
Zxxx0:admin# show rspan vlan_id 63
Command: show rspan vlan_id 63
RSPAN   : Enabled

RSPAN VLAN ID : 63
-----
Mirror Group ID : 1
Target Port     : 1:1
Source Ports
RX              : 1:2-1:5
TX              : 1:2-1:5
Redirect Ports  : 1:9-1:12

Total RSPAN VLAN : 1
Zxxx0:admin#
```

To display all RSPAN settings:

```
Zxxx0:admin# show rspan
Command: show rspan

RSPAN: Enabled

RSPAN VLAN ID: 1
-----
Mirror Group ID   : 1
Target Port       : 1:1
Source Ports
                  RX:
                  TX:

RSPAN VLAN ID: 2
-----
Redirect Ports    : 1:6-1:10

RSPAN VLAN ID: 3
-----
Redirect Ports    : 1:6-1:10

Total RSPAN VLAN :3
Zxxx0:admin#
```



## 73. SNMPv1/v2/v3 Commands

SNMP (Simple Network Management Protocol) is a protocol to monitor and manage network-connected devices via network. Target devices have a management information database called MIB (Management Information Base). SNMP monitors and controls them through access to their MIBs using an external management manager.

In this chapter, you will configure the management settings for a SNMP group (SNMP community) comprising the management manager and management targets (agents).

SNMP has different versions such as v1/v2c/v3. This Switching Hub supports all versions.

---

```

create snmp user <user_name 32> <groupname 32> { encrypted [by_password auth [sha
    <auth_password 8-20>] priv [none | des <priv_password 8-16>] | by_key auth [sha <auth_key
    40-40>] priv [none | des <priv_key 32-32>]]}
delete snmp user <user_name 32>
show snmp user
show snmp groups
create snmp view <view_name 32> <oid> view_type [included | excluded]
delete snmp view <view_name 32> [all | <oid>]
show snmp view {<view_name 32>}
create snmp community <community_string 32> view <view_name 32> [read_only | read_write]
delete snmp community <community_string 32>
show snmp community {<community_string 32>}
create snmp community_masking view <view_name 32> [read_only | read_write]
config snmp engineID <snmp_engineID 10-64>
show snmp engineID
create snmp group <groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]]
    {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name
    32>}(1)
delete snmp group <groupname 32>
create snmp [host <ipaddr> | v6host <ipv6addr>] [v1 | v2c | v3 [noauth_nopriv | auth_nopriv |
    auth_priv]] <auth_string 32>
delete snmp [host <ipaddr> | v6host <ipv6addr>]
show snmp v6host {<ipv6addr>}
show snmp host {<ipaddr>}
enable community_encryption
disable community_encryption
show community_encryption

```

---

## 73.1. create snmp user

### ● Description

This command is used to create a new user to an SNMP group originated by this command. Users can choose input authentication and privacy by password or by key.

### ● Format

```
create snmp user <user_name 32> <groupname 32> {encrypted [by_password auth [sha
<auth_password 8-20>] priv [none | des <priv_password 8-16>] | by_key auth [sha
<auth_key 40-40>] priv [none | des <priv_key 32-32>]]}
```

### ● Parameters

|                             |                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;user_name 32&gt;</b> | Specify the name of the user on the host that connects to the agent. The range is 1 to 32 characters.                                                                                                                                                                                                                                 |
| <b>&lt;groupname 32&gt;</b> | Specify the name of the group to which the user is associated. The range is 1 to 32 characters.                                                                                                                                                                                                                                       |
| <b>encrypted</b>            | (Optional) Specify whether the password appears in encrypted format.                                                                                                                                                                                                                                                                  |
| <b>by_password auth</b>     | Indicate the input password for authentication                                                                                                                                                                                                                                                                                        |
| <b>md5</b>                  | Specify the HMAC-MD5-96 authentication level between 8 and 16 characters.<br><b>&lt;auth_password 8-20&gt;</b><br>Specify the HMAC-MD5-96 authentication level between 8 and 16 characters.                                                                                                                                           |
| <b>sha</b>                  | Specify the HMAC-SHA-96 authentication level between 8 and 20 characters.<br><b>&lt;auth_password 8-20&gt;</b><br>Specify the HMAC-SHA-96 authentication level between 8 and 20 characters.                                                                                                                                           |
| <b>priv</b>                 | Indicate the input password for privacy. The options are none and DES.<br><b>none</b> Specify there will be no privacy string.<br><b>des</b> Specify a privacy string used by DES between 8 and 16 characters.<br><b>&lt;priv_password 8-16&gt;</b><br>Specify a privacy string used by DES between 8 and 16 characters.              |
| <b>by_key auth</b>          | Indicate the input key for authentication.                                                                                                                                                                                                                                                                                            |
| <b>sha</b>                  | Specify an authentication key used by SHA1. This is a hex string type of 40 characters.<br><b>&lt;auth_key 40-40&gt;</b><br>Specify an authentication key used by SHA1. This is a hex string type of 40 characters.                                                                                                                   |
| <b>priv</b>                 | Indicate the input key for privacy. The options are none and DES.<br><b>none</b> Specify there will be no privacy key.<br><b>des</b> Specify a privacy key used by DES. This is a hex string type of 32 characters<br><b>&lt;priv_key 32-32&gt;</b><br>Specify a privacy key used by DES. This is a hex string type of 32 characters. |

### ● Restrictions

### 73. SNMPv1/v2/v3 Commands

Only Administrator-level users can issue this command.

### ● Example

To create a new user to an SNMP group originated by this command:

```
Zxxx0:admin#create snmp user manager MANAGER_group encrypted by_password auth sha
12345678 priv des 12345678
Command: create snmp user manager MANAGER_group encrypted by_password auth sha
12345678 priv des 12345678

Success.

Zxxx0:admin#
```

## 73.2. delete snmp user

---

### ● Description

This command is used to remove a user from an SNMP group and deletes the associated group in the SNMP group.

### ● Format

delete snmp user <user\_name 32>

### ● Parameters

---

<user\_name 32>

Specify the name of the user on the host to be deleted. The range is 1 to 32 characters.

---

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To delete an SNMP user:

```
Zxxx0:admin#delete snmp user manager
Command: delete snmp user manager

Success.

Zxxx0:admin#
```

## 73.3. show snmp user

---

### ● Description

This command is used to display information on each SNMP username in the group username table.

### ● Format

show snmp user

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display SNMP user information:

```
Zxxx0:admin#show snmp user
Command: show snmp user

Username                               Group Name                             VerAuthPriv
-----                               -
initial                               initial                                V3 NoneNone

Total Entries : 1

Zxxx0:admin#
```

## 73.4. show snmp groups

---

### ● Description

This command is used to display the names of groups on the Switching Hub, and the security model, level, and the status of the different views.

### ● Format

show snmp groups

### ● Parameters

None.

## ● Restrictions

None.

## ● Example

To display the names of the SNMP groups on the Switching Hub:

```
Zxxx0:admin#show snmp groups
Command: show snmp groups

Vacm Access Table Settings

Group      Name      : public
ReadView Name : CommunityView
WriteView Name :
Notify View Name : CommunityView
Security Model : SNMPv1
Security Level : NoAuthNoPriv

Group      Name      : public
ReadView Name : CommunityView
WriteView Name :
Notify View Name : CommunityView
Security Model : SNMPv2
Security Level : NoAuthNoPriv

Group      Name      : private
ReadView Name : CommunityView
WriteView Name : CommunityView
Notify View Name : CommunityView
Security Model : SNMPv2
Security Level : NoAuthNoPriv

Total Entries: 3

Zxxx0:admin#
```

## 73.5. create snmp view

---

### ● Description

This command is used to assign views to community strings to limit which MIB objects an SNMP manager can access.

### ● Format

**create snmp view <view\_name 32> <oid> view\_type [included | excluded]**

## 73. SNMPv1/v2/v3 Commands

### ● Parameters

---

**<view\_name 32>**

Specify the view name to be created.

---

**<oid>** Specify the object-identified tree (the MIB tree).

---

**view\_type**

Specify the access type of of the MIB tree in this view.

---

**included** Specify to include this view.

---

**excluded** Specify to exclude this view.

---

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To assign views to community strings to limit which MIB objects an SNMP manager can access:

```
Zxxx0:admin#create snmp view managerview 1.3.6 view_type included
Command: create snmp view managerview 1.3.6 view_type included

Success.

Zxxx0:admin#
```

## 73.6. delete snmp view

---

### ● Description

This command is used to delete the view record.

### ● Format

**delete snmp view <view\_name 32> [all | <oid>]**

### ● Parameters

---

**<view\_name 32>**

Specify the view name of the user who will be deleted.

---

**all** Specify to view all records.

---

**<oid>** Specify the object-identified tree (the MIB tree).

---

### ● Restrictions

Only Administrator-level users can issue this command.

## ● Example

To remove a view record:

```
Zxxx0:admin#delete snmp view managerview all
Command: delete snmp view managerview all

Success.

Zxxx0:admin#
```

## 73.7. show snmp view

### ● Description

This command is used to display SNMP view records.

### ● Format

**show snmp view {<view\_name 32>}**

### ● Parameters

---

**<view\_name 32>**  
(Optional) Specify the view name of the user to be displayed.

---

### ● Restrictions

None.

## ● Example

To display SNMP view records:

```
Zxxx0:admin#show snmp view
Command: show snmp view

Vacm View Table Settings
View Name          Subtree                View Type
-----
restricted         1.3.6.1.2.1.1          Included
restricted         1.3.6.1.2.1.11         Included
restricted         1.3.6.1.6.3.10.2.1     Included
restricted         1.3.6.1.6.3.11.2.1     Included
restricted         1.3.6.1.6.3.15.1.1     Included
CommunityView      1                      Included
CommunityView      1.3.6.1.6.3            Excluded
CommunityView      1.3.6.1.6.3.1          Included

Total Entries: 8

Zxxx0:admin#
```



## 73.8. create snmp community

### ● Description

This command is used to create an SNMP community string. Use an SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the Switching Hub. You can specify one or more of the following characteristics associated with the string: A MIB view, which defines the subset of all MIB objects accessible to the given community; Read and write or read-only permission for the MIB objects accessible to the community.

### ● Format

**create snmp community** <community\_string 32> view <view\_name 32> [read\_only | read\_write]

### ● Parameters

|                                    |                                                                           |
|------------------------------------|---------------------------------------------------------------------------|
| <b>&lt;community_string 32&gt;</b> | Specify the community string. The maximum string length is 32 characters. |
| <b>view</b>                        | Specify the view name of the MIB. The maximum length is 32 characters.    |
| <b>&lt;view_name 32&gt;</b>        | Specify the view name of the MIB. The maximum length is 32 characters.    |
| <b>read_only</b>                   | Specify read-only permission.                                             |
| <b>read_write</b>                  | Specify read and write permission.                                        |

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To create an SNMP community string:

```
Zxxx0:admin#create snmp community manager view CommunityView read_write
Command: create snmp community manager view CommunityView read_write

Success.

Zxxx0:admin#
```

## 73.9. delete snmp community

---

### ● Description

This command is used to remove a specific community string.

### ● Format

delete snmp community <community\_string 32>

### ● Parameters

---

<community\_string 32>

Specify the community string that will be deleted.

---

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To delete an SNMP community:

```
Zxxx0:admin#delete snmp community manager
Command: delete snmp community manager

Success.

Zxxx0:admin#
```

## 73.10. show snmp community

---

### ● Description

This command is used to display community string configurations.

### ● Format

show snmp community {<community\_string 32>}

### ● Parameters

---

<community\_string 32>

(Optional) Specify the community string to be displayed.

---

## 73. SNMPv1/v2/v3 Commands

**NOTE** If a community string is not specified, all community string information will be displayed.

### ● Restrictions

None.

### ● Example

To display the current community string configurations:

```
Zxxx0:admin#show snmp community
Command: show snmp community

SNMP Community Table
Community Name          View Name              Access Right
-----
private                 CommunityView          read_write
public                  CommunityView          read_only

Total Entries : 2

Zxxx0:admin#
```

## 73.11. create snmp community\_masking view

### ● Description

This command is used to choose a security method for creating an SNMP community string, but the community string encrypted or not depends on the SNMP community encryption state.

If users use this command to create an SNMP community string, the community string that the user inputs will be displayed as "\*", and the user will have to double input (confirm) the SNMP community string when creating an SNMP community.

### ● Format

**create snmp community\_masking view <view\_name 32> [read\_only | read\_write]**

### ● Parameters

**<view\_name 32>**

Enter the MIB view name used here. This name can be up to 32 characters long.

**read\_only**

Specifies that the user, using the community string, will have read only access to the Switching Hub's SNMP agent.

**read\_write**

Specifies that the user, using the community string, will have read/write access to the Switching Hub's SNMP agent.

## ● Restrictions

Only Administrator-level users can issue this command.

## ● Example

To create an SNMP community string called "community123" with the "read\_only" security method:

```
Zxxx0:admin# create snmp community_masking view CommunityView read_only
Command: create snmp community_masking view CommunityView read_only

Enter a case-sensitive community:*****
Enter the community again for confirmation:*****

Success.

Zxxx0:admin#
```

# 73.12. config snmp engineID

## ● Description

This command is used to configure an identifier for the SNMP engine on the Switching Hub. Associated with each SNMP entity is a unique engine ID.

## ● Format

**config snmp engineID <snmp\_engineID 10-64>**

## ● Parameters

---

**<snmp\_engineID 10-64>**  
Specify the identify for the SNMP engine on the Switching Hub.

---

## ● Restrictions

Only Administrator-level users can issue this command.

## ● Example

To configure an identifier for the SNMP engine on the Switching Hub:

```
Zxxx0:admin#config snmp engineID 1023457890
Command: config snmp engineID 1023457890

Success.

Zxxx0:admin#
```

## 73.13. show snmp engineID

---

### ● Description

This command is used to display the identification of the SNMP engine on the Switching Hub.

### ● Format

**show snmp engineID**

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display the identification of an SNMP engine:

```
Zxxx0:admin#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 1023457890

Zxxx0:admin#
```

## 73.14. create snmp group

---

### ● Description

This command is used to create a new SNMP group.

### ● Format

**create snmp group <groupname 32> [v1 | v2c | v3 [noauth\_nopriv | auth\_nopriv | auth\_priv]] {read\_view <view\_name 32> | write\_view <view\_name 32> | notify\_view <view\_name 32>}(1)**

### ● Parameters

---

**<groupname 32>**

Specify the name of the group.

---

**v1** Specify the least secure of the possible security models.

---

**v2c** Specify the second least secure of the possible security models.

---

|                      |                                                                                                                                         |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <b>v3</b>            | Specify the most secure of the possible security models. Specifies authentication of a packet.                                          |
| <b>noauth_nopriv</b> | Specify to neither support packet authentication nor encrypting.                                                                        |
| <b>auth_nopriv</b>   | Specify to support packet authentication.                                                                                               |
| <b>auth_priv</b>     | Specify to support packet authentication and encrypting.                                                                                |
| <b>read_view</b>     | Specify the view name between 1 and 32 characters.<br><b>&lt;view_name 32&gt;</b><br>Specify the view name between 1 and 32 characters. |
| <b>write_view</b>    | Specify the view name between 1 and 32 characters.<br><b>&lt;view_name 32&gt;</b><br>Specify the view name between 1 and 32 characters. |
| <b>notify_view</b>   | Specify the view name between 1 and 32 characters.<br><b>&lt;view_name 32&gt;</b><br>Specify the view name between 1 and 32 characters. |

## ● Restrictions

Only Administrator-level users can issue this command.

## ● Example

To create a new SNMP group:

```
Zxxx0:admin#create snmp group MANAGER_group v3 auth_priv read_view
CommunityViewwrite_view CommunityView notify_view CommunityView
Command: create snmp group MANAGER_group v3 auth_priv read_view CommunityView
write_view CommunityView notify_view CommunityView

Success.

Zxxx0:admin#
```

## 73.15. delete snmp group

### ● Description

This command is used to remove an SNMP group.

### ● Format

**delete snmp group <groupname 32>**

## 73. SNMPv1/v2/v3 Commands

### ● Parameters

---

**<groupname 32>**

Specify the name of the group that will be deleted.

---

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To remove an SNMP group:

```
Zxxx0:admin#delete snmp group MANAGER_group
Command: delete snmp group MANAGER_group

Success.

Zxxx0:admin#
```

## 73.16. create snmp

---

### ● Description

This command is used to create a recipient of an SNMP operation.

### ● Format

**create snmp [host <ipaddr> | v6host <ipv6addr>] [v1 | v2c | v3 [noauth\_nopriv | auth\_nopriv | auth\_priv] ] <auth\_string 32>**

### ● Parameters

---

|                      |                                                                                                                                                                                 |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>host</b>          | Specify the IP address of the recipient for which the traps are targeted.<br><b>&lt;ipaddr&gt;</b><br>Specify the IP address of the recipient for which the traps are targeted. |
| <b>v6host</b>        | Specify the v6host IP address to which the trap packet will be sent.<br><b>&lt;ipv6addr&gt;</b><br>Specify the v6host IP address to which the trap packet will be sent.         |
| <b>v1</b>            | Specify the least secure of the possible security models.                                                                                                                       |
| <b>v2c</b>           | Specify the second least secure of the possible security models.                                                                                                                |
| <b>v3</b>            | Specify the most secure of the possible security models.                                                                                                                        |
| <b>noauth_nopriv</b> | Specify to neither support packet authentication nor encrypting.                                                                                                                |
| <b>auth_nopriv</b>   | Specify to support packet authentication.                                                                                                                                       |
| <b>auth_priv</b>     | Specify to support packet authentication and encrypting.                                                                                                                        |

---

**<auth\_string 32>**

Specify the authentication string. If v1 or v2 is specified, the auth\_string presents the community string, and it must be one of the entries in the community table. If v3 is specified, the auth\_string presents the user name, and it must be one of the entries in the user table.

## ● Restrictions

Only Administrator-level users can issue this command.

## ● Example

To create a recipient of an SNMP operation:

```
Zxxx0:admin#create snmp host 10.48.74.100 v3 noauth_nopriv initial
Command: create snmp host 10.48.74.100 v3 noauth_nopriv initial

Success.

Zxxx0:admin#
```

# 73.17. delete snmp

## ● Description

This command is used to delete a recipient of an SNMP trap operation.

## ● Format

**delete snmp** [host <ipaddr> | v6host <ipv6addr>]

## ● Parameters

|               |                                                                                  |
|---------------|----------------------------------------------------------------------------------|
| <b>host</b>   | Specify the IP address of the SNMP host recipient to be deleted.<br><ipaddr>     |
|               | Specify the IP address of the SNMP host recipient to be deleted.                 |
| <b>v6host</b> | Specify the IPv6 address of the SNMP host recipient to be deleted.<br><ipv6addr> |
|               | Specify the IPv6 address of the SNMP host recipient to be deleted.               |

## ● Restrictions

Only Administrator-level users can issue this command.

## ● Example

To delete a recipient of an SNMP trap operation:



## 73. SNMPv1/v2/v3 Commands

```
Zxxx0:admin#delete snmp host 10.48.74.100
Command: delete snmp host 10.48.74.100

Success.

Zxxx0:admin#
```

### 73.18. show snmp host

#### ● Description

This command is used to display the recipient for which the traps are targeted.

#### ● Format

show snmp host {<ipaddr>}

#### ● Parameters

---

<ipaddr>(Optional) Specify the IP address of the recipient for which the traps are targeted.

---

---

**NOTE** If no parameter is specified, all SNMP hosts will be displayed.

---

#### ● Restrictions

None.

#### ● Example

To display the recipient for which the traps are targeted:

```
Zxxx0:admin# show snmp host
Command: show snmp host

SNMP Host Table
Host IP Address  SNMP Version      Community Name / SNMPv3 User Name
-----
10.48.76.100    V3 noauthnopriv   initial
10.51.17.1      V2c               public

Total Entries : 2

Zxxx0:admin#
```

## 73.19. show snmp v6host

---

### ● Description

This command is used to display the recipient for which the traps are targeted.

### ● Format

**show snmp v6host {<ipv6addr>}**

### ● Parameters

---

**<ipv6addr>**  
(Optional) Specify the v6host IP address.

---



---

**NOTE** If no parameter is specified, all SNMP IPv6 hosts will be displayed.

---

### ● Restrictions

None.

### ● Example

To display the recipient for which the traps are targeted:

```
Zxxx0:admin# show snmp v6host
Command: show snmp v6host

SNMP Host Table
-----
Host IPv6 Address: FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
SNMP Version      : V3 na/np
Community Name/SNMPv3 User Name: 123456789101234567890

Host IPv6 Address: FEC0:1A49:2AA:FF:FE34:CA8F
SNMP Version      : V3 a/np
Community Name/SNMPv3 User Name: abcdefghijk

Total Entries : 2

Zxxx0:admin#
```

## 73.20. enable community\_encryption

---

### ● Description

This command is used to enable the encryption state on the SNMP community string.

### ● Format

`enable community_encryption`

### ● Parameters

None.

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To enable the encryption state on an SNMP community string:

```
Zxxx0:admin# enable community_encryption
Command: enable community_encryption

Success.

Zxxx0:admin#
```

When creating an SNMP community string after the encryption state has been enabled, the community string will be displayed as an encrypted string (six "\*"), otherwise displayed as plaintext, for example:

```
Zxxx0:admin# show snmp community
Command: show snmp community

SNMP Community Table
Community Name      View Name           Access Right
-----
*****             CommunityView       read_write
*****             CommunityView       read_only
private             CommunityView       read_write
public              CommunityView       read_only

Total Entries : 4

Zxxx0:admin#
```

## 73.21. disable community\_encryption

---

- **Description**

This command is used to disable the encryption state on the SNMP community string.

- **Format**

`disable community_encryption`

- **Parameters**

None.

- **Restrictions**

Only Administrator-level users can issue this command.

- **Example**

To disable the encryption state on the SNMP community string:

```
Zxxx0:admin# disable community_encryption
Command: disable community_encryption

Success.

Zxxx0:admin#
```

## 73.22. show community\_encryption

---

- **Description**

This command is used to display the encryption state on the SNMP community string.

- **Format**

`show community_encryption`

- **Parameters**

None.

- **Restrictions**

None.

- **Example**

To show the encryption state on the SNMP community string:

```
Zxxx0:admin# show community_encryption
Command: show community_encryption

SNMP Community Encryption State : Enabled

Zxxx0:admin#
```

## 74.Spanning Tree Protocol (STP) commands

### ● STP

STP (Spanning Tree Protocol) is a function to provide path redundancy while preventing loops in a network established by connecting multiple bridges. Even if one end of a communication route is down, the function can continue communications by detouring the route.

In general, if a cable is connected in a loop form, a phenomenon called broadcast storm, where frames keep looping permanently, occurs and causes the network to go down.

The STP function interchanges control frames called BPDU frames between Switching Hubs to calculate the shortest route. Automatic port blocking to prevent frames from looping allows you to establish a network which logically never has loops.

If a failure occurs on a route, the communication route can be recovered within 50 seconds or less.

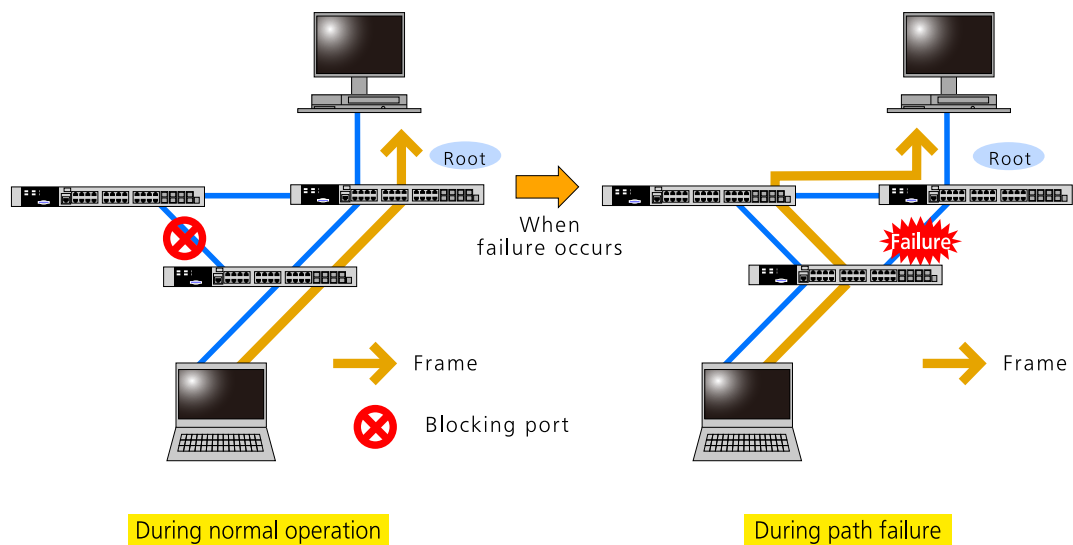


Figure 74-1 STP overview

### ● RSTP

RSTP (Rapid Spanning Tree Protocol) is a modified STP protocol to reduce recovery time to several seconds during a route failure.

When changing a route, the RSTP function determines port roles and changes the route immediately through information exchanges (proposal/agreement) between Switching Hubs instead of timers used in STP.

## 74. Spanning Tree Protocol (STP) commands

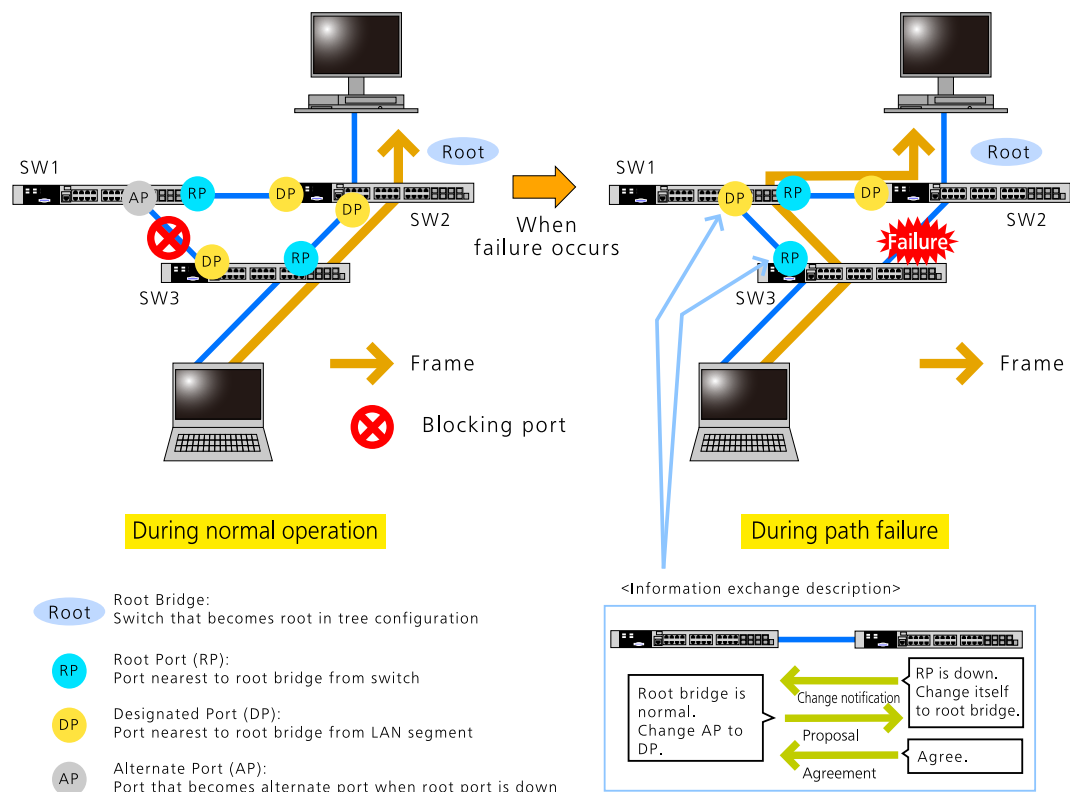


Figure 74-2 RSTP overview

### ● MSTP

MSTP (Multiple Spanning Tree Protocol) is also a modified STP protocol to communicate data for each VLAN using different routes. This allows for effective use of bandwidth.

Consolidating multiple VLANs into a group called instance can reduce more CPU loads compared to when designing a spanning tree instance for each VLAN.

The MSTP function allows for supporting a large-size network.

<Physical configuration>

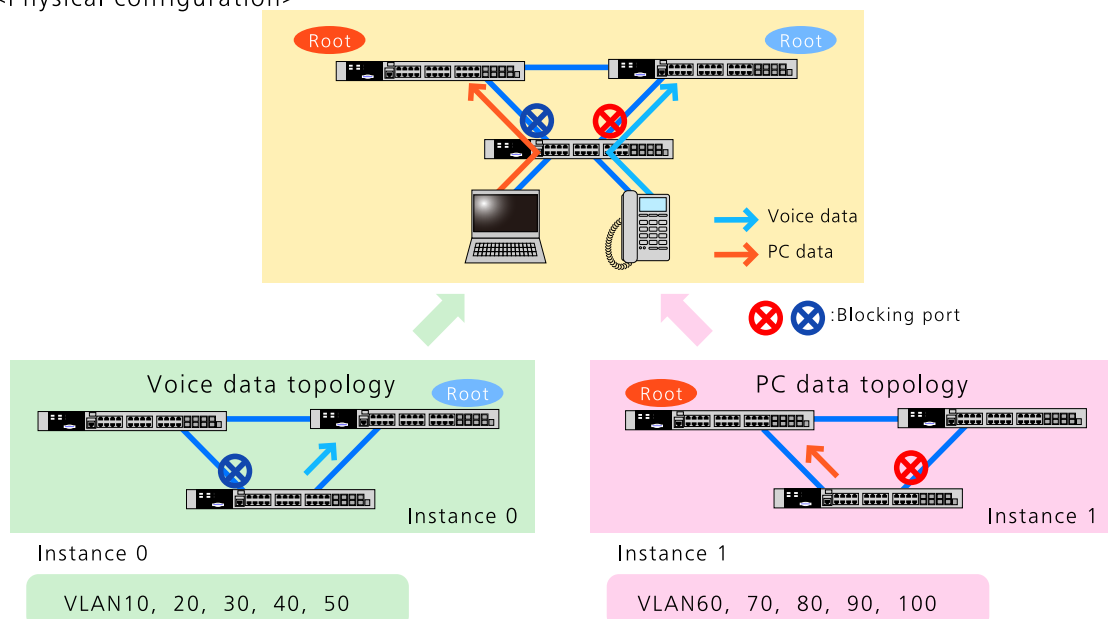


Figure 74-3 MSTP overview

---

```

show stp
show stp instance {<value 0-64>}
show stp ports {<portlist>}
show stp mst_config_id
create stp instance_id <value 1-64>
delete stp instance_id <value 1-64>
config stp instance_id <value 1-64> [add_vlan | remove_vlan] <vidlist>
config stp mst_config_id {revision_level <int 0-65535> | name <string>} (1)
enable stp
disable stp
config stp version [mstp | rstp | stp]
config stp priority <value 0-61440> instance_id <value 0-64>
config stp {maxage <value 6-40> | maxhops <value 6-40> | hellotime <value 1-2> | forwarddelay
    <value 4-30> | txholdcount <value 1-10> | fbpdu [enable | disable] | nni_bpdu_addr [dot1d |
    dot1ad]] (1)
config stp ports <portlist> {externalCost [auto | <value 1-2000000000>] | hellotime <value 1-2> |
    migrate [yes | no] | edge [true | false | auto] | p2p [true | false | auto] | state [enable |
    disable] | restricted_role [true | false] | restricted_tcn [true | false] | fbpdu [enable |
    disable]} (1)
config stp mst_ports <portlist> instance_id <value 0-64> {internalCost [auto | <value 1-
    2000000000>] | priority <value 0-240>}(1)

```

---

## 74.1. show stp

---

### ● Description

This command is used to display the bridge parameters global settings.

### ● Format

show stp

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display STP:



## 74. Spanning Tree Protocol (STP) commands

```
Zxxx0:admin#show stp
Command: show stp

STP Bridge Global Settings
-----
STP Status           : Enabled
STP Version          : MSTP
Max Age              : 20
Forward Delay        : 15
Max Hops             : 20
TX Hold Count        : 6
Forwarding BPDU      : Enabled
NNI BPDU Address     : dot1d

Zxxx0:admin#
```

### 74.2. show stp instance

---

#### ● Description

This command is used to display each instance parameters settings. Value means the instance ID, if there is no input of this value, all instances will be shown.

#### ● Format

**show stp instance {<value 0-64>}**

#### ● Parameters

---

**<value 0-64>**

(Optional) Specify the MSTP instance ID. Instance 0 represents the default instance: CIST.  
This value must be between 0 and 64.

---

#### ● Restrictions

None.

#### ● Example

To display STP instances:

```

Zxxx0:admin#show stp instance
Command: show stp instance

STP Instance Settings
-----
Instance Type           : CIST
Instance Status         : Enabled
Instance Priority        : 32768 (Bridge Priority : 32768, SYS ID Ext : 0 )

STP Instance Operational Status
-----
Designated Root Bridge : 32768/00-22-22-22-22-00
External Root Cost      : 0
Regional Root Bridge    : 32768/00-22-22-22-22-00
Internal Root Cost      : 0
Designated Bridge       : 32768/00-22-22-22-22-00
Root Port               : None
Max Age                 : 20
Forward Delay           : 15
Last Topology Change    : 2430
Topology Changes Count  : 0

Zxxx0:admin#

```

## 74.3. show stp ports

---

### ● Description

This command is used to display the Switching Hub's current per-port STP configuration:

STP port configuration, STP port role (Disabled, Alternate, Backup, Root, Designated, NonStp), and STP port status (Disabled, Discarding, Learning, Forwarding).

### ● Format

**show stp ports {<portlist>}**

### ● Parameters

---

**<portlist>**(Optional) Specify a range of ports to be displayed.

---

### ● Restrictions

None.

### ● Example

To show STP ports:

## 74. Spanning Tree Protocol (STP) commands

```
Zxxx0:admin#show stp ports
Command: show stp ports

MSTP Port Information
Port Index      : 1      , Hello Time      : 2 /2 , Port STP : enabled
External PathCost : Auto/200000 , Edge Port : No /No , P2P      : False/No
Port RestrictedRole : False, Port RestrictedTCN : False
Port Forward BPDU : Enabled

MSTI   Designated Bridge   Internal PathCost   Prio   Status   Role
-----
0      N/A                 200000              128    Disabled Disabled
2      N/A                 200000              128    Disabled Disabled

Zxxx0:admin#
```

### 74.4. show stp mst\_config\_id

#### ● Description

This command is used to display the three elements of the MST configuration Identification, including Configuration Name, Revision Level, and the MST configuration Table. The default Configuration name is the MAC address of the bridge. If two bridges have the same three elements in **mst\_config\_id**, that means they are in the same MST region.

#### ● Format

**show stp mst\_config\_id**

#### ● Parameters

None.

#### ● Restrictions

None.

#### ● Example

Display the STP MST Config ID:

```

Zxxx0:admin#show stp mst_config_id
Command: show stp mst_config_id

Current MST Configuration Identification
-----

Configuration Name : 00-22-22-22-22-00                      Revision Level :0
MSTI ID      Vid list
-----
CIST         1-4094

Zxxx0:admin#

```

## 74.5. create stp instance\_id

### ● Description

This command is used to create a new MST instance independent from the default Instance: CIST (Instance 0). After creating the MST instance, a user needs to configure the VLANs (using commands in 70-7), or the newly created MST instance will still be in a disabled state.

### ● Format

**create stp instance\_id <value 1-64>**

### ● Parameters

**<value 1-64>**

Specify the MSTP instance ID. Instance 0 represents a default instance CIST. This value must be between 1 and 64.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create an MSTP instance:

```

Zxxx0:admin#create stp instance_id 2
Command: create stp instance_id 2

Warning:There is no VLAN mapping to this instance_id!
Success.

Zxxx0:admin#

```

## 74.6. delete stp instance\_id

---

### ● Description

This command is used to delete the specified MST Instance. CIST (Instance 0) cannot be deleted and you can only delete one instance at a time.

### ● Format

**delete stp instance\_id <value 1-64>**

### ● Parameters

---

**<value 1-64>**

Specify the MSTP instance ID. Instance 0 represents the default instance CIST. This value must be between 1 and 64.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete an MSTP instance:

```
Zxxx0:admin#delete stp instance_id 2
Command: delete stp instance_id 2

Success.

Zxxx0:admin#
```

## 74.7. config stp instance\_id

---

### ● Description

There are two different action types to deal with an MST instance. They are listed as follows:

- 1) add\_vlan: To map specified VLAN lists to an existing MST instance.
- 2) remove\_vlan: To delete specified VLAN lists from an existing MST instance.

### ● Format

**config stp instance\_id <value 1-64> [add\_vlan | remove\_vlan] <vidlist>**

## ● Parameters

### <value 1-64>

Specify the MSTP instance ID. Instance 0 represents a default instance CIST. The DUT supports 65 instances (0-64) at most.

**add\_vlan** Defined action type to configure an MST instance.

### remove\_vlan

Defined action type to configure an MST instance.

**<vidlist>** Specify the newly added CLI Value Type. It is similar to **<portlist>** type, but the value range is 1 to 4094.

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To map a VLAN ID to an MSTP instance:

```
Zxxx0:admin#config stp instance_id 2 add_vlan 1
Command: config stp instance_id 2 add_vlan 1

Success.

Zxxx0:admin#
```

To remove a VLAN ID from an MSTP instance:

```
Zxxx0:admin#config stp instance_id 2 remove_vlan 2
Command: config stp instance_id 2 remove_vlan 2

Success.

Zxxx0:admin#
```

## 74.8. config stp mst\_config\_id

### ● Description

This command is used to configure a configuration name or revision level in the MST configuration identification. The default configuration name is the MAC address of the bridge.

### ● Format

**config stp mst\_config\_id {revision\_level <int 0-65535> | name <string>} (1)**

## 74. Spanning Tree Protocol (STP) commands

### ● Parameters

---

**revision\_level**

Specify the revision level.

<int 0-65535>

Specify the revision level.

---

**name** Specify the name given for a specified MST region.

<string>

Specify the name given for a specified MST region.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To change the name and revision level of the MST configuration identification:

```
Zxxx0:admin#config stp mst_config_id revision_level 1 name R&D_BlockG
Commands: config stp mst_config_id revision_level 1 name R&D_BlockG

Success.

Zxxx0:admin#
```

## 74.9. enable stp

---

### ● Description

Although it is possible to modify to allow a user to enable STP per instance, CIST should be enabled first before enabling other instances. When a user enables the CIST, all MSTIs will be enabled automatically if FORCE\_VERSION is set to MSTP and there is at least one VLAN mapped to this instance.

### ● Format

enable stp

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable STP:

```
Zxxx0:admin#enable stp
Command: enable stp

Success.

Zxxx0:admin#
```

### 74.10. disable stp

---

- **Description**

This command is used to disable STP functionality in every existing instance.

- **Format**

**disable stp**

- **Parameters**

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To disable STP:

```
Zxxx0:admin#disable stp
Command: disable stp

Success.

Zxxx0:admin#
```



## 74.11. config stp version

---

### ● Description

This command is used to enable STP globally. If the version is configured as STP or RSTP, all currently running MSTIs should be disabled. If the version is configured as MSTP, the current chip design is enabled for all available MSTIs (assuming that CIST is enabled).

### ● Format

**config stp version [mstp | rstp | stp]**

### ● Parameters

|             |                                                                   |
|-------------|-------------------------------------------------------------------|
| <b>mstp</b> | Specify to use Multiple Spanning Tree Protocol.                   |
| <b>rstp</b> | Specify to use Rapid Spanning Tree Protocol. This is the default. |
| <b>stp</b>  | Specify to use Spanning Tree Protocol.                            |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the STP version:

```
Zxxx0:admin#config stp version mstp
Command: config stp version mstp

Success.

Zxxx0:admin#
```

## 74.12. config stp priority

---

### ● Description

One of the parameters used to select the Root Bridge.

### ● Format

**config stp priority <value 0-61440> instance\_id <value 0-64>**

### ● Parameters

---

**<value 0-61440>**

Specify the bridge priority value, which must be divisible by 4096. The default value is 32768.

---

**instance\_id**

Specify the identifier value, which is used to distinguish different STP instances.

**<value 0-64>**

Specify the identifier value, which is used to distinguish different STP instances.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the STP instance ID:

```
Zxxx0:admin#config stp priority 61440 instance_id 0
Command: config stp priority 61440 instance_id 0

Success.

Zxxx0:admin#
```

## 74.13. config stp

---

### ● Description

This command is used to configure the bridge parameter global settings.

### ● Format

**config stp {maxage <value 6-40> | maxhops <value 6-40> | hellotime <value 1-2> | forwarddelay <value 4-30> | txholdcount <value 1-10> | fbpdu [enable | disable] | nni\_bpdu\_addr [dot1d | dot1ad]} (1)**

## 74. Spanning Tree Protocol (STP) commands

### ● Parameters

---

**maxage** Specify to determine if a BPDU is valid.

**<value 6-40>**

Specify to determine if a BPDU is valid. The default value is 20.

---

**maxhops** Specify to restrict the forwarded times of one BPDU.

**<value 6-40>**

Specify to restrict the forwarded times of one BPDU. The default value is 20.

---

**hellotime** Specify the time interval for sending Configuration BPDUs by the Root Bridge. This parameter is for STP and RSTP version. MSTP version uses per-port hellotime parameter.

**<value 1-2>**

Specify the time interval for sending Configuration BPDUs by the Root Bridge. This parameter is for STP and RSTP version. MSTP version uses per-port hellotime parameter. The default value is 2 seconds.

---

**forwarddelay**

Specify the maximum delay time for one BPDU to be transmitted by a bridge and received from another bridge.

**<value 4-30>**

Specify the maximum delay time for one BPDU to be transmitted by a bridge and received from another bridge. The default value is 15.

---

**txholdcount**

Specify to restrict the numbers of BPDU transmitted in a time interval (per Hello Time).

**<value 1-10>**

Specify to restrict the numbers of BPDU transmitted in a time interval (per Hello Time).

---

**fbpdu** To decide if the Bridge will flood STP BPDU when STP functionality is disabled.

**enable**

Specify to enable FBPDU.

**disable**

Specify to disable FBPDU.

---

**nni\_bpdu\_addr**

Specify to determine the BPDU protocol address for STP in service provide site. It can use 802.1d STP address, 802.1ad service provider STP address.

**dot1d**

Specify to use an 802.1d STP address.

**dot1ad**

Specify to use an 802.1ad service provider STP address.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure STP:

```
Zxxx0:admin# config stp maxage 25
Command: config stp maxage 25

Success.

Zxxx0:admin#
```

## 74.14. config stp ports

### ● Description

This command is used to configure all the parameters of ports, except for Internal Path Cost and Port Priority.

### ● Format

```
config stp ports <portlist> {externalCost [auto | <value 1-200000000> ] | hellotime
<value 1-2> | migrate [yes | no] | edge [true | false | auto] | p2p [true | false | auto] |
state [enable | disable] | restricted_role [true | false] | restricted_tcn [true | false] |
fbpdu [enable | disable ]} (1)
```

### ● Parameters

|                         |                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;portlist&gt;</b> | Specify a range of ports.                                                                                                                                                                                                                                                                                                                                                   |
| <b>externalCost</b>     | Specify the path cost between the MST regions from the transmitting Bridge to the CIST Root Bridge. It is only used at CIST level.<br><b>auto</b> Specify to automatically choose the path cost.<br><b>&lt;value 1-200000000&gt;</b> Specify a value between 1 and 200000000.                                                                                               |
| <b>hellotime</b>        | This is a per-Bridge parameter in RSTP, but it becomes a per-Port parameter in MSTP.<br><b>&lt;value 1-2&gt;</b> This is a per-Bridge parameter in RSTP, but it becomes a per-Port parameter in MSTP. The default value is 2.                                                                                                                                               |
| <b>migrate</b>          | Operation of management in order to specify the port to send MSTP BPDU for a delay time.<br><b>yes</b> Specify for port to send MSTP BPDU for a delay time.<br><b>no</b> Specify for port not to send MSTP BPDU for a delay time.                                                                                                                                           |
| <b>edge</b>             | Decide if this port is connected to a LAN or a Bridged LAN. In <b>auto</b> mode, the bridge will delay for a period to become edge port if no bridge BPDU is received.<br><b>true</b> Specify a true edge connection.<br><b>false</b> Specify a false edge connection.<br><b>auto</b> The bridge will delay for a period to become edge port if no bridge BPDU is received. |
| <b>p2p</b>              | Decide if this port is in Full-Duplex or Half-Duplex mode.<br><b>true</b> Specify full-duplex mode.<br><b>false</b> Specify half-duplex mode.<br><b>auto</b> The Switching Hub will automatically determine the P2P mode.                                                                                                                                                   |
| <b>state</b>            | Decide if this port supports the STP functionality.<br><b>enable</b> Enable to support STP functionality.<br><b>disable</b> Disable STP functionality support.                                                                                                                                                                                                              |
| <b>restricted_role</b>  | Decide if this port is to be selected as Root Port or not. The default value is false.<br><b>true</b> Decide that this port is not to be selected as Root Port.<br><b>false</b> Decide that this port is to be selected as Root Port.                                                                                                                                       |

## 74. Spanning Tree Protocol (STP) commands

---

### restricted\_tcn

Decide if this port is to propagate a topology change or not. The default value is false.

**true** Specify not to propagate a topology change.

**false** Specify to propagate a topology change.

---

### fbpdu

Decide if this port will flood STP BPDU when STP functionality is disabled.

**enable**

Enable port to flood STP BPDU when STP functionality is disabled.

**disable**

Disable port from flooding STP BPDU when STP functionality is disabled.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure STP ports:

```
Zxxx0:admin# config stp ports 1 externalCost auto
Command: config stp ports 1 externalCost auto

Success.

Zxxx0:admin#
```

## 74.15. config stp mst\_ports

---

## ● Description

Internal Path Cost and Port Priority of a Port in MSTI can be separately configured to different values from the configuration of CIST (instance ID = 0).

## ● Format

**config stp mst\_ports <portlist> instance\_id <value 0-64> {internalCost [auto | <value 1-200000000>] | priority <value 0-240>}(1)**

## ● Parameters

---

**<portlist>**Specify a range of ports.

---

### instance\_id

Specify an instance ID.

**<value 0-64>**

Instance = 0 represents CIST, Instance from 1 to 64 represents MSTI 1 to MSTI 64.

---

### internalCost

The Port Path Cost used in MSTP.

**auto** Specify to automatically determine the internal cost.

**<value 1-200000000>**

Specify a value between 1 and 200000000.

---

---

**priority** Specify the Port Priority.  
**<value 0-240>**  
Specify a value between 0 and 240.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure STP MST ports:

```
Zxxx0:admin# config stp mst_ports 1 instance_id 0 internalCost auto
Command: config stp mst_ports 1 instance_id 0 internalCost auto

Success.

Zxxx0:admin#
```

---

## 75.SSH Commands

---

SSH (Secure Shell) is a function to prevent spoofing and wiretapping by the authentication function and communication encryption. It allows you to remotely log in to this Switching Hub more safely than general Telnet access.

The commands are used to function this Switching Hub as an SSH server to be connected from SSH clients.

The following user authentication methods are supported.

- Password authentication (password)
- Public key authentication (publickey)
- Host-based authentication (hostbased)

You can configure the following settings as an encryption algorithm of messages exchanged between the server and clients.

- 3DES
- blowfish
- AES (128, 192, 256)
- arcfour
- cast128
- twofish (128, 192, 256)

---

```

config ssh algorithm [3DES | AES128 | AES192 | AES256 | arcfour | blowfish | cast128 |
    twofish128 | twofish192 | twofish256 | SHA1 | RSA | DSA] [enable | disable]
show ssh algorithm
config ssh authmode [password | publickey | hostbased] [enable | disable]
show ssh authmode
config ssh user <username 15> authmode [hostbased [hostname <domain_name 32> |
    hostname_IP <domain_name 32> [<ipaddr> | <ipv6addr>]] | password | publickey]
show ssh user authmode
config ssh server {maxsession <int 1-8> | contimeout <sec 120-600> | authfail <int 2-20> | rekey
    [10min | 30min | 60min | never] | port <tcp_port_number 1-65535>}(1)
enable ssh
disable ssh
show ssh server
  
```

---

## 75.1. config ssh algorithm

### ● Description

This command is used to configure the SSH service algorithm.

### ● Format

**config ssh algorithm** [3DES | AES128 | AES192 | AES256 | arcfour | blowfish | cast128 | twofish128 | twofish192 | twofish256 | SHA1 | RSA | DSA] [enable | disable]

### ● Parameters

|                              |                                                 |
|------------------------------|-------------------------------------------------|
| <b>3DES</b>                  | Specify an SSH server encryption algorithm.     |
| <b>blowfish</b>              | Specify an SSH server encryption algorithm.     |
| <b>AES(128,192,256)</b>      | Specify an SSH server encryption algorithm.     |
| <b>arcfour</b>               | Specify an SSH server encryption algorithm.     |
| <b>cast128</b>               | Specify an SSH server encryption algorithm.     |
| <b>twofish (128,192,256)</b> | Specify an SSH server encryption algorithm.     |
| <b>MD5</b>                   | Specify an SSH server data integrity algorithm. |
| <b>SHA1</b>                  | Specify an SSH server data integrity algorithm. |
| <b>DSA</b>                   | Specify an SSH server public key algorithm.     |
| <b>RSA</b>                   | Specify an SSH server public key algorithm.     |
| <b>enable</b>                | Specify to enable the algorithm.                |
| <b>disable</b>               | Specify to disable the algorithm.               |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable an SSH server public key algorithm:

```
Zxxx0:admin#config ssh algorithm DSA enable
Command: config ssh algorithm DSA enable

Success.

Zxxx0:admin#
```



## 75.2. show ssh algorithm

---

### ● Description

This command is used to display the SSH authentication algorithm.

### ● Format

show ssh algorithm

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To show the SSH server algorithms:

```
Zxxx0:admin#show ssh algorithm
Command: show ssh algorithm

Encryption Algorithm
-----
3DES      : Enabled
AES128    : Enabled
AES192    : Enabled
AES256    : Enabled
arcfour   : Enabled
blowfish  : Enabled
cast128   : Enabled
twofish128 : Enabled
twofish192 : Enabled
twofish256 : Enabled

Data Integrity Algorithm
-----
SHA1      : Enabled

Public Key Algorithm
-----
RSA       : Enabled
DSA       : Enabled

Zxxx0:admin#
```

## 75.3. config ssh authmode

---

### ● Description

This command is used to update the user authentication for SSH configuration.

### ● Format

**config ssh authmode** [password | publickey | hostbased] [enable | disable]

### ● Parameters

|                  |                                                    |
|------------------|----------------------------------------------------|
| <b>password</b>  | Specify the user authentication method.            |
| <b>publickey</b> | Specify the user authentication method.            |
| <b>hostbased</b> | Specify the user authentication method.            |
| <b>enable</b>    | Specify to enable the user authentication method.  |
| <b>disable</b>   | Specify to disable the user authentication method. |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the SSH user authentication method:

```
Zxxx0:admin#config ssh authmode publickey enable
Command: config ssh authmode publickey enable

Success.

Zxxx0:admin#
```

## 75.4. show ssh authmode

---

### ● Description

This command is used to display the user authentication methods.

### ● Format

**show ssh authmode**

## 75. SSH Commands

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display the SSH user authentication method:

```
Zxxx0:admin#show ssh authmode
Command: show ssh authmode

The SSH Authentication Method:
Password      : Enabled
Public Key    : Enabled
Host-based    : Enabled

Zxxx0:admin#
```

## 75.5. config ssh user

---

### ● Description

This command is used to update SSH user information.

### ● Format

**config ssh user <username 15> authmode [hostbased [hostname <domain\_name 32> | hostname\_IP <domain\_name 32> [<ipaddr> | <ipv6addr>]] | password | publickey]**

### ● Parameters

---

**<username 15>**

Specify the user name.

---

**authmode**

Specify the authentication mode.

---

---

**hostbased**

Specify the user authentication method.

**hostname**

Specify the host domain name.

**<domain\_name 32>**

Specify the host domain name. The hostname value can be up to 32 characters long.

**hostname\_IP**

Specify the host domain name and IP address.

**<domain\_name 32>**

Specify the host domain name. The hostname value can be up to 32 characters long.

**<ipaddr>**

Specify the host IPv4 address.

**<ipv6addr>**

Specifies the host IPv6 address.

---

**password**

Specify the user authentication method.

---

**publickey**

Specify the user authentication method.

---

## ● Restrictions

Only Administrator-level users can issue this command.

---

**NOTE** The user account must be created first.

---

## ● Example

To update user "danilo" in authentication mode:

```
Zxxx0:admin#config ssh user admin authmode publickey
Command: config ssh user admin authmode publickey

Success.

Zxxx0:admin#
```

## 75.6. show ssh user authmode

---

### ● Description

This command is used to display SSH user information.

### ● Format

show ssh user authmode

### ● Parameters

None.

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To show user information about SSH configuration:

```
Zxxx0:admin# show ssh user authmode
Command: show ssh user authmode

Current Accounts
User Name      Authentication      Host Name      Host IP
-----
test           Public Key
manager        Host-based          manager-local   172.18.61.180
beta           Host-based          beta-local      3000::105

Total Entries : 3

Zxxx0:admin#
```

## 75.7. config ssh server

---

### ● Description

This command is used to configure SSH server general information.

### ● Format

config ssh server {maxsession <int 1-8> | contimeout <sec 120-600> | authfail <int 2-20> | rekey [10min | 30min | 60min | never] | port <tcp\_port\_number 1-65535>}(1)

## ● Parameters

---

### **maxsession**

Specify the SSH server maximum session at the same time.

**<int 1-8>**

Specify the SSH server maximum session at the same time. The maximum session value must be between 1 and 8. The default value is 8.

---

### **contimeout**

Specify the SSH server connection timeout.

**<sec 120-600>**

Specify the SSH server connection timeout. The connection timeout value must be between 120 and 600 seconds. The default value is 120 seconds.

---

### **authfail** Specify the user maximum fail attempts.

**<int 2-20>**

Specify the user maximum fail attempts. The maximum authentication fail attempts must be between 2 and 20. The default value is 2.

---

### **rekey** (Optional) Specify the time to re-generate the session key.

**10min**

Specify 10 minutes to re-generate the session key.

**30min**

Specify 30 minutes to re-generate the session key.

**60min**

Specify 60 minutes to re-generate the session key.

**never** Do not re-generate the session key.

---

### **port** Specify a TCP port number between 1 and 65535.

**<tcp\_port\_number 1-65535>**

Specify a TCP port number between 1 and 65535.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure an SSH server maximum session of 3:

```
Zxxx0:admin#config ssh server maxsession 3
Command: config ssh server maxsession 3

Success.

Zxxx0:admin#
```

## 75.8. enable ssh

---

- **Description**

This command is used to enable SSH server services.

- **Format**

enable ssh

- **Parameters**

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To enable SSH:

```
Zxxx0:admin#enable ssh
Command: enable ssh

Success.

Zxxx0:admin#
```

## 75.9. disable ssh

---

- **Description**

This command is used to disable SSH server services.

- **Format**

disable ssh

- **Parameters**

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To disable SSH:

```
Zxxx0:admin#disable ssh
Command: disable ssh

Success.

Zxxx0:admin#
```

## 75.10. show ssh server

---

- **Description**

This command is used to display SSH server general information.

- **Format**

show ssh server

- **Parameters**

None.

- **Restrictions**

None.

- **Example**

To show SSH server:

```
Zxxx0:admin# show ssh server
Command: show ssh server

The SSH Server Configuration
Maximum Session           : 3
Connection Timeout        : 300
Authentication Fail Attempts : 2
Rekey Timeout              : 60min
TCP Port Number           : 22

Zxxx0:admin#
```

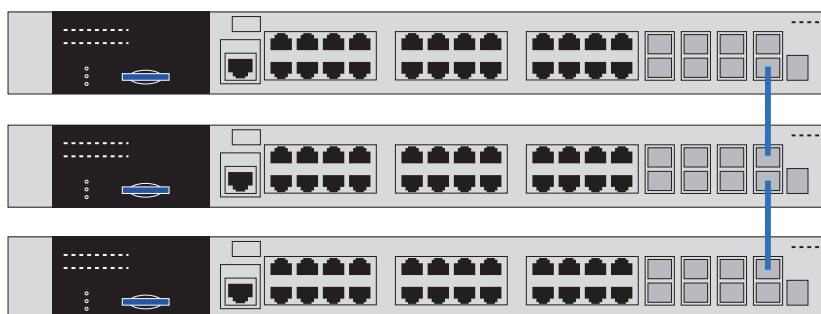


## 76. Stacking Commands

Stacking is a function to manage multiple Switching Hubs as one virtual Switching Hub. It is used to multiplex Switching Hubs for disaster planning. This Switching Hub supports a stack of up to four units.

Stacked devices are interconnected through stacking ports (port 27 and 28). Chain or ring type connection is available. It can also will stacking ZEQUO 6400 and ZEQUO 6500.

Chain topology



Ring topology

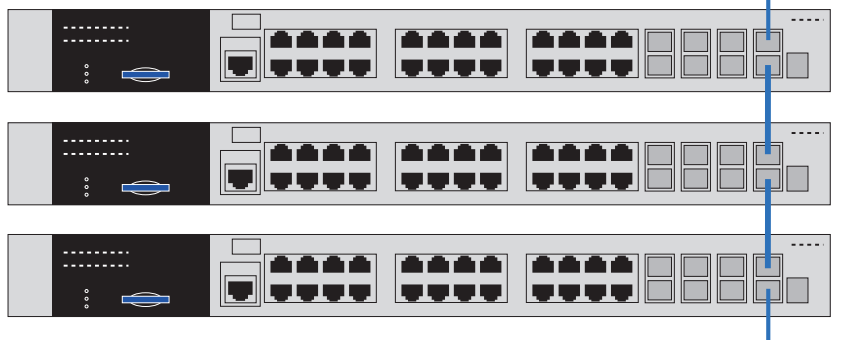


Figure 76-1 Chain or ring type stacking

Switches in a stack are divided into three roles: a Master box which controls the stacking, a Backup-Master box which operates in place of a failed Master box, and a Slave box which prepares even for a Backup-Master box failure. They are allocated based on the priority of each box specified in the stacking settings.

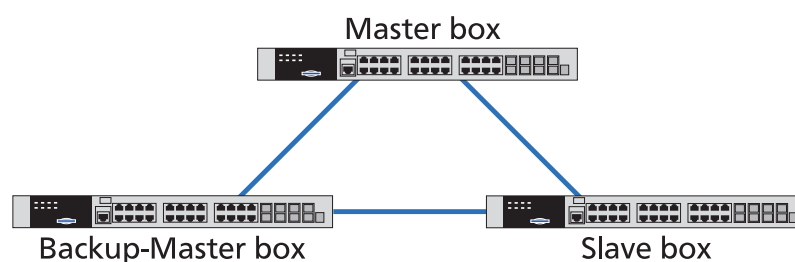


Figure 76-2 Stacking configuration

---

```

config stacking_mode [disable | enable]
config stacking_force_master_role state [enable | disable]
show stacking_mode
show stack_information
show stack_device
config box_id current_box_id <value 1-4> new_box_id [auto | <value 1-4>]
config box_priority current_box_id <value 1-4> priority <value 1-63>
config my_box_id [auto | <value 1-4>]
config my_box_priority <value 1-63>

```

---

## 76.1. config stacking\_mode

---

### ● Description

This command configures the state of stacking function. By default stacking mode is disabled. Administrators need to specifically configure the stacking mode to make the Switching Hub stackable. Stacking mode can be changed under standalone mode only!

### ● Format

```
config stacking_mode [disable | enable]
```

### ● Parameters

---

|                |                                                                   |
|----------------|-------------------------------------------------------------------|
| <b>enable</b>  | Specifies that the Switch's stacking capability will be enabled.  |
| <b>disable</b> | Specifies that the Switch's stacking capability will be disabled. |

---

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To enable stacking mode:

```

Zxxx0:admin# config stacking_mode enable
Command: config stacking_mode enable

Change Box stacking_mode may cause devices restart!
Please wait, the switch is rebooting...

```

---

**NOTE** The device will be rebooted immediately without the confirmation after executing this command, so please save the configuration first.

---

## 76.2. config stacking force\_master\_role state

### ● Description

This command is used to configure stacking force master role state. If state is enabled, when device is in election state, it still uses old priority setting and MAC to compare device priority. After stacking is stable, master's priority will become zero. If stacking topology change again, Master will use priority zero and MAC address to determine who new primary master is.

### ● Format

`config stacking force_master_role state [enable | disable]`

### ● Parameters

|                |                                                                                |
|----------------|--------------------------------------------------------------------------------|
| <b>enable</b>  | Specifies that the Switch's Stacking Force Master Role state will be enabled.  |
| <b>disable</b> | Specifies that the Switch's Stacking Force Master Role state will be disabled. |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable stacking force master role state:

```
Zxxx0:admin# config stacking force_master_role state enable
Command: config stacking force_master_role state enable

Success.

Zxxx0:admin#
```

## 76.3. show stacking\_mode

### ● Description

This command displays the current stacking mode.

### ● Format

`show stacking_mode`

### ● Parameters

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To display stacking mode:

```
Zxxx0:admin# show stacking_mode
Command: show stacking_mode

Stacking mode   : Enabled

Zxxx0:admin#
```

## **76.4. show stack\_information**

- **Description**

This command displays stacking information.

- **Format**

**show stack\_information**

- **Parameters**

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To display the stack information:

## 76. Stacking Commands

```
Zxxx0:admin# show stack_information
Command: show stack_information

Stack topology status:
New device is detected, hot insert may happen after 7 seconds.

Topology      :Duplex_Chain
My Box ID     :3
Master ID     :3
Box Count     :1
Force Master Role: Enable
```

| Box ID | User Set | Type      | Exist | Prio- rity | MAC               | Prom Version | Runtime Version | H/W Version |
|--------|----------|-----------|-------|------------|-------------------|--------------|-----------------|-------------|
| 1      | -        | Zxxx0     | No    |            |                   |              |                 |             |
| 2      | -        | NOT_EXIST | No    |            |                   |              |                 |             |
| 3      | User     | Zxxx0     | Exist | 1          | xx-xx-xx-xx-xx-xx | 1.0.0.xx     | 1.0.1.xx        | A1          |
| 4      | -        | Zxxx0     | No    |            |                   |              |                 |             |

```
Zxxx0:admin#
```

### 76.5. show stack\_device

#### ● Description

This command displays stack device information.

#### ● Format

**show stack\_device**

#### ● Parameters

None.

#### ● Restrictions

None.

#### ● Example

To display the stack information:

```
Zxxx0:admin# show stack_device
Command: show stack_device

Box ID      Box Type      H/W Version  Serial Number
-----
1           Zxxx0         A1
2           Zxxx0         A1

Zxxx0:admin#
```

## 76.6. config box\_id current\_box\_id

### ● Description

This command configures the box ID. By default, the box ID is automatically assigned by the system based topology election results. Administrators can assign box IDs statically. The new box ID will take effect after unit reboot. Each unit in the Switch stack must have a unique box IDs. If the IDs duplicate, the stack system cannot stack normally.

### ● Format

**config box\_id current\_box\_id <value 1-4> new\_box\_id [auto | <value 1-4>]**

### ● Parameters

---

**<value 1-3>** Enter the current box ID value used here. This value must be between 1 and 4.

---

**new\_box\_id**

Specifies the new ID assigned to the box.

**auto** Specifies that the box ID to be assigned automatically by the stack system. The new box ID will take effect after the next boot.

**<value 1-4>**

Enter the new box ID used here. This value must be between 1 and 4.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure box ID of box 1 to be auto:

```
Zxxx0:admin# config box_id current_box_id 1 new_box_id auto
Command: config box_id current_box_id 1 new_box_id auto

Success.

Zxxx0:admin#
```

## 76.7. `config box_priority current_box_id`

---

### ● Description

This command configures the priority of Switching Hub, which will determines which box becomes master. Lower number means higher priority. New priority will take effect after user reboot

### ● Format

`config box_priority current_box_id <value 1-4> priority <value 1-63>`

### ● Parameters

---

**<value 1-4>**

Enter the current box ID value used here. This value must be between 1 and 4.

---

**priority** Specifies the priority assigned to the box, with lower number meaning higher priority.  
**<value 1-63>**

Enter the priority value used here. This value must be between 1 and 63.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure box priority:

```
Zxxx0:admin# config box_priority current_box_id 1 priority 1
Command: config box_priority current_box_id 1 priority 1

Success.

Zxxx0:admin#
```

## 76.8. `config my_box_id`

---

### ● Description

This command is used to configure the box ID to the specified value for the local device. This configuration will take affect after the **save** command was issued and the Switching Hub was rebooted.

### ● Format

`config my_box_id [auto | <value 1-4>]`

### ● Parameters

---

**<value 1-4>**

Enter the box ID, manually, here. This value must be between 1 and 4.

---

**auto** Specify that the box ID will be assigned automatically.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the box ID of the Switching Hub to 2:

```
Zxxx0:admin# config my_box_id auto
Command: config my_box_id auto

Success.

Zxxx0:admin#
```

## 76.9. config my\_box\_priority

---

### ● Description

This command is used to configure the box priority to the specified value for the local device. This configuration will take affect after the **save** command was issued and the Switching Hub was rebooted.

### ● Format

**config my\_box\_priority <value 1-63>**

### ● Parameters

---

**<value 1-63>**

Enter the box priority value here. This value must be between 1 and 63.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.



## 76. Stacking Commands

### ● Example

To configure the box priority to 2:

```
Zxxx0:admin# config my_box_priority 1
Command: config my_box_priority 1

Success.

Zxxx0:admin#
```

## 77.Static MAC-based VLAN Commands

MAC-based VLAN is used to determine a VLAN to which a port belongs based on the source MAC address.

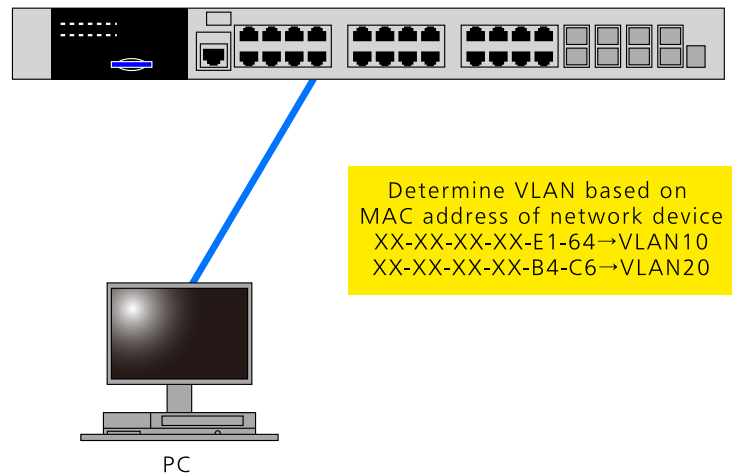


Figure 77-1 Static MAC-based Subnet VLAN overview

**NOTE** MAC-based VLAN and subnet VLAN can be used simultaneously. When using them simultaneously, you can configure which MAC-based VLAN or subnet VLAN function is prioritized.

```
create mac_based_vlan mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]
    {priority <value 0-7>}
delete mac_based_vlan {mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}
show mac_based_vlan {mac_address <macaddr> | [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}
```

### 77.1. create mac\_based\_vlan mac\_address

#### ● Description

This command is used to create static MAC-based VLAN entries.

#### ● Format

```
create mac_based_vlan mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] {priority <value 0-7>}
```

#### ● Parameters

**<macaddr>**  
Specify the MAC address.

## 77. Static MAC-based VLAN Commands

|                 |                                                                                                                                                                                                                                       |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vlan</b>     | Specify the VLAN to be associated with the MAC address. The name must be an existing static VLAN name.<br><b>&lt;vlan_name 32&gt;</b><br>Specify the VLAN name. The maximum length is 32 characters.                                  |
| <b>vlanid</b>   | Specify the VLAN ID to be associated with the MAC address. The ID must be an existing static VLAN ID.<br><b>&lt;vlanid 1-4094&gt;</b><br>Specify the VLAN ID between 1 and 4094.                                                      |
| <b>priority</b> | (Optional) Specifies the priority that is assigned to untagged packets. If not specified, the priority is the default value 0.<br><b>&lt;value 0-7&gt;</b><br>Enter the priority value used here. This value must be between 0 and 7. |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create a static MAC-based VLAN entry:

```
Zxxx0:admin#create mac_based_vlan mac_address 00-00-00-00-00-01 vlan default
Command: create mac_based_vlan mac_address 00-00-00-00-00-01 vlan default
Success.

Zxxx0:admin#
```

## 77.2. delete mac\_based\_vlan

### ● Description

This command is used to delete static MAC-based VLAN entries.

### ● Format

**delete mac\_based\_vlan {mac\_address <macaddr> [vlan <vlan\_name 32> | vlanid <vlanid 1-4094>]}**

### ● Parameters

|                    |                                                                                                                                                            |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mac_address</b> | (Optional) Specify the MAC address to be deleted.<br><b>&lt;macaddr&gt;</b><br>Specify the MAC address to be deleted.                                      |
| <b>vlan</b>        | (Optional) Specify the VLAN associated with the MAC address.<br><b>&lt;vlan_name 32&gt;</b><br>Specify the VLAN name. The maximum length is 32 characters. |
| <b>vlanid</b>      | (Optional) Specify the VLAN ID associated with the MAC address.<br><b>&lt;vlanid 1-4094&gt;</b><br>Specify the VLAN ID between 1 and 4094.                 |

---

**NOTE** If the MAC address and VLAN are not specified, all static entries associated with the port will be removed.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete a static MAC-based VLAN entry:

```
Zxxx0:admin#delete mac_based_vlan mac_address 00-00-00-00-00-01 vlan default
Command: delete mac_based_vlan mac mac_address 00-00-00-00-00-01 vlan default
Success.

Zxxx0:admin#
```

## 77.3. show mac\_based\_vlan

---

### ● Description

This command is used to display the MAC-based VLAN entries.

### ● Format

**show mac\_based\_vlan {mac\_address <macaddr> | [vlan <vlan\_name 32> | vlanid <vlanid 1-4094>]}**

### ● Parameters

---

**mac\_address**

(Optional) Specify the MAC address to be displayed.

**<macaddr>**

Specify the MAC address to be displayed.

---

**vlan**

(Optional) Specify the VLAN associated with the MAC address.

**<vlan\_name 32>**

Specify the VLAN name. The maximum length is 32 characters.

---

**vlanid**

(Optional) Specify the VLAN ID associated with the MAC address.

**<vlanid 1-4094>**

Specify the VLAN ID between 1 and 4094.

---

### ● Restrictions

None.

## 77. Static MAC-based VLAN Commands

### ● Example

In the following example, MAC address "00-80-c2-33-c3-45" is assigned to VLAN 300 by manual configuration. It is assigned to VLAN 400 by MAC-AC. Since MAC AC has higher priority than manual configuration, the manually configured entry will become inactive. To display the MAC-based VLAN entries:

```
Zxxx0:admin#show mac_based_vlan
```

| MAC Address       | VLAN ID | Status   | Type                     |
|-------------------|---------|----------|--------------------------|
| -----             | -----   | -----    | -----                    |
| 00-80-e0-14-a7-57 | 200     | Active   | Static                   |
| 00-80-c2-33-c3-45 | 300     | Inactive | Static                   |
| 00-80-c2-33-c3-45 | 400     | Active   | MAC_based Access Control |
| 00-a2-44-17-32-98 | 400     | Active   | WAC                      |

```
Total Entries : 4
```

```
Zxxx0:admin#
```

## 78.Subnet VLAN Commands

Subnet VLAN is used to determine a VLAN to which a port belongs based on the source IP address. Specify the IP address range with the subnet and map it with a VLAN.

This is available for both IPv4 and IPv6.

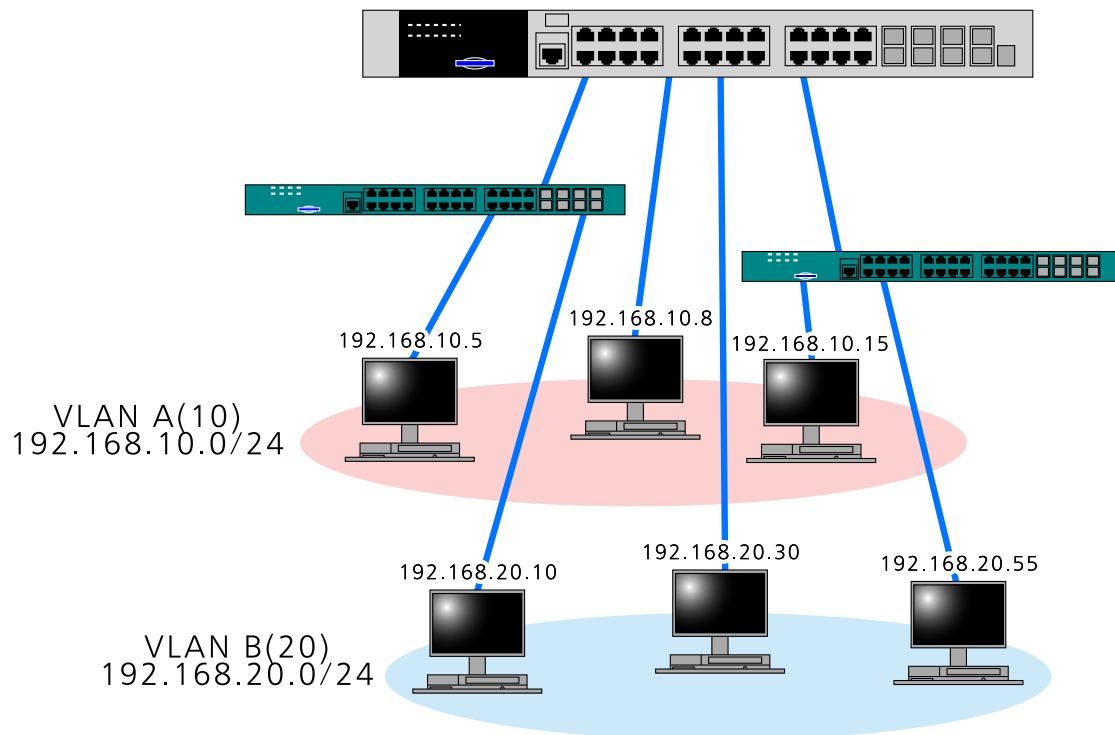


Figure 78-1 Subnet VLAN overview

**NOTE** MAC-based VLAN and subnet VLAN can be used simultaneously. When using them simultaneously, you can configure which MAC-based VLAN or subnet VLAN function is prioritized.

```
create subnet_vlan [network <network_address> | ipv6network <ipv6networkaddr>] [vlan
  <vlan_name 32> | vlanid <vlanid 1-4094>] {priority <value 0-7>}
delete subnet_vlan [network <network_address> | ipv6network <ipv6networkaddr> | vlan
  <vlan_name 32> | vlanid <vidlist> | all]
show subnet_vlan {[network <network_address> | ipv6network <ipv6networkaddr> | vlan
  <vlan_name 32> | vlanid <vidlist>]}
config vlan_precedence ports <portlist> [mac_based_vlan | subnet_vlan]
show vlan_precedence ports {<portlist>}
```

## 78.1. create subnet\_vlan

---

### ● Description

This command is used to create a subnet VLAN entry. A subnet VLAN entry is an IP subnet-based VLAN classification rule. If an untagged or priority-tagged IP packet is received on a port, its source IP address will be used to match the subnet VLAN entries. If the source IP is in the subnet of an entry, the packet will be classified to the VLAN defined for this subnet.

### ● Format

**create subnet\_vlan** [network <network\_address> | ipv6network <ipv6networkaddr>]  
[vlan <vlan\_name 32> | vlanid <vlanid 1-4094>] {priority <value 0-7>}

### ● Parameters

|                    |                                                                                                                                                                                                                       |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>network</b>     | Specify an IPv4 network address.<br><b>&lt;network_address&gt;</b><br>Specify an IPv4 network address. The format is ipaddress/prefix length.                                                                         |
| <b>ipv6network</b> | Specify an IPv6 network address.<br><b>&lt;ipv6networkaddr&gt;</b><br>Specify an IPv6 network address. The format is ipaddress/prefix length. The prefix length of IPv6 network address shall not be greater than 64. |
| <b>vlan</b>        | Specify a VLAN name to be associated with the subnet. The VLAN must be an existing static VLAN.<br><b>&lt;vlan_name 32&gt;</b><br>Specify a VLAN name. The maximum length is 32 characters.                           |
| <b>vlanid</b>      | Specify the VLAN ID to be associated with the subnet. The VLAN must be an existing static VLAN.<br><b>&lt;vlanid 1-4094&gt;</b><br>Specify the VLAN ID between 1 and 4094.                                            |
| <b>priority</b>    | (Optional) Specify the priority to be associated with the subnet.<br><b>&lt;value 0-7&gt;</b><br>(Optional) Specify the priority to be associated with the subnet. The range is 0 to 7.                               |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To create a subnet VLAN entry:

```
Zxxx0:admin#create subnet_vlan network 172.168.1.1/24 vlan v2 priority 2
Command: create subnet_vlan network 172.168.1.1/24 vlan v2 priority 2

Success.

Zxxx0:admin#
```

To create an IPv6 subnet VLAN entry:

```
Zxxx0:admin# create subnet_vlan ipv6network fe80:250:baff::0/64 vlan v2 priority 2
Command: create subnet_vlan ipv6network fe80:250:baff::0/64 vlan v2 priority 2

Success.

Zxxx0:admin#
```

## 78.2. delete subnet\_vlan

### ● Description

This command is used to delete a subnet VLAN from the Switching Hub. Users can delete a subnet VLAN entry by IP subnet or VLAN, or delete all subnet VLAN entries.

### ● Format

**delete subnet\_vlan** [**network** <network\_address> | **ipv6network** <ipv6networkaddr> | **vlan** <vlan\_name 32> | **vlanid** <vidlist> | **all**]

### ● Parameters

|                    |                                                                                                                                                     |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>network</b>     | Specify an IPv4 network address.<br><network_address><br>Specify an IPv4 network address. The format is ipaddress/prefix length.                    |
| <b>ipv6network</b> | Specify an IPv6 network address.<br><ipv6networkaddr><br>Specify an IPv6 network address. The format is ipaddress/prefix length.                    |
| <b>vlan</b>        | Specify to delete all subnet VLAN entries associated with this VLAN.<br><vlan_name 32><br>Specify a VLAN name. The maximum length is 32 characters. |
| <b>vlanid</b>      | Specify a list of VLANs by VLAN ID.<br><vidlist><br>Specify the VLAN ID.                                                                            |
| <b>all</b>         | Specify to delete all subnet VLAN entries.                                                                                                          |



## 78. Subnet VLAN Commands

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete a subnet VLAN entry:

```
Zxxx0:admin#delete subnet_vlan network 172.168.1.1/24
Command: delete subnet_vlan network 172.168.1.1/24

Success.

Zxxx0:admin#
```

To delete all subnet VLAN entries:

```
Zxxx0:admin#delete subnet_vlan all
Command: delete subnet_vlan all

Success.

Zxxx0:admin#
```

## 78.3. show subnet\_vlan

### ● Description

This command is used to display a subnet VLAN.

### ● Format

**show subnet\_vlan** {[network <network\_address> | ipv6network <ipv6networkaddr> | vlan <vlan\_name 32> | vlanid <vidlist>]}

### ● Parameters

|                    |                                                                                                                                                                              |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>network</b>     | (Optional) Specify an IPv4 network address.<br><b>&lt;network_address&gt;</b><br>Specify an IPv4 network address. The format is ipaddress/prefix length.                     |
| <b>ipv6network</b> | (Optional) Specify an IPv6 network address.<br><b>&lt;ipv6networkaddr&gt;</b><br>Specify an IPv6 network address. The format is ipaddress/prefix length.                     |
| <b>vlan</b>        | (Optional) Specify to display all subnet VLAN entries associated with this VLAN.<br><b>&lt;vlan_name 32&gt;</b><br>Specify a VLAN name. The maximum length is 32 characters. |
| <b>vlanid</b>      | (Optional) Specify a list of VLANs by VLAN ID.<br><b>&lt;vidlist&gt;</b><br>Specify the VLAN ID.                                                                             |

---

**NOTE** If no parameter is specified, all subnet VLAN information will be displayed.

---

## ● Restrictions

None.

## ● Example

To display a specified subnet VLAN entry:

```
Zxxx0:admin#show subnet_vlan network 172.168.1.1/24
Command: show subnet_vlan network 172.168.1.1/24

IP Address/Subnet Mask          VLAN      Priority
-----
172.168.1.0/255.255.255.0      10        2

Zxxx0:admin#
```

To display a specied IPv6 subnet VLAN entry:

```
Zxxx0:admin# show subnet_vlan ipv6network fe80:250:baff::0/64
Command: show subnet_vlan ipv6network FE80:250:BAFF::/64

IP Address/Subnet Mask          VLAN      Priority
-----
FE80:250:BAFF::/64             10        2

Zxxx0:admin#
```

To display all subnet VLAN entries:

```
Zxxx0:admin#show subnet_vlan
Command: show subnet_vlan

IP Address/Subnet Mask          VLAN      Priority
-----
172.18.211.0/255.255.255.0      20        3
172.168.1.0/255.255.255.0      10        2
FE80:250:BAFF::/64             10        2

Total Entries: 3

Zxxx0:admin#
```

## 78.4. config vlan\_precedence ports

---

### ● Description

This command is used to configure vlan classification precedence on each port. You can specify the order of MAC-based VLAN classification and subnet VLAN classification.

If a port's VLAN classification is MAC-based precedence, MAC-based VLAN classification will process at first. If MAC-based VLAN classification fails, the subnet VLAN classification will be executed.

If a port's VLAN classification is subnet VLAN precedence, the subnet VLAN classification will process at first. If subnet VLAN classification fails, the MAC-based VLAN classification will be executed.

### ● Format

**config vlan\_precedence ports <portlist> [mac\_based\_vlan | subnet\_vlan]**

### ● Parameters

---

**<portlist>** Enter a list of ports used for this configuration here.

---

**mac\_based\_vlan**

Specifies that the MAC-based VLAN classification is precedence than subnet VLAN classification

---

**subnet\_vlan**

Specifies that the subnet VLAN classification is precedence than MAC-based VLAN classification

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure subnet VLAN classification precedence on port 1:

```
Zxxx0:admin# config vlan_precedence ports 1 subnet_vlan
Command: config vlan_precedence ports 1 subnet_vlan

Success.

Zxxx0:admin#
```

## 78.5. show vlan\_precedence ports

---

### ● Description

This command is used to display the VLAN classification precedence.

### ● Format

show vlan\_precedence ports {<portlist>}

### ● Parameters

---

<portlist>(Optional) Specifies the list of ports used for this display.

---

### ● Restrictions

None.

### ● Example

To display VLAN classification precedence on ports 1-5:

```
Zxxx0:admin#show vlan_precedence ports 1:1-1:5
```

```
Command: show vlan_precedence ports 1:1-1:5
```

| Port | VLAN Precedence |
|------|-----------------|
| ---- | -----           |
| 1    | MAC-Based VLAN  |
| 2    | Subnet VLAN     |
| 3    | MAC-Based VLAN  |
| 4    | MAC-Based VLAN  |
| 5    | Subnet VLAN     |

```
Zxxx0:admin#
```

## 79. Switch Port Commands

Configure the following settings for each port of this Switching Hub.

- Port speed, flow control
- Auto-negotiation option
- Whether the MAC address learning is enabled or disabled
- MDI/MDIX settings
- Combo port media settings

---

```
config ports [<portlist> | all] {medium_type [fiber | copper]} {speed [auto {capability_advertised
{10_half | 10_full | 100_half | 100_full | 1000_full}} | 10_half | 10_full | 100_half |
100_full | 1000_full {[master | slave]}} | auto_negotiation [restart_an |
remote_fault_advertised [disable | offline | link_fault | auto_negotiation_error]] |
flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | mdix
[auto | normal | cross] | [description <desc 1-32> | clear_description]](1)
show ports [<portlist>] {[description | err_disabled | auto_negotiation | details | media_type]}
```

---

### 79.1. config ports

#### • Description

This command is used to change Switching Hub port settings.

#### • Format

```
config ports [<portlist> | all] {medium_type [fiber | copper]} {speed [auto
{capability_advertised {10_half | 10_full | 100_half | 100_full | 1000_full}} | 10_half |
10_full | 100_half | 100_full | 1000_full {[master | slave]}} | auto_negotiation
[restart_an | remote_fault_advertised [disable | offline | link_fault |
auto_negotiation_error]] | flow_control [enable | disable] | learning [enable |
disable] | state [enable | disable] | mdix [auto | normal | cross] | [description <desc 1-
32> | clear_description]](1)
```

#### • Parameters

---

**<portlist>** Specify a range of ports to be configured.

---

**all** Specify to set all ports in the system.

---

**medium\_type**

(Optional) Specify the medium type when configuring ports that are combo ports.

**fiber** Specify the fiber port.

**copper** Specify the copper port.

---

---

|                              |                                                                                                                                                                                                                       |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>speed</b>                 | Set port speed for the specified ports.                                                                                                                                                                               |
| <b>auto</b>                  | Set port speed to auto negotiation.                                                                                                                                                                                   |
| <b>capability_advertised</b> | Specifies that the capability will be advertised.                                                                                                                                                                     |
| <b>10_half</b>               | Set port speed to 10_half.                                                                                                                                                                                            |
| <b>10_full</b>               | Set port speed to 10_full.                                                                                                                                                                                            |
| <b>100_half</b>              | Set port speed to 100_half.                                                                                                                                                                                           |
| <b>100_full</b>              | Set port speed to 100_full.                                                                                                                                                                                           |
| <b>1000_full</b>             | Set port speed to 1000_full. When setting copper port speed to 1000_full, users should specify master and slave mode in pair for 1000-BASE TX, and leave the 1000_full without any master or slave setting for fiber. |
| <b>master</b>                | (Optional) Set to master.                                                                                                                                                                                             |
| <b>slave</b>                 | (Optional) Set to slave.                                                                                                                                                                                              |

---

|                                |                                                                                                                                                                                                                                                                                      |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>auto_negotiation</b>        | Specifies that the auto-negotiation option will be configured.                                                                                                                                                                                                                       |
| <b>restart_an</b>              | Specifies to restart the auto-negotiation process.                                                                                                                                                                                                                                   |
| <b>remote_fault_advertised</b> | Specifies that the remote fault advertisement option will be configured.                                                                                                                                                                                                             |
| <b>disable</b>                 | Specifies to disable remote fault advertisement.                                                                                                                                                                                                                                     |
| <b>offline</b>                 | Specifies that a local device may indicate Offline prior to powering off, running transmitter tests, or removing the local device from the active configuration. If it is set and detected offline, it will advertise at the next auto-negotiation. It interacted for 1000Mbps MAUs. |
| <b>link_fault</b>              | Specifies that if set and local device was detected, a Link_Failure condition indicated by the loss of synchronization, will advertise at the next auto-negotiation. It interacted for 1000Mbps MAUs.                                                                                |
| <b>auto_negotiation_error</b>  | Specifies the resolution which precludes operation between a local device and link partner advertised at the next auto-negotiation. It interacted for 1000Mbps MAUs.                                                                                                                 |

---

|                     |                                                                                                                                   |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <b>flow_control</b> | Turn on or turn off flow control on one or more ports by setting flow_control to enable or disable. The default value is disable. |
| <b>enable</b>       | Turn on flow control.                                                                                                             |
| <b>disable</b>      | Turn off flow control.                                                                                                            |

---

|                 |                                                                                             |
|-----------------|---------------------------------------------------------------------------------------------|
| <b>learning</b> | Turn on or turn off MAC address learning on one or more ports. The default value is enable. |
| <b>enable</b>   | Turn on MAC address learning.                                                               |
| <b>disable</b>  | Turn off MAC address learning.                                                              |

---

## 79. Switch Port Commands

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>state</b>       | Enable or disable the state of the specified port. If the ports are in error-disabled status, configuring their state to enable will recover these ports from a disabled to an enabled state. The default value is enable.<br><b>enable</b><br>Enable the specified port(s).<br><b>disable</b><br>Disable the specified port(s).                                                                                                                                                                                                                                                        |
| <b>mdix</b>        | Specify the type of cabling. The default value is auto.<br><b>auto</b> Select auto for auto sensing of the optimal type of cabling.<br><b>normal</b><br>Select normal for normal cabling. If set to normal state, the port is in MDI mode and can be connected to a PC NIC using a straight-through cable or a port (in MDI mode) on another Switching Hub through a cross-over cable.<br><b>cross</b> Select cross for cross cabling. If set to cross state, the port is in MDIX mode, and can be connected to a port (in MDI mode) on another Switching Hub through a straight cable. |
| <b>description</b> | (Optional) Describe the port interface.<br><b>&lt;desc 1-32&gt;</b><br>Describe the port interface.<br><b>clear_description</b><br>(Optional) Deletes the present description of the port interface.                                                                                                                                                                                                                                                                                                                                                                                    |

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To configure the speed of ports 1 to 3 to be 10 Mbps, with full duplex, learning enabled, state enabled, and flow control enabled:

```
Zxxx0:admin#config ports 1-3 speed 10_full state enable learning enable
flow_control enable
Command: config ports 1-3 speed 10_full state enable learning enable flow_control
enable

Success.

Zxxx0:admin#
```

# 79.2. show ports

## ● Description

This command is used to display the current configurations of a range of ports.

## ● Format

show ports {<portlist>} {[description | err\_disabled | auto\_negotiation | details | media\_type]}

## ● Parameters

|                  |                                                                                                                                                                                                                                                                                                                   |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <portlist>       | (Optional) Specify a range of ports to be displayed.                                                                                                                                                                                                                                                              |
| description      | (Optional) Specify to display the port description.                                                                                                                                                                                                                                                               |
| err_disabled     | (Optional) Specify to display disabled information.                                                                                                                                                                                                                                                               |
| auto_negotiation | (Optional) Specifies to display detailed auto-negotiation information.                                                                                                                                                                                                                                            |
| details          | (Optional) Specify to indicate if port detail information will be included in the display.                                                                                                                                                                                                                        |
| media_type       | (Optional) Specify to display the current port media type. For FE ports, the media type should be 100BASE-T. For GE ports (the combo port), if the current active port is the fiber port, the media type is 1000BASE-X or 100BASE-X; if the current active port is the copper port, the media type is 1000BASE-T. |

**NOTE** If no parameter is specified, all ports will be displayed.

## ● Restrictions

None.

## ● Example

To display the configuration of ports 1 to 4:



## 79. Switch Port Commands

```
Zxxx0:admin#show ports 1:1-1:4
```

```
Command: show ports 1:1-1:4
```

| Port | State/<br>MDIX  | Settings<br>Speed/Duplex/FlowCtrl | Connection<br>Speed/Duplex/FlowCtrl | Address<br>Learning |
|------|-----------------|-----------------------------------|-------------------------------------|---------------------|
| 1:1  | Enabled<br>Auto | Auto/Disabled                     | Link Down                           | Enabled             |
| 1:2  | Enabled<br>Auto | Auto/Disabled                     | Link Down                           | Enabled             |
| 1:3  | Enabled<br>Auto | Auto/Disabled                     | Link Down                           | Enabled             |
| 1:4  | Enabled<br>Auto | Auto/Disabled                     | Link Down                           | Enabled             |

```
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

To display the description information of ports 1 to 4:

```
Zxxx0:admin# show ports 1-4 description
```

```
Command: show ports 1:1-1:4 description
```

| Port | State/<br>MDIX                  | Settings<br>Speed/Duplex/FlowCtrl | Connection<br>Speed/Duplex/FlowCtrl | Address<br>Learning |
|------|---------------------------------|-----------------------------------|-------------------------------------|---------------------|
| 1:1  | Enabled<br>Auto<br>Description: | Auto/Disabled                     | Link Down                           | Enabled             |
| 1:2  | Enabled<br>Auto<br>Description: | Auto/Disabled                     | Link Down                           | Enabled             |
| 1:3  | Enabled<br>Auto<br>Description: | Auto/Disabled                     | Link Down                           | Enabled             |
| 1:4  | Enabled<br>Auto<br>Description: | Auto/Disabled                     | Link Down                           | Enabled             |

```
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

### NOTE

Connection status has the following situations: Link Down, Speed/Duplex/FlowCtrl (link up), and Err-Disabled.

To display port error-disabled information:

```
Zxxx0:admin# show ports err_disabled
```

```
Command: show ports err_disabled
```

| Port  | Port<br>State       | Connection Status | Reason        |
|-------|---------------------|-------------------|---------------|
| ----- | -----               | -----             | -----         |
| 1     | Enabled             | Err-Disabled      | Storm control |
|       | Description: port1. |                   |               |
| 8     | Enabled             | Err-Disabled      | Storm control |
|       | Description: port8. |                   |               |

```
Zxxx0:admin#
```

## 80. System Severity Commands

The commands are used to configure the significance level of events, such as trapping or logging, in trap and log management using SNMP (Simple Network Management Protocol).

```
config system_severity [trap | log | all] [emergency | alert | critical | error | warning | notice |
information | debug | <level 0-7>]
show system_severity
```

### 80.1. config system\_severity

#### ● Description

This command is used to configure severity level control for the system.

#### ● Format

```
config system_severity [trap | log | all] [emergency | alert | critical | error | warning |
notice | information | debug | <level 0-7>]
```

#### ● Parameters

|                          |                                                                     |
|--------------------------|---------------------------------------------------------------------|
| <b>trap</b>              | Configure severity level control for a trap.                        |
| <b>log</b>               | Configure severity level control for a log.                         |
| <b>all</b>               | Configure severity level control for a trap and a log.              |
| <b>emergency</b>         | Specify to configure the severity level for emergency messages.     |
| <b>alert</b>             | Specify to configure the severity level for alert messages.         |
| <b>critical</b>          | Specify to configure the severity level for critical messages.      |
| <b>error</b>             | Specify to configure the severity level for error messages.         |
| <b>warning</b>           | Specify to configure the severity level for warning messages.       |
| <b>notice</b>            | Specify to configure the severity level for notice messages.        |
| <b>informational</b>     | Specify to configure the severity level for informational messages. |
| <b>debug</b>             | Specify to configure the severity level for debug messages.         |
| <b>&lt;level 0-7&gt;</b> | Specify to configure a severity level between 0 and 7.              |

#### ● Restrictions

Only Administrator and Operator-level users can issue this command.

- **Example**

To configure severity level control for information level for a trap:

```
Zxxx0:admin#config system_severity trap information
Command: config system_severity trap information

Success.

Zxxx0:admin#
```

## **80.2. show system\_severity**

---

- **Description**

This command is used to show the severity level control for a system.

- **Format**

**show system\_severity**

- **Parameters**

None.

- **Restrictions**

None.

- **Example**

To show the severity level control for a system:

```
Zxxx0:admin#show system_severity
Command: show system_severity

System Severity Trap : warning
System Severity Log  : information

Zxxx0:admin#
```

---

## 81.Tech Support Commands

---

Information, such as this Switching Hub's operation status, is output. It is used as reference data for technical support.

You can send an output result to a specified TFTP server.

---

```
show tech_support
upload tech_support_toTFTP <ipaddr> <path_filename 64>
```

---

### 81.1. show tech\_support

---

#### ● Description

This command is used to display technical support information. It is especially useful for technical support personnel that need to view the overall device operation information.

#### ● Format

`show tech_support`

#### ● Parameters

None.

#### ● Restrictions

Only Administrator and Operator-level users can issue this command.

---

**NOTE** The Switching Hub may become inaccessible when dumping the technical support data.

---

---

**NOTE** The management session may time out if dumping technical support data takes longer than the configured session timeout period. It is strongly recommended to set the serial port timeout to never to disable the auto disconnection of the console session.

---

#### ● Example

To display technical support information:

```

Zxxx0:admin#show tech_support
Command: show tech_support

#-----
#                               Zxxx0 Gigabit Ethernet Switch
#                               Technical Support Information
#
#                               Firmware: Build 1.0.x.xx
#-----

*****      Basic System Information      *****

[SYS 2000-2-29 22:41:48]

Boot Time           : 29 Feb 2000  17:54:29
RTC Time            : 2000/02/29 22:41:48
Boot PROM Version   : Build 1.0.x.xx
Firmware Version    : Build 1.0.x.xx
Hardware Version     : A1
Serial number       :
MAC Address          : 00-01-02-03-04-00
[STACKING 2000-2-29 22:41:48]

#Topology Information

Stable Topology:
My Box ID : 1                Role           : Master
Box Cnt   : 1                Topology Type : Duplex Chain
Unit Prio-                               Device Runtime   Stacking
ID  rity  Role           MAC           Type           option version   version
-----
1    32 32 Master    00-01-02-03-04-00  Zxxx0 0x0002  1.0.0.xx   2.0.1

```

## 81.2. upload tech\_support\_toTFTP

### ● Description

This command is used to upload technical support information to a TFTP server. This command can be interrupted by Ctrl ? C or ESC when it is executing.

### ● Format

upload tech\_support\_toTFTP <ipaddr> <path\_filename 64>

### ● Parameters

---

<ipaddr> Specify the IPv4 address of the TFTP server.

---

<path\_filename 64>

Specify the file name of the technical support information file sent to the TFTP server. The maximum size of the file name is 64 characters.

---

## 81. Tech Support Commands

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To upload technical support information:

```
Zxxx0:admin#upload tech_support_toTFTP 10.0.0.66 tech_support.txt
Command: upload tech_support_toTFTP 10.0.0.66 tech_support.txt

Connecting to server..... Done.
Upload techsupport file..... Done.

Success.

Zxxx0:admin#
```

## 82. Time and SNTP Commands

The commands are used to set the time for the internal clock of this Switching Hub.

The time can be set manually or automatically using SNTP (Simple Network Time Protocol).

You can also configure the time zone and summer time settings.

```

config sntp {primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>} (1)
show sntp
enable sntp
disable sntp
config time <date ddmthyyy> <time hh:mm:ss>
config time_zone {operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>} (3)
config dst [disable | repeating {s_week <start_week 1-4,last> | s_day <start_day sun-sat> | s_mth
    <start_mth 1-12> | s_time <start_time hh:mm> | e_week <end_week 1-4, last> | e_day
    <end_day sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 |
    90 | 120]} (9) | annual {s_date <start_date 1-31> | s_mth <start_mth 1-12> | s_time
    <start_time hh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_time
    hh:mm> | offset [30 | 60 | 90 | 120]}(7)]
show time
  
```

### 82.1. config sntp

#### ● Description

This command is used to change SNTP configurations.

#### ● Format

```
config sntp {primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>} (1)
```

#### ● Parameters

|                       |                                                        |
|-----------------------|--------------------------------------------------------|
| <b>primary</b>        | (Optional) Specify the SNTP primary server IP address. |
| <b>&lt;ipaddr&gt;</b> | Specify the SNTP primary server IP address.            |

|                       |                                                          |
|-----------------------|----------------------------------------------------------|
| <b>secondary</b>      | (Optional) Specify the SNTP secondary server IP address. |
| <b>&lt;ipaddr&gt;</b> | Specify the SNTP secondary server IP address.            |

|                             |                                                                  |
|-----------------------------|------------------------------------------------------------------|
| <b>poll-interval</b>        | (Optional) Specify the polling interval range.                   |
| <b>&lt;int 30-99999&gt;</b> | Specify the polling interval range between 30 and 99999 seconds. |

#### ● Restrictions



## 82. Time and SNTP Commands

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure SNTP:

```
Zxxx0:admin#config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30
Command: config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30

Success.

Zxxx0:admin#
```

## 82.2. show sntp

---

### ● Description

This command is used to display the current SNTP time source and configuration.

### ● Format

**show sntp**

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To show SNTP:

```
Zxxx0:admin#show sntp
Command: show sntp

Current Time Source   : System Clock
SNTP                  : Disabled
SNTP Primary Server   : 10.1.1.1
SNTP Secondary Server : 10.1.1.2
SNTP Poll Interval    : 720 sec

Zxxx0:admin#
```

## 82.3. enable sntp

---

- **Description**

This command is used to turn on SNTP support.

- **Format**

enable sntp

- **Parameters**

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To enable SNTP:

```
Zxxx0:admin#enable sntp
Command: enable sntp

Success.

Zxxx0:admin#
```

## 82.4. disable sntp

---

- **Description**

This command is used to turn off SNTP support.

- **Format**

disable sntp

- **Parameters**

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

## 82. Time and SNTP Commands

### ● Example

To disable SNTP:

```
Zxxx0:admin#disable sntp
Command: disable sntp

Success.

Zxxx0:admin#
```

## 82.5. config time

---

### ● Description

This command is used to change the time settings.

### ● Format

**config time <date ddmthyyyy> <time hh:mm:ss>**

### ● Parameters

---

**<date ddmthyyyy>**  
Specify the system clock date.

---

**<time hh:mm:ss>**  
Specify the system clock time.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure time:

```
Zxxx0:admin# config time 30jun2003 16:30:30
Command: config time 30jun2003 16:30:30

Success.

Zxxx0:admin#
```

## 82.6. config time\_zone

---

### ● Description

This command is used to change time zone settings.

### ● Format

**config time\_zone {operator [+ | -] | hour <gmt\_hour 0-13> | min <minute 0-59>} (3)**

### ● Parameters

|                 |                                                                                                                             |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>operator</b> | Specify the operator of the time zone.<br>+      Positive.<br>-      Negative.                                              |
| <b>hour</b>     | Specify the hour of the time zone.<br><b>&lt;gmt_hour 0-13&gt;</b><br>Specify the hour of the time zone between 0 and 13.   |
| <b>min</b>      | Specify the minute of the time zone.<br><b>&lt;minute 0-59&gt;</b><br>Specify the minute of the time zone between 0 and 59. |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the time zone:

```
Zxxx0:admin#config time_zone operator + hour 2 min 30
Command: config time_zone operator + hour 2 min 30

Success.

Zxxx0:admin#
```

## 82.7. config dst

### ● Description

This command is used to change Daylight Saving Time settings.

### ● Format

```
config dst [disable | repeating {s_week <start_week 1-4,last> | s_day <start_day sun-sat> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_week <end_week 1-4,last> | e_day <end_day sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} (9) | annual {s_date <start_date 1-31> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} (7) ]
```

### ● Parameters

|                  |                                                                                                                                                                           |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>disable</b>   | Disable the DST of the Switching Hub.                                                                                                                                     |
| <b>repeating</b> | Set the DST to repeating mode.                                                                                                                                            |
| <b>annual</b>    | Configure the DST period.                                                                                                                                                 |
| <b>s_week</b>    | Configure the start week number of DST.<br><b>&lt;start_week 1-4,last&gt;</b><br>Configure the start week number of DST. The values are 1 to 4.                           |
| <b>s_day</b>     | Configure the start day number of DST.<br><b>&lt;start_day sun-sat&gt;</b><br>Configure the start day number of DST. The values are sun, mon, tue, wed, thu, fri and sat. |
| <b>s_mth</b>     | Configure the start month number of DST.<br><b>&lt;start_mth 1-12&gt;</b><br>Configure the start month number of DST. The values are 1 to 12.                             |
| <b>s_time</b>    | Configure the start time of DST.<br><b>&lt;start_time hh:mm&gt;</b><br>Configure the start time in hh:mm of DST.                                                          |
| <b>e_week</b>    | Configure the end week number of DST.<br><b>&lt;end_week 1-4,last&gt;</b><br>Configure the end week number of DST. The values are 1 to 4.                                 |
| <b>e_day</b>     | Configure the end day number of DST.<br><b>&lt;end_day sun-sat&gt;</b><br>Configure the end day number of DST. The values are sun, mon, tue, wed, thu, fri and sat.       |
| <b>e_mth</b>     | Configure the end month number of DST.<br><b>&lt;end_mth 1-12&gt;</b><br>Configure the end month number of DST. The values are 1 to 12.                                   |
| <b>e_time</b>    | Configure the end time of DST.<br><b>&lt;end_time hh:mm&gt;</b><br>Configure the end time in hh:mm of DST.                                                                |

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>offset</b> | Specify the number of minutes to add or to subtract during summertime. The range of offsets are 30, 60, 90, and 120. The default value is 60.<br><b>30</b> Specify 30 minutes to add or to subtract during summertime.<br><b>60</b> Specify 60 minutes to add or to subtract during summertime.<br><b>90</b> Specify 90 minutes to add or to subtract during summertime.<br><b>120</b> Specify 120 minutes to add or to subtract during summertime. |
| <b>annual</b> | Set the DST to annual mode.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>s_date</b> | Configure the start date number of DST.<br><b>&lt;start_date 1-31&gt;</b><br>Configure the start date number of DST. The values are 1 to 31.                                                                                                                                                                                                                                                                                                        |
| <b>e_date</b> | Configure the end date number of DST.<br><b>&lt;end_date 1-31&gt;</b><br>Configure the end date number of DST. The values are 1 to 31.                                                                                                                                                                                                                                                                                                              |

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure time:

```
Zxxx0:admin#config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00 e_week 2
e_day wed e_mth 10 e_time 15:30 offset 30
Command: config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00 e_week 2
e_day wed e_mth 10 e_time 15:30 offset 30

Success.

Zxxx0:admin#
```

## 82.8. show time

---

### ● Description

This command is used to display current time states.

### ● Format

show time

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To show time:

```
Zxxx0:admin#show time
Command: show time

Current Time Source  : System Clock
Boot Time           : 8 Jan 2000  21:44:33
Current Time        : 9 Jan 2000  03:25:17
Time Zone           : GMT +00:00
Daylight Saving Time : Disabled
Offset In Minutes: 60
    Repeating From   : Apr 1st  Sun 00:00
                   To   : Oct last Sun 00:00
    Annual   From   : 29 Apr 00:00
                   To   : 12 Oct 00:00
Zxxx0:admin#
```

## 83. Traffic Segmentation Commands

Traffic segmentation is used to configure ports to which each port can forward receive data.

It is used for more detailed traffic restrictions in a VLAN.

---

```
config traffic_segmentation [<portlist> | all] forward_list [null | all | <portlist>]
show traffic_segmentation {<portlist>}
```

---

### 83.1. config traffic\_segmentation

#### ● Description

This command is used to configure traffic segmentation.

#### ● Format

```
config traffic_segmentation [<portlist> | all] forward_list [null | all | <portlist>]
```

#### ● Parameters

---

**<portlist>** Specify a range of ports to be configured.

---

**all** Specify all ports.

---

**forward\_list**

Specify a range of port forwarding domains.

**null** Specify the range of the port forwarding domain is null.

**all** Specify all ports.

**<portlist>** Specify a range of ports to be configured.

---

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To configure traffic segmentation:

```
Zxxx0:admin#config traffic_segmentation 1-6 forward_list 7-8
Command: config traffic_segmentation 1-6 forward_list 7-8

Success.

Zxxx0:admin#
```



## 83.2. show traffic\_segmentation

---

### ● Description

This command is used to display the traffic segmentation table.

### ● Format

show traffic\_segmentation {<portlist>}

### ● Parameters

---

<portlist>(Optional) Specify a range of ports to be displayed.

---

#### NOTE

If no parameter is specified, the system will display all current traffic segmentation tables.

---

### ● Restrictions

None.

### ● Example

To display the traffic segmentation table for ports 1 to 3:

```
Zxxx0:admin#show traffic_segmentation 1-3
Command: show traffic_segmentation 1-3
```

```
Traffic Segmentation Table
```

```
Port      Forward Portlist
```

```
-----
```

```
1         1-28
```

```
2         1-28
```

```
3         1-28
```

```
Zxxx0:admin#
```

## 84. Utility Commands

This chapter describes the following utility commands.

- Downloading and uploading firmware, configuration files, and log files using TFTP or RCP server
- Selecting firmware and configuration files used during a boot
- RCP server settings
- Ping, traceroute for IPv4 or IPv6
- Logging in to the Telnet server
- Ping response settings to broadcast address

---

```

download [firmware_fromTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] src_file
    <path_filename 64> {[unit <unit_id 1-4> | all]} {dest_file <pathname>} {boot_up} |
    cfg_fromTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] src_file <path_filename 64>
    {[unit <unit_id 1-4> | all]} {[increment | dest_file <pathname>}]}
download cfg_fromRCP [{username <username>} {<ipaddr>} src_file <path_filename 64> |
    rcp:<string 128>] {[unit <unit_id 1-4> | all]} {dest_file <pathname>}
download firmware_fromRCP [{username <username>} {<ipaddr>} src_file <path_filename 64> |
    rcp:<string 128>] {[unit <unit_id 1-4> | all]} {dest_file <pathname>} {boot_up}
upload [cfg_toTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename 64>
    {unit <unit_id>} {src_file <pathname>} {[include | exclude | begin] <filter_string 80>
    {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80>
    {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80>
    {<filter_string 80> {<filter_string 80>}}}] | log_toTFTP [<ipaddr> | <ipv6addr> |
    <domain_name 255>] dest_file <path_filename 64> | attack_log_toTFTP [<ipaddr> |
    <ipv6addr> | <domain_name 255>] dest_file <path_filename 64> {unit <unit_id 1-4>} |
    firmware_toTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename
    64> {unit <unit_id 1-4>} {src_file <pathname>}]}
upload attack_log_toRCP [{username <username>} {<ipaddr>} dest_file <path_filename 64> |
    rcp:<string 128>] {unit <unit_id 1-4>}
upload cfg_toRCP [{username <username>} {<ipaddr>} dest_file <path_filename 64> |
    rcp:<string 128>] {unit <unit_id 1-4>} {src_file <pathname>} {[include | exclude | begin]
    <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin]
    <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin]
    <filter_string 80> {<filter_string 80> {<filter_string 80>}}}]
upload firmware_toRCP [{username <username>} {<ipaddr>} dest_file <path_filename 64> |
    rcp:<string 128>] {unit <unit_id 1-4>} {src_file <pathname>}
upload log_toRCP [{username <username>} {<ipaddr>} dest_file <path_filename 64> |
    rcp:<string 128>]
config firmware image {unit <unit_id 1-4>} <pathname> boot_up
config configuration {unit <unit_id 1-4>} <pathname> [boot_up | active]
show config [effective | modified | current_config | boot_up | file <pathname>] {[include |
    exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude
    | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude |
    begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}]
show boot_file
config rcp server {ipaddress <ipaddr> | username <username>}
config rcp server clear [ipaddr | username | both]
  
```

---

---

```

show rcp server
ping [<ipaddr> | <domain_name 255>] {times <value 1-255> | timeout <sec 1-99> | source_ip
    <ipaddr>}
ping6 <ipv6addr> {times <value 1-255> | size <value 1-6000> | timeout <sec 1-99> | source_ip
    <ipv6addr>}
traceroute [<ipaddr> | <domain_name 255>] {ttl <value 1-60> | port <value 30000-64900> |
    timeout <sec 1-65535> | probe <value 1-9>}
traceroute6 <ipv6addr> {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> |
    probe <value 1-9>}
telnet [<ipaddr> | <domain_name 255> | <ipv6addr>] {tcp_port <value 1-65535>}
enable broadcast_ping_reply
disable broadcast_ping_reply
show broadcast_ping_reply

```

---

## 84.1. download

---

### ● Description

This command is used to download a new firmware or a Switching Hub configuration file.

### ● Format

```

download [firmware_fromTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] src_file
    <path_filename 64> {[unit <unit_id 1-4> | all]} {dest_file <pathname>} {boot_up} |
cfg_fromTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] src_file <path_filename
    64> {[unit <unit_id 1-4> | all]} {[increment | dest_file <pathname>}]]

```

### ● Parameters

---

|                                 |                                                                                                                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>firmware_fromTFTP</b>        | Download and install new firmware on the Switching Hub from a TFTP server.                                                                                                                                              |
| <b>&lt;ipaddr&gt;</b>           | Specify the IP address of the TFTP server.                                                                                                                                                                              |
| <b>&lt;ipv6addr&gt;</b>         | Specify the IPv6 address of the TFTP server.                                                                                                                                                                            |
| <b>&lt;domain_name 255&gt;</b>  | Specifies the domain name of the TFTP server. This name can be up to 255 characters long.                                                                                                                               |
| <b>src_file</b>                 | Specify the path name and file name of the TFTP server. It can be a relative path name or an absolute path name. If path name is not specified, it refers to the TFTP server path. The maximum length is 64 characters. |
| <b>&lt;path_filename 64&gt;</b> | Specify the path name and file name of the TFTP server. It can be a relative path name or an absolute path name. If path name is not specified, it refers to the TFTP server path. The maximum length is 64 characters. |
| <b>unit</b>                     | Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.                                                                                                                      |
| <b>&lt;unit_id 1-4&gt;</b>      | Enter the unit ID used here.                                                                                                                                                                                            |
| <b>all</b>                      | Specifies that all the units in the stacking system will be used.                                                                                                                                                       |

---

---

**dest\_file** (Optional) Specify an absolute path name on the device file system. If path name is not specified, it overwrites the bootup image on the Switch.

**<pathname>**

Specify an absolute path name on the device file system.

---

**boot\_up** (Optional) Specify as boot up file.

---

**cfg\_fromTFTP**

Download and install new configuration file on the Switching Hub from a TFTP server.

**<ipaddr>**

Specify the IP address of the TFTP server.

**<ipv6addr>**

Specify the IPv6 address of the TFTP server.

**<domain\_name 255>**

Specifies the domain name of the TFTP server. This name can be up to 255 characters long.

---

**src\_file** Specify the path name and file name of the FTP server. It can be a relative path name or an absolute path name. If path name is not specified, it refers to the TFTP server path. The maximum length is 64 characters.

**<path\_filename 64>**

Specify the path name and file name of the FTP server. It can be a relative path name or an absolute path name. If path name is not specified, it refers to the TFTP server path. The maximum length is 64 characters.

---

**unit** Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.

**<unit\_id 1-4>** Enter the unit ID used here.

**all** Specifies that all the units in the stacking system will be used.

---

**increment**

If increment is specified, then the existing configuration will not be cleared before applying of the new configuration. If it is not specified, then the existing configuration will be cleared before applying of the new configuration.

---

**dest\_file** (Optional) Specify an absolute path name on the device. If path name is not specified, it refers to the boot up configuration file.

**<pathname>**

Specify an absolute path name on the device.

---

## ● Restrictions

Only Administrator-level users can issue this command.

## ● Example

To download runtime firmware from a TFTP server:

```
Zxxx0:admin#download firmware_fromTFTP 10.0.0.66 src_file runtime.rom dest_file
runtime.rom
Command: download firmware_fromTFTP 10.0.0.66 src_file runtime.rom dest_file
runtime.rom

Connecting to server..... Done.
Download firmware..... Done.   Do not power off!
Please wait, programming flash..... Done.

Zxxx0:admin#
```

## 84.2. download cfg\_fromRCP

---

### ● Description

This command is used to download a configuration file from a Remote Copy Protocol (RCP) server.

### ● Format

**download cfg\_fromRCP** [{username <username>} {<ipaddr>} src\_file <path\_filename 64> | rcp: <string 128>] [[unit <unit\_id 1-4> | all]] {dest\_file <pathname>}

### ● Parameters

---

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>username</b>       | (Optional) Specify the remote user name on the RCP server.<br><b>&lt;username&gt;</b><br>Specify the remote user name on the RCP server.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>&lt;ipaddr&gt;</b> | (Optional) Specify the IP address of the RCP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>src_file</b>       | Specify the path and file name of the Switching Hub configuration file on the RCP server. The maximum length is 64.<br><b>&lt;path_filename 64&gt;</b><br>Specify the path and file name of the Switching Hub configuration file on the RCP server. The maximum length is 64.                                                                                                                                                                                                                                                                                                |
| <b>rcp:</b>           | Syntax: rcp: username@ipaddr/directory/filename.<br>Example for full path: user_name@10.1.1.1/home/user_name/desxxxx.had;<br>Example for relative path: user_name@10.1.1.1./desxxxx.had.<br>Note: No spaces in the whole <string>.<br><b>&lt;string 128&gt;</b><br>Syntax: rcp: username@ipaddr/directory/filename.<br>Example for full path: user_name@10.1.1.1/home/user_name/desxxxx.had;<br>Example for relative path: user_name@10.1.1.1./desxxxx.had.<br>Example for omitted user name in RCP string: 10.1.1.1./desxxxx.had.<br>Note: No spaces in the whole <string>. |
| <b>unit</b>           | Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.<br><b>&lt;unit_id 1-4&gt;</b><br>Enter the unit ID used here. This value must be between 1 and 4.<br><b>all</b> Specifies that all the units in the stacking system will be used.                                                                                                                                                                                                                                                                                         |
| <b>dest_file</b>      | (Optional) Specify the path and file name of the destination file on the device.<br><b>&lt;pathname&gt;</b><br>Specify the path and file name of the destination file.                                                                                                                                                                                                                                                                                                                                                                                                       |

---

### ● Restrictions

Only Administrator-level users can issue this command.

## ● Example

To download a configuration file from an RCP server:

```
Zxxx0:admin#download cfg_fromRCP username rcp_user 172.18.212.106 src_file /home/
runtime.cfg
Command: download cfg_fromRCP username rcp_user 172.18.212.106 src_file /home/
runtime.cfg

Connecting to server..... Done.
Download configuration..... Done.

Zxxx0:admin#
```

## 84.3. download firmware\_fromRCP

### ● Description

This command is used to download a firmware file from a Remote Copy Protocol (RCP) server..

### ● Format

```
download firmware_fromRCP [{username <username>} {<ipaddr>} src_file
<path_filename 64> | rcp: <string 128>] [[unit <unit_id 1-4> | all]] {dest_file
<pathname>} {boot_up}
```

### ● Parameters

---

**username**(Optional) Specify the remote user name on the RCP server.

**<username>**

Specify the remote user name on the RCP server.

---

**<ipaddr>**(Optional) Specify the IP address of the RCP server.

---

**src\_file** Specify the path name on the RCP server or local. Note: If a user specifies the relative file path, the path search strategy depends on the server system.

**<path\_filename 64>**

Specify the path name on the RCP server or local. Note: If a user specifies the relative file path, the path search strategy depends on the server system.

---

## 84. Utility Commands

---

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>rcp:</b>      | Syntax: rcp: username@ipaddr/directory/filename.<br>Example for full path: user_name@10.1.1.1/home/user_name/desxxxx.rom;<br>Example for relative path: user_name@10.1.1.1./desxxxx.rom;<br>Example for omitted user name in RCP string: 10.1.1.1./desxxxx.rom.<br>Note: No spaces are allowed in the <string>.<br><b>&lt;string 128&gt;</b><br>Syntax: rcp: username@ipaddr/directory/filename.<br>Example for full path: user_name@10.1.1.1/home/user_name/desxxxx.rom;<br>Example for relative path: user_name@10.1.1.1./desxxxx.rom;<br>Example for omitted user name in RCP string: 10.1.1.1./desxxxx.rom;<br>Note: No spaces are allowed in the <string>. |
| <b>unit</b>      | Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.<br><b>&lt;unit_id 1-4&gt;</b><br>Enter the unit ID used here. This value must be between 1 and 4.<br><b>all</b> Specifies that all the units in the stacking system will be used.                                                                                                                                                                                                                                                                                                                                                                            |
| <b>dest_file</b> | (Optional) Specify the path and file name of the destination file on the device.<br><b>&lt;pathname&gt;</b><br>Specify the path and file name of the destination file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>boot_up</b>   | Specify as boot up file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

---

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To download firmware from an RCP server:

```
Zxxx0:admin#download firmware_fromRCP username rcp_user 10.90.90.90 src_file /
home/Zxxx0.rom
Command: download firmware_fromRCP username rcp_user 10.90.90.90 src_file /home/
Zxxx0.rom

Connecting to server..... Done.
Download firmware..... Done.      Do not power off !!
Please wait, programming flash..... Done.
Saving current settings to NV-RAM..... Done.

Zxxx0:admin#
```

## 84.4. upload

---

### ● Description

This command is used to upload a firmware or a configuration file from device to TFTP server.

### ● Format

```
upload [cfg_toTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file
<path_filename 64> {unit <unit_id 1-4>} {src_file <pathname>} {[include | exclude |
begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude |
begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude |
begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}] | log_toTFTP
[<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename 64> |
attack_log_toTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file
<path_filename 64> {unit <unit_id 1-4>} | firmware_toTFTP [<ipaddr> | <ipv6addr> |
<domain_name 255>] dest_file <path_filename 64> {unit <unit_id 1-4>} {src_file
<pathname>}]
```

### ● Parameters

---

#### cfg\_toTFTP

Used to upload a configuration file from a device to a TFTP server.

#### <ipaddr>

Specify the IP address of the TFTP server.

#### <ipv6addr>

Specify the IPv6 address of the TFTP server.

#### <domain\_name 255>

Enter the domain name of the TFTP server here. This name can be up to 255 characters long.

---

**dest\_file** Specify the path name on the TFTP server. It can be a relative path name or an absolute path name

#### <path\_filename 64>

Specify the location of the Switching Hub configuration file on the TFTP server. This file will be replaced by the uploaded file from the Switching Hub. The maximum length is 64 characters.

---

**unit** (Optional) Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.

#### <unit\_id 1-4>

Enter the unit ID used here.

---

**src\_file** (Optional) Specify an absolute path name on the device file system. If a path name is not specified, it refers to the boot up configuration file.

#### <pathname>

Specify the location of the Switching Hub configuration file on device.

---

**include** (Optional) Includes lines that contain the specified filter string.

---

**exclude** (Optional) Excludes lines that contain the specified filter string.

---



## 84. Utility Commands

---

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>begin</b> | (Optional) The first line that contains the specified filter string will be the first line of the output.<br><b>&lt;filter_string 80&gt;</b><br>Specify a filter string enclosed by the quotation mark symbol. Thus, the filter string itself cannot contain the quotation mark character. The filter string is case sensitive.<br><b>&lt;filter_string 80&gt;</b><br>Specify a filter string enclosed by the quotation mark symbol.<br><b>&lt;filter_string 80&gt;</b><br>Specify a filter string enclosed by the quotation mark symbol. |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

|                   |                                                                                                                                                                                                                                                                                                                                               |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>log_toTFTP</b> | Used to upload a log file from the device to a TFTP server.<br><b>&lt;ipaddr&gt;</b><br>Specify the IP address of the TFTP server.<br><b>&lt;ipv6addr&gt;</b><br>Specify the IPv6 address of the TFTP server.<br><b>&lt;domain_name 255&gt;</b><br>Enter the domain name of the TFTP server here. This name can be up to 255 characters long. |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

|                  |                                                                                                                                                                                   |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dest_file</b> | Specify the path name if the TFTP server.<br><b>&lt;path_filename 64&gt;</b><br>Specify the path name on the TFTP server. It can be a relative path name or an absolute path name |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

|                          |                                                                                                                                                                                                                                                                                                                                   |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>attack_log_toTFTP</b> | Used to upload the attack log to a TFTP server.<br><b>&lt;ipaddr&gt;</b><br>Specify the IP address of the TFTP server.<br><b>&lt;ipv6addr&gt;</b><br>Specify the IPv6 address of the TFTP server.<br><b>&lt;domain_name 255&gt;</b><br>Enter the domain name of the TFTP server here. This name can be up to 255 characters long. |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

|                  |                                                                                                                                                                                   |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dest_file</b> | Specify the path name if the TFTP server.<br><b>&lt;path_filename 64&gt;</b><br>Specify the path name on the TFTP server. It can be a relative path name or an absolute path name |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

|             |                                                                                                                                                                             |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>unit</b> | (Optional) Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.<br><b>&lt;unit_id 1-4&gt;</b><br>Enter the unit ID used here. |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

|                        |                                                                                                                                                                                                                                                                                                                                             |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>firmware_toTFTP</b> | Used to upload firmware from the device to a TFTP server.<br><b>&lt;ipaddr&gt;</b><br>Specify the IP address of the TFTP server.<br><b>&lt;ipv6addr&gt;</b><br>Specify the IPv6 address of the TFTP server.<br><b>&lt;domain_name 255&gt;</b><br>Enter the domain name of the TFTP server here. This name can be up to 255 characters long. |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

|                  |                                                                                                                           |
|------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>dest_file</b> | Specify the path name if the TFTP server.<br><b>&lt;path_filename 64&gt;</b><br>Specify the path name if the TFTP server. |
|------------------|---------------------------------------------------------------------------------------------------------------------------|

---

|                 |                                                                                                                                                                                                                                                                                                  |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>unit</b>     | (Optional) Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.<br><b>&lt;unit_id 1-4&gt;</b><br>Enter the unit ID used here.                                                                                                                      |
| <b>src_file</b> | (Optional) Specify an absolute path name on the device file system. If the path name is not specified, it refers to the boot up image.<br><b>&lt;pathname&gt;</b><br>Specify an absolute path name on the device file system. If the path name is not specified, it refers to the boot up image. |

## ● Restrictions

Only Administrator and Operator-level users can issue this command.

## ● Example

To upload firmware from a file system device to a TFTP server:

```
Zxxx0:admin#upload firmware_toTFTP 10.1.1.1 dest_file D:\firmware.rom src_file
1.0.0.xx.rom
Command: upload firmware_toTFTP 10.1.1.1 dest_file D:\firmware.rom src_file
1.0.0.xx.rom

Connecting to server..... Done.
Upload firmware..... Done.

Zxxx0:admin#
```

To upload the current configuration file to a TFTP server:

```
Zxxx0:admin#upload cfg_toTFTP 10.48.74.121 dest_file c:\cfg\Zxxx0.cfg
Command: upload cfg_toTFTP 10.48.74.121 dest_file c:\cfg\Zxxx0.cfg

Connecting to server..... Done.
Upload configuration..... Done.

Zxxx0:admin#
```

To upload all logs to a TFTP server:

```
Zxxx0:admin#upload log_toTFTP 10.48.74.121 dest_file c:\log\Zxxx0.log
Command: upload log_toTFTP 10.48.74.121 dest_file c:\log\Zxxx0.log

Connecting to server..... Done.
Upload log..... Done.

Zxxx0:admin#
```

To upload a dangerous log:

## 84. Utility Commands

```
Zxxx0:admin# upload attack_log_toTFTP 10.48.74.121 dest_file c:\alert.txt
Command: upload attack_log_toTFTP 10.48.74.121 dest_file c:\alert.txt

Connecting to server..... Done.
Upload attack log..... Done.

Success.

Zxxx0:admin#
```

### 84.5. upload attack\_log\_toRCP

#### ● Description

This command is used to upload the attack log file from the device to an RCP server.

**NOTE** If a user specifies the relative file path, the path search strategy will depend on the server system. For some systems, it will search the current user working directory first, and then search the environment paths.

#### ● Format

**upload attack\_log\_toRCP** [{username <username>} {<ipaddr>} dest\_file  
<path\_filename 64> | rcp: <string 128>] {unit <unit\_id 1-4>}

#### ● Parameters

**username**(Optional) The remote user name on the RCP Server.

<username>

Enter the remote username used here.

**<ipaddr>**(Optional) Enter the IP address used for the configuration here.

**dest\_file** Specifies the destination file used.

<path\_filename 64>

The pathname specifies the pathname on the RCP server or local device.

**rcp:** Syntax: rcp: username@ipaddr/directory/filename.

Example for full path: user\_name@10.1.1.1/home/user\_name/desxxxxx.rom;

Example for relative path: user\_name@10.1.1.1./desxxxxx.rom;

Note: Do not use any blank spaces in the <string>.

<string 128>

Enter the RCP string here.

**unit** (Optional) Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.

<unit\_id 1-4>

Enter the unit ID used here. This value must be between 1 and 4.

#### ● Restrictions

Only Administrator and Operator-level users can issue this command.

## ● Example

To upload the attack log from the device to an RCP server:

```
Zxxx0:admin# upload attack_log_toRCP username rcp_user 172.18.212.104 dest_file /
home/Zxxx0.log unit 2
Command: upload attack_log_toRCP username rcp_user 172.18.212.104 dest_file /home/
Zxxx0.log unit 2

Connecting to server..... Done.
Upload Attack log..... Done.
Success.

Zxxx0:admin#
```

## 84.6. upload cfg\_toRCP

### ● Description

This command is used to upload a configuration file from the device to a Remote Copy Protocol (RCP) server.

### ● Format

```
upload cfg_toRCP [{username <username>} {<ipaddr>} dest_file <path_filename 64> |
rcp: <string 128>] {unit <unit_id 1-4>} {src_file <pathname>} {[include | exclude |
begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude |
begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude |
begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}]}
```

### ● Parameters

---

**username**(Optional) Specify the remote user name on the RCP server.

**<username>**

Specify the remote user name on the RCP server.

---

**<ipaddr>**(Optional) Specify the IP address of the RCP server.

---

**dest\_file** Specify the path name on the RCP server. Note: If a user specifies the relative file path, the path search strategy will depend on the server system. For some systems, the current user working directory will be searched first, followed by the environment paths.

**<path\_filename 64>**

Specify the path name on the RCP server or local RCP client.

---

**rcp:** Specify the path on the RCP server or local RCP client. Note: If a user specifies the relative file path, the path search strategy will depend on the server system. For some systems, the current user working directory will be searched first, followed by the environment paths.

**<string 128>**

Specify the path on the RCP server or local RCP client.

---

## 84. Utility Commands

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>unit</b>     | (Optional) Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.<br><b>&lt;unit_id 1-4&gt;</b><br>Enter the unit ID used here. This value must be between 1 and 4.                                                                                                                                                                                                                                                                                                                           |
| <b>src_file</b> | (Optional) Specify the path name of the source file.<br><b>&lt;pathname&gt;</b><br>Specify the path name of the source file. Note that if no path name is specified, only the current device configuration will be uploaded.                                                                                                                                                                                                                                                                                                              |
| <b>include</b>  | (Optional) Includes lines that contain the specified filter string.                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>exclude</b>  | (Optional) Excludes lines that contain the specified filter string.                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>begin</b>    | (Optional) The first line that contains the specified filter string will be the first line of the output.<br><b>&lt;filter_string 80&gt;</b><br>Specify a filter string enclosed by the quotation mark symbol. Thus, the filter string itself cannot contain the quotation mark character. The filter string is case sensitive.<br><b>&lt;filter_string 80&gt;</b><br>Specify a filter string enclosed by the quotation mark symbol.<br><b>&lt;filter_string 80&gt;</b><br>Specify a filter string enclosed by the quotation mark symbol. |

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To upload the current configuration from the device to an RCP server:

```
Zxxx0:admin#upload cfg_toRCP username rcp_user 10.48.74.121 dest_file /home/  
Zxxx0.cfg  
Command: upload cfg_toRCP username rcp_user 10.48.74.121 dest_file /home/Zxxx0.cfg  
  
Connecting to server... Done.  
Upload configuration... Done.  
  
Zxxx0:admin#
```

## 84.7. upload firmware\_toRCP

### ● Description

This command is used to upload firmware from a device to a Remote Copy Protocol (RCP) server.

### ● Format

```
upload firmware_toRCP [{username <username>} {<ipaddr>} dest_file  
<path_filename 64> | rcp: <string 128>} {unit <unit_id 1-4>} {src_file <pathname>}]
```

## ● Parameters

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>username</b>       | (Optional) Specify the remote user name on the RCP server.<br><b>&lt;username&gt;</b><br>Specify the remote user name on the RCP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>&lt;ipaddr&gt;</b> | (Optional) Specify the IP address of the RCP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>dest_file</b>      | Specify the path name on the RCP server. Note: If a user specifies the relative file path, the path search strategy will depend on the server system. For some systems, the current user working directory will be searched first, followed by the environment paths.<br><b>&lt;path_filename 64&gt;</b><br>Specify the path name on the RCP server.                                                                                                                                                                                                                                                                                                  |
| <b>rcp:</b>           | Specify the path name on the RCP server or local RCP client.<br>Syntax: rcp: username@ipaddr/directory/filename.<br>Example for full path: user_name@10.1.1.1/home/user_name/desxxxxx.rom;<br>Example for relative path: user_name@10.1.1.1./desxxxxx.rom;<br>Note: No spaces are allowed in the <string>.<br><b>&lt;string 128&gt;</b><br>Specify the path name on the RCP server or local RCP client.<br>Syntax: rcp: username@ipaddr/directory/filename.<br>Example for full path: user_name@10.1.1.1/home/user_name/desxxxxx.rom;<br>Example for relative path: user_name@10.1.1.1./desxxxxx.rom;<br>Note: No spaces are allowed in the <string>. |
| <b>unit</b>           | (Optional) Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.<br><b>&lt;unit_id 1-4&gt;</b><br>Enter the unit ID used here. This value must be between 1 and 4.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>src_file</b>       | (Optional) Specify the path name of the source file. If not specified, the bootup image on the device will be uploaded.<br><b>&lt;pathname&gt;</b><br>Specify the path name of the source file.                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## ● Restrictions

Only Administrator and Operator-level users can issue this command.

## ● Example

To upload firmware image to an RCP server:

```
Zxxx0:admin#upload firmware_toRCP rcp: rcp_user@172.18.212.106/Zxxx0.rom src_file
2.00.009.rom
Command: upload firmware_toRCP rcp: rcp_user@172.18.212.106/Zxxx0.rom src_file
2.00.009.rom

Connecting to server..... Done.
Upload firmware..... Done.

Zxxx0:admin#
```

## 84.8. upload log\_toRCP

---

### ● Description

This command is used to upload a log file from the device to a Remote Copy Protocol (RCP) server.

### ● Format

**upload log\_toRCP** [{username <username>} {<ipaddr>} **dest\_file** <path\_filename 64> | **rcp:** <string 128>]

### ● Parameters

---

**username**(Optional) Specify the remote user name on the RCP server.  
     <username>

Specify the remote user name on the RCP server.

---

**<ipaddr>**(Optional) Specify the IP address of the RCP server.

---

**dest\_file** Specify the path name of the RCP server. Note: If a user specifies the relative file path, the path search strategy will depend on the server system. For some systems, the current user working directory will be searched first, followed by the environment paths.

    <path\_filename 64>

Specify the path name of the RCP server.

---

**rcp:** Specify the path name on the RCP server.  
     <string 128>

Specify the path name on the RCP server.

Syntax: rcp: username@ipaddr/directory/filename.

Example for full path: user\_name@10.1.1.1/home/user\_name/desxxxxx.rom;

Example for relative path: user\_name@10.1.1.1./desxxxxx.rom;

Note: No spaces are allowed in the <string>.

---

### ● Restrictions

Only Administrator and Operator-level users can issue this command.

### ● Example

To upload the log from the device to an RCP server:

```
Zxxx0:admin#upload log_toRCP username rcp_user 172.18.212.104 dest_file /home/
Zxxx0.log
Command: upload log_toRCP username rcp_user 172.18.212.104 dest_file /home/
Zxxx0.log

Connecting to server..... Done.
Upload log..... Done.

Success.
```

To upload log from the device to an RCP server using an RCP string:

```
Zxxx0:admin#upload log_toRCP rcp: tld2@172.18.212.104/home/Zxxx0.log
Command: upload log_toRCP rcp: tld2@172.18.212.104/home/Zxxx0.log

Connecting to server..... Done.
Upload log..... Done.

Success.

Zxxx0:admin#
```

## 84.9. config firmware image

### ● Description

This command is used to configure firmware as a boot-up image.

### ● Format

**config firmware image {unit <unit\_id 1-4>} <pathname> boot\_up**

### ● Parameters

---

|             |                                                                                             |
|-------------|---------------------------------------------------------------------------------------------|
| <b>unit</b> | (Optional) Specifies the unit ID used for this configuration.<br><b>&lt;unit_id 1-4&gt;</b> |
|-------------|---------------------------------------------------------------------------------------------|

---

Enter the unit ID used for this configuration here.

---

|                         |                                               |
|-------------------------|-----------------------------------------------|
| <b>&lt;pathname&gt;</b> | Specify a firmware on the device file system. |
|-------------------------|-----------------------------------------------|

---

|                |                          |
|----------------|--------------------------|
| <b>boot_up</b> | Specify as boot up file. |
|----------------|--------------------------|

---

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To configure a firmware file to bootup:

```
Zxxx0:admin#config firmware image 1.0.0.xx.rom boot_up
Command: config firmware image 1.0.0.xx.rom boot_up

Success.

Zxxx0:admin#
```



## 84.10. config configuration

---

### ● Description

This command is used to select a configuration file as the next boot up configuration or to apply a specific configuration to the system.

### ● Format

**config configuration {unit <unit\_id 1-4> <pathname> [boot\_up | active]}**

### ● Parameters

---

|             |                                                                      |
|-------------|----------------------------------------------------------------------|
| <b>unit</b> | (Optional) Specifies the unit ID used.<br><b>&lt;unit_id 1-4&gt;</b> |
|-------------|----------------------------------------------------------------------|

---

Enter the unit ID used here.

---

|                         |                                                           |
|-------------------------|-----------------------------------------------------------|
| <b>&lt;pathname&gt;</b> | Specifies a configuration file on the device file system. |
|-------------------------|-----------------------------------------------------------|

---

|                |                          |
|----------------|--------------------------|
| <b>boot_up</b> | Specify as boot up file. |
|----------------|--------------------------|

---

|               |                                       |
|---------------|---------------------------------------|
| <b>active</b> | Specifies to apply the configuration. |
|---------------|---------------------------------------|

---

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To configure the specific configuration file as boot up:

```
Zxxx0:admin#config configuration 1 boot_up
Command: config configuration 1 boot_up

Success

Zxxx0:admin#
```

## 84.11. show config

---

### ● Description

This command is used to display configuration information. The output stream of the configuration data can be filtered by the expression specified at the end of the command. The expression can contain up to three multiple filter evaluations. A filter evaluation begins with a filter type (include, exclude, and begin), followed by up to three filter strings (ex: "stp"). A filter string is enclosed by symbol ". The following describes the meaning of the each filter type: include: Includes lines that contain the specified filter string; exclude: Excludes lines that contain the specified filter string; and begin: The first line that contains the specified filter string will be the first line of the output.

The relationship of multiple filter strings following the same filter type is OR. That is, one line is qualified if one of specified filter strings is matched. If more than one filter evaluation is specified, the output of filtered by the former evaluation will be used as the input of the latter evaluation.

### ● Format

```
show config [effective | modified | current_config | boot_up | file <pathname>]
{[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}
{[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}
{[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string
80>}}}}}
```

### ● Parameters

|                                 |                                                                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>effective</b>                | Specifies to display only commands which affect the behavior of the device.                                                                                                     |
| <b>modified</b>                 | Specifies to display only the commands which are not from the 'reset' default setting.                                                                                          |
| <b>current_config</b>           | Specifies the current configuration.                                                                                                                                            |
| <b>boot_up</b>                  | Specifies the boot up configuration.                                                                                                                                            |
| <b>file</b>                     | Specify an absolute path name on the device file system.                                                                                                                        |
| <b>&lt;pathname&gt;</b>         | Specify an absolute path name on the device file system.                                                                                                                        |
| <b>include</b>                  | (Optional) Includes lines that contain the specified filter string.                                                                                                             |
| <b>exclude</b>                  | (Optional) Excludes lines that contain the specified filter string.                                                                                                             |
| <b>begin</b>                    | (Optional) The first line that contains the specified filter string will be the first line of the output.                                                                       |
| <b>&lt;filter_string 80&gt;</b> | Specify a filter string enclosed by the quotation mark symbol. Thus, the filter string itself cannot contain the quotation mark character. The filter string is case sensitive. |
| <b>&lt;filter_string 80&gt;</b> | Specify a filter string enclosed by the quotation mark symbol.                                                                                                                  |
| <b>&lt;filter_string 80&gt;</b> | Specify a filter string enclosed by the quotation mark symbol.                                                                                                                  |

## 84. Utility Commands

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To display configuration information:

```
Zxxx0:admin#show config current_config
Command: show config current_config

#-----
#                               Zxxx0 Gigabit Ethernet Switch
#                               Configuration
#
#                               Firmware: Build 1.0.x.xx
#-----

# STACK

config stacking force_master_role state disable

# DEVICE

config temperature threshold high 79
config temperature threshold low 11
config temperature trap state enable
config temperature log state enable

CTRL+C  ESC  q  Quit  SPACE  n  Next Page  ENTER  Next Entry  a  All
```

## 84.12. show boot\_file

---

### ● Description

This command is used to display the configuration file and firmware image assigned as boot up files.

### ● Format

show boot\_file

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display the configuration file and firmware image assigned as a boot up file:

```
Zxxx0:admin#show boot_file
Command: show boot_file

Bootup Firmware      : c:/runtime.rom
Bootup Configuration : c:/config.cfg

Zxxx0:admin#
```

## 84.13. config rcp server

### ● Description

This command is used to configure Remote Copy Protocol (RCP) global server information. This global RCP server setting can be used when the server or remote user name is not specified. Only one RCP server can be configured for each system. If a user does not specify the RCP server in the CLI command, and the global RCP server was not configured, the Switching Hub will ask the user to input the server IP address or remote user name while executing the RCP commands.

### ● Format

**config rcp server {ipaddress <ipaddr> | username <username>}**

### ● Parameters

#### ipaddress

(Optional) Specify the IP address of the global RCP server. By default, the server is unspecified.

#### <ipaddr>

Specify the IP address of the RCP server.

---

**username**(Optional) Specify the remote user name on the RCP server.

#### <username>

Specify the remote user name on the RCP server.

---

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To configure RCP global server information for the username "travel":

## 84. Utility Commands

```
Zxxx0:admin#config rcp server username travel
Command: config rcp server username travel

Success.

Zxxx0:admin#
```

### 84.14. config rcp server clear

#### ● Description

This command is used to clear Remote Copy Protocol (RCP) global server information.

#### ● Format

`config rcp server clear [ipaddr | username | both]`

#### ● Parameters

|                 |                                                               |
|-----------------|---------------------------------------------------------------|
| <b>ipaddr</b>   | Clear the IP address of the RCP server.                       |
| <b>username</b> | Clear the username of the RCP server.                         |
| <b>both</b>     | Clear both the IP address and the username of the RCP server. |

#### ● Restrictions

Only Administrator-level users can issue this command.

#### ● Example

To clear the current username of the RCP global server:

```
Zxxx0:admin#config rcp server clear username
Command: config rcp server clear username

Success.

Zxxx0:admin#
```

## 84.15. show rcp server

---

### ● Description

This command is used to display Remote Copy Protocol (RCP) global server information.

### ● Format

show rcp server

### ● Parameters

None.

### ● Restrictions

Only Administrator-level users can issue this command.

### ● Example

To display RCP global server information:

```
Zxxx0:admin#show rcp server
Command: show rcp server

RCP Server Address      :
RCP Server Username     : travel

Zxxx0:admin#
```

## 84.16. ping

---

### ● Description

This command is used to send Internet Control Message Protocol (ICMP) echo messages to a remote IP address. The remote IP address will then "echo" or return the message. This is used to confirm connectivity between the Switching Hub and the remote device.

### ● Format

ping [<ipaddr> | <domain\_name 255>] {times <value 1-255> | timeout <sec 1-99> | source\_ip <ipaddr>}

### ● Parameters

---

<ipaddr> Specify the IP address of the host.

---

## 84. Utility Commands

---

### <domain\_name 255>

Specifies the domain name of the host. This name can be up to 255 characters long.

---

**times** (Optional) Specify the number of individual ICMP echo messages to be sent.

#### <value 1-255>

Specify the number of individual ICMP echo messages to be sent. A value of 0 will send an infinite ICMP echo messages. The maximum value is 255. The default is 0

---

**timeout** (Optional) Specify the time-out period while waiting for a response from the remote device. A value of 1 to 99 seconds can be specified. The default is 1 second.

#### <sec 1-99>

Specify the time-out period while waiting for a response from the remote device. A value of 1 to 99 seconds can be specified. The default is 1 second.

---

### source\_ip

Specifies the source IP address of the ping packets. If specified, the IP address will be used as the packets' source IP address that ping send to remote host.

#### <ipaddr>

Enter the source IP address used here.

---

## ● Restrictions

None.

## ● Example

To send ICMP echo message to "10.51.17.1" for 4 times:

```
Zxxx0:admin#ping 10.51.17.1 times 4
Command: ping 10.51.17.1 times 4

Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms

Ping Statistics for 10.51.17.1
Packets: Sent =4, Received =4, Lost =0

Zxxx0:admin#
```

## 84.17. ping6

---

## ● Description

This command is used to send Internet Control Message Protocol (ICMP) echo messages to a remote IPv6 address. The remote IPv6 address will then "echo" or return the message. This is used to confirm connectivity between the Switching Hub and the remote device.

## ● Format

**ping6 <ipv6addr> {times <value 1-255> | size <value 1-6000> | timeout <sec 1-99> | source\_ip <ipv6addr>}**

## ● Parameters

|                         |                                                                                                                                                                                                                                                                                |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;ipv6addr&gt;</b> | Specify the IPv6 address of the host.                                                                                                                                                                                                                                          |
| <b>times</b>            | (Optional) Specify the number of individual ICMP echo messages to be sent.<br><b>&lt;value 1-255&gt;</b><br>Specify the number of individual ICMP echo messages to be sent. A value of 0 will send an infinite ICMP echo messages. The maximum value is 255. The default is 0. |
| <b>size</b>             | (Optional) Specify the size.<br><b>&lt;value 1-6000&gt;</b><br>Specify the size. A value of 1 to 6000 can be specified. The default is 100.                                                                                                                                    |
| <b>timeout</b>          | (Optional) Specify the time-out period while waiting for a response from the remote device.<br><b>&lt;value 1-99&gt;</b><br>Specify the time-out period while waiting for a response from the remote device. A value of 1 to 99 can be specified. The default is 1 second.     |
| <b>source_ip</b>        | Specifies the source IPv6 address of the ping packets. If specified, the IPv6 address will be used as the packets' source IPv6 address that ping send to remote host.<br><b>&lt;ipv6addr&gt;</b><br>Enter the source IPv6 address used here.                                   |

## ● Restrictions

None.

## ● Example

To send ICMP echo message to "3FFE:2::D04D:7878:66D:E5BC" for 10 times:

```
Zxxx0:admin#ping6 3FFE:2::D04D:7878:66D:E5BC times 10 size 6000 timeout 10
Command: ping6 3FFE:2::D04D:7878:66D:E5BC times 10 size 6000 timeout 10

Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Ping Statistics for 3FFE:2::D04D:7878:66D:E5BC
Packets: Sent =10, Received =10, Lost =0

Zxxx0:admin#
```



## 84.18. traceroute

---

### ● Description

This command is used to trace a route between the Switching Hub and a given host on the network.

### ● Format

**traceroute** [**<ipaddr>** | **<domain\_name 255>**] {**ttl <value 1-60>** | **port <value 30000-64900>** | **timeout <sec 1-65535>** | **probe <value 1-9>**}

### ● Parameters

|                                |                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;ipaddr&gt;</b>          | Specify the IP address of the destination end station.                                                                                                                                                                                                                                                                                                        |
| <b>&lt;domain_name 255&gt;</b> | Specify the domain name of the destination end station.                                                                                                                                                                                                                                                                                                       |
| <b>ttl</b>                     | (Optional) Specify the time to live value of the trace route request.<br><b>&lt;value 1-60&gt;</b><br>Specify the time to live value of the trace route request. This is the maximum number of routers that a trace route packet can pass while seeking the network path between two devices. The range for the TTL is 1 to 60 hops. The default value is 30. |
| <b>port</b>                    | (Optional) Specify the port number.<br><b>&lt;value 30000-64900&gt;</b><br>Specify the port number. The value range is from 30000 to 64900. The default is 33435.                                                                                                                                                                                             |
| <b>timeout</b>                 | (Optional) Specify the timeout period while waiting for a response from the remote device.<br><b>&lt;sec 1-65535&gt;</b><br>Specify the timeout period while waiting for a response from the remote device. A value of 1 to 65535 seconds can be specified. The default is 5 seconds.                                                                         |
| <b>probe</b>                   | (Optional) Specify the number of probes.<br><b>&lt;value 1-9&gt;</b><br>Specify the number of probes. The range is from 1 to 9. If unspecified, the default value is 1.                                                                                                                                                                                       |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To trace the route path between the Switching Hub and 10.48.74.121:

```

Zxxx0:admin#traceroute 10.48.74.121 probe 3
Command: traceroute 10.48.74.121 probe 3

<10 ms  10.12.73.254
<10 ms  10.12.73.254
<10 ms  10.12.73.254
<10 ms  10.19.68.1
<10 ms  10.19.68.1
<10 ms  10.19.68.1
<10 ms  10.48.74.121
Trace complete.

Zxxx0:admin#

```

## 84.19. traceroute6

### ● Description

This command is used to trace the IPv6 routed path between the Switch and a destination end station.

### ● Format

**traceroute6** <ipv6addr> {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value 1-9>}

### ● Parameters

|                         |                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;ipv6addr&gt;</b> | Specify the IPv6 address of the destination end station.                                                                                                                                                                                                                                                                                                      |
| <b>ttl</b>              | (Optional) Specify the time to live value of the trace route request.<br><b>&lt;value 1-60&gt;</b><br>Specify the time to live value of the trace route request. This is the maximum number of routers that a trace route packet can pass while seeking the network path between two devices. The range for the TTL is 1 to 60 hops. The default value is 30. |
| <b>port</b>             | (Optional) Specify the port number.<br><b>&lt;value 30000-64900&gt;</b><br>Specify the port number. The value range is from 30000 to 64900. The default is 33435.                                                                                                                                                                                             |
| <b>timeout</b>          | (Optional) Specify the timeout period while waiting for a response from the remote device.<br><b>&lt;sec 1-65535&gt;</b><br>Specify the timeout period while waiting for a response from the remote device. A value of 1 to 65535 seconds can be specified. The default is 5 seconds.                                                                         |
| <b>probe</b>            | (Optional) Specify the number of probes.<br><b>&lt;value 1-9&gt;</b><br>Specify the number of probes. The range is from 1 to 9. If unspecified, the default value is 1.                                                                                                                                                                                       |

## 84. Utility Commands

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

Trace the IPv6 routed path between the Switching Hub and 3000::1:

```
Zxxx0:admin# traceroute6 3000::1 probe 3
Command: traceroute6 3000::1 probe 3

1    <10 ms.      1345:142::11
2    <10 ms.      2011:14::100
3    <10 ms.      3000::1

Trace complete.
Zxxx0:admin#
```

Trace the IPv6 routed path between the Switching Hub and 1210:100::11 with port 40000:

```
Zxxx0:admin# traceroute6 1210:100::11 port 40000
Command: traceroute6 1210:100::11 port 40000

1    <10 ms.      3100::25
2    <10 ms.      4130::100
3    <10 ms.      1210:100::11

Trace complete.
Zxxx0:admin#
```

## 84.20. telnet

### ● Description

This command is used to login a Telnet server.

### ● Format

telnet [<ipaddr> | <domain\_name 255> | <ipv6addr>] {tcp\_port <value 1-65535>}

### ● Parameters

---

<ipaddr>(Optional) Specify the IP address of the Telnet server.

---

<domain\_name 255>

Specify the domain name of the telnet server.

---

<ipv6addr>

Specify the IPv6 address of the Telnet server.

---

---

**tcp\_port** (Optional) Specify the Telnet server port number to be connected to. If not specified, the default port is 23.

<value 1-65535>

Enter a value between 1 and 65535.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To Telnet to a Switching Hub by specifying the IP address:

```
Zxxx0:admin#telnet 10.1.1.1
Command: telnet 10.1.1.1

Zxxx0 Gigabit Ethernet Switch
Command Line Interface

Firmware: Build 1.0.0.xx

UserName:
```

## **84.21. enable broadcast\_ping\_reply**

---

### ● Description

The enable broadcast\_ping\_reply command used to enable broadcast ping reply state, device will reply broadcast ping request.

### ● Format

enable broadcast\_ping\_reply

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable broadcast ping reply state:

## 84. Utility Commands

```
Zxxx0:admin# enable broadcast_ping_reply
Command: enable broadcast_ping_reply

Success.

Zxxx0:admin#
```

### **84.22. disable broadcast\_ping\_reply**

#### ● Description

The disable broadcast\_ping\_reply command used to disable broadcast ping reply state, device won't reply broadcast ping request.

#### ● Format

**disable broadcast\_ping\_reply**

#### ● Parameters

None.

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To disable broadcast ping reply state:

```
Zxxx0:admin# disable broadcast_ping_reply
Command: disable broadcast_ping_reply

Success.

Zxxx0:admin#
```

## 84.23. show broadcast\_ping\_reply

---

- **Description**

The show broadcast\_ping\_reply command is used to show the broadcast ping reply state.

- **Format**

show broadcast\_ping\_reply

- **Parameters**

None.

- **Restrictions**

None.

- **Example**

To show broadcast ping reply state:

```
Zxxx0:admin# show broadcast_ping_reply
Command: show broadcast_ping_reply

Broadcast Ping Reply State:  Enabled

Zxxx0:admin#
```

## 85. Virtual Router Redundancy Protocol (VRRP) Command List

VRRP is a function to group multiple routers (VRRP group) and manage routers in a group as one virtual router. It is used to multiplex routers for disaster planning.

A virtual IP address and a virtual MAC address are assigned to a VRRP group, and other devices on the network communicate with the virtual router through the virtual address.

Routers in a VRRP are divided into one master router which actually performs routing, and other backup routers. They are automatically allocated based on the priority settings through information exchanges between VRRP enabled routers. If the master router fails, one of the backup routers automatically becomes the master router.

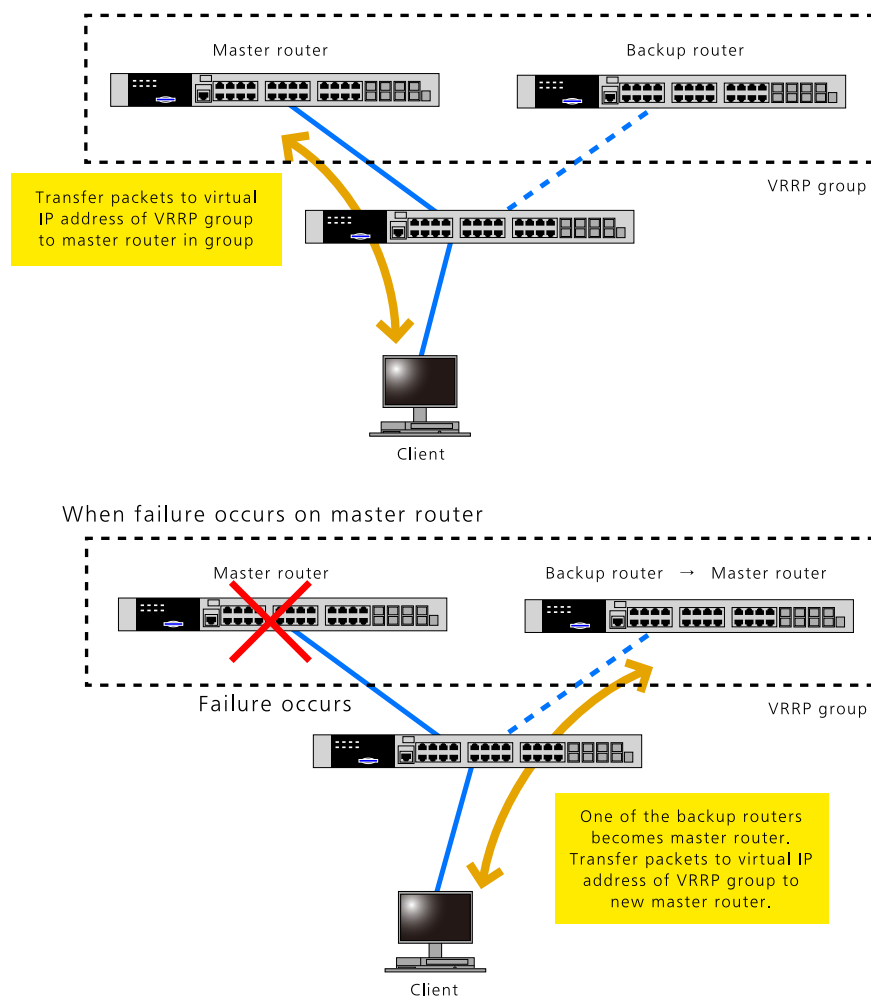


Figure 85-1 VRRP overview

---

```

enable vrrp {ping}
disable vrrp {ping}
create vrrp vrid <vrid 1-255> ipif <ipif_name 12> ipaddress <ipaddr> {state [enable | disable] |
priority <int 1-254> | advertisement_interval <int 1-255> | preempt [true | false] | critical_ip
<ipaddr> | critical_ip_state [enable | disable]}
config vrrp vrid <vrid 1-255> ipif <ipif_name 12> {state [enable | disable] | priority <int 1-254> |
ipaddress <ipaddr> | advertisement_interval <int 1-255> | preempt [true | false] | critical_ip
<ipaddr> | critical_ip_state [enable | disable]}
config vrrp ipif <ipif_name 12> [authtype [none | simple authdata <string 8> | ip authdata <string
16>]]
delete vrrp {vrid <vrid 1-255> ipif <ipif_name 12>}
show vrrp {ipif <ipif_name 12> {vrid <vrid 1-255>}}
config vrrp trap state [enable | disable]

```

---

## 85.1. enable vrrp

---

### ● Description

This command is used to enable VRRP globally.

### ● Format

```
enable vrrp {ping}
```

### ● Parameters

---

|             |                                                            |
|-------------|------------------------------------------------------------|
| <b>ping</b> | (Optional) Specifies that the ping option will be enabled. |
|-------------|------------------------------------------------------------|

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable VRRP:

```

Zxxx0:admin# enable vrrp
Command: enable vrrp

Success.

Zxxx0:admin#

```



## 85.2. disable vrrp

---

### ● Description

This command is used to disable VRRP globally.

### ● Format

**disable vrrp {ping}**

### ● Parameters

---

|             |                                                             |
|-------------|-------------------------------------------------------------|
| <b>ping</b> | (Optional) Specifies that the ping option will be disabled. |
|-------------|-------------------------------------------------------------|

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To disable VRRP:

```
Zxxx0:admin# disable vrrp
Command: disable vrrp

Success.

Zxxx0:admin#
```

## 85.3. create vrrp vrid

---

### ● Description

This command is used to create a virtual router entry by VRID.

### ● Format

**create vrrp vrid <vrid 1-255> ipif <ipif\_name 12> ipaddress <ipaddr> {state [enable | disable] | priority <int 1-254> | advertisement\_interval <int 1-255> | preempt [true | false] | critical\_ip <ipaddr> | critical\_ip\_state [enable | disable]}**

### ● Parameters

---

|             |                                                                                                                                                           |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vrid</b> | Specifies the ID of the Virtual Router used.<br><b>&lt;vrid 1-255&gt;</b><br>Enter the Virtual Router ID used here. This value must be between 1 and 255. |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|

---

## 85. Virtual Router Redundancy Protocol (VRRP) Command List

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b>                   | Specifies the IP interface used for this configuration.<br><b>&lt;ipif_name 12&gt;</b><br>Enter the IP interface name used here. This name can be up to 12 characters long.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>ipaddress</b>              | Specifies the virtual router's IP address used.<br><b>&lt;ipaddr&gt;</b><br>Enter the virtual router's IP address used here.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>state</b>                  | (Optional) Specifies the state of the virtual router function.<br><b>enable</b><br>Specifies that the virtual router function will be enabled.<br><b>disable</b><br>Specifies that the virtual router function will be disabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>priority</b>               | (Optional) Specifies the priority to be used for the Virtual Router Master election process<br><b>&lt;int 1-254&gt;</b><br>Enter the priority value used here. This value must be between 1 and 254.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>advertisement_interval</b> | (Optional) Specifies the time interval used between sending advertisement messages.<br><b>&lt;int 1-255&gt;</b><br>Enter the advertisement interval value here. This value must be between 1 and 255 seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>preempt</b>                | (Optional) Controls whether a higher priority virtual router will preempt a lower priority master. The preempt setting must be consistent with all the routers participating within the same VRRP group. Default is settings is true.<br><b>true</b> Specifies that if the backup router's priority is set higher than the masters priority, it will become the master instead of the current one.<br><b>false</b> Specifies that if the backup router's priority is higher than the masters priority, it will not become the master until the master failed.                                                                                                                                                                            |
| <b>critical_ip</b>            | (Optional) Specifies an IP address that will provide the most direct route to the Internet or other critical network connections from this virtual router. This IP address must be a real IP address of a real device on the network. If the connection from the virtual router to this IP address fails, the virtual router will automatically be disabled. A new Master will be elected from the backup routers participating in the VRRP group. Different critical IP addresses may be assigned to different routers participating in the VRRP group and can therefore define multiple routes to the Internet or other critical network connections.<br><b>&lt;ipaddr&gt;</b><br>Enter the critical interface's IP address used here. |
| <b>critical_ip_state</b>      | (Optional) Specifies the state of checking the status (active or inactive) of a critical IP address.<br><b>enable</b><br>Specifies that the critical IP state checking will be enabled.<br><b>disable</b><br>Specifies that the critical IP state checking will be disabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create a VRRP entry:

## 85. Virtual Router Redundancy Protocol (VRRP) Command List

```
Zxxx0:admin# create vrrp vrid 1 ipif System ipaddress 10.90.90.91 state enable
Command: create vrrp vrid 1 ipif System ipaddress 10.90.90.91 state enable

Success.

Zxxx0:admin#
```

### 85.4. config vrrp vrid

#### ● Description

This command is used to configure the virtual router settings by VRID.

#### ● Format

**config vrrp vrid <vrid 1-255> ipif <ipif\_name 12> {state [enable | disable] | priority <int 1-254> | ipaddress <ipaddr> | advertisement\_interval <int 1-255> | preempt [true | false] | critical\_ip <ipaddr> | critical\_ip\_state [enable | disable]}**

#### ● Parameters

|                               |                                                                                                                                                                                                                                  |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vrid</b>                   | Specifies the ID of the Virtual Router used.<br><b>&lt;vrid 1-255&gt;</b><br>Enter the Virtual Router ID used here. This value must be between 1 and 255.                                                                        |
| <b>ipif</b>                   | Specifies the IP interface used for this configuration.<br><b>&lt;ipif_name 12&gt;</b><br>Enter the IP interface name used here. This name can be up to 12 characters long.                                                      |
| <b>state</b>                  | (Optional) Specifies the state of the virtual router function.<br><b>enable</b><br>Specifies that the virtual router function will be enabled.<br><b>disable</b><br>Specifies that the virtual router function will be disabled. |
| <b>priority</b>               | (Optional) Specifies the priority to be used for the Virtual Router Master election process<br><b>&lt;int 1-254&gt;</b><br>Enter the priority value used here. This value must be between 1 and 254.                             |
| <b>ipaddress</b>              | Specifies the virtual router's IP address used.<br><b>&lt;ipaddr&gt;</b><br>Enter the virtual router's IP address used here.                                                                                                     |
| <b>advertisement_interval</b> | (Optional) Specifies the time interval used between sending advertisement messages.<br><b>&lt;int 1-255&gt;</b><br>Enter the advertisement interval value here. This value must be between 1 and 255 seconds.                    |

## 85. Virtual Router Redundancy Protocol (VRRP) Command List

---

**preempt** (Optional) Controls whether a higher priority virtual router will preempt a lower priority master. The preempt setting must be consistent with all the routers participating within the same VRRP group. Default is settings is true.

**true** Specifies that if the backup router's priority is set higher than the masters priority, it will become the master instead of the current one.

**false** Specifies that if the backup router's priority is higher than the masters priority, it will not become the master until the master failed.

---

### **critical\_ip**

(Optional) specifies an IP address that will provide the most direct route to the Internet or other critical network connections from this virtual router. This IP address must be a real IP address of a real device on the network. If the connection from the virtual router to this IP address fails, the virtual router will automatically be disabled. A new Master will be elected from the backup routers participating in the VRRP group. Different critical IP addresses may be assigned to different routers participating in the VRRP group and can therefore define multiple routes to the Internet or other critical network connections.

**<ipaddr>**

Enter the critical interface's IP address used here.

---

### **critical\_ip\_state**

(Optional) Specifies the state of checking the status (active or inactive) of a critical IP address.

**enable**

Specifies that the critical IP state checking will be enabled.

**disable**

Specifies that the critical IP state checking will be disabled.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure VRRP:

```
Zxxx0:admin# config vrrp vrid 1 ipif System state enable
Command: config vrrp vrid 1 ipif System state enable

Success.

Zxxx0:admin#
```

## 85.5. config vrrp ipif

---

### ● Description

This command is used to configure a virtual router authentication type on an interface.

### ● Format

**config vrrp ipif <ipif\_name 12> [authtype [none | simple authdata <string 8> | ip authdata <string 16>]]**

### ● Parameters

---

|                 |                                                                                                                                                                                                                                                   |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ipif</b>     | Specifies the name of IP interface used for this configuration.<br><b>&lt;ipif_name 12&gt;</b><br>Enter the IP interface name used here. This name can be up to 12 characters long.                                                               |
| <b>authtype</b> | Specifies the VRRP's authentication type.                                                                                                                                                                                                         |
| <b>none</b>     | Specifies that no authentication algorithm will be used on this interface.                                                                                                                                                                        |
| <b>simple</b>   | Specifies that the authentication algorithm will be set to simple text on this interface.                                                                                                                                                         |
| <b>authdata</b> | Specifies the authentication data used in the simple text authentication algorithm.<br><b>&lt;string 8&gt;</b><br>Enter the authentication data used in the simple text authentication algorithm here. This value can be up to 8 characters long. |
| <b>ip</b>       | Specifies that the authentication algorithm will be set to IP authentication header on this interface.                                                                                                                                            |
| <b>authdata</b> | Specifies the authentication data used in the IP authentication header algorithm.<br><b>&lt;string 16&gt;</b><br>Enter the authentication data used in the IP authentication header algorithm here. This value can be up to 16 characters long.   |

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure a VRRP IP interface:

```
Zxxx0:admin# config vrrp ipif System authtype simple authdata 12345678
Command: config vrrp ipif System authtype simple authdata 12345678

Success.

Zxxx0:admin#
```



## 85.6. delete vrrp

---

### ● Description

This command is used to delete the VRRP settings.

### ● Format

`delete vrrp {vrid <vrid 1-255> ipif <ipif_name 12>}`

### ● Parameters

|                                                                     |                                                                                                                                                         |
|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>vrid</b>                                                         | (Optional) Specifies the Virtual Router ID used.<br><vrid 1-255><br>Enter the Virtual Router ID used here. This value must be between 1 and 255.        |
| <b>ipif</b>                                                         | (Optional) Specifies the IP interface name used.<br><ipif_name 12><br>Enter the IP interface name used here. This name can be up to 12 characters long. |
| If no parameter is specified, all the VRRP entries will be deleted. |                                                                                                                                                         |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete VRRP:

```
Zxxx0:admin# delete vrrp vrid 3 ipif System
Command: delete vrrp vrid 3 ipif System

Success.

Zxxx0:admin#
```

## 85.7. show vrrp

---

### ● Description

This command is used to display the VRRP settings.

### ● Format

`show vrrp {ipif <ipif_name 12> {vrid <vrid 1-255>}}`

## ● Parameters

---

**ipif** (Optional) Specifies the IP interface name to be displayed.  
**<ipif\_name 12>**  
 Enter the IP interface name to be displayed here. This name can be up to 12 characters long.

---

**vrid** (Optional) Specifies the Virtual Router ID to be displayed.  
**<vrid 1-255>**  
 Enter the Virtual Router ID to be displayed here. This value must be between 1 and 255.

---

If no parameter is specified, then all the VRRP entries will be displayed.

---

## ● Restrictions

None.

## ● Example

To display the VRRP configuration:

```
Zxxx0:admin# show vrrp
Command: show vrrp

Global VRRP           : Disabled
Non-owner response Ping: Disabled

Interface Name         : System
Authentication type    : No Authentication

VRID                   : 1
Virtual IP Address     : 10.90.90.91
Virtual MAC Address    : 00-00-5E-00-01-01
Virtual Router State   : Initialize
State                  : Enabled
Priority                : 100
Master IP Address      : 10.90.90.90
Critical IP Address    : 0.0.0.0
Checking Critical IP   : Disabled
Advertisement Interval : 1 secs
Preempt Mode           : True
Virtual Router Up Time : 0 centi-secs
Total Entries: 1

Zxxx0:admin#
```

## 85.8. config vrrp trap state

---

### ● Description

This command is used to configure the trap sending state of the VRRP.



## 85. Virtual Router Redundancy Protocol (VRRP) Command List

### ● Format

`config vrrp trap state [enable|disable]`

### ● Parameters

---

**enable**

Specifies that the VRRP trap will be enabled.

**disable**

Specifies that the VRRP trap will be disabled.

---

### ● Restrictions

None.

### ● Example

To enable the VRRP trap:

```
Zxxx0:admin# config vrrp trap state enable
Command: config vrrp trap state enable

Success.

Zxxx0:admin#
```

## 86. Voice VLAN Commands

Voice VLAN is a function to configure a voice-specific VLAN to secure the bandwidth of voice data when normal communication data and voice data such as an IP phone coexist on the network. It prevents voice data delay and maintains the quality at the constant level regardless of the traffic status on the network.

To use a voice VLAN, you need to pre-register the vendor code (OUI) of an IP phone connected.

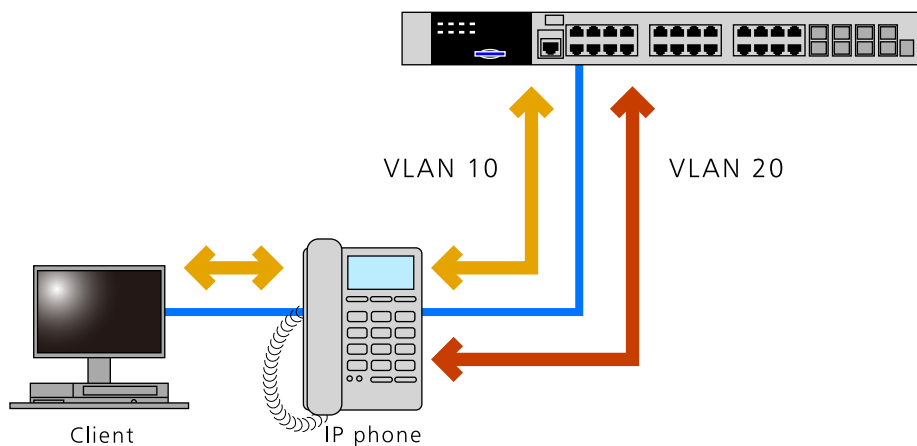


Figure 86-1 Voice VLAN overview

```
enable voice_vlan [<vlan_name 32> | vlanid <vlanid 1-4094>]
disable voice_vlan
config voice_vlan priority <int 0-7>
config voice_vlan oui [add | delete] <macaddr> <macmask> {description <desc 32>}
config voice_vlan ports [<portlist> | all] [state [enable | disable] | mode [auto{[tag | untag]}
    | manual]]
config voice_vlan log state [enable | disable]
config voice_vlan aging_time <min 1-65535>
show voice_vlan
show voice_vlan lldp_med voice_device
show voice_vlan oui
show voice_vlan ports {<portlist>}
show voice_vlan voice_device {ports <portlist>}
```

## 86.1. enable voice\_vlan

---

### ● Description

This command is used to enable the global voice VLAN function on a Switching Hub. To enable the voice VLAN, the voice VLAN must be also assigned. At the same time, the VLAN must be an existing static 802.1Q VLAN. To change the voice VLAN, the user must disable the voice VLAN function, and re-issue this command. By default, the global voice VLAN state is disabled.

### ● Format

**enable voice\_vlan** [**<vlan\_name 32>** | **vlanid <vlanid 1-4094>**]

### ● Parameters

---

**<vlan\_name 32>**

Specify the name of the voice VLAN. The maximum length is 32 characters. The name must be an existing static VLAN name.

---

**vlanid**

Specify the VLAN ID of the voice VLAN. The ID must be an existing static VLAN ID.

**<vlanid 1-4094>** Specify the VLAN ID between 1 and 4094.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable voice VLAN named v2:

```
Zxxx0:admin#enable voice_vlan Voice
Command: enable voice_vlan Voice

Success.

Zxxx0:admin#
```

## 86.2. disable voice\_vlan

---

### ● Description

This command is used to disable the voice VLAN function on a Switching Hub. When the voice VLAN function is disabled, the voice VLAN will become unassigned.

### ● Format

`disable voice_vlan`

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To disable voice VLAN:

```
Zxxx0:admin#disable voice_vlan
Command: disable voice_vlan

Success.

Zxxx0:admin#
```

## 86.3. config voice\_vlan priority

---

### ● Description

This command is used to configure voice VLAN priority. The voice VLAN priority will be the priority associated with the voice VLAN traffic to distinguish the QoS of the voice traffic from data traffic.

### ● Format

`config voice_vlan priority <int 0-7>`

### ● Parameters

---

<int 0-7> Specify the priority of the voice VLAN. The range is 0 to 7. The default priority is 5.

---

## 86. Voice VLAN Commands

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To set the priority of the voice VLAN to be six:

```
Zxxx0:admin#config voice_vlan priority 6
Command: config voice_vlan priority 6

Success.

Zxxx0:admin#
```

## 86.4. config voice\_vlan oui

### ● Description

This command is used to configure the user-defined voice traffic's OUI. The OUI is used to identify the voice traffic. There are a number of pre-defined OUIs. The user can further define the user-defined OUIs if needed. The user-defined OUI cannot be the same as the pre-defined OUI. The following are the pre-defined voice traffic's OUI:

| OUI      | Vendor      | Mnemonic Name |
|----------|-------------|---------------|
| 00:E0:BB | 3COM        | 3com          |
| 00:03:6B | Cisco       | cisco         |
| 00:E0:75 | Veritel     | veritel       |
| 00:D0:1E | Pingtel     | pingtel       |
| 00:01:E3 | Siemens     | siemens       |
| 00:60:B9 | NEC/Philips | nec&philips   |
| 00:0F:E2 | Huawei-3COM | huawei&3com   |
| 00:09:6E | Avaya       | avaya         |

### ● Format

**config voice\_vlan oui [add | delete] <macaddr> <macmask> {description <desc 32>}**

### ● Parameters

|                        |                                                                                      |
|------------------------|--------------------------------------------------------------------------------------|
| <b>add</b>             | Specify to add a user-defined OUI of Voice device vendor.                            |
| <b>delete</b>          | Specify to delete a user-defined OUI of Voice device vendor.                         |
| <b>&lt;macaddr&gt;</b> | Specify a user-defined OUI MAC address.                                              |
| <b>&lt;macmask&gt;</b> | Specify a user-defined OUI MAC address mask.                                         |
| <b>description</b>     | (Optional) Specify a description for the user-defined OUI.                           |
| <b>&lt;desc 32&gt;</b> | Specify a description for the user-defined OUI. The maximum length is 32 characters. |

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To add a user-defined OUI of a voice device:

```
Zxxx0:admin#config voice_vlan oui add 00-C0-8F-00-00-00 FF-FF-FF-00-00-00
Command: config voice_vlan oui add 00-C0-8F-00-00-00 FF-FF-FF-00-00-00

Success.

Zxxx0:admin#
```

# 86.5. config voice\_vlan ports

## ● Description

This command is used to enable or disable the voice VLAN function on ports or mode per port.

## ● Format

**config voice\_vlan ports** [<portlist> | all] [state [enable | disable] | mode [auto{[tag | untag]} | manual]]

## ● Parameters

|                         |                                                                                                                                                                                                                                                                                    |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;portlist&gt;</b> | Specify a range of ports to set.                                                                                                                                                                                                                                                   |
| <b>all</b>              | Specify to set all ports.                                                                                                                                                                                                                                                          |
| <b>state</b>            | Specify the voice VLAN function state on ports. The default state is disabled.                                                                                                                                                                                                     |
| <b>enable</b>           | Specify to enable the voice VLAN function state on ports.                                                                                                                                                                                                                          |
| <b>disable</b>          | Specify to disable the voice VLAN function state on ports.                                                                                                                                                                                                                         |
| <b>mode</b>             | The voice VLAN mode. The default mode is auto.                                                                                                                                                                                                                                     |
| <b>auto</b>             | When the mode is auto, the port may become the voice VLAN member port by auto-learning. If the MAC address of the received packet matches the configured OUI, the port will be learned as dynamic member port. The dynamic membership will be removed via the aging out mechanism. |
| <b>manual</b>           | When the mode is set to manual, the port needs to be manually added into or removed from the voice VLAN by 802.1Q VLAN configuration command.                                                                                                                                      |

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To configure voice VLAN ports 4 to 6 to enable:

## 86. Voice VLAN Commands

```
Zxxx0:admin#config voice_vlan ports 4-6 state enable
Command: config voice_vlan ports 4-6 state enable

Success.

Zxxx0:admin#
```

To set voice VLAN ports 4 to 6 to auto mode:

```
Zxxx0:admin#config voice_vlan ports 4-6 mode auto
Command: config voice_vlan ports 4-6 mode auto

Success.

Zxxx0:admin#
```

### 86.6. config voice\_vlan log state

---

#### ● Description

This command is used to configure the voice VLAN log state.

#### ● Format

config voice\_vlan log state [enable | disable]

#### ● Parameters

|                |                                              |
|----------------|----------------------------------------------|
| <b>enable</b>  | Specify to enable the voice VLAN log state.  |
| <b>disable</b> | Specify to disable the voice VLAN log state. |

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To enable the voice VLAN log state:

```
Zxxx0:admin#config voice_vlan log state enable
Command: config voice_vlan log state enable

Success.

Zxxx0:admin#
```

## 86.7. config voice\_vlan aging\_time

---

### ● Description

This command is used to set the aging time of the voice VLAN. The aging time is used to remove a port from voice VLAN if the port is an automatic VLAN member. When the last voice device stops sending traffic and the MAC address of this voice device is aged out, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after expiration of voice VLAN aging timer. If the voice traffic resumes during the aging time, the aging timer will be reset and stop.

### ● Format

config voice\_vlan aging\_time <min 1-65535>

### ● Parameters

---

<min 1-65535>

Specify the aging time. The range is 1 to 65535 minutes. The default value is 720 minutes.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To set 60 minutes as the aging time of voice VLAN:

```
Zxxx0:admin#config voice_vlan aging_time 60
Command: config voice_vlan aging_time 60

Success.

Zxxx0:admin#
```

## 86.8. show voice\_vlan

---

### ● Description

This command is used to display voice VLAN global information.

### ● Format

show voice\_vlan



## 86. Voice VLAN Commands

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display voice VLAN information:

```
Zxxx0:admin#show voice_vlan
Command: show voice_vlan

Voice VLAN State      : Disabled
Voice VLAN           : Unassigned
Priority              : 5
Aging Time            : 720 minutes
Log State             : Enabled

Zxxx0:admin#
```

## **86.9. show voice\_vlan lldp\_med voice\_device**

### ● Description

This command is used to display the voice devices that are discovered by LLDP-MED.

### ● Format

**show voice\_vlan lldp\_med voice\_device**

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display the voice devices that were discovered by LLDP-MED:

```

Zxxx0:admin# show voice_vlan lldp_med voice_device
Command: show voice_vlan lldp_med voice_device

Index          : 1
Local Port     : 1:1
Chassis ID Subtype : MAC Address
Chassis ID     : 00-C0-8F-00-00-11
Port ID Subtype : Network Address
Port ID        : 00-C0-8F-00-00-00
Create Time    : 9/1/2013 08:30
Remain Time    : 120 Seconds

Index          : 2
Local Port     : 1:3
Chassis ID Subtype : MAC Address
Chassis ID     : 00-C0-8F-00-00-12
Port ID Subtype : Network Address
Port ID        : 00-C0-8F-00-00-00
Create Time    : 9/1/2013 08:30
Remain Time    : 120 Seconds

Total Entries: 2

Zxxx0:admin#

```

## 86.10. show voice\_vlan oui

---

### ● Description

This command is used to display the OUI information for voice VLAN.

### ● Format

**show voice\_vlan oui**

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

To display voice VLAN OUI:

## 86. Voice VLAN Commands

```
Zxxx0:admin#show voice_vlan oui  
Command: show voice_vlan oui
```

| OUI               | Address           | Mask         | Description |
|-------------------|-------------------|--------------|-------------|
| 00-01-E3-00-00-00 | FF-FF-FF-00-00-00 | Siemens      |             |
| 00-03-6B-00-00-00 | FF-FF-FF-00-00-00 | Cisco        |             |
| 00-09-6E-00-00-00 | FF-FF-FF-00-00-00 | Avaya        |             |
| 00-0F-E2-00-00-00 | FF-FF-FF-00-00-00 | Huawei&3COM  |             |
| 00-60-B9-00-00-00 | FF-FF-FF-00-00-00 | NEC&Phillips |             |
| 00-D0-1E-00-00-00 | FF-FF-FF-00-00-00 | Pingtel      |             |
| 00-E0-75-00-00-00 | FF-FF-FF-00-00-00 | Veritel      |             |
| 00-E0-BB-00-00-00 | FF-FF-FF-00-00-00 | 3COM         |             |

```
Total Entries: 8
```

```
Zxxx0:admin#
```

### 86.11. show voice\_vlan ports

#### ● Description

This command is used to display port voice VLAN information.

#### ● Format

**show voice\_vlan ports {<portlist>}**

#### ● Parameters

---

**<portlist>**(Optional) Specify a range of ports to display.

---

---

**NOTE** If no parameter is specified, all voice VLAN port information will be displayed.

---

#### ● Restrictions

None.

#### ● Example

To display voice VLAN ports 1 to 3:

```
Zxxx0:admin#show voice_vlan ports 1-3
Command: show voice_vlan ports 1-3
```

| Ports | Status   | Mode  |
|-------|----------|-------|
| ----- | -----    | ----- |
| 1     | Disabled | Auto  |
| 2     | Disabled | Auto  |
| 3     | Disabled | Auto  |

```
Zxxx0:admin#
```

## 86.12. show voice\_vlan voice\_device

### ● Description

This command is used to show voice devices that are connected to the ports. The start time is the time when the device is detected on this port and the activate time is the latest time when the device sends the traffic.

### ● Format

**show voice\_vlan voice\_device {ports <portlist>}**

### ● Parameters

---

**<portlist>**(Optional) Specify a range of ports to display.

---



---

**NOTE** If no parameter is specified, the system will display the connected Voice device of all ports.

---

### ● Restrictions

None.

### ● Example

To display voice VLAN device ports 1 to 2:

```
Zxxx0:admin#show voice_vlan voice_device ports 1-2
Command: show voice_vlan voice_device ports 1-2
```

| Ports             | Voice Device | Start Time | Last Active Time |
|-------------------|--------------|------------|------------------|
| -----             | -----        | -----      | -----            |
| Total Entries : 0 |              |            |                  |

```
Zxxx0:admin#
```

## 87. VLAN Commands

VLAN (Virtual LAN) is a function to divide ports of this Switching Hub into groups and create multiple virtual LAN environments. As one VLAN corresponds to the broadcast domain, this function allows to improve security by restraining communications between VLANs, as well as reducing traffic on the network.

This Switching Hub supports many VLAN types, including port-based VLAN, IEEE 802.1Q compliant tagged VLAN, MAC-based VLAN, and subnet VLAN.

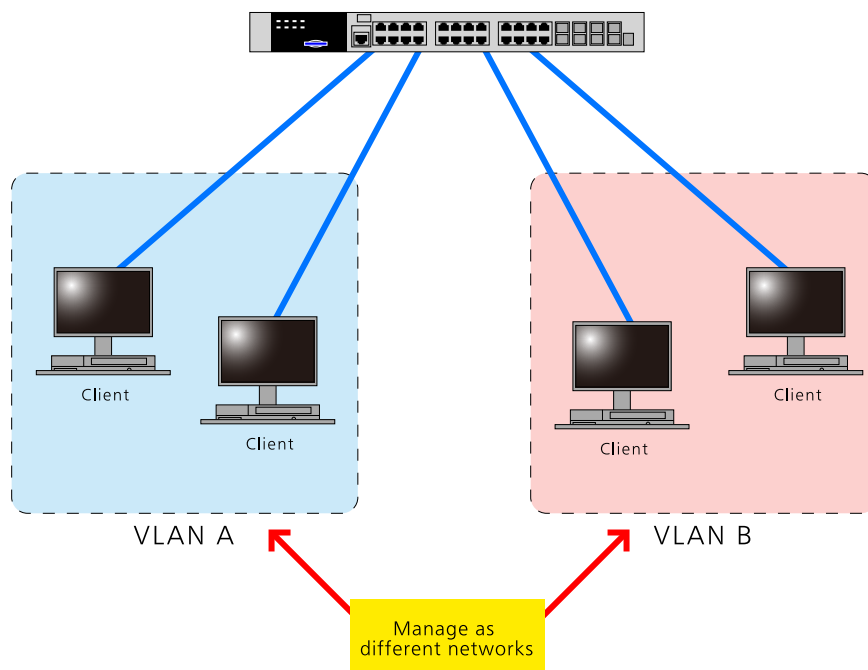


Figure 87-1 VLAN overview

```

create vlan <vlan_name 32> tag <vlanid 2-4094> {type [1q_vlan | private_vlan]} {advertisement}
create vlan <vlanid <vidlist> {type [1q_vlan | private_vlan]} {advertisement}
delete vlan <vlan_name 32>
delete vlan <vlanid <vidlist>
config vlan <vlan_name 32> {[add [tagged | untagged | forbidden] | delete] <portlist> |
  advertisement [enable | disable]}(1)
config vlan <vlanid <vidlist> {[add [tagged | untagged | forbidden] | delete] <portlist> |
  advertisement [enable | disable] | name <vlan_name 32>}(1)
config port_vlan [<portlist> | all] {gvrp_state [enable | disable] | ingress_checking [enable |
  disable] | acceptable_frame [tagged_only | admit_all] | pvid <vlanid 1-4094>}(1)
show port_vlan {<portlist>}
config gvrp [timer [join | leave | leaveall] <value 100-100000> | nni_bpdu_addr [dot1d | dot1ad]]
enable gvrp
disable gvrp
show vlan {<vlan_name 32>}
  
```

---

```
show vlan vlanid <vidlist>
show vlan ports {<portlist>}
show gvrp
config private_vlan [<vlan_name 32> | vid <vlanid 1-4094>] [add [isolated | community] | remove]
    [<vlan_name 32> | vlanid <vidlist>]
show private_vlan {[<vlan_name 32> | vlanid <vidlist>]}
```

---

## 87.1. create vlan

---

### ● Description

This command is used to create a VLAN on the Switching Hub. The VLAN ID must be always specified for creating a VLAN.

### ● Format

```
create vlan <vlan_name 32 > tag <vlanid 2-4094> {type [1q_vlan | private_vlan]}
{advertisement}
```

### ● Parameters

---

|                              |                                                                                                                                                                          |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;vlan_name 32 &gt;</b> | Specify the name of the VLAN to be created. The maximum length is 32 characters.                                                                                         |
| <b>tag</b>                   | Specify the VLAN ID of the VLAN to be created.<br><b>&lt;vlanid 2-4094&gt;</b><br>The range is from 2 to 4094.                                                           |
| <b>type</b>                  | (Optional) Specify the type of VLAN to be created.<br><b>1q_vlan</b><br>Specify the VLAN is a 802.1q VLAN.<br><b>private_vlan</b><br>Specify the VLAN is a private VLAN. |
| <b>advertisement</b>         | (Optional) Specify to allow the Switch sending out GVRP packets to outside sources, notifying that they may join the existing VLAN.                                      |

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create a VLAN with the name "v2" and VLAN ID 2:

```
Zxxx0:admin#create vlan v2 tag 2 type 1q_vlan advertisement
Command: create vlan v2 tag 2 type 1q_vlan advertisement

Success.

Zxxx0:admin#
```

## 87. VLAN Commands

To create a private VLAN with the name "v3" and VLAN ID 3:

```
Zxxx0:admin#create vlan v3 tag 3 type private_vlan
Command: create vlan v3 tag 3 type private_vlan

Success.

Zxxx0:admin#
```

## 87.2. create vlan vlanid

### ● Description

This command is used to create a VLAN on the Switching Hub. The VLAN ID must be always specified for creating a VLAN.

### ● Format

**create vlan vlanid <vidlist> {type [1q\_vlan | private\_vlan]} {advertisement}**

### ● Parameters

---

**<vidlist>** Specify the VLAN ID of the VLAN to be created.

---

**type** (Optional) Specify the type of VLAN to be created.

**1q\_vlan**

Specify the VLAN is a 802.1q VLAN.

**private\_vlan**

Specify the VLAN is a private VLAN.

---

**advertisement**

(Optional) Specify to allow the Switch sending out GVRP packets to outside sources, notifying that they may join the existing VLAN.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create a VLAN with VLAN ID 2:

```
Zxxx0:admin#create vlan vlanid 2 type 1q_vlan advertisement
Command: create vlan vlanid 2 type 1q_vlan advertisement

Success.

Zxxx0:admin#
```

To create a private VLAN with VLAN ID 3:

```
Zxxx0:admin#create vlan vlanid 3 type private_vlan
Command: create vlan vlanid 3 type private_vlan

Success.

Zxxx0:admin#
```

## 87.3. delete vlan

---

### ● Description

This command is used to delete a previously configured VLAN on the Switching Hub.

### ● Format

**delete vlan <vlan\_name 32>**

### ● Parameters

---

**<vlan\_name 32>**

Specify the VLAN name of the VLAN to be deleted. The maximum length is 32 characters.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To remove VLAN v1:

```
Zxxx0:admin#delete vlan v1
Command: delete vlan v1

Success.

Zxxx0:admin#
```

## 87.4. delete vlan vlanid

---

### ● Description

This command is used to delete a previously configured VLAN ID on the Switching Hub.

### ● Format

**delete vlan vlanid <vidlist>**



## 87. VLAN Commands

### ● Parameters

---

**<vidlist>** Specify a range of VLAN ID to be deleted.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To remove a VLAN ID 2:

```
Zxxx0:admin#delete vlan vlanid 2
Command: delete vlan vlanid 2

Success.

Zxxx0:admin#
```

## 87.5. config vlan

---

### ● Description

This command is used to add or delete ports to or from the port list of a previously configured VLAN. Users can specify the additional ports as tagged, untagged, or forbidden.

### ● Format

**config vlan <vlan\_name 32> {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable]}(1)**

### ● Parameters

---

|                             |                                                                                                                               |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;vlan_name 32&gt;</b> | Specify the name of the VLAN to add or delete ports to. The maximum length is 32 characters.                                  |
| <b>add</b>                  | Specify the port attribute to add.                                                                                            |
| <b>tagged</b>               | Specify the additional ports as tagged.                                                                                       |
| <b>untagged</b>             | Specify the additional ports as untagged.                                                                                     |
| <b>forbidden</b>            | Specify the ports to be forbidden from becoming members of the VLAN dynamically and not able to forward packets in this VLAN. |
| <b>delete</b>               | Specify the port status to delete.                                                                                            |
| <b>&lt;portlist&gt;</b>     | Specify a range of ports to add or delete to the VLAN.                                                                        |

---

---

**advertisement**

Specify to send GVRP out for this VLAN or not. If not, the VLAN cannot be joint dynamically.

**enable**

Specify to enable GVRP.

**disable**

Specify to disable GVRP.

---

**● Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

**● Example**

To add 4 through 8 as tagged ports to the VLAN v1:

```
Zxxx0:admin#config vlan v1 add tagged 4-8
Command: config vlan v1 add tagged 4-8

Success.

Zxxx0:admin#
```

To delete ports 4 through 8 from VLAN v1:

```
Zxxx0:admin#config vlan v1 delete 4-8
Command: config vlan v1 delete 4-8

Success.

Zxxx0:admin#
```

To enable the VLAN default advertisement:

```
Zxxx0:admin#config vlan default advertisement enable
Command: config vlan default advertisement enable

Success.

Zxxx0:admin#
```

## 87.6. config vlan vlanid

### ● Description

This command is used to add or delete ports to the port list of a previously configured VLAN. Users can specify the additional ports as tagged, untagged, or forbidden.

### ● Format

**config vlan vlanid <vidlist> {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable] | name <vlan\_name 32>}(1)**

### ● Parameters

|                             |                                                                                                                               |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;vidlist&gt;</b>      | Specify the VLAN ID of the VLAN to add or delete ports to.                                                                    |
| <b>add</b>                  | Specify the port attribute to add.                                                                                            |
| <b>tagged</b>               | Specify the additional ports as tagged.                                                                                       |
| <b>untagged</b>             | Specify the additional ports as untagged.                                                                                     |
| <b>forbidden</b>            | Specify the ports to be forbidden from becoming members of the VLAN dynamically and not able to forward packets in this VLAN. |
| <b>delete</b>               | Specify the port status to delete.                                                                                            |
| <b>&lt;portlist&gt;</b>     | Specify a range of ports to add or delete to the VLAN.                                                                        |
| <b>advertisement</b>        | Specify to send GVRP out for this VLAN or not. If not, the VLAN cannot be joint dynamically.                                  |
| <b>enable</b>               | Specify to enable GVRP.                                                                                                       |
| <b>disable</b>              | Specify to disable GVRP.                                                                                                      |
| <b>name</b>                 | Specify the VLAN name.                                                                                                        |
| <b>&lt;vlan_name 32&gt;</b> | The maximum length is 32 characters.                                                                                          |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To add 4 through 8 as tagged ports to the VLAN 1:

```
Zxxx0:admin#config vlan vlanid 1 add tagged 4-8
Command: config vlan vlanid 1 add tagged 4-8

Success.

Zxxx0:admin#
```

To delete ports 4 through 8 from VLAN 1:

```
Zxxx0:admin#config vlan vlanid 1 delete 4-8
Command: config vlan vlanid 1 delete 4-8

Success.

Zxxx0:admin#
```

To enable the VLAN default advertisement:

```
Zxxx0:admin#config vlan vlanid default advertisement enable
Command: config vlan vlanid default advertisement enable

Success.

Zxxx0:admin#
```

## 87.7. config port\_vlan

### ● Description

This command is used to set the ingress checking status and the sending and receiving of GVRP information.

### ● Format

**config port\_vlan** [<portlist> | all] {gvrp\_state [enable | disable] | ingress\_checking [enable | disable] | acceptable\_frame [tagged\_only | admit\_all] | pvid <vlanid 1- 4094>} (1)

### ● Parameters

---

**<portlist>** Specify a range of ports to be configured.

---

**all** Specify to configure all ports.

---

#### **gvrp\_state**

Specify if the port is allowed to dynamically become a member of a VLAN when receiving GVRP.

##### **enable**

Enable GVRP for the ports specified in the port list.

##### **disable**

Disable GVRP for the ports specified in the port list.

---

#### **ingress\_checking**

When ingress checking is enabled, the Switch checks if the incoming packet was assigned a VLAN on which the ingress port is a VLAN member. If the incoming packet and the ingress port are not in the same VLAN, the packet will be dropped.

##### **enable**

Enable ingress checking for the specified port list.

##### **disable**

Disable ingress checking for the specified port list.

---

## 87. VLAN Commands

---

### **acceptable\_frame**

Specify the type of frame that will be accepted by the port.

#### **tagged\_only**

Only tagged frame will be received.

#### **admit\_all**

Both tagged and untagged frames will be accepted.

---

### **pvid**

Specify the Port VID (PVID) that will be associated with the port.

**<vlanid 1- 4094>**

Specify the VLAN ID between 1 and 4094.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the port VLAN:

```
Zxxx0:admin#config port_vlan 1-5 gvrp_state enable ingress_checking enable
acceptable_frame tagged_only pvid 2
Command: config port_vlan 1-5 gvrp_state enable ingress_checking enable
acceptable_frame tagged_only pvid 2
```

Success.

Zxxx0:admin#

## 87.8. show port\_vlan

---

### ● Description

This command is used to display the GVRP status for a port list on the Switching Hub.

### ● Format

**show port\_vlan {<portlist>}**

### ● Parameters

---

**<portlist>**(Optional) Specify a range of ports to be displayed.

---

---

#### **NOTE**

If no parameter is specified, the system will display GVRP information for all ports.

---

### ● Restrictions

None.

## ● Example

To display 802.1q port settings for ports 1 to 3:

```
Zxxx0:admin#show port_vlan 1-3
Command: show port_vlan 1-3
```

| Port | PVID | GVRP     | Ingress Checking | Acceptable Frame Type |
|------|------|----------|------------------|-----------------------|
| 1    | 1    | Disabled | Enabled          | All Frames            |
| 2    | 1    | Disabled | Enabled          | All Frames            |
| 3    | 1    | Disabled | Enabled          | All Frames            |

```
Total Entries : 3

Zxxx0:admin#
```

## 87.9. config gvrp

### ● Description

This command is used to set the GVRP timer's value.

### ● Format

**config gvrp** [timer [join | leave | leaveall] <value 100-100000> | nni\_bpdu\_addr [dot1d | dot1ad]]

### ● Parameters

|                                 |                                                                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>timer</b>                    | Specify GVRP timer.                                                                                                                                                                       |
| <b>join</b>                     | Specify the Join time will be set. The default value is 200 milliseconds.                                                                                                                 |
| <b>leave</b>                    | Specify the Leave time will be set. The default value is 600 milliseconds.                                                                                                                |
| <b>leaveall</b>                 | Specify the LeaveAll time. The default value is 10000 milliseconds.                                                                                                                       |
| <b>&lt;value 100-100000&gt;</b> | Specify the time value. The value range is 100 to 100000 milliseconds. In addition, the Leave time should greater than 2 Join times and the LeaveAll time should greater than Leave time. |
| <b>nni_bpdu_addr</b>            | Determine the BPDU protocol address for GVRP in service provide site. It can use 802.1d GVRP address, or 802.1ad service provider GVRP address.                                           |
| <b>dot1d</b>                    | Specify a 802.1d GVRP address.                                                                                                                                                            |
| <b>dot1ad</b>                   | Specify a 802.1ad service provider GVRP address.                                                                                                                                          |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## 87. VLAN Commands

### ● Example

To set the Join time to 200 milliseconds:

```
Zxxx0:admin#config gvrp timer join 200
Command: config gvrp timer join 200

Success.

Zxxx0:admin#
```

## 87.10. enable gvrp

---

### ● Description

This command is used to enable the Generic VLAN Registration Protocol (GVRP). The default is disabled.

### ● Format

**enable gvrp**

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable the generic VLAN Registration Protocol (GVRP):

```
Zxxx0:admin#enable gvrp
Command: enable gvrp

Success.

Zxxx0:admin#
```

## 87.11. disable gvrp

---

### ● Description

This command is used to disable Generic VLAN Registration Protocol (GVRP).

### ● Format

`disable gvrp`

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To disable Generic VLAN Registration Protocol (GVRP):

```
Zxxx0:admin#disable gvrp
Command: disable gvrp

Success.

Zxxx0:admin#
```

## 87.12. show vlan

---

### ● Description

This command is used to display summary information about each VLAN, which includes: VLAN ID, VLAN Name, Tagged/Untagged/Forbidden status for each port, and Member/Non-member status for each port.

### ● Format

`show vlan {<vlan_name 32>}`

### ● Parameters

---

`<vlan_name 32>`(Optional) Specify the name of the VLAN to be displayed. The maximum length is 32 characters.

---



## 87. VLAN Commands

### ● Restrictions

None.

### ● Example

To display VLAN settings:

```
Zxxx0:admin#show vlan
Command: show vlan

VLAN Trunk State      : Disabled
VLAN Trunk Member Ports :

VID                  : 1                VLAN Name      : default
VLAN Type            : Static            Advertisement : Enabled
Member Ports        : 1-28
Static Ports         : 1-28
Current Tagged Ports :
Current Untagged Ports: 1-28
Static Tagged Ports  :
Static Untagged Ports: 1-28
Forbidden Ports      :

Total Static VLAN Entries: 1
Total GVRP VLAN Entries: 0

Zxxx0:admin#
```

## 87.13. show vlan vlanid

---

### ● Description

This command is used to display summary information about each VLAN, which includes: VLAN ID, VLAN Name, Tagged/Untagged/Forbidden status for each port, and Member/Non-member status for each port.

### ● Format

**show vlan vlanid <vidlist>**

### ● Parameters

---

**<vidlist>** Specify the VLAN ID number to be displayed.

---

### ● Restrictions

None.

## ● Example

To display VLAN settings for VLAN ID 1:

```
Zxxx0:admin#show vlan vlanid 1
Command: show vlan vlanid 1

VID                : 1                VLAN Name          : default
VLAN Type          : Static           Advertisement     : Enabled
Member Ports       : 1-28
Static Ports       : 1-28
Current Tagged Ports :
Current Untagged Ports: 1-28
Static Tagged Ports :
Static Untagged Ports : 1-28
Forbidden Ports     :

Total Entries : 1

Zxxx0:admin#
```

## 87.14. show vlan ports

---

### ● Description

This command is used to display summary information about Tagged, Untagged, and Forbidden status for each port.

### ● Format

**show vlan ports {<portlist>}**

### ● Parameters

---

**<portlist>**(Optional) Specify a range of ports for which you want to display VLAN. The beginning and end of the port list range are separated by a dash.

---

### ● Restrictions

None.

### ● Example

To display VLAN port settings:

## 87. VLAN Commands

```
Zxxx0:admin#show vlan ports 1-2
Command: show vlan ports 1-2
```

| Port  | VID   | Untagged | Tagged | Dynamic | Forbidden |
|-------|-------|----------|--------|---------|-----------|
| ----- | ----- | -----    | -----  | -----   | -----     |
| 1     | 1     | X        | -      | -       | -         |
| 2     | 1     | X        | -      | -       | -         |

```
Zxxx0:admin#
```

### 87.15. show gvrp

---

#### ● Description

This command is used to display the GVRP status for the Switching Hub.

#### ● Format

**show gvrp**

#### ● Parameters

None.

#### ● Restrictions

None.

#### ● Example

To display the GVRP status of the Switching Hub:

```
Zxxx0:admin#show gvrp
Command: show gvrp

Global GVRP      : Disabled
Join Time        : 200 Milliseconds
Leave Time        : 600 Milliseconds
LeaveAll Time     : 10000 Milliseconds
NNI BPDU Address: dot1d

Zxxx0:admin#
```

## 87.16. config private\_vlan

---

### ● Description

A private VLAN is comprised of a primary VLAN, up to one isolated VLAN, and a number of community VLANs. A private VLAN ID is presented by the VLAN ID of the primary VLAN. The command used to associate or de-associate a secondary VLAN with a primary VLAN. A primary VLAN is created via the command **create vlan type private\_vlan**. A secondary VLAN is created via the command **create vlan type 1q\_vlan**. A secondary VLAN cannot be associated with multiple primary VLANs. The untagged member port of the primary VLAN is named as the promiscuous port. The tagged member port of the primary VLAN is named as the trunk port. A promiscuous port of a private VLAN cannot be promiscuous port of other private VLANs. The primary VLAN member port cannot be a secondary VLAN member at the same time, or vice versa. A secondary VLAN can only have the untagged member port. The member port of a secondary VLAN cannot be member port of other secondary VLAN at the same time. When a VLAN is associated with a primary VLAN as the secondary VLAN, the promiscuous port of the primary VLAN will behave as the untagged member of the secondary VLAN, and the trunk port of the primary VLAN will behave as the tagged member of the secondary VLAN. A secondary VLAN cannot be specified with advertisement. Only the primary VLAN can be configured as a layer 3 interface. The private VLAN member port cannot be configured with the traffic segmentation function.

### ● Format

**config private\_vlan** [<vlan\_name 32> | vid <vlanid 1-4094>] [add [isolated | community] | remove] [<vlan\_name 32> | vlanid <vidlist>]

### ● Parameters

|                              |                                                                                                                                   |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;vlan_name 32&gt;</b>  | Specify the name of the private VLAN. The maximum length is 32 characters.                                                        |
| <b>vid</b>                   | Specify the VLAN ID of the private VLAN.                                                                                          |
| <b>&lt;vlanid 1-4094&gt;</b> | Specify the VLAN ID between 1 and 4094.                                                                                           |
| <b>add</b>                   | Specify to add isolated or community.                                                                                             |
| <b>isolated</b>              | Specify the secondary VLAN as an isolated VLAN.                                                                                   |
| <b>community</b>             | Specify the secondary VLAN as a community VLAN.                                                                                   |
| <b>remove</b>                | Specify to remove the specified private VLAN.                                                                                     |
| <b>&lt;vlan_name 32&gt;</b>  | Specify the VLAN of a range of secondary VLANs to add to the private VLAN or remove from it. The maximum length is 32 characters. |
| <b>vlanid</b>                | Specify a range of the second VLAN IDs to add to the private VLAN or remove from it.                                              |
| <b>&lt;vidlist&gt;</b>       | Specifies a VLAN ID.                                                                                                              |

## 87. VLAN Commands

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To associate secondary VLAN to private VLAN p1:

```
Zxxx0:admin#config private_vlan p1 add community vlanid 2-5
Command: config private_vlan p1 add community vlanid 2-5

Success.

Zxxx0:admin#
```

## 87.17. show private\_vlan

---

### ● Description

This command is used to display private VLAN information on the Switching Hub.

### ● Format

show private\_vlan {[<vlan\_name 32> | vlanid <vidlist>]}

### ● Parameters

---

|                |                                                                                       |
|----------------|---------------------------------------------------------------------------------------|
| <vlan_name 32> | (Optional) Specify the name of the private VLAN. The maximum length is 32 characters. |
| vlanid         | (Optional) Specify the VLAN ID of the private VLAN.                                   |
| <vidlist>      | Specify the private VLAN ID.                                                          |

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To display private VLAN settings:

```
Zxxx0:admin#show private_vlan  
Command: show private_vlan
```

```
Private VLAN 100
```

```
-----
```

|                    |        |                    |
|--------------------|--------|--------------------|
| Promiscuous Ports: | 1      |                    |
| Trunk Ports        | : 2    |                    |
| Isolated Ports     | : 3-5  | Isolated VLAN : 20 |
| Community Ports    | : 6-8  | Community VLAN: 30 |
| Community Ports    | : 9-10 | Community VLAN: 40 |

```
Private VLAN 200
```

```
-----
```

|                    |         |                    |
|--------------------|---------|--------------------|
| Promiscuous Ports: | 11      |                    |
| Trunk Ports        | : 12    |                    |
| Isolated Ports     | : 13-15 | Isolated VLAN : 50 |
| Community Ports    | : 16-18 | Community VLAN: 60 |

```
Zxxx0:admin#
```

## 88.VLAN Trunking Commands

To establish a VLAN that spans multiple Switching Hubs, you need to enable VLAN Trunking on ports connecting the Switching Hubs. In a trunking port, packets with a VLAN tag added are transferred from Switching Hub to Switching Hub and sent to the VLAN specified by the tag information on the destination Switching Hub.

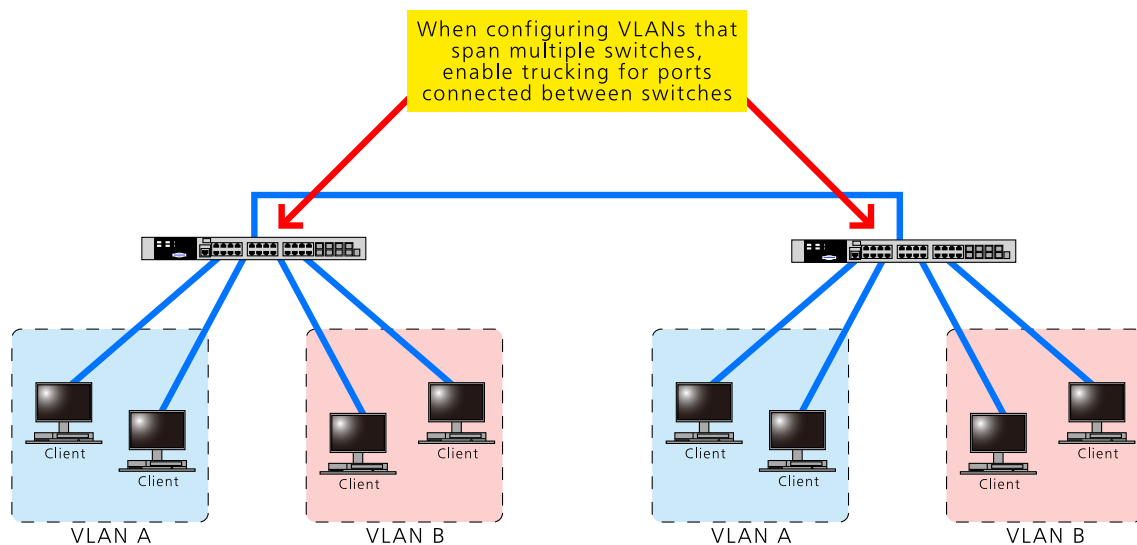


Figure 88-1 VLAN Trunking overview

**NOTE** For VLAN Trunking configuration on ports with link aggregation, configure the settings for the master port of link aggregation.

```
enable vlan_trunk
disable vlan_trunk
config vlan_trunk ports [<portlist> | all] state [enable | disable]
show vlan_trunk
```

### 88.1. enable vlan\_trunk

#### • Description

This command is used to enable VLAN trunking. When VLAN trunking function is enabled, the VLAN trunk ports shall be able to forward all tagged frames with any VID.

- **Format**

enable vlan\_trunk

- **Parameters**

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To enable VLAN trunking:

```
Zxxx0:admin#enable vlan_trunk
Command: enable vlan_trunk

Success

Zxxx0:admin#
```

## 88.2. disable vlan\_trunk

---

- **Description**

This command is used to disable VLAN trunking.

- **Format**

disable vlan\_trunk

- **Parameters**

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To disable VLAN trunking:



## 88. VLAN Trunking Commands

```
Zxxx0:admin#disable vlan_trunk
Command: disable vlan_trunk

Success.

Zxxx0:admin#
```

### 88.3. config vlan\_trunk ports

---

#### ● Description

This command is used to configure a port as a VLAN trunking port. By default, none of the ports is a VLAN trunking port. A VLAN trunking port and a non-VLAN trunking port cannot be grouped as an aggregated link. To change the VLAN trunking setting for an aggregated link, the user must apply the command to the master port. If the command is applied to link aggregation member port excluding the master, the command will be rejected. Ports with different VLAN configurations are not allowed to form an aggregated link. However, if they are specified as a VLAN trunking port, they are allowed to form an aggregated link.

For a VLAN trunking port, the VLANs on which the packets can be by passed will not be advertised by GVRP on this port. However, since the traffic on these VLANs is forwarded, this VLAN trunking port should participate in the MSTP instances corresponding to these VLANs.

#### ● Format

**config vlan\_trunk ports [<portlist> | all] | state [enable | disable]**

#### ● Parameters

|              |                                                                                                                                                                                        |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ports</b> | Specify the ports to be configured.<br><b>&lt;portlist&gt;</b><br>Specify the list of ports to be configured.<br><b>all</b><br>Specify all ports will be configured.                   |
| <b>state</b> | Specify the ports as VLAN or non-VLAN trunking ports.<br><b>enable</b><br>Specify the ports as VLAN trunking ports.<br><b>disable</b><br>Specify the ports as non-VLAN trunking ports. |

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To configure ports 1 to 5 as VLAN trunking ports:

## 88. VLAN Trunking Commands

```
Zxxx0:admin#config vlan_trunk ports 1-5 state enable
Command: config vlan_trunk ports 1-5 state enable

Success.

Zxxx0:admin#
```

### 88.4. show vlan\_trunk

---

- **Description**

This command is used to display VLAN trunking information.

- **Format**

show vlan\_trunk

- **Parameters**

None.

- **Restrictions**

None.

- **Example**

To display the current VLAN trunking information:

```
Zxxx0:admin#show vlan_trunk
Command: show vlan_trunk

VLAN Trunk Global Setting
-----
VLAN Trunk Status   : Disabled
VLAN Trunk Member Ports :

Zxxx0:admin#
```

## 89. Web-based Access Control (WAC) Commands

WAC (Web-based Access Control, Web-based authentication) is a terminal authentication method using a PC web browser.

It uses the HTTP or HTTPS protocol to perform an authentication process through a local database in this Switching Hub or an external RADIUS server as the authentication server.

```
enable wac
disable wac
config wac authorization attributes {radius [enable | disable] | local [enable | disable]](1)
config wac ports [<portlist> | all] {state [enable | disable] | aging_time [infinite | <min 1-1440>] |
  idle_time [infinite | <min 1-1440>] | block_time [<sec 0-300>]](1)
config wac method [local | radius]
config wac default_redirpath <string 128>
config wac clear_default_redirpath
config wac virtual_ip {<ipaddr>}
config wac switch_http_port <tcp_port_number 1-65535> {[http | https]}
create wac user <username 15> {[vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}
delete wac [user <username 15> | all_users]
config wac user <username 15> [vlan <vlan_name 32> | vlanid <vlanid 1-4094> | clear_vlan]
show wac
show wac ports {<portlist>}
show wac user
show wac auth_state ports {<portlist>}
clear wac auth_state [ports [<portlist> | all] {authenticated | authenticating | blocked} | macaddr
  <macaddr>]
config wac authentication_page element [default | page_title <desc 128> | login_window_title
  <desc 64> | user_name_title <desc 32> | password_title <desc 32> | logout_window_title
  <desc 64> | notification_line <value 1-5> <desc 128>]
show wac authenticate_page
```

### 89.1. enable wac

#### ● Description

This command is used to enable the WAC function.

#### ● Format

```
enable wac
```

## 89. Web-based Access Control (WAC) Commands

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable the WAC function:

```
Zxxx0:admin#enable wac
Command: enable wac

Success.

Zxxx0:admin#
```

## 89.2. disable wac

---

### ● Description

This command is used to disable the WAC function.

### ● Format

**disable wac**

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To disable the WAC function:

```
Zxxx0:admin#disable wac
Command: disable wac

Success.

Zxxx0:admin#
```

## 89.3. config wac authorization attributes

---

### ● Description

This command is used to configure the acceptance of an authorized configuration. When the authorization is enabled for WAC's RADIUS, the authorized data assigned by the RADIUS server will be accepted if the global authorization network is enabled. When the authorization is enabled for WAC's local, the authorized data assigned by the local database will be accepted.

### ● Format

**config wac authorization attributes {radius [enable | disable] | local [enable | disable]}(1)**

### ● Parameters

|               |                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>radius</b> | If specified to enable, the authorized data assigned by the RADIUS server will be accepted if the global authorization network is enabled. The default state is enabled.<br><b>enable</b> Specify to enable authorized data assigned by the RADIUS server to be accepted.<br><b>disable</b> Specify to disable authorized data assigned by the RADIUS server from being accepted.    |
| <b>local</b>  | If specified to enable, the authorized data assigned by the local database will be accepted if the global authorization network is enabled. The default state is enabled.<br><b>enable</b> Specify to enable authorized data assigned by the local database to be accepted.<br><b>disable</b> Specify to disable authorized data assigned by the local database from being accepted. |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the acceptance of an authorized configuration:

```
Zxxx0:admin#config wac authorization attributes local disable
Command: config wac authorization attributes local disable

Success.

Zxxx0:admin#
```

## 89.4. config wac ports

### ● Description

This command is used to configure the WAC port parameters.

### ● Format

**config wac ports [<portlist> | all] {state [enable | disable] | aging\_time [infinite | <min 1-1440>] | idle\_time [infinite | <min 1-1440>] | block\_time [<sec 0-300>]](1)**

### ● Parameters

|                           |                                                                                                                                                                           |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;portlist&gt;</b>   | Specify a range of ports to configure.                                                                                                                                    |
| <b>all</b>                | Specify to configure all ports.                                                                                                                                           |
| <b>state</b>              | Specify to enable or disable the WAC state.                                                                                                                               |
| <b>enable</b>             | Specify to enable the WAC state.                                                                                                                                          |
| <b>disable</b>            | Specify to disable the WAC state.                                                                                                                                         |
| <b>aging_time</b>         | Specify a time period during which an authenticated host will be kept in authenticated state. The default value is 1440 minutes.                                          |
| <b>infinite</b>           | Specify to indicate the authenticated host on the port will not ageout.                                                                                                   |
| <b>&lt;min 1-1440&gt;</b> | Specify an ageout value between 1 and 1440 minutes.                                                                                                                       |
| <b>idle_time</b>          | Specify a time period after which an authenticated host will be moved to un-authenticated state if there is no traffic during that period. The default value is infinite. |
| <b>infinite</b>           | Specify to indicate the host will not be removed from the authenticated state due to idle of traffic.                                                                     |
| <b>&lt;min 1-1440&gt;</b> | Specify an idle time between 1 and 1440 minutes.                                                                                                                          |
| <b>block_time</b>         | If a host fails to pass the authentication, it will be blocked for this period of time before it can be re-authenticated. The default value is 60 seconds.                |
| <b>&lt;sec 0-300&gt;</b>  | Specify a block time between 0 and 300 seconds.                                                                                                                           |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the WAC port state:

```
Zxxx0:admin#config wac ports 1-8 state enable
Command: config wac ports 1-8 state enable

Success.

Zxxx0:admin#
```

To configure the WAC port aging time:

```
Zxxx0:admin#config wac ports 1-5 aging_time 200
Command: config wac ports 1-5 aging_time 200

Success.

Zxxx0:admin#
```

### 89.5. config wac method

---

#### ● Description

This command is used to allow specification of the RADIUS protocol used by WAC to complete RADIUS authentication. WAC shares other RADIUS configuration with 802.1X. When using this command to set the RADIUS protocol, users must make sure the RADIUS server added by the config radius command supports the protocol.

#### ● Format

config wac method [local | radius]

#### ● Parameters

|               |                                                                 |
|---------------|-----------------------------------------------------------------|
| <b>local</b>  | Specify the authentication will be done via the local database. |
| <b>radius</b> | Specify the authentication will be done via the RADIUS server.  |

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To configure the WAC authentication method:

```
Zxxx0:admin#config wac method radius
Command: config wac method radius

Success.

Zxxx0:admin#
```



## 89.6. `config wac default_redirpath`

---

### ● Description

This command is used to configure the WAC default redirect path. If default redirect path is configured, the user will be redirected to the default redirect path after successful authentication. When the string is cleared, the client will not be redirected to another URL after successful authentication.

### ● Format

`config wac default_redirpath <string 128>`

### ● Parameters

---

`<string 128>`

Specify the URL that the client will be redirected to after successful authentication. By default, the redirected path is cleared.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the WAC default redirect path:

```
Zxxx0:admin#config wac default_redirpath http://www.manager.com
Command: config wac default_redirpath http://www.manager.com

Success.

Zxxx0:admin#
```

## 89.7. `config wac clear_default_redirpath`

---

### ● Description

This command is used to clear the WAC default redirect path. When the string is cleared, the client will not be redirected to another URL after successful authentication.

### ● Format

`config wac clear_default_redirpath`

### ● Parameters

None.

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To clear the WAC default redirect path:

```
Zxxx0:admin#config wac clear_default_redirpath
Success.

Zxxx0:admin#
```

## 89.8. config wac virtual\_ip

---

- **Description**

This command is used to configure the WAC virtual IP address. When virtual IP is specified, the TCP packets sent to the virtual IP will get a reply. If virtual IP is enabled, TCP packets sent to the virtual IP or physical IPIF's IP address will both get the reply. When virtual IP is set 0.0.0.0, the virtual IP will be disabled. By default, the virtual IP is 0.0.0.0. The virtual IP will not respond to any ARP requests or ICMP packets. To make this function work properly, the virtual IP should not be an existing IP address. It also cannot be located on an existing subnet.

- **Format**

config wac virtual\_ip {<ipaddr>}

- **Parameters**

---

<ipaddr>(Optional) Specifies the IPv4 address of the virtual IP.

---

- **Restrictions**

Only Administrator, Operator and Power-User level users can issue this command.

- **Example**

To configure the WAC virtual IP address used to accept authentication requests from unauthenticated hosts:

```
Zxxx0:admin# config wac virtual_ip 1.1.1.1
Command: config wac virtual_ip 1.1.1.1

Success.

Zxxx0:admin#
```

## 89.9. `config wac switch_http_port`

---

### ● Description

This command is used to configure the TCP port which the WAC Switching Hub listens to. The TCP port for HTTP or HTTPS is used to identify the HTTP or HTTPS packets that will be trapped to CPU for authentication processing, or to access the login page. If not specified, the default port number for HTTP is 80, and the default port number for HTTPS is 443. If no protocol is specified, the protocol is HTTP.

### ● Format

`config wac switch_http_port <tcp_port_number 1-65535> {[http | https]}`

### ● Parameters

---

**<tcp\_port\_number 1-65535>**

Specify a TCP port which the WAC Switching Hub listens to and uses to finish the authenticating process.

---

**http** (Optional) Specify that WAC runs HTTP protocol on this TCP port.

---

**https** (Optional) Specify that WAC runs HTTPS protocol on this TCP port.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure a TCP port which the WAC Switching Hub listens to:

```
Zxxx0:admin# config wac switch_http_port 8888 http
Command: config wac switch_http_port 8888 http

Success.

Zxxx0:admin#
```

## 89.10. create wac user

---

### ● Description

This command is used to create accounts for Web-based Access Control. This user account is independent of the login user account. If VLAN is not specified, the user will not get a VLAN assigned after the authentication.

### ● Format

**create wac user <username 15> {[vlan <vlan\_name 32> | vlanid <vlanid 1-4094>]}**

### ● Parameters

---

**<username 15>**

Specify the user account for Web-based Access Control.

---

**vlan** (Optional) Specify the authentication VLAN name.

**<vlan\_name 32>**

Specify the authentication VLAN name. The VLAN name can be up to 32 characters long.

---

**vlanid** (Optional) Specify the authentication VLAN ID number.

**<vlanid 1-4094>**

Specify the authentication VLAN ID number. The VLAN ID must be between 1 and 4094.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To create a WAC account:

```
Zxxx0:admin# create wac user abc vlanid 123
Command: create wac user abc vlanid 123
Enter a case-sensitive new password:**
  Enter the new password again for confirmation:**
Success.

Zxxx0:admin#
```

## 89.11. delete wac

---

### ● Description

This command is used to delete an account.

### ● Format

**delete wac** [**user** <username 15> | **all\_users**]

### ● Parameters

---

|                  |                                                                                                                                                                                              |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>user</b>      | Specify the user account for Web-based Access Control.<br><b>&lt;username 15&gt;</b><br>Specify the user account for Web-based Access Control. The username can be up to 15 characters long. |
| <b>all_users</b> | Specify this option to delete all current WAC users.                                                                                                                                         |

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete a WAC account:

```
Zxxx0:admin#delete wac user duhon
Command: delete wac user duhon

Success.

Zxxx0:admin#
```

## 89.12. config wac user

---

### ● Description

This command is used to change the VLAN associated with a user.

### ● Format

**config wac user <username 15> [vlan <vlan\_name 32> | vlanid <vlanid 1-4094> | clear\_vlan]**

### ● Parameters

|                              |                                                                                      |
|------------------------------|--------------------------------------------------------------------------------------|
| <b>&lt;username 15&gt;</b>   | Specify the name of user account which will change its VID.                          |
| <b>vlan</b>                  | Specify the authentication VLAN name.                                                |
| <b>&lt;vlan_name 32&gt;</b>  | Specify the authentication VLAN name. The VLAN name can be up to 32 characters long. |
| <b>vlanid</b>                | Specify the authentication VLAN ID.                                                  |
| <b>&lt;vlanid 1-4094&gt;</b> | Specify the authentication VLAN ID. The VLAN ID must be between 1 and 4094.          |
| <b>clear_vlan</b>            | Specify to clear the specified VLAN.                                                 |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the user's VLAN:

```
Zxxx0:admin# config wac user abc vlanid 100
Command: config wac user abc vlanid 100

Enter a old password:**
Enter a case-sensitive new password:**
Enter the new password again for confirmation:**
Success.

Zxxx0:admin#
```

## 89.13. show wac

---

- **Description**

This command is used to display the WAC global setting.

- **Format**

show wac

- **Parameters**

None.

- **Restrictions**

None.

- **Example**

To show WAC:

```
Zxxx0:admin# show wac
Command: show wac

Web-based Access Control
-----
State                : Enabled
Method               : RADIUS
Redirect Path        : http://www.manager.com
Virtual IP           : 0.0.0.0
Switch HTTP Port     : 80 (HTTP)
RADIUS Authorization : Enabled
Local Authorization  : Enabled

Zxxx0:admin#
```

## 89.14. show wac ports

---

- **Description**

This command is used to display WAC port information.

- **Format**

show wac ports {<portlist>}

- **Parameters**

---

<portlist>(Optional) Specify a range of member ports to display the status.

---

## ● Restrictions

None.

## ● Example

To display WAC ports 1 to 3:

```
Zxxx0:admin# show wac ports 1-3
Command: show wac ports 1-3
```

| Port  | State    | Aging Time<br>(min) | Idle Time<br>(min) | Block Time<br>(sec) |
|-------|----------|---------------------|--------------------|---------------------|
| ----- | -----    | -----               | -----              | -----               |
| 1     | Disabled | 1440                | Infinite           | 60                  |
| 2     | Disabled | 1440                | Infinite           | 60                  |
| 3     | Disabled | 1440                | Infinite           | 60                  |

```
Zxxx0:admin#
```

## 89.15. show wac user

---

## ● Description

This command is used to display WAC user accounts.

## ● Format

show wac user

## ● Parameters

None.

## ● Restrictions

None.

## ● Example

To show Web authentication user accounts:

```
Zxxx0:admin# show wac user
Command: show wac user
```

| User Name | Password | VID   |
|-----------|----------|-------|
| -----     | -----    | ----- |
| 123       | *****    | 1000  |

```
Total Entries : 1
```

```
Zxxx0:admin#
```



## 89.16. show wac auth\_state ports

---

### ● Description

This command is used to display the authentication state for ports.

### ● Format

show wac auth\_state ports {<portlist>}

### ● Parameters

---

<portlist>(Optional) Specify the list of ports whose WAC authentication state will be displayed.

---

### ● Restrictions

None.

### ● Example

To display the WAC authentication status of ports:

```
Zxxx0:admin# show wac auth_state ports
Command: show wac auth_state ports

P:Port-based   Pri:Priority

Port      MAC Address      Original  State      VID Pri Aging Time/ Idle
          RX VID
-----
  31    00-05-5D-F9-16-76    1    Authenticating -    -    27      -

Total Authenticating Hosts : 1
Total Authenticated Hosts  : 0
Total Blocked Hosts       : 0

Zxxx0:admin#
```

## 89.17. clear wac auth\_state

---

### ● Description

This command is used to clear the authentication state of a port. The port will return to un-authenticated state. All the timers associated with the port will be reset.

### ● Format

clear wac auth\_state [ports [<portlist> | all] {authenticated | authenticating | blocked} | macaddr <macaddr>]

## ● Parameters

---

**ports** Specify the list of ports whose WAC state will be cleared.

**<portlist>**

Specify a range of ports.

**all** Specify to clear all ports.

---

**authenticated**

(Optional) Specify to clear all authenticated users for a port.

---

**authenticating**

(Optional) Specify to clear all authenticating users for a port.

---

**blocked** (Optional) Specify to clear all blocked users for a port.

---

**macaddr** Specify to clear a specific user.

**<macaddr>**

Enter the MAC address here.

---

## ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

## ● Example

To clear the WAC authentication state of ports 1 to 5:

```
Zxxx0:admin# clear wac auth_state ports 1-5
```

```
Command: clear wac auth_state ports 1-5
```

```
Success.
```

```
Zxxx0:admin#
```

## 89.18. config wac authentication\_page element

---

### ● Description

This command is used to customize the authenticate page elements.

### ● Format

config wac authentication\_page element [default | page\_title <desc 128> | login\_window\_title <desc 64> | user\_name\_title <desc 32> | password\_title <desc 32> | logout\_window\_title <desc 64> | notification\_line <value 1-5> <desc 128>]

### ● Parameters

---

**default** Specifies to reset the page elements to default.

---

**page\_title**

Specifies to configure the title of the authentication page.

<desc 128>

Enter the page title used here. This value can be up to 128 characters long.

---

**login\_window\_title**

Specifies to configure the login window title of the authentication page

<desc 64>

Enter the login window title used here. This value can be up to 64 characters long.

---

**user\_name\_title**

Specifies to configure the user name title of the authentication page

<desc 32>

Enter the user name title used here. This value can be up to 32 characters long.

---

**password\_title**

Specifies to configure the password title of the authentication page.

<desc 32>

Enter the password title used here. This value can be up to 32 characters long.

---

**logout\_window\_title**

Specifies to configure the logout window title of the authentication page.

<desc 64>

Enter the logout window title used here. This value can be up to 64 characters long.

---

**notification\_line**

Specifies to set the notification information by line in authentication Web pages.

<value 1-5>

Enter the notification line number used here. This value must be between 1 and 5.

<desc 128>

Enter the notification line description used here. This value can be up to 128 characters long.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To customize the authenticate page elements:

```
Zxxx0:admin# config wac authentication_page element notification_line 1 Copyright
@ All Rights Reserved
Command: config wac authentication_page element notification_line 1 Copyright @ All
Rights Reserved

Success.

Zxxx0:admin#
```

## **89.19. show wac authenticate\_page**

---

### ● Description

This command is used to show the elements of the customized authenticate pages.

### ● Format

**show wac authenticate\_page**

### ● Parameters

None.

### ● Restrictions

None.

### ● Example

The following example displays the authentication page elements:

```
Zxxx0:admin# show wac authenticate_page
Command: show wac authenticate_page

Page Title                               : MANAGER
Login Window Title                       : Authentication Login
User Name Title                          : User Name
Password Title                           : Password
Logout Window Title                      : Logout
Notification                             :
Copyright @ All Rights Reserved
Site: http://support.manager.com

Zxxx0:admin#
```

## 90. Weighted Random Early Detection (WRED) Commands

Weighted Random Early Detection (WRED) is a function to prevent congestion by discarding packets accumulated in the buffer in advance.

You can specify packets to be discarded with the threshold of bandwidth or priority.

---

```

create wred profile <int 2-128> profile_name <profile_name 32>
config wred ports [<portlist> | all] [cos <class_id 0-7> [profile [default | profile_id <int 2-128> |
  <profile_name 32>] | weight <int 0-15>] | profile [default | profile_id <int 2-128> |
  <profile_name 32>] | weight <int 0-15>]
config wred profile [default | profile_id <int 2-128> | <profile_name 32>] {tcp | non_tcp} {green
  | yellow | red} min_threshold <int 0-100> max_threshold <int 0-100> max_drop_rate <int 0-
  100>
enable wred
disable wred
delete wred profile [profile_id <int 2-128> | <profile_name 32> | all]
show wred {ports {<portlist>}}
show wred profile {[default | profile_id <int 2-128> | <profile_name 32>]}

```

---

### 90.1. create wred profile

#### ● Description

This command is used to create a WRED profile.

#### ● Format

```
create wred profile <int 2-128> profile_name <profile_name 32>
```

#### ● Parameters

---

```

<int 2-128>
    Enter the WRED profile ID to be added.

```

---

```

profile_name
    Specify the profile name to be added.
    <profile_name 32>
        Enter the profile name.

```

---

#### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

#### ● Example

To create a wred profile id 2:

```

Zxxx0:admin# create wred profile 2 profile_name wred-2
Command: create wred profile 2 profile_name wred-2

Success.

Zxxx0:admin#

```

## 90.2. config wred ports

### ● Description

This command is used to configure the WRED parameters of the ports.

### ● Format

```

config wred ports [<portlist> | all] [cos <class_id 0-7> [profile [default | profile_id <int 2-128> |
<profile_name 32>] | weight <int 0-15>] | profile [default | profile_id <int 2-128> |
<profile_name 32>]

```

### ● Parameters

|            |                                                                                                                                                                                                                                                                |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <portlist> | Specify a range of ports to be configured.                                                                                                                                                                                                                     |
| all        | Specify all ports to be configured.                                                                                                                                                                                                                            |
| cos        | Specify the hardware priority queues.<br><class_id 0-7><br>Enter the priority between 0 and 7.                                                                                                                                                                 |
| profile    | Specify the profile to be used.<br>default<br>Specify the default profile to be used.<br>profile_id<br>Specify the profile ID to be used.<br><int 2-128><br>Enter the profile ID between 2 and 128.<br><profile_name 32><br>Enter the profile name to be used. |
| weight     | Specify the weight of average queue size formular.<br><int 0-15><br>Enter the weight between 0 and 15.                                                                                                                                                         |

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To configure the port 1:1 as queue 2 and to use the profile 2:

## 90. Weighted Random Early Detection (WRED) Commands

```
Zxxx0:admin# config wred ports 1:1 cos 2 profile profile_id 2
Command: config wred ports 1 cos 2 profile profile_id 2

Success.

Zxxx0:admin#
```

### 90.3. config wred profile

#### ● Description

This command is used to configure the WRED profile.

#### ● Format

**config wred profile** [default | profile\_id <int 2-128> | <profile\_name 32>] {tcp | non\_tcp} {green | yellow | red} min\_threshold <int 0-100> max\_threshold <int 0-100> max\_drop\_rate <int 0-100>

#### ● Parameters

---

**default** Specify the default WRED profile to be configured.

---

**profile\_id**

Specify the WRED profile ID to be configured.

<int 2-128>

Enter the WRED profile ID.

---

**<profile\_name 32>**

Enter the WRED profile name.

---

**tcp** (Optional) Specify the TCP type of packets to be dropped.

**non\_tcp** (Optional) Specify the non-TCP type of packets to be dropped.

---

**green** (Optional) Specify the green packets to be dropped.

**yellow** (Optional) Specify the yellow packets to be dropped.

**red** (Optional) Specify the red packets to be dropped.

---

**min\_threshold**

Specify the minimum threshold value used. If the queue size is higher than this value, then the color yellow will be assigned to it. If the queue size is lower than this value, then the color green will be assigned to it and then it will be guaranteed not to be dropped. Yellow packet behavior depends on the profile setting for this color.

<int 0-100>

Enter the value between 0 and 100.

---

**max\_threshold**

Specify the maximum threshold value used. If the queue size is lower than this value, then the color yellow will be assigned to it. If the queue size is higher than this value, then the color red will be assigned to it and then it will be dropped. Yellow packet behavior depends on the profile setting for this color.

<int 0-100>

Enter the value between 0 and 100.

---

---

### **max\_drop\_rate**

Specify the maximum drop rate value.

**<int 0-100>**

Enter the value between 0 and 100.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To config the profile 2 to drop all type and all color packets:

```
Zxxx0:admin# config wred profile profile_id 2 min_threshold 30 max_threshold 50
max_drop_rate 10
Command: config wred profile profile_id 2 min_threshold 30 max_threshold 50
max_drop_rate 10
```

Success.

```
Zxxx0:admin#
```

## 90.4. enable wred

---

### ● Description

This command is used to enable the WRED global state.

### ● Format

**enable wred**

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To enable global WRED state:

```
Zxxx0:admin# enable wred
Command: enable wred
```

Success.

```
Zxxx0:admin#
```



## 90.5. disable wred

---

### ● Description

This command is used to disable the WRED global state.

### ● Format

**disable wred**

### ● Parameters

None.

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To disable WRED global state:

```
Zxxx0:admin# disable wred
Command: disable wred

Success.

Zxxx0:admin#
```

## 90.6. delete wred profile

---

### ● Description

This command is used to delete a WRED profile. The default WRED profile 1 is reserved by the system. When a profile was deleted by the user, the ports which bound the profile will bind the default profile.

### ● Format

**delete wred profile [profile\_id <int 2-128> | <profile\_name 32> | all]**

### ● Parameters

---

**profile\_id**

Specify the profile ID to be deleted.

**<int 2-128>**

Enter the profile ID between 2 and 128.

---

---

**<profile\_name 32>**

Enter the profile name to be delete.

---

**all**

Specify all profiles to be delete.

---

### ● Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

### ● Example

To delete the profile 2:

```
Zxxx0:admin# delete wred profile all
Command: delete wred profile all

Success.

Zxxx0:admin#
```

## 90.7. show wred

---

### ● Description

This command is used to display the WRED port information.

### ● Format

**show wred {ports {<portlist>}}**

### ● Parameters

---

**ports** (Optional) Specify a range of ports.

**<portlist>**

(Optional) Enter a range of ports.

---

### ● Restrictions

None.

## 90. Weighted Random Early Detection (WRED) Commands

### ● Example

To display wred of port 1:1 and 1:2 settings:

```
Zxxx0:admin# show wred ports 1-2
Command: show wred ports 1-2

Global WRED : Disabled

Port: 1
Class_ID   Weight    Profile_id Profile_Name
-----
0          9         1         default
1          9         1         default
2          9         2         profilename
3          9         1         default
4          9         1         default
5          9         1         default
6          9         1         default
7          9         1         default

Port: 2
Class_ID   Weight    Profile_id Profile_Name
-----
0          9         1         default
1          9         1         default
2          9         1         default
3          9         1         default
4          9         1         default
5          9         1         default
6          9         1         default
7          9         1         default

Zxxx0:admin#
```

## 90.8. show wred profile

---

### ● Description

This command is used to display the WRED profile information.

### ● Format

**show wred profile** {[default | profile\_id <int 2-128> | <profile\_name 32>]}

## ● Parameters

---

**default** Specify the default profile to be displayed.

---

**profile\_id**

(Optional) Specify the profile ID to be displayed.

**<int 2-128>**

Enter the profile ID between 2 and 128.

---

**<profile\_name 32>**

Specify the profile name to be displayed.

---

## ● Restrictions

None.

## ● Example

To display the WRED profile information:

```
Zxxx0:admin# show wred profile
Command: show wred profile

Total Profile Number: 2

WRED Profile ID: 1      Profile Name: default
Packet Type      Min-Threshold  Max-Threshold  Max-Drop-Rate
-----
TCP-GREEN        50             100            50
TCP-YELLOW        50             100            50
TCP-RED           50             100            50
NON-TCP-GREEN    50             100            50
NON-TCP-YELLOW   50             100            50
NON-TCP-RED      50             100            50

WRED Profile ID: 2      Profile Name: profilename
Packet Type      Min-Threshold  Max-Threshold  Max-Drop-Rate
-----
TCP-GREEN        30             50             10
TCP-YELLOW        30             50             10
TCP-RED           30             50             10
NON-TCP-GREEN    30             50             10
NON-TCP-YELLOW   30             50             10
NON-TCP-RED      30             50             10

Zxxx0:admin#
```

## 91. System Log Lists

### 91.1. MAC Access Control

| # | Severity      | Log message / Explanation                                                                                                          |
|---|---------------|------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Critical      | MAC-based Access Control unauthenticated host (MAC: <macaddr>, Port <[unitID:]portNum>, VID: <vid>)                                |
|   |               | A host failed to pass the authentication                                                                                           |
| 2 | Warning       | Port < [unitID:]portNum> enters MAC-based Access Control stop learning state.                                                      |
|   |               | The authorized user number on a port has reached the maximum user limit.                                                           |
| 3 | Warning       | Port <[unitID:]portNum> recovers from MAC-based Access Control stop learning state.                                                |
|   |               | The authorized user number on a port is below the maximum user limit in a time interval (interval is project dependent).           |
| 4 | Warning       | MAC-based Access Control enters stop learning state.                                                                               |
|   |               | The authorized user number on the whole device has reached the maximum user limit.                                                 |
| 5 | Warning       | MAC-based Access Control recovers from stop learning state.                                                                        |
|   |               | The authorized user number on the whole device is below the maximum user limit in a time interval (interval is project dependent). |
| 6 | Warning       | MAC-based Access Control host login successful (MAC: <macaddr>, port: <[unitID]portNum>, VID: <vid>)                               |
|   |               | A host has passed the authentication.                                                                                              |
| 7 | Informational | MAC-based Access Control host aged out (MAC: <macaddr>, port: <[unitID]portNum>, VID: <vid>)                                       |
|   |               | A host has aged out.                                                                                                               |

## 91.2. PTP

| # | Serverity     | Log message / Explanation                                                                   |
|---|---------------|---------------------------------------------------------------------------------------------|
| 1 | Informational | PTP port <[unitID:]portNum> role changed to <ptp_role>                                      |
|   |               | PTP port role changed.                                                                      |
| 2 | Informational | The boundary clock synchronized to its master, the offset value is <+ -><Offset> second(s). |
|   |               | PTP clock synchronized.                                                                     |

## 91.3. DHCPv6 Relay

| # | Serverity     | Log message / Explanation                                                   |
|---|---------------|-----------------------------------------------------------------------------|
| 1 | Informational | DHCPv6 relay on interface <ipif-name> changed state to [enabled   disabled] |
|   |               | DHCPv6 relay on a specify interface' s administrator state changed.         |

## 91.4. DHCPv6 Server

| # | Serverity     | Log message / Explanation                                                            |
|---|---------------|--------------------------------------------------------------------------------------|
| 1 | Informational | The address of the DHCPv6 Server pool <pool-name> is used up.                        |
|   |               | The address of the DHCPv6 Server pool is used up.                                    |
| 2 | Informational | The number of allocated ipv6 addresses of the DHCPv6 Server pool is equal to MAX-NUM |
|   |               | The number of allocated ipv6 addresses is equal to MAX-NUM(4096).                    |

## 91.5. IP Directed Broadcast

---

| # | Serverity     | Log message / Explanation                                                    |
|---|---------------|------------------------------------------------------------------------------|
| 1 | Informational | IP Directed Broadcast packet rate is high on subnet. [(IP: %s)]              |
|   |               | IP Directed-broadcast rate exceed 50 packets per second on a certain subnet. |
| 2 | Informational | IP Directed Broadcast rate is high.                                          |
|   |               | IP Directed-broadcast rate exceed 100 packets per second/                    |

## 91.6. RCP

| #  | Severity      | Log message / Explanation                                                                                              |
|----|---------------|------------------------------------------------------------------------------------------------------------------------|
| 1  | Informational | [Unit <unitID>] Firmware upgraded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)      |
|    |               | Firmware upgraded successfully.                                                                                        |
| 2  | Warning       | [Unit <unitID>] Firmware upgrade by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)     |
|    |               | Firmware upgrade was unsuccessful.                                                                                     |
| 3  | Informational | Firmware uploaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)                      |
|    |               | Firmware upgraded successfully.                                                                                        |
| 4  | Warning       | Firmware upload by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)                      |
|    |               | Firmware upgrade was unsuccessful.                                                                                     |
| 5  | Informational | Configuration downloaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)               |
|    |               | Configuration downloaded successfully.                                                                                 |
| 6  | Warning       | Configuration download by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)               |
|    |               | Configuration download was unsuccessful.                                                                               |
| 7  | Informational | Configuration uploaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)                 |
|    |               | Configuration uploaded successfully.                                                                                   |
| 8  | Warning       | Configuration upload by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)                 |
|    |               | Configuration upload unsuccessful.                                                                                     |
| 9  | Informational | Log message uploaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)                   |
|    |               | Log message uploaded successfully.                                                                                     |
| 10 | Warning       | Log message upload by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)                   |
|    |               | Log message upload was unsuccessful.                                                                                   |
| 11 | Informational | The downloaded configurations executed by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) |
|    |               | The downloaded configurations executed successfully.                                                                   |



## 91. System Log Lists

| #  | Serverity     | Log message / Explanation                                                                                                |
|----|---------------|--------------------------------------------------------------------------------------------------------------------------|
| 12 | Warning       | The downloaded configurations executed by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) |
|    |               | The downloaded configurations execute was unsuccessful.                                                                  |
| 13 | Informational | Attack log message uploaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)              |
|    |               | Attack log message uploaded successfully.                                                                                |
| 14 | Warning       | Attack log message upload by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)              |
|    |               | Attack log message upload was unsuccessful.                                                                              |

## 91.7. TFTP Client

| #  | Severity      | Log message / Explanation                                                                                            |
|----|---------------|----------------------------------------------------------------------------------------------------------------------|
| 1  | Informational | [Unit <unitID>] Firmware upgraded by <session> successfully (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)     |
|    |               | Firmware upgraded successfully.                                                                                      |
| 2  | Warning       | [Unit <unitID>] Firmware upgrade by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) |
|    |               | Firmware upgrade was unsuccessful.                                                                                   |
| 3  | Informational | Firmware successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)                     |
|    |               | Firmware successfully uploaded.                                                                                      |
| 4  | Warning       | Firmware upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)                  |
|    |               | Firmware upload was unsuccessful.                                                                                    |
| 5  | Informational | Configuration successfully downloaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)              |
|    |               | Configuration successfully downloaded.                                                                               |
| 6  | Warning       | Configuration download by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)           |
|    |               | Configuration download was unsuccessful.                                                                             |
| 7  | Informational | Configuration successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)                |
|    |               | Configuration successfully uploaded.                                                                                 |
| 8  | Warning       | Configuration upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)             |
|    |               | Configuration upload was unsuccessful.                                                                               |
| 9  | Informational | Log message successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)                  |
|    |               | Log message successfully uploaded.                                                                                   |
| 10 | Warning       | Log message upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)               |
|    |               | Log message upload was unsuccessful.                                                                                 |
| 11 | Informational | Attack log message successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)           |
|    |               | Attack log message successfully uploaded.                                                                            |

## 91. System Log Lists

| #  | Serverity | Log message / Explanation                                                                                        |
|----|-----------|------------------------------------------------------------------------------------------------------------------|
| 12 | Warning   | Attack log message upload by <session> was unsuccessful!<br>(Username: <username>, IP: <ipaddr>, MAC: <macaddr>) |
|    |           | Attack log message upload was unsuccessful.                                                                      |

## 91.8. DNS Resolver

---

| # | Serverity     | Log message / Explanation                                                               |
|---|---------------|-----------------------------------------------------------------------------------------|
| 1 | Informational | Duplicate Domain name case name: <domainname>, static IP: <ipaddr>, dynamic IP:<ipaddr> |
|   |               | Duplicate Domain name cache added, leads a dynamic domain name cache be deleted.        |

## 91.9. ARP

---

| # | Serverity | Log message / Explanation                                                                                                  |
|---|-----------|----------------------------------------------------------------------------------------------------------------------------|
| 1 | Warning   | Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>, Interface: <ipif_name>). |
|   |           | Gratuitous ARP detected duplicate IP.                                                                                      |

## 91.10. Telnet

| # | Severity      | Log message / Explanation                                            |
|---|---------------|----------------------------------------------------------------------|
| 1 | Informational | Successful login through Telnet (Username: <username>, IP: <ipaddr>) |
|   |               | Successful login through Telnet.                                     |
| 2 | Warning       | Login failed through Telnet (Username: <username>, IP: <ipaddr>)     |
|   |               | Login failed through Telnet.                                         |
| 3 | Informational | Logout through Telnet (Username: <username>, IP: <ipaddr>)           |
|   |               | Logout through Telnet.                                               |
| 4 | Informational | Telnet session timed out (Username: <username>, IP: <ipaddr>).       |
|   |               | Telnet session timed out.                                            |

## 91.11. Interface

| # | Severity      | Log message / Explanation                     |
|---|---------------|-----------------------------------------------|
| 1 | Informational | Port <[unitID:]portNum> link up, <link state> |
|   |               | Port link up.                                 |
| 2 | Informational | Port <[unitID:]portNum> link down             |
|   |               | Port link down.                               |

## 91.12. IEEE802.1X

| # | Severity      | Log message / Explanation                                                                                            |
|---|---------------|----------------------------------------------------------------------------------------------------------------------|
| 1 | Warning       | 802.1X Authentication failure [for <reason> ] from (Username: <username>, Port: <[unitID:]portNum>, MAC: <macaddr> ) |
|   |               | IEEE802.1X Authentication failure.                                                                                   |
| 2 | Informational | 802.1X Authentication successful from (Username: <username>, Port: <[unitID:]portNum>, MAC: <macaddr>)               |
|   |               | IEEE802.1X Authentication successful.                                                                                |

## 91.13. RADIUS

| # | Severity      | Log message / Explanation                                                                                                                                                                      |
|---|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Informational | RADIUS server <ipaddr> assigned VID :<vlanID> to port <[unitID:]portNum> (account :<username> )                                                                                                |
|   |               | VID assigned from RADIUS server after RADIUS client is authenticated by RADIUS server successfully .This VID will be assigned to the port and this port will be the VLAN untagged port member. |
| 2 | Informational | RADIUS server <ipaddr> assigned ingress bandwidth :<ingressBandwidth> to port <[unitID:]portNum> (account :<username>)                                                                         |
|   |               | Ingress bandwidth assigned from RADIUS server after RADIUS client is authenticated by RADIUS server successfully .This Ingress bandwidth will be assigned to the port.                         |
| 3 | Informational | RADIUS server <ipaddr> assigned egress bandwidth :<egressBandwidth> to port <[unitID:]portNum> (account:<username>)                                                                            |
|   |               | Egress bandwidth assigned from RADIUS server after RADIUS client is authenticated by RADIUS server successfully. This egress bandwidth will be assigned to the port.                           |
| 4 | Informational | RADIUS server <ipaddr> assigned 802.1p default priority:<priority> to port <[unitID:]portNum> (account :<username>)                                                                            |
|   |               | 802.1p default priority assigned from RADIUS server after RADIUS client is authenticated by RADIUS server successfully. This 802.1p default priority will be assigned to the port.             |
| 5 | Warning       | RADIUS server <ipaddr> assigns <username> ACL failure at port <[unitID:]portNum> (<string>)                                                                                                    |
|   |               | Failed to assign ACL profiles/rules from RADIUS server.                                                                                                                                        |

## 91.14. LLDP-MED

| # | Severity | Log message / Explanation                                                                                                                                           |
|---|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Notice   | LLDP-MED topology change detected (on port <portNum>. chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>)           |
|   |          | LLDP-MED topology change detected.                                                                                                                                  |
| 2 | Notice   | Conflict LLDP-MED device type detected ( on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>) |
|   |          | Conflict LLDP-MED device type detected.                                                                                                                             |
| 3 | Notice   | Incompatible LLDP-MED TLV set detected ( on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>) |
|   |          | Incompatible LLDP-MED TLV set detected.                                                                                                                             |

## 91.15. Voice VLAN

| # | Severity      | Log message / Explanation                                                                                                                              |
|---|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Informational | New voice device detected (Port <portNum>, MAC <macaddr>)                                                                                              |
|   |               | When a new voice device is detected in the port.                                                                                                       |
| 2 | Informational | Port < portNum > add into Voice VLAN <vid >                                                                                                            |
|   |               | When a port which is in auto Voice VLAN mode joins the Voice VLAN.                                                                                     |
| 3 | Informational | Port < portNum > remove from Voice VLAN <vid >                                                                                                         |
|   |               | When a port leaves the Voice VLAN and at the same time, no voice device is detected in the aging interval for that port, the log message will be sent. |

## 91.16. Stacking

---

| # | Serverity     | Log message / Explanation                                                                       |
|---|---------------|-------------------------------------------------------------------------------------------------|
| 1 | Informational | Unit: <unitID>, MAC: <macaddr> Hot insertion.                                                   |
|   |               | Hot insersion.                                                                                  |
| 2 | Informational | Unit: <unitID>, MAC: <macaddr> Hot removal.                                                     |
|   |               | Hot removal.                                                                                    |
| 3 | Informational | Stacking topology is <Stack_TP_TYPE>. Master(Unit <unitID>, MAC:<macaddr>).                     |
|   |               | Stacking topology change.                                                                       |
| 4 | Informational | Backup master changed to master. Master (Unit: <unitID>).                                       |
|   |               | Backup-Master changed to Master.                                                                |
| 5 | Informational | Slave changed to master. Master (Unit: <unitID>).                                               |
|   |               | Slave changed to Master.                                                                        |
| 6 | Critical      | Hot insert failed, box ID conflict: Unit <unitID> conflict (MAC: <macaddr> and MAC: <macaddr>). |
|   |               | Box ID conflict.                                                                                |

## 91.17. SNMP

---

| # | Serverity     | Log message / Explanation                                          |
|---|---------------|--------------------------------------------------------------------|
| 1 | Informational | SNMP request received from <ipaddr> with invalid community string. |
|   |               | SNMP request received with invalid community string.               |

## 91.18. OSPFv2

| #  | Serverity     | Log message / Explanation                                                     |
|----|---------------|-------------------------------------------------------------------------------|
| 1  | Informational | OSPF interface <intf-name> changed state to [Up   Down]                       |
|    |               | OSPF interface link state changed.                                            |
| 2  | Informational | OSPF protocol on interface <intf-name> changed state to [Enabled   Disabled]  |
|    |               | OSPF interface administrator state changed.                                   |
| 3  | Informational | OSPF interface <intf-name> changed from area <area-id> to area <area-id>      |
|    |               | One OSPF interface changed from one area to another.                          |
| 4  | notice        | OSPF nbr <nbr-id> on interface <intf-name> changed state from Loading to Full |
|    |               | One OSPF neighbor state changed from Loading to Full.                         |
| 5  | notice        | OSPF nbr <nbr-id> on interface <intf-name> changed state from Full to Down    |
|    |               | One OSPF neighbor state changed from Full to Down.                            |
| 6  | notice        | OSPF nbr <nbr-id> on interface <intf-name> dead timer expired                 |
|    |               | One OSPF neighbor state' s dead timer expired.                                |
| 7  | notice        | OSPF nbr <nbr-id> on virtual link changed state from Loading to Full          |
|    |               | One OSPF virtual neighbor state changed from Loading to Full.                 |
| 8  | notice        | OSPF nbr <nbr-id> on virtual link changed state from Full to Down             |
|    |               | One OSPF virtual neighbor state changed from Full to Down.                    |
| 9  | Informational | OSPF router ID changed to <router-id>                                         |
|    |               | OSPF router ID was changed.                                                   |
| 10 | Informational | OSPF state changed to Enabled                                                 |
|    |               | Enable OSPF.                                                                  |
| 11 | Informational | OSPF state changed to Disabled                                                |
|    |               | Disable OSPF.                                                                 |



## 91.19. VRRP

| #  | Severity      | Log message / Explanation                                                          |
|----|---------------|------------------------------------------------------------------------------------|
| 1  | Informational | VR <vr-id> at interface <intf-name> switch to Master                               |
|    |               | One virtual router state becomes Master.                                           |
| 2  | Informational | VR <vr-id> at interface <intf-name> switch to Backup                               |
|    |               | One virtual router state becomes Backup.                                           |
| 3  | Informational | VR <vr-id> at interface <intf-name> switch to Init                                 |
|    |               | One virtual router state becomes Init.                                             |
| 4  | Warning       | Authentication type mismatch on VR <vr-id> at interface <intf-name>                |
|    |               | Authentication type mismatch of one received VRRP advertisement message.           |
| 5  | Warning       | Authentication fail on VR <vr-id> at interface <intf-name>. Auth type <auth-type>  |
|    |               | Authentication checking fail of one received VRRP advertisement message.           |
| 6  | Warning       | Received an ADV msg with incorrect checksum on VR <vr-id> at interface <intf-name> |
|    |               | Checksum error of one received VRRP advertisement message.                         |
| 7  | Warning       | Received ADV msg virtual router ID mismatch. VR <vr-id> at interface <intf-name>   |
|    |               | Virtual router ID mismatch of one received VRRP advertisement message.             |
| 8  | Warning       | Received ADV msg adv interval mismatch. VR <vr-id> at interface <intf-name>        |
|    |               | Advertisement interval mismatch of one received VRRP advertisement message.        |
| 9  | Notice        | Added a virtual MAC <vrrp-mac-addr> into L2 table                                  |
|    |               | A virtual MAC address is added into switch L2 table.                               |
| 10 | Notice        | Deleted a virtual MAC <vrrp-mac-addr> from L2 table                                |
|    |               | A virtual MAC address is deleted from switch L2 table.                             |
| 11 | Notice        | Added a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table                |
|    |               | A virtual MAC address is adding into switch L3 table.                              |

| #  | Serverity | Log message / Explanation                                                                                      |
|----|-----------|----------------------------------------------------------------------------------------------------------------|
| 12 | Notice    | Deleted a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from L3 table                                          |
|    |           | A virtual MAC address is deleting from switch L3 table.                                                        |
| 13 | Error     | Failed to add virtual MAC <vrrp-mac-addr> into chip L2 table. Errcode <vrrp-errcode>                           |
|    |           | Failed when adding a virtual MAC into switch chip L2 table.                                                    |
| 14 | Error     | Failed to delete virtual MAC <vrrp-mac-addr> from chip L2 table. Errcode <vrrp-errcode>                        |
|    |           | Failed when deleting a virtual MAC from switch chip L2 table.                                                  |
| 15 | Error     | Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. L3 table is full                    |
|    |           | Failed when adding a virtual MAC into switch L3 table. The L3 table is full.                                   |
| 16 | Error     | Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Port <mac-port> is invalid          |
|    |           | Failed when adding a virtual MAC into switch L3 table. The port where the MAC is learned from is invalid.      |
| 17 | Error     | Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Interface <mac-intf> is invalid     |
|    |           | Failed when adding a virtual MAC into switch L3 table. The interface where the MAC is learned from is invalid. |
| 18 | Error     | Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Box id <mac-box> is invalid         |
|    |           | Failed when adding a virtual MAC into switch L3 table. The box where the MAC is learned from is invalid.       |
| 19 | Error     | Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into chip L3 table. Errcode <vrrp-errcode>         |
|    |           | Failed when adding a virtual MAC into switch chip' s L3 table.                                                 |
| 20 | Error     | Failed to delete virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from chip L3 table. Errcode <vrrp-errcode>      |
|    |           | Failed when deleting a virtual MAC from switch chip' s L3 table.                                               |

## 91.20. Port Security

---

| # | Serverity | Log message / Explanation                                                   |
|---|-----------|-----------------------------------------------------------------------------|
| 1 | Warning   | Port security violation<br>(MAC: < macaddr > on port:: < unitID: portNum >) |
|   |           | Address full on a port.                                                     |

## 91.21. AAA

| #  | Severity      | Log message / Explanation                                                                                                                                                                  |
|----|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Informational | Successful login through <Console   Telnet   Web(SSL)   SSH>(Username: <username>, IP: <ipaddr   ipv6address>).                                                                            |
|    |               | Successful login.                                                                                                                                                                          |
| 2  | Warning       | Login failed through <Console   Telnet   Web(SSL)  SSH> (Username: <username>, IP: <ipaddr   ipv6address>).                                                                                |
|    |               | Login failed.                                                                                                                                                                              |
| 3  | Informational | Logout through <Console   Telnet   Web(SSL)  SSH> (Username: <username>, IP: <ipaddr   ipv6address>).                                                                                      |
|    |               | Logout.                                                                                                                                                                                    |
| 4  | Informational | <Console   Telnet   Web(SSL)  SSH> session timed out (Username: <username>, IP: <ipaddr   ipv6address>).                                                                                   |
|    |               | Session timed out.                                                                                                                                                                         |
| 5  | Informational | SSH server is enabled                                                                                                                                                                      |
|    |               | SSH server is enabled.                                                                                                                                                                     |
| 6  | Informational | SSH server is disabled                                                                                                                                                                     |
|    |               | SSH server is disabled.                                                                                                                                                                    |
| 7  | Informational | Authentication Policy is enabled (Module: AAA).                                                                                                                                            |
|    |               | Authentication Policy is enabled.                                                                                                                                                          |
| 8  | Informational | Authentication Policy is disabled (Module: AAA).                                                                                                                                           |
|    |               | Authentication Policy is disabled.                                                                                                                                                         |
| 9  | Warning       | Login failed through <Console   Telnet   Web(SSL)  SSH> from <ipaddr   ipv6address> due to AAA server <ipaddr   ipv6address> timeout or improper configuration (Username: <username>).     |
|    |               | Login failed due to AAA server timeout or improper configuration.                                                                                                                          |
| 10 | Informational | Successful Enable Admin through <Console   Telnet   Web(SSL)  SSH> from <ipaddr   ipv6address> authenticated by AAA <local   none   server <ipaddr   ipv6address>> (Username: <username>). |
|    |               | Successful Enable Admin authenticated by AAA local or none or server.                                                                                                                      |

## 91. System Log Lists

| #  | Serverity     | Log message / Explanation                                                                                                                                                                     |
|----|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11 | Warning       | Enable Admin failed through <Console   Telnet   Web(SSL)   SSH> from <ipaddr   ipv6address> due to AAA server <ipaddr   ipv6address> timeout or improper configuration (Username: <username>) |
|    |               | Enable Admin failed due to AAA server timeout or improper configuration.                                                                                                                      |
| 12 | Warning       | Enable Admin failed through <Console   Telnet   Web(SSL)   SSH> from <ipaddr   ipv6address> authenticated by AAA <local   server <ipaddr   ipv6address>> (Username: <username>).              |
|    |               | Enable Admin failed authenticated by AAA local or server.                                                                                                                                     |
| 13 | Informational | Successful login through <Console   Telnet   Web(SSL)   SSH> from < ipaddr   ipv6address > authenticated by AAA <local   none   server <ipaddr   ipv6address>> (Username: <username>).        |
|    |               | Successful login authenticated by AAA local or none or server.                                                                                                                                |
| 14 | Warning       | Login failed through <Console   Telnet   Web(SSL)   SSH> from <ipaddr   ipv6address> authenticated by AAA <local   server <ipaddr   ipv6address>> (Username: <username>).                     |
|    |               | Login failed authenticated by AAA local or server.                                                                                                                                            |

## 91.22. WAC

| # | Serverity     | Log message / Explanation                                                                                  |
|---|---------------|------------------------------------------------------------------------------------------------------------|
| 1 | Warning       | WAC unauthenticated user (User Name: <string>, IP: <ipaddr>, MAC: <macaddr>, Port: <[unitID:]portNum>)     |
|   |               | A client host fails to authenticate.                                                                       |
| 2 | Warning       | WAC enters stop learning state.                                                                            |
|   |               | The number of authorized users reaches the maximum user limit on the whole device.                         |
| 3 | Warning       | WAC recovered from stop learning state.                                                                    |
|   |               | The number of authorized users is below the maximum user limit on whole device in a time interval (5 min). |
| 4 | Informational | WAC authenticated user (Username: <string>, IP: <ipaddr>, MAC: <macaddr>, Port: <[unitID:] portNum>)       |
|   |               | A client host authenticated successful.                                                                    |

## 91.23. Traffic Control

| # | Serverity     | Log message / Explanation                                   |
|---|---------------|-------------------------------------------------------------|
| 1 | Warning       | Port <portNum> Broadcast storm is occurring.                |
|   |               | Broadcast storm occurrence.                                 |
| 2 | Informational | Port <portNum> Broadcast storm has cleared.                 |
|   |               | Broadcast storm cleared.                                    |
| 3 | Warning       | Port <portNum> Multicast storm is occurring.                |
|   |               | Multicast storm occurrence.                                 |
| 4 | Informational | Port <portNum>Multicast storm has cleared.                  |
|   |               | Multicast storm cleared.                                    |
| 5 | Warning       | Port <portNum> is currently shut down due to a packet storm |
|   |               | Port shutdown due to a packet storm.                        |

## 91.24. DHCP Server Screening

---

| # | Serverity     | Log message / Explanation                                     |
|---|---------------|---------------------------------------------------------------|
| 1 | Informational | Detected untrusted DHCP server(IP: <ipaddr>, Port <portNum> ) |
|   |               | Detected untrusted DHCP server IP address.                    |

## 91.25. MSTP Debug Enhancement

| #  | Serverity     | Log message / Explanation                                                                                                        |
|----|---------------|----------------------------------------------------------------------------------------------------------------------------------|
| 1  | Notice        | Topology changed [( [Instance:<InstanceID> ],port:<[unitID:] portNum> ,MAC: <macaddr>)]                                          |
|    |               | Topology changed.                                                                                                                |
| 2  | Informational | [CIST   CIST Regional   MSTI Regional] New Root bridge selected( [Instance: <InstanceID> ]MAC: <macaddr> Priority :<value>)      |
|    |               | A new Root Bridge is selected.                                                                                                   |
| 3  | Informational | Spanning Tree Protocol is enabled                                                                                                |
|    |               | STP is enabled.                                                                                                                  |
| 4  | Informational | Spanning Tree Protocol is disabled                                                                                               |
|    |               | STP is disabled.                                                                                                                 |
| 5  | Notice        | New root port selected [( [Instance:<InstanceID> ], port:<[unitID:] portNum>)]                                                   |
|    |               | A new Root Port is selected.                                                                                                     |
| 6  | Notice        | Spanning Tree port status changed [( [Instance:<InstanceID> ], port:<[unitID:] portNum>)] <old_status> -> <new_status>           |
|    |               | STP port status is changed.                                                                                                      |
| 7  | Informational | Spanning Tree port status changed. [( [Instance:<InstanceID> ], port:<[unitID:] portNum>)] <old_role> -> <new_role>              |
|    |               | STP port role is changed.                                                                                                        |
| 8  | Informational | Spanning Tree instance created. Instance:<InstanceID>                                                                            |
|    |               | STP instance is created.                                                                                                         |
| 9  | Informational | Spanning Tree instance deleted. Instance:<InstanceID>                                                                            |
|    |               | STP instance is deleted.                                                                                                         |
| 10 | Informational | Spanning Tree version changed. New version:<new_version>                                                                         |
|    |               | STP version is changed.                                                                                                          |
| 11 | Informational | Spanning Tree MST configuration ID name and revision level changed (name:<name> ,revision level <revision_level>).               |
|    |               | MST Configuration ID name and revision level are changed.                                                                        |
| 12 | Informational | Spanning Tree MST configuration ID VLAN mapping table changed (instance: <InstanceID> delete vlan <startvlanid> [-<endvlanid>]). |
|    |               | MST configuration ID VLAN mapping table is deleted.                                                                              |



## 91. System Log Lists

| #  | Serverity     | Log message / Explanation                                                                                                     |
|----|---------------|-------------------------------------------------------------------------------------------------------------------------------|
| 13 | Informational | Spanning Tree MST configuration ID VLAN mapping table changed (instance: <InstanceID> add vlan <startvlanid> [-<endvlanid>]). |
|    |               | MST configuration ID VLAN mapping is added.                                                                                   |

## 91.26. IP and Password Changed Summary

| # | Serverity     | Log message / Explanation                                                                      |
|---|---------------|------------------------------------------------------------------------------------------------|
| 1 | Informational | [Unit <unitID>] Management IP address was changed by console(Username: <username>,IP:<ipaddr>) |
|   |               | IP address change activity.                                                                    |
| 2 | Informational | [Unit <unitID>] Password was changed by console (Username: <username>,IP:<ipaddr> )            |
|   |               | Password change activity.                                                                      |

## 91.27. DDM

| # | Serverity | Log message / Explanation                                                                         |
|---|-----------|---------------------------------------------------------------------------------------------------|
| 1 | Critical  | Port <[unitID:]portNum> SFP [thresholdType] [exceedType] the [thresholdSubType] alarm threshold   |
|   |           | DDM exceeded or recover from DDM alarm threshold.                                                 |
| 2 | Warning   | Port <[unitID:]portNum> SFP [thresholdType] [exceedType] the [thresholdSubType] warning threshold |
|   |           | DDM exceeded or recover from DDM warning threshold.                                               |

## 91.28. BPDU

---

| # | Serverity     | Log message / Explanation                                                               |
|---|---------------|-----------------------------------------------------------------------------------------|
| 1 | Informational | Port<[unitID:]portNum> enter BPDU under attacking state (mode: drop / block / shutdown) |
|   |               | BPDU attack happend.                                                                    |
| 2 | Informational | Port <[unitID:]portNum> recover from BPDU under attacking state automatically           |
|   |               | BPDU attack automatically recovered.                                                    |
| 3 | Informational | Port<[unitID:]portNum> recover from BPDU under attacking state manually                 |
|   |               | BPDU attack manually recovered.                                                         |

## 91.29. Fan

---

| # | Serverity | Log message / Explanation                       |
|---|-----------|-------------------------------------------------|
| 1 | Critical  | Unit <unitID>, Right Side Fan <value> failed    |
|   |           | Right side fan failed.                          |
| 2 | Critical  | Unit <unitID>, Right Side Fan <value> recovered |
|   |           | Right side fan recovered.                       |

## 91.30. Temperature

| # | Severity      | Log message / Explanation                                                                                     |
|---|---------------|---------------------------------------------------------------------------------------------------------------|
| 1 | Warning       | [Unit <unitID>] Temperature sensor: <sensorID> enter alarm state. (current Temperature: <temperature>)        |
|   |               | Temperature sensor enters alarm state.                                                                        |
| 2 | Informational | [Unit <unitID>] Temperature sensor: <sensorID> recovers to normal state. (current Temperature: <temperature>) |
|   |               | Temperature recovers to normal.                                                                               |
| 3 | Informational | Sensor value <value>                                                                                          |
|   |               | Temperature sensor read successfully.                                                                         |
| 4 | Informational | Sensor value fail                                                                                             |
|   |               | Temperature sensor read failed.                                                                               |

## 91.31. IP Source Address

| # | Severity | Log message / Explanation                                                                                                    |
|---|----------|------------------------------------------------------------------------------------------------------------------------------|
| 1 | Warning  | Dynamic DHCP binding entry conflicts with static ARP (IP:<ipaddr>, MAC:<macaddr>, Port:<[unitID:]portNum>).                  |
|   |          | Dynamic DHCP binding entry conflicts with static ARP.                                                                        |
| 2 | Warning  | Dynamic DHCP binding entry conflicts with static IPSG entry (IP:<ipaddr>, MAC:<macaddr>, Port:<[unitID:]portNum>).           |
|   |          | Dynamic DHCP binding entry conflicts with static IPSG entry.                                                                 |
| 3 | Warning  | Creating DHCP binding entry failed due to no ACL rule being available (IP:<ipaddr>, MAC:<macaddr>, Port:<[unitID:]portNum>). |
|   |          | Creating DHCP binding entry failed due to no ACL rule being available.                                                       |
| 4 | Warning  | Unauthenticated IP-MAC address and discarded by [IPSG   DAI] (IP:< ipaddr >, MAC:< macaddr >, Port:<[unitID:]portNum >).     |
|   |          | IPSG or DAI checks a host illegal.                                                                                           |

## 91.32. Spoofing Attack

| # | Serverity | Log message / Explanation                                                         |
|---|-----------|-----------------------------------------------------------------------------------|
| 1 | Critical  | Possible spoofing attack from IP: <ipaddr>, MAC:<macaddr>, port:<portNum>         |
|   |           | Received the switch itself IP with source IP is the same as the ARP or IP packet. |

## 91.33. Ring Redundant Protocol (RRP)

| # | Serverity     | Log message / Explanation                                               |
|---|---------------|-------------------------------------------------------------------------|
| 1 | Notice        | Ring topology was recovered to complete.                                |
|   |               | The status in “Master Node” changes from “Failed” to “Complete” .       |
| 2 | Warning       | Ring topology was failed.                                               |
|   |               | The status in “Master Node” changes from “Complete” to “Failed” .       |
| 3 | Informational | FDB was flushed.                                                        |
|   |               | Flushes its Forwarding Database based on RRP packets or state machine.  |
| 4 | Warning       | RRP ring status was changed to Link-Up                                  |
|   |               | The RRP status in “Transit Node” changes to “Link-Up” .                 |
| 5 | Notice        | RRP ring status was changed to Link-Down                                |
|   |               | The RRP status in “Transit Node” changes to “Link-Down” .               |
| 6 | Informational | RRP ring status was changed to Pre-Forwarding                           |
|   |               | The RRP status in “Transit Node” changes to “Pre-Forwarding” .          |
| 7 | Informational | Ring Guard was activated on “<domain name>” domain at port < port num>. |
|   |               | Worked ring guard function at the specific domain and port.             |

## 91.34. Others

---

| # | Serverity | Log message / Explanation                                  |
|---|-----------|------------------------------------------------------------|
| 1 | Emergency | [Uint <unitID>] System re-start reason: system fatal error |
|   |           | CPU exception lead to reboot system.                       |



---

## Appendix A. Specifications

---

### ○ Interface

- SFP extension ports: Ports 1 to 24
  - Transmission system    IEEE802.3z 1000BASE-SX/1000BASE-LX
  - Diagnostic Monitoring Interface (DMI):  
SFF-8472
  
- Copper ports: Ports 21 to 24 (RJ45 connector)  
(Select either of copper port or SFP for use)
  - Transmission system    IEEE802.3 10BASE-T  
IEEE802.3u 100BASE-TX  
IEEE802.3ab 1000BASE-T
  
- SFP+ extension ports: Ports 25 to 26
  - Transmission system    IEEE802.3z 1000BASE-SX/1000BASE-LX  
IEEE802.3ae 10GBASE-SR/10GBASE-LR
  - Diagnostic Monitoring Interface (DMI):  
SFF-8472
  
- SFP+ extension ports and stacking ports: Ports 27 to 28
  - Transmission system    IEEE802.3z 1000BASE-SX/1000BASE-LX  
IEEE802.3ae 10GBASE-SR/10GBASE-LR
  - Diagnostic Monitoring Interface (DMI):  
SFF-8472
  
- Console port x 1 (RJ45 connector)
  - Compliant with RS-232C (ITU-TS V.24)
  
- SD card slot x 1
  - Standard: SD/SDHC
  - Class: 2/4/6/10
  - Size: 128 MB to 32 GB

## ○ System Performance

- Store-and-forward system
- Switching capacity 128 Gbps
- Forwarding rate
 

|            |                |
|------------|----------------|
| 10BASE-T   | 14,880 pps     |
| 100BASE-TX | 148,800 pps    |
| 1000BASE-T | 1,488,000 pps  |
| 10GBASE-X  | 14,880,000 pps |
- Buffered memory 2 MB
- Flow control
  - Back pressure (half-duplex)
  - IEEE802.3x (full duplex)
  - HOL blocking prevention

## ○ Stacking Function

- Number of units Four units max.
- Bandwidth 40 Gbps max.

## ○ Layer-2 Functions

- MAC address table 32k entries/unit
- IGMP Snooping v1/v2/v3, 4k groups, fixed 64 groups
- MLD Snooping v1/v2, 4k groups, fixed 64 groups
- IGMP Proxy
- MLD Proxy
- Spanning tree IEEE802.1D
- Rapid spanning tree IEEE802.1D
- Multiple spanning tree IEEE802.1Q (instance: 32)
- Link aggregation IEEE802.1ad (8 ports max. per group/48 groups)
- Port monitoring Capable of monitoring multiple ports (1 set), RSPAN
- Ring Redundant Protocol 8 domains max.



## Appendix A. Specifications

### ○ Layer-3 Functions

- IP forwarding 95 Mpps max.
- Routing protocol RIPv1/v2, OSPFv2/v3  
PIM-DM/SM/SSM/Sparse-Dense-Mode  
DVMRP  
Policy-based routing
- Routing table 12K max. (IPv4: 12k, IPv6: 6k)
- Multicast IGMP v1/v2/v3, MLD v1/v2
- VRRP 256 max.
- DHCP v4 server Allocatable IP address: 1024/pool  
Max. pool: 10  
Max. manual binding address: 16
- DHCP v6 server Allocatable IP address: 4096 (shared by all pools)  
Max. pool: 10  
Max. manual binding address: 64
- DHCP relay(IPv4/v6) Capable of DHCP option 60/61/82

### ○ Other Major Functions

- Tagged VLAN IEEE802.1Q, 4094 max. including default VLAN
- QoS IEEE802.1p (eight levels), PQ/WRR, WRED
- Access control
- Storm control
- Port-based authentication(IEEE802.1X, Guest VLAN)
- MAC-based authentication w/Guest VLAN
- Web-based authentication w/Guest VLAN

### ○ Management Methods

- Console, Telnet, SSHv2, SNMP v1/v2c/v3, ZEUQUO assist Plus

### ○ Agent Specifications

- SNMP v1/v2c/v3 (RFC1157,1901,2570,2575)
- TELNET (RFC854)
- SSH v2 (RFC4250,4251,4252,4253,4254)
- TFTP (RFC783)
- BOOTP (RFC951)
- SNTP (RFC1769)

## ○ Supported MIB

- RFC1213-MIB(MIBII) (RFC1213)
- BRIDGE-MIB (RFC4188)
- SNMPv2-MIB (RFC1907)
- RMON-MIB (RFC1757,2819) [Group 1, 2, 3, 9]
- RMON2-MIB (RFC2021)
- EtherLike-MIB (RFC1643,2358,2665)
- MAU-MIB (RFC4836)
- P-BRIDGE-MIB (RFC4363)
- IF-MIB (RFC2233,2863)
- RADIUS-AUTH-CLIENT-MIB (RFC2618)
- MGMD-STD-MIB (RFC5519)
- RIPv2-MIB (RFC1724)
- IP-FORWARD-MIB (CIDR) (RFC4292)
- IPMROUTE-STD-MIB (RFC2932)
- PIM-MIB (RFC2934)
- RADIUS-ACC-CLIENT-MIB (RFC2620)
- DISMAN-PING-MIB (RFC2925)
- DISMAN-TRACEROUTE-MIB (RFC2925)
- OSPF-MIB (RFC1850)
- VRRP-MIB (RFC2787)
- ENTITY-MIB (RFC2737)
- IPV6-MIB (RFC2465)

## ○ Power Supply Specifications

- Power supply AC 100 - 240 V, 50/60 Hz, 2.0 A
- Power consumption Normally Max. 45.2 W, Min. 30.6 W

## ○ Environment Specifications

- Operating temperature 0 to 45 degrees C
- Operating humidity 20 to 80 % RH (no condensation)
- Storage temperature -20 to 70 degrees C
- Storage humidity 10 to 90 % RH (no condensation)

## ○ External Specifications

- Dimensions 44 mm (Height) x 440 mm (Width) x 312 mm (Depth)  
(Excluding protruding sections)
- Mass (Weight) 4,500 g

---

## Appendix B. Procedures for Configuration Using ZEQUO assist Plus

---

You can configure the Switching Hub via Console, Telnet, or SSH using a terminal emulator software. Our free support application, called “ZEQUO assist Plus” , is also included it.

(Please refer the operation manual included in ZEQUO asssit Plus archive file for more detail.)

1. Unzip the archive file “ZEQUOASSISTPLUS\_vxxxx.zip” included in attached CD-ROM.
2. Run “ZEQUOASSIST.exe” and set login ID and password for this application.
3. Click “The ZEQUO series” button in the “ZEQUO assist Launcher” .
4. Click “Terminal Emulator” button in the ZEQUO assist main window.
5. Check “Console” in “Terminal emulator connection method” field and choose the COM port number.
6. Click “Start a terminal emulator” button.

---

# Troubleshooting

---

If you find any problem, please take the following steps to check.

## LED

- \* The POWER LED is not lit.
  - Is the power plug connected?  
Check that the power plug is firmly connected, so the connection is not loose at the power port.
  - Is this Switching Hub used in a place where operating temperature is between 0 and 45 degrees C?  
Use the Switching Hub within the range of operating temperature.
- \* The SD CARD LED is not lit.
  - Is the SD card installed?  
Check that the SD card is firmly inserted.

## Communication Failure

- \* Is the UTP/fiber cable connected to the correct port?
- \* Are the SFP modules complied with the same standard each other?
- \* Is the fiber cable correct the fiber mode (single or multi)?
- \* Attempt to disable “Power Saving” function at target port.
- \* Are the communication speed and mode settings correct?  
If the communication mode signal cannot be properly obtained, the Switching Hub operates in half-duplex mode. Check the auto negotiation setting again.  
Do not fix the speed/duplex mode of the connected terminal to full-duplex mode.
- \* Is the usage rate of the network to which this Switching Hub is connected excessively high?  
Try separating this Switching Hub from the network.

## Stacking Failure

- \* Is the stacking function enabled?
- \* Is the SFP+ direct attached cable connected to stacking port (port 27 or 28) correctly?
- \* Is the STACK ID LED displayed the correct ID?
- \* Are all of the firmware versions for the devices that are connected to the stacks identical?

---

# Warranty and After-sales Service

---

## 1. Warranty card

A warranty card is included in the Installation Guide provided with this Switching Hub. Be sure to confirm that the date of purchase, shop (company) name, etc., have been entered in the warranty card and then receive it from the shop. Read it carefully, and then keep it in a safe place. The warranty period is one year from the date of purchase.

## 2. Repair request

If a problem is not solved even after taking the steps shown in the "Troubleshooting" section in this manual, please use the Memo shown on the next page and make a repair request with the following information to the shop where you purchased this Switching Hub.

- **Product name**
- **Model number**
- **Product serial number**  
(11-alphanumeric characters labeled on the back of the product.)
- **Firmware version** (The number after "Ver." labeled on the unit package)
- **Problem status** (Please give as concrete information as possible.)

\* Within the warranty period:

Repair service will be provided in accordance with the conditions stipulated in the warranty card.

Please bring your product and warranty card in the shop where you purchased it.

\* After the warranty period expires:

If our check determines that your product is repairable, a chargeable repair service is available upon your request.

Please contact the shop where you purchased the product.

## 3. Inquiries about after-sales service and the product

Contact the shop where you purchased the product.

## Memo (Fill in for future reference)

|                          |                                                     |  |  |  |              |            |  |  |  |  |  |  |
|--------------------------|-----------------------------------------------------|--|--|--|--------------|------------|--|--|--|--|--|--|
| Date of purchase         |                                                     |  |  |  | Model name   | ZEQUO 6500 |  |  |  |  |  |  |
|                          |                                                     |  |  |  | Model number | PN36242E-  |  |  |  |  |  |  |
| Firmware Version         | Boot PROM                                           |  |  |  |              |            |  |  |  |  |  |  |
|                          | Firmware (*)                                        |  |  |  |              |            |  |  |  |  |  |  |
| Serial number            |                                                     |  |  |  |              |            |  |  |  |  |  |  |
|                          | (11-alphanumeric characters labeled on the product) |  |  |  |              |            |  |  |  |  |  |  |
| Shop/Sales company       | Tel:                                                |  |  |  |              |            |  |  |  |  |  |  |
| Customer service contact |                                                     |  |  |  |              |            |  |  |  |  |  |  |
|                          | Tel:                                                |  |  |  |              |            |  |  |  |  |  |  |

(\* Check screen is described in Section 5.8 of the Operation Manual.)

© Panasonic Eco Solutions Networks Co., Ltd. 2016

---

**Panasonic Eco Solutions Networks Co., Ltd.**

2-12-7, Higashi-Shimbashi, Minato-ku, Tokyo Japan, 105-0021

URL: <http://panasonic.co.jp/es/pesnw/english/>

---

P0816-0