CLI Management

In CLI Management:

This switch provides a CLI (Command Line Interface) management interface. You can make all settings and monitor system status with this management CLI.

You can access the CLI via serial console, telnet, or SSH. All the commands for these three different connection types are the same and can be related. Please see the follow section for detailed descriptions about the commands.

Table of Contents

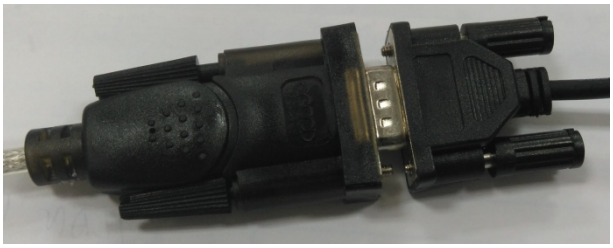
Hardware installation

In order to connect switch's CLI via its console port, you need to prepare two different cables, which are:

- A USB to RS232 Male Cable, as shown in the figure down below:

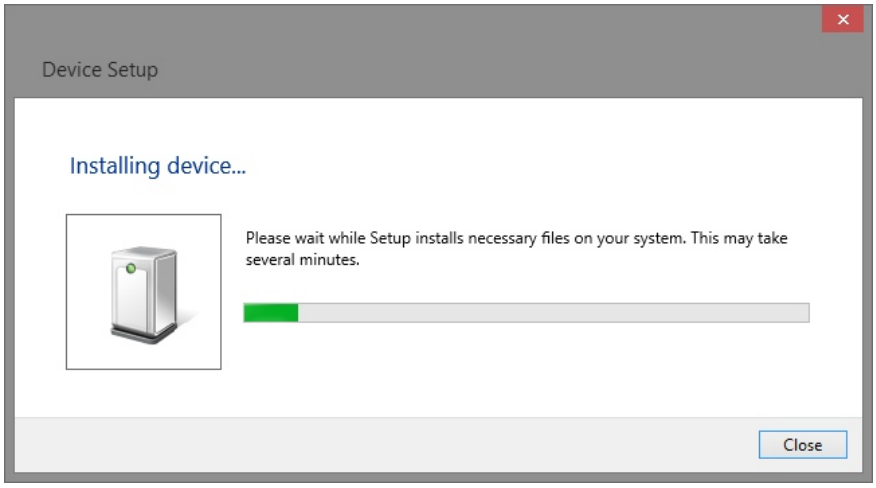
- An RJ45 to RS232 Female Cable, as shown in the figure down below:

In order to connect these two cables to switch's console port and use the CLI, please connect one of the Male RS232 connector to the Female RS232 connector, as shown in the figure down below:

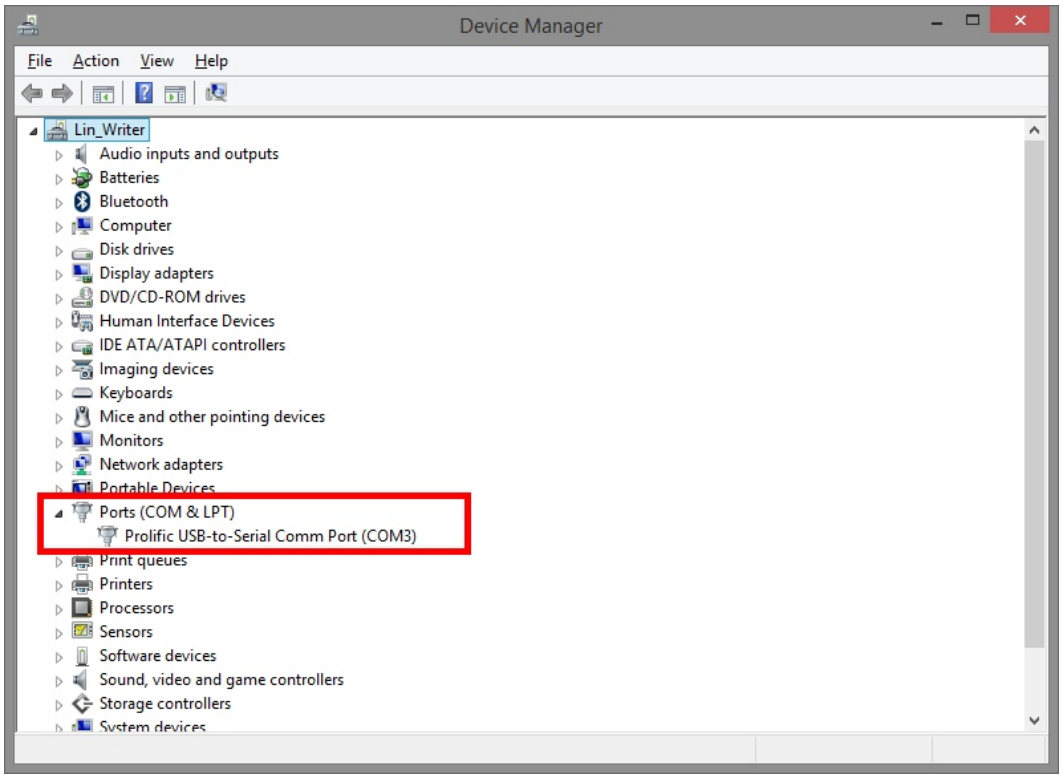


Connect the USB connector to your PC, and the RJ45 connector to the switch's console port.

The PC should install the driver for the console cable automatically.



If the driver is installed properly, you should be able to see it in Device Manager, under “Ports (COM & LPT)” category. Here in the figure down below, a serial port called “COM3” is installed as the new serial port.



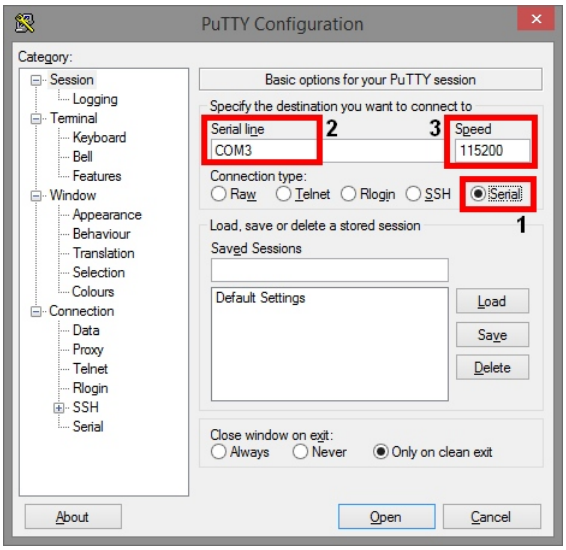
Now that the hardware is installed, we are ready to log into the switch’s CLI. The following section will show you how to connect to switch’s CLI with PuTTY.

PuTTY is a free and open-source software for terminal emulation, and can be downloaded here.

Connecting to CLI via PuTTY

Before using PuTTY to connect to the switch's CLI, please make sure that the USB to Serial cables are connected correctly as mentioned in this Quick Guide (Page 1). Also, please make sure that the USB to Serial cables are installed and working properly.

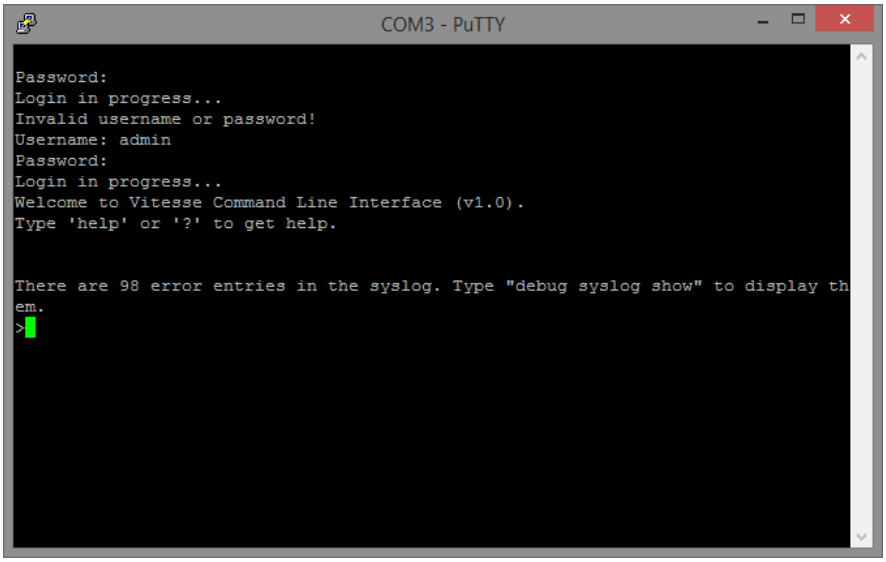
To start connecting to CLI via PuTTY, please double-click the PuTTY icon. A PuTTY Configuration window will pop up.



Please set the PuTTY as following:

1. Set the Connection Type to Serial.
2. Set the Serial Line according to the serial port number on your PC. For more information regarding to the serial port number, please refer to Page 2 of this Quick Guide.
3. Set the Speed to 115200.

After all the settings are done, please press the "Open" button to start the connection.



To start a CLI session, please press the "Enter" key. The default login name and password are both "admin".

Basic Operating Keys and Commands of CLI

The CLI is composed of different command groups, and each command group can be used to set variables of different functions such IP settings, PoE, or QoS.

Here we will introduce some of the basic and commonly-used commands of CLI. Please see the table down below for reference:

Command	Description
?	Type in "?" and press enter to list all the commands available in the current command layer. Type "?" after a command allows you to view the parameters available for that command and the function of these parameters.
exit	Go back to the previous layer of the command line structure.
end	Return to the root layer of the command line structure.
Ctrl + Z	Press Ctrl + Z on your keyboard to go back to user EXEC mode.
"↑" "↓"	Press the "↑" "↓" arrow key on the keyboard to go through the previous commands that you've typed.
Tab	Press the Tab key on the keyboard to complete a partially typed command.
configure terminal	Enter the global mode of the command line structure.

CLI Command Modes

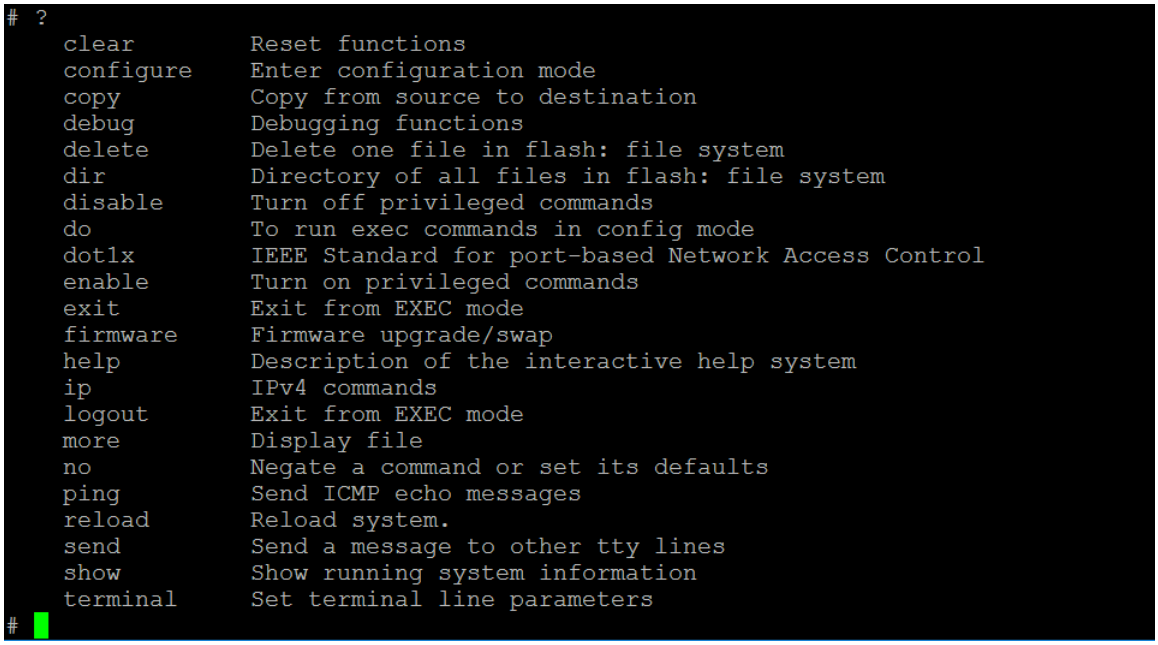
This section describes the CLI command mode structure. Some of the commands only work under certain modes. For example, command “aaa” works only when entered in global configuration mode. The command modes include:

Command Mode	Access Method	Prompt
User EXEC Mode	This is the first level of access. In this mode you can change terminal settings, perform basic tasks, and list system information.	#
Global Mode	From user EXEC mode, enter the enable command “configure terminal”.	(config)#
Interface Mode	From global configuration mode, specify an interface by entering the interface command (for example: “interface *”).	(config-if)#
Config-vlan	In global configuration mode, enter the “vlan <vlan_ID>” command.	(config-vlan)#

User EXEC Mode

After you access the device, you are automatically in user EXEC command mode. The user EXEC commands available at the user level are a subset of those available at the privileged level. In general, use the user EXEC commands to change terminal settings temporarily, to perform basic tests, and to list system information.

To view a comprehensive list of commands, enter a question mark (?) at the prompt.



Global Configuration Mode

Global configuration commands apply to features that affect the device as a whole. Use the “configure terminal” command to enter global configuration mode.

To view a comprehensive list of commands, enter a question mark (?) at the prompt.

```
(config)# ?
   aaa              Authentication, Authorization and Accounting
   access           Access management
   access-list      Access list
   aggregation      Aggregation mode
   banner           Define a login banner
   clock            Configure time-of-day clock
   default          Set a command to its defaults
   do               To run exec commands in config mode
   dot1x            IEEE Standard for port-based Network Access Control
   enable           Modify enable password parameters
   end              Go back to EXEC mode
   exit             Exit from current mode
   gvrp             Enable GVRP feature
   help             Description of the interactive help system
   hostname         Set system's network name
   interface        Select an interface to configure
   ip               Internet Protocol
   ipmc             IPv4/IPv6 multicast configuration
   ipv6             IPv6 configuration commands
   lacp             LACP settings
   line             Configure a terminal line
   lldp             LLDP configurations.
-- more --, next page: Space, continue: g, quit: ^C
```

```
   lldp             LLDP configurations.
   logging          Syslog
   loop-protect     Loop protection configuration
   mac              MAC table entries/configuration
   monitor          Set monitor configuration.
   mvr              Multicast VLAN Registration configuration
   no               Negate a command or set its defaults
   ntp              Configure NTP
   poe              Power Over Ethernet.
   port-security    Enable/disable port security globally.
   privilege        Command privilege parameters
   qos              Quality of Service
   radius-server    Configure RADIUS
   rmon             Remote Monitoring
   sflow            Statistics flow.
   snmp-server      Set SNMP server's configurations
   spanning-tree    Spanning Tree protocol
   tacacs-server    Configure TACACS+
   upnp             Set UPnP's configurations
   username         Establish User Name Authentication
   vlan             VLAN commands
   voice            Voice appliance attributes
   web              Web
(config)#
```

To exit global configuration command mode and to return to user EXEC mode, enter the “end” or “exit” command, or press Ctrl-Z on your keyboard.

Interface Configuration Mode

Interface configuration commands modify the operation of the interface. Interface configuration commands always follow a global configuration command, which defines the interface type.

Use the “interface” command to access interface configuration mode. The new prompt will be changed to “(config-if)#”, indicating that you’re in interface configuration mode.

The supported commands can vary depending on the version of IOS software in use. To view a comprehensive list of commands, enter a question mark (?) at the prompt.

```
(config-if)# ?
    access-list          Access list
    aggregation          Create an aggregation
    do                   To run exec commands in config mode
    dot1x                IEEE Standard for port-based Network Access Control
    duplex               Interface duplex
    end                  Go back to EXEC mode
    excessive-restart    Restart backoff algorithm after 16 collisions (No
                         excessive-restart means discard frame after 16
                         collisions)
    exit                 Exit from current mode
    flowcontrol          Traffic flow control.
    green-ethernet       Green ethernet (Power reduction)
    gvrp                 Enable GVRP on port(s)
    help                 Description of the interactive help system
    ip                   Internet Protocol
    ipv6                 IPv6 configuration commands
    lacp                 Enable LACP on this interface
    lldp                 LLDP configurations.
    loop-protect         Loop protection configuration on port
    mac                  MAC keyword
    media-type           Media type.
    mtu                  Maximum transmission unit
-- more --, next page: Space, continue: g, quit: ^C
```

```
    ipv6                 IPv6 configuration commands
    lacp                 Enable LACP on this interface
    lldp                 LLDP configurations.
    loop-protect         Loop protection configuration on port
    mac                  MAC keyword
    media-type           Media type.
    mtu                  Maximum transmission unit
    mvr                  Multicast VLAN Registration configuration
    no                   Negate a command or set its defaults
    pdip                 Power Over Ethernet.
    poe                  Power Over Ethernet.
    port-security        Enable/disable port security per interface.
    pvlan                Private VLAN
    qos                  Quality of Service
    rmon                 Configure Remote Monitoring on an interface
    sflow                Statistics flow.
    shutdown             Shutdown of the interface.
    snmp-server          Set SNMP server's configurations
    spanning-tree        Spanning Tree protocol
    speed                Configures interface speed. If you use 10, 100, or
                         1000 keywords with the auto keyword the port will only
                         advertise the specified speeds.
    switchport           Switching mode characteristics
(config-if)#
```

To exit interface configuration mode and to return to global configuration mode, enter the exit command. To exit interface configuration mode and to return to privileged EXEC mode, enter the end command, or press Ctrl-Z.

Config-vlan Mode

Use this mode to configure VLANs (VLAN ID 1~4095).

Enter the “vlan <vlan_id>” command under global configuration mode to access config-vlan mode:

```
(config)# vlan 30
(config-vlan)#
```

The supported keywords can vary but are similar to the commands available in VLAN configuration mode. To view a comprehensive list of commands, enter a question mark (?) at the prompt.

```
(config-vlan)# ?
    do      To run exec commands in config mode
    end     Go back to EXEC mode
    exit    Exit from current mode
    help    Description of the interactive help system
    name    ASCII name of the VLAN
    no
(config-vlan)#
```

To return to global configuration mode, enter exit; to return to privileged EXEC mode, enter end or press Ctrl + Z on your keyboard.

System Configuration

System Information Configuration

The following section will guide you to set the switch's System Contact, System Name, and System Location. This information can be used to identify the switch's system contact, name, and its location.

Step 1	config terminal	Enter global configuration mode.
Step 2	snmp-server contact <System_Contact>	Set the System Contact. Only alphanumeric characters can be used here.
Step 3	hostname <System_Name>	Set the System Name. Only alphanumeric characters can be used here.
Step 4	snmp-server location <System_Location>	Set the System Location. Only alphanumeric characters can be used here.

To negate the command, use the "no snmp-server contact", "no hostname" and "no snmp-server location" global configuration command.

【Configuration Example】

(config)# snmp-server contact RD
(config)# hostname RDSWITCH
RDSWITCH(config)# snmp-server location LAB

IP Configuration

The following section will guide you to set the switch's IP address and subnet mask. Please note that different VLAN may be in different IP address network. For example, by default, VLAN 1 is in the IP address network of 192.168.2.X, and you can set VLAN 2 in the IP address network of 192.168.3.X.

Step 1	config terminal	Enter global configuration mode.
Step 2	interface vlan <VLAN_ID>	Enter the configuration interface of the set VLAN ID.
Step 3	ip address <IPv4_Address> <IPv4_Subnetmask>	Set that specific VLAN's IP address and subnet mask.

To negate the command, use the "no ip address <IPv4_Address> <IPv4_Subnetmask>" global configuration command.

【Configuration Example】

(config)# interface vlan 1
(config-if-vlan)# ip address 192.168.2.3 255.255.255.0
(config-if-vlan)# exit
(config)# interface vlan 2
(config-if-vlan)# ip address 192.168.3.5 255.255.255.0

DNS Server Configuration

The following section will guide you to set the switch's DNS server. This switch allows you to add up to 4 different DNS servers (No. 0~3).

Step 1	config terminal	Enter global configuration mode.
Step 2	ip name-server <DNS_Server_No> <DNS_ Server_IP>	Add a DNS server.

To negate the command, use the "no ip name-server" global configuration command.

【Configuration Example】

(config)# ip name-server 1 8.8.8.8
(config)# ip name-server 2 168.95.1.1

IP Route Configuration

The following section will guide you to set the switch's static route table.

Step 1	config terminal	Enter global configuration mode.
Step 2	ip route <Network_IP> <Subnetmask> <Gateway>	Add a static route with the set network IP, subnetmask, and gateway.

To negate the command, use the "no ip route <Network_IP> <Subnetmask> <Gateway>" global configuration command.

【Configuration Example】

(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1
(config)# ip route 0.0.0.0 0.0.0.0 192.168.3.1

NTP Configuration

The following section will guide you to set the switch's NTP server. NTP server allows you to set the switch's internal clock to the current time and date for system management convenience.

Step 1	config terminal	Enter global configuration mode.
Step 2	ntp	Enable NTP function.
Step 3	ntp server <NTP_Server_No> ip-address <NTP_Server_Domain/IP>	Add a NTP server. You can set up to 5 NTP servers with NTP server domain name or its IP address.

To negate the command, use the "no ntp" and "no ntp server <NTP_Server_No>" global configuration command.

【Configuration Example】

(config)# ntp
(config)# ntp server 1 ip-address tick.stdtime.gov.tw
(config)# ntp server 2 ip-address 216.239.35.0

System Log Server Configuration

The following section will guide you to set the switch's system log server. The switch generates system logs when an event happens for management reference. However, these logs are stored in the switch's volatile memory, which means all these logs will be lost once the switch is powered off. To keep the switch system logs, you will have to set a system log server. All system logs will be sent to the system log server and can be kept even the switch is powered off.

Step 1	config terminal	Enter global configuration mode.
Step 2	logging on	Enable system log server function.
Step 3	logging host <<LOG_Server_Domain/IP>	Set the system log server by its domain name or IP address. Please note that there can be only 1 system log server.
Step 4	logging level <error/informational/notice /warning>	Set the system log server noting level. The severity of the log, from most severe to least severe, is: error (system error, usually result in system crash), warning (a severe event just happened), notice (port up/down), and informational (switch reboot).

To negate the command, use the "no logging on" global configuration command.

【Configuration Example】

(config)# logging on
(config)# logging host syslog.com
(config)# logging level notice

Port Configuration

Shutdown Port

The following section will guide you to shutdown certain ports of the switch. Ports that are shutdown will not receive/transmit and network packets.

Step 1	config terminal	Enter global configuration mode.
Step 2	interface GigabitEthernet <Switch_No/Port>	Enter the port configuration interface. For example, if you would like to enter port 1~4's port configuration interface, type in "interface GigabitEthernet 1/1-4".
Step 3	shutdown	Shutdown the ports of the port configuration interface.

To negate the command, use the "no shutdown" in port configuration interface.

【Configuration Example】

(config)# interface GigabitEthernet 1/1-4
(config-if)# shutdown
(config-if)# no shutdown

Set Port Transmitting Speed

The following section will guide you to set the transmitting speed of specific ports.

Step 1	config terminal	Enter global configuration mode.
Step 2	interface GigabitEthernet <Switch_No/Port>	Enter the port configuration interface. For example, if you would like to enter port 1~4's port configuration interface, type in "interface GigabitEthernet 1/1-4".
Step 3	speed <Transmitting_Speed>	Set the speed of ports of the port configuration interface. • 10: 10Mbps • 100: 100Mbps • 1000: 1Gbps • auto: Auto negotiation

To negate the command, use the "no speed" in port configuration interface.

【Configuration Example】

(config)# interface GigabitEthernet 1/1-4
(config-if)# speed 100

Enable Port Flow-Control

The following section will guide you to enable flow-control function.

Step 1	config terminal	Enter global configuration mode.
Step 2	interface GigabitEthernet <Switch_No/Port>	Enter the port configuration interface. For example, if you would like to enter port 1~4's port configuration interface, type in "interface GigabitEthernet 1/1-4".
Step 3	flowcontrol <on/off>	Enable/disable flow-control function • on: Enable flow-control. • off: Disable flow-control.

To negate the command, use the "no flowcontrol" in port configuration interface.

【Configuration Example】

(config)# interface GigabitEthernet 1/1-4
(config-if)# flowcontrol on

Set Port MTU (Jumbo Frame)

The following section will guide you to set the MTU value of specific ports. In computer networking, jumbo frames or jumbos are Ethernet frames with more than 1500 bytes of payload, the limit set by the IEEE 802.3 standard.

Step 1	config terminal	Enter global configuration mode.
Step 2	interface GigabitEthernet <Switch_No/Port>	Enter the port configuration interface. For example, if you would like to enter port 1~4's port configuration interface, type in "interface GigabitEthernet 1/1-4".
Step 3	mtu <Max_Frame_Size>	Set the max frame size. The value can be an integer from 1518 to 9300

To negate the command, use the "no mtu" in port configuration interface.

【Configuration Example】

(config)# interface GigabitEthernet 1/1-4
(config-if)# mtu 1518

DHCP Configuration

Setting a DHCP Server & DHCP IP Pool

The following section will guide you to set a DHCP IP pool. With this function, devices in the same VLAN can acquire a set of IP address from the switch.

Step 1	config terminal	Enter global configuration mode.
Step 2	ip dhcp server	Enable the DHCP server function globally.
Step 3	interface vlan <VLAN_ID>	Enter the configuration interface of the set VLAN ID.
Step 4	ip dhcp server	Add and enable a DHCP server to the set VLAN.
Step 5	exit	Exit the VLAN configuration interface and go back to global configuration mode.
Step 6	ip dhcp excluded-address <Lower_IP> <Higher_IP>	Set the excluded IP address range. The IP addresses in this range will not be assign to DHCP client devices.
Step 7	ip dhcp pool <DHCP_Pool_Name>	Create a DHCP pool with the <DHCP_Pool_Name> and enter its configuration interface.
Step 8	network <IPv4_Address> <IPv4_Subnetmask>	Set that specific DHCP pool's IP address and subnet mask and set the DHCP pool type to "Network".
Step 9	broadcast <IPv4_Address>	Set the broadcast IP address.
Step 10	domain-name <Domain_Name>	Set the DHCP pool domain name.
Step 11	default-router <Router_IP>	Set the router's IP address.

To negate the command, use the "no ip dhcp server" in port configuration interface.

【Configuration Example】

```
(config)# ip dhcp server
(config)# interface vlan 1
(config-if-vlan)# ip dhcp server
(config-if-vlan)# exit
(config)# ip dhcp excluded-address 192.168.2.1 192.168.2.100
(config)# ip dhcp pool POOL1
(config-dhcp-pool)# broadcast 192.168.2.255
(config-dhcp-pool)# network 192.168.2.0 255.255.255.0
(config-dhcp-pool)# domain-name POOL1
(config-dhcp-pool)# default-router 192.168.2.1
```

DHCP Snooping

The following section will guide you to set DHCP snooping function. DHCP Snooping is used to block intruder on the un-trusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

Step 1	config terminal	Enter global configuration mode.
Step 2	ip dhcp snooping	Enable the global DHCP snooping function.
Step 3	interface GigabitEthernet <Switch_No/Port>	Enter the port configuration interface. For example, if you would like to enter port 1~4's port configuration interface, type in "interface GigabitEthernet 1/1-4".
Step 3	no ip dhcp snooping trust	Set these ports as DHCP un-trusted ports, which means DHCP server connects to these ports won't be able to assign IP addresses to other devices in the network.

To negate the command, use the "no ip dhcp snooping" in port configuration interface.

【Configuration Example】

(config)# ip dhcp snooping
(config)# interface GigabitEthernet 1/1-4
(config-if)# no ip dhcp snooping trust

DHCP Relay

The following section will guide you to set the DHCP relay. A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain. It stores the incoming interface IP address in the GIADDR field of the DHCP packet. The DHCP server can use the value of GIADDR field to determine the assigned subnet. For such condition, please make sure the switch configuration of VLAN interface IP address and PVID (Port VLAN ID) correctly.

Step 1	config terminal	Enter global configuration mode.
Step 2	ip dhcp relay	Enable DHCP relay function globally.
Step 3	ip helper-address <IPv4_Relay_Server>	Set the DHCP relay server IP address.
Step 4	ip dhcp relay information option	Enable DHCP relay information mode operation.
Step 5	ip dhcp relay information policy <drop/keep/replace>	Indicates the DHCP relay information option policy. • Replace: Replace the original relay information when a DHCP message that already contains it is received. • Keep: Keep the original relay information when a DHCP message that already contains it is received. • Drop: Drop the package when a DHCP message that already contains relay information is received.

To negate the command, use the “no ip dhcp relay” in port configuration interface.

【Configuration Example】

(config)# ip dhcp relay
(config)# ip helper-address 192.168.2.254
(config)# ip dhcp relay information option
(config)# ip dhcp relay information policy drop.

Aggregation

Static Aggregation

The following section will guide you to set static aggregation. Port trunk (or port aggregation) allows multiple links to be bundled together and act as a single physical link for increased throughput. It provides load balancing, and redundancy of links in a switched inter-network. Actually, the link does not have an inherent total bandwidth equal to the sum of its component physical links. Traffic in a trunk is distributed across an individual link within the trunk in a deterministic method that called a hash algorithm. The hash algorithm automatically applies load balancing to the ports in the trunk. A port failure within the trunk group causes the network traffic to be directed to the remaining ports. Load balancing is maintained whenever a link in a trunk is lost or returned to service.

Static aggregation set designated ports as static trunk port. Please note that these ports can only function as connection ports for switches with the same static trunk settings, which means if these designated ports won't be able to function normally when connected to network devices.

Step 1	config terminal	Enter global configuration mode.
Step 2	interface GigabitEthernet <Switch_No/Port>	Enter the port configuration interface. For example, if you would like to enter port 1~4's port configuration interface, type in "interface GigabitEthernet 1/1-4".
Step 3	aggregation group <Static_Aggr_Group>	Set the specific ports as a static aggregation group with the <Static_Aggr_Group>. <Static_Aggr_Group> is an integer.

To negate the command, use the "no aggregation group" in port configuration interface.

【Configuration Example】

(config)# interface GigabitEthernet 1/1-4
(config-if)# aggregation group 1

LACP Aggregation

The following section will guide you to set LACP aggregation.

LACP stands for Link Aggregation Control Protocol. Two switches will communicate with each other with the Link Aggregation Control Protocol and combine set ports as aggregation ports automatically, which means these ports can still connect to network devices.

Step 1	config terminal	Enter global configuration mode.
Step 2	interface GigabitEthernet <Switch_No/Port>	Enter the port configuration interface. For example, if you would like to enter port 1~4's port configuration interface, type in "interface GigabitEthernet 1/1-4".
Step 3	lacp	Set the specific ports as a LACP aggregation. By default setting, these ports will connect other LACP enabled ports automatically, so no more settings are required.

To negate the command, use the "no lacp" in port configuration interface.

【Configuration Example】

(config)# interface GigabitEthernet 1/1-4
(config-if)# lacp

Loop Protection

Enable Loop Protection

The following section will guide you to set loop protection. If loop protection is enabled, the switch will take action you assigned here when a network loop occurs.

Step 1	config terminal	Enter global configuration mode.
Step 2	loop-protect	Enable global loop protection function.
Step 3	interface GigabitEthernet <Switch_No/Port>	Enter the port configuration interface. For example, if you would like to enter port 1~4's port configuration interface, type in "interface GigabitEthernet 1/1-4".
Step 4	loop-protect action <log/shutdown>	Set these ports' action when a network loop occurs. • log: Make a system log when a network loop happens. • shutdown: Shutdown port with network loop for a set period of time. You can choose both, which means the port will make a system log and shutdown port.

To negate the command, use the "no loop-protect" in global configuration interface.

【Configuration Example】

(config)# loop-protect
(config)# interface GigabitEthernet 1/1-4
(config-if)# loop-protect action log shutdown

Power over Ethernet Configuration

Enable/Disable PoE per Port

The following section will guide you to enable/disable PoE function on a (or a series of) port. Please note that switch ports can still transmit/receive packets even their PoE function are disable.

Step 1	config terminal	Enter global configuration mode.
Step 2	interface GigabitEthernet <Switch_No/Port>	Enter the port configuration interface. For example, if you would like to enter port 1~4's port configuration interface, type in "interface GigabitEthernet 1/1-4".
Step 3	no poe mode	Disable PoE function in these ports.

To negate the command, use the "poe mode plus" in port intreface configuration interface.

【Configuration Example】

(config)# interface GigabitEthernet 1/1-4
(config-if)# no poe mode

Set PoE Priority

The following section will guide you to set PoE priority for each port. PoE priority decides which port can get power first when the PoE power budget is not enough to satisfy all the PoE port requirement.

Step 1	config terminal	Enter global configuration mode.
Step 2	interface GigabitEthernet <Switch_No/Port>	Enter the port configuration interface. For example, if you would like to enter port 1~4's port configuration interface, type in "interface GigabitEthernet 1/1-4".
Step 3	poe priority <critical/high/low>	Set the port PoE priority. The priority levels include: • critical: For ports that connected to the most essential device. Ports with "critical" priority level will get PoE power first. • high: Ports with "high" priority level will get PoE power when the PoE requirement of ports with "critical" priority level are met. • low: Ports with the lowest priority level. These ports will not be assigned PoE power first if the PoE budget is not enough.

To negate the command, use the "no poe priority" in port intreface configuration interface.

【Configuration Example】

(config)# interface GigabitEthernet 1/1-4
(config-if)# poe priority critical

Set PoE Management Mode

The following section will guide you to set PoE management mode. Settings here affect overall PoE power assigning behavior.

Step 1	config terminal	Enter global configuration mode.
Step 2	poe management mode <allocation-consumption/allocation-reserved-power /class-consumption/class-reserved-power /lldp-consumption/lldp-reserved-power>	Set the PoE management mode. The management modes include: • allocation-consumption: Max. port power determined by allocated, and power is managed according to power consumption. • allocation-reserved-power: Max. port power determined by alocated, and power is managed according to reserved power. • class-consumption: Max. port power determined by class, and power is managed according to power consumption. • class-reserved-power: Max. port power determined by class, and power is managed according to reserved power. • lldp-consumption: Max. port power determined by LLDP Media protocol, and power is managed according to power consumption. • lldp-reserved-power: Max. port power determined by LLDP Media protocol, and power is managed according to reserved power.

To negate the command, use the “no poe management mode” in port intreface configuration interface.

【Configuration Example】

(config)# poe management mode allocation-consumption

MAC Table Configuration

Setting MAC Table Aging

The following section will guide you to set MAC table aging function. By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

Step 1	config terminal	Enter global configuration mode.
Step 2	mac address-table aging-time <Aging_Time>	Set the MAC address table aging time. If you want to disable MAC aging function, put “0” in <Aging_Time>.

To negate the command, use the “no mac address-table aging-time” in global configuration interface.

【Configuration Example】

(config)# mac address-table aging-time 500

Enable/Disable MAC Address Learning

The following section will guide you to enable/disable MAC address learning in specific ports.

Step 1	config terminal	Enter global configuration mode.
Step 2	interface GigabitEthernet <Switch_No/Port>	Enter the port configuration interface. For example, if you would like to enter port 1~4’s port configuration interface, type in “interface GigabitEthernet 1/1-4”.
Step 3	no mac address-table learning	Disable MAC address learning in these ports.
Step 4	mac address-table learning	Enable MAC address learning in these ports.
Step 5	mac address-table learning secure	Set MAC learning as “secure”. Only static MAC entries are learned, all other frames are dropped.

【Configuration Example】

(config)# interface GigabitEthernet 1/1-4
(config-if)# no mac address-table learning
(config-if)# mac address-table learning
(config-if)# mac address-table learning secure

Setting Static MAC Table

The following section will guide you to set static MAC table.

Step 1	config terminal	Enter global configuration mode.
Step 2	mac address-table static <MAC_Address> vlan <VALN_ID> interface GigabitEthernet < Port_No>	Set static MAC table entry.

To negate the command, use the “no mac address-table static <MAC_Address> vlan <VALN_ID> interface GigabitEthernet < Port_No>” in global configuration interface.

【Configuration Example】

(config)# mac address-table static 00:01:cc:cc:cc:cc vlan 1 interface GigabitEthernet 1/1-4

Voice VLAN

Voice VLAN Global Setting

The following section will guide you to make Voice VLAN global settings. The settings done here will be applied to global voice VLAN environment.

By creating Voice VLAN group and adding full-management switch's ports that are connected to VoIP (Voice over IP) devices (such as VoIP phones) to the Voice VLAN group you created, all packets related to voice streaming will be transmitted within the Voice VLAN group, therefore providing QoS (Quality of Service) function that prioritizes voice streaming packets and ensures the quality of VoIP phone communications.

Step 1	config terminal	Enter global configuration mode.
Step 2	voice vlan	Enable voice VLAN function.
Step 3	voice vlan vid <VLAN_ID>	Set the VLAN ID of the VoIP phone. Please note that the VLAN ID you set here must be the same with the VLAN ID of your VoIP device.
Step 4	voice vlan oui <OUI_Valne> description <Device_Description>	The switch identifies VoIP devices via their OUI (Organizationally Unique Identifier). You can input your device's OUI and add a description of that device with this command.

To negate the command, use the "no voice vlan" in global configuration interface.

【Configuration Example】

(config)# voice vlan
(config)# voice vlan vid 1200
(config)# voice vlan oui 00:cc:bb description VoIP

Voice VLAN Port Setting

The following section will guide you to make Voice VLAN settings for each port. The settings done here will be applied only to specific ports.

Step 1	config terminal	Enter global configuration mode.
Step 2	interface GigabitEthernet <Switch_No/Port>	Enter the port configuration interface. For example, if you would like to enter port 1~4's port configuration interface, type in "interface GigabitEthernet 1/1-4".
Step 3	switchport voice vlan mode <auto/disable /force>	Set the voice VLAN mode. • auto: Enable auto detect mode • disable: disjoin Voice VLAN • force: Force to join Voice VLAN
Step 4	switchport voice vlan discovery-protocol <both/lldp/oui>	Set the voice VLAN discovery protocol. • both: Detect telephony device by OUI address and LLDP • lldp: Detect telephony device by LLDP • oui: Detect telephony device by OUI address
Step 5	switchport voice vlan security	Enable Voice VLAN security mode.

To negate the command, use the "no voice vlan" in global configuration interface.

【Configuration Example】

(config)# interface GigabitEthernet 1/1-4
(config-if)# switchport voice vlan security
(config-if)# switchport voice vlan mode auto
(config-if)# switchport voice vlan discovery-protocol both

IGMP Snooping

IGMP Snooping Setting

The following section will guide you to make IGMP snooping settings.

IGMP is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

Step 1	config terminal	Enter global configuration mode.
Step 2	ip igmp snooping	Enable IGMP snooping function.
Step 3	ip igmp snooping vid <VLAN_ID>	Set the VLAN ID of the IGMP snooping.
Step 4	no ip igmp unknown-flooding	Disable the Unregistered IPMCv4 Flooding function.
Step 5	interface vlan vid <VLAN_ID>	Enter the IGMP VLAN's configuration interface.
Step 6	ip igmp snooping	Enable IGMP VLAN's IGMP snooping function.

【Configuration Example】

(config)# ip igmp snooping
(config)# ip igmp snooping vlan 1
(config)# no ip igmp unknown-flooding
(config)# interface vlan 1
(config-if-vlan)# ip igmp snooping

UPnP

UPnP Global Setting

The following section will guide you to set UPnP.

UPnP is an acronym for Universal Plug and Play. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components.

Step 1	config terminal	Enter global configuration mode.
Step 2	interface GigabitEthernet <Switch_No/Port>	Enter the port configuration interface. For example, if you would like to enter port 1~4's port configuration interface, type in "interface GigabitEthernet 1/1-4".
Step 3	sflow	Enable sFlow function on these ports.
Step 4	sflow counter-poll-interval <Connter_Poller_Interval>	With counter polling enabled, this specifies the interval - in seconds - between counter poller samples. Valid range is 1 to 3600 seconds.
Step 5	sflow max-sampling-size <Max_Sampling_Size>	Set Max Sampling Size, the maximum number of bytes that should be copied from a sampled packet to the sFlow datagram.
Step 6	sflow sampling-rate <sFlow_Sampling_Rate>	The statistical sampling rate for packet sampling.

To negate the command, use the "no sflow" in global configuration interface.

【Configuration Example】

(config)# sflow agent-ip ipv4 192.168.2.66
(config)# sflow collector-address 192.168.2.200
(config)# sflow collector-port 5000
(config)# sflow max-datagram-size 200
(config)# sflow timeout 70

UPnP Port Setting

The following section will guide you to set UPnP.

Step 1	config terminal	Enter global configuration mode.
Step 2	sflow agent-ip <ipv4/ipv6> <IP_Address>	Set sFlow agent IP address. It serves as a unique key that will identify this agent over extended periods of time.
Step 3	sflow collector-address <domain_name> <ipv4_addr> <ipv6_ucast>	Set sFlow receiver. You can set the receiver with domain name, IPv4 or IPv6 addresses.
Step 4	sflow collector-port <UDP_Port>	Set sFlow receiver UDP port number.
Step 5	sflow max-datagram-size <Datagram_Size>	The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes.
Step 6	sflow timeout <Timeout_Time>	The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings. Valid range is 0 to 2147483647 seconds.

【Configuration Example】

(config)# interface GigabitEthernet 1/1-4
(config-if)# sflow counter-poll-interval 180
(config-if)# sflow max-sampling-size 200
(config-if)# sflow sampling-rate 50000

UDLD

UDLD Setting

The following section will guide you to set UDLD.

UDLD is an acronym for Uni Directional Link Detection. UDLD protocol monitors the physical configuration of the links between devices and ports that support UDLD. It detects the existence of unidirectional links.Its functionality is to provide mechanisms useful for detecting one way connections before they create a loop or other protocol malfunction. RFC 5171 specifies a way at data link layer to detect Uni directional link.

Step 1	config terminal	Enter global configuration mode.
Step 2	udld enable	Enable UDLD function globally (all ports) and set them to “Normal” mode. In normal mode, if the link state of the port was determined to be unidirectional, it will not affect the port state.
Step 3	udld aggressive	Set all ports to “Aggressive” mode. In aggressive mode, unidirectional detected ports will get shutdown.
Step 4	udld message time-interval <Message_Interval>	Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional.

To negate the command, use the “no udld enable” in global configuration interface.

【Configuration Example】

(config)# udld enable
(config)# udld message time-interval 80

Diagnostic Tool

Ping (IPv4 or IPv6)

The following section will guide you to use the switch's diagnostic tool Ping.

Ping is a tool that allows you to determine if a device is connected to the switch. You can ping IPv4/IPv6 address or network domain name.

Step 1	ping <ipv4/ipv6> <IP_Address /Domain_Name>	Ping the device with the set IP address or domain name.

【Configuration Example】

```
# ping ip 192.168.2.33
PING server 192.168.2.33, 56 bytes of data.
64 bytes from 192.168.2.33: icmp_seq=0, time=10ms
64 bytes from 192.168.2.33: icmp_seq=1, time=0ms
64 bytes from 192.168.2.33: icmp_seq=2, time=0ms
64 bytes from 192.168.2.33: icmp_seq=3, time=0ms
64 bytes from 192.168.2.33: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

VeriPHY

The following section will guide you to use the switch's diagnostic tool VeriPHY.

While running, VeriPHY will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 - 140 meters.

10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

Step 1	veriphy interface <Port_Interface>	Perform VeriPHY on the switch ports. If no other parameter is given, the switch will perform VeriPHY on all switch ports.

【Configuration Example】

```
# veriphy interface GigabitEthernet 1/1-3
Starting VeriPHY - Please wait
Interface            Pair A  Length  Pair B, Length  Pair C  Length  Pair D  Length
-------------------- ------ ------ -------------- ------ ------ ------ -------
GigabitEthernet 1/1  Open   0      Open   0       Open   0      Open   0
GigabitEthernet 1/2  Open   0      Open   0       OK     189    Open   0
GigabitEthernet 1/3  Open   0      Open   0       Open   0      Open   0
```

System Maintenance

Reboot Device

The following section will guide you to reboot the switch.

Please note that if you did not save any previously-made configurations before reboot the switch, all settings you've made will be lost.

Step 1	reload cold	Reboot the switch

【Configuration Example】

reload cold
% Cold reload in progress, please stand by.

Reload Factory Default Value

The following section will guide you to reload switch's default value.

All settings will be reset back to factory value. You can use the "keep-id" parameter to keep the original IP address of the switch.

Step 1	reload default <keep-id>	Reset all settings back to factory default value. The "keep-id" parameter allows you to keep the switch's original IP address.

【Configuration Example】

reload default
% Reloading defaults. Please stand by.
#

Upgrading Firmware

The following section will guide you to upgrade the switch's firmware.

Before upgrading the switch's firmware, a TFTP server is needed. The firmware file must be in the TFTP server.

Step 1	firmware upgrade <File_Path>	Upgrading the firmware in the <File_Path>. The <File_Path> must be in this format: tftp://IP_Address_of_TFTP_Server/Firmware_Name

【Configuration Example】

```
# firmware upgrade tftp://192.168.2.33/firmware.dat
Downloaded "/firmware.dat", 5063354 bytes
Waiting for firmware update to complete
Starting flash update - do not power off device!
Erasing image...
Programming image...
... Erase from 0x40ff0000-0x40ffffff: .
... Program from 0x87fef000-0x87fff000 to 0x40ff0000: .
... Program from 0x87fef00a-0x87fef00c to 0x40ff000a: .
Flash update succeeded.
Rebooting system...+M25PXX : Init device with JEDEC ID 0xC22018.
```

Swapping Firmware

The following section will guide you to swap the firmware of the switch. This switch can contain 2 firmwares and you can swap them with this command.

Step 1	firmware swap	Swap firmware to the other in-active firmware.

【Configuration Example】

```
# firmware swap
... Erase from 0x40fd0000-0x40fdffff: .
... Program from 0x87fef000-0x87fff000 to 0x40fd0000: .
... Program from 0x87fef00a-0x87fef00c to 0x40fd000a: .
Alternate image activated, now rebooting.
```

Save Current Running Configuration

The following section will guide you to save the current running configuration to the start-up configuration file.

The switch contains 3 different configuration files:

- Start-up Configuration: The configuration that will be loaded into the switch when the switch is booting.
- Running Configuration: The configuration that the switch is currently running.
- Default Configuration: The default configuration of the switch. This configuration file is read-only.

If you made any setting to the switch without saving the Running Configuration to Start-up Configuration, all the settings will be lost if you reboot the switch.

Step 1	copy running-config startup-config	Saving the current running configuration to the start-up configuration.

【Configuration Example】

copy running-config startup-config
Building configuration...
% Saving 1195 bytes to flash:startup-config

Download Configuration File to PC

The following section will guide you to save configuration file to your TFTP server.

The switch contains 3 different configuration files:

- Start-up Configuration: The configuration that will be loaded into the switch when the switch is booting.
- Running Configuration: The configuration that the switch is currently running.
- Default Configuration: The default configuration of the switch. This configuration file is read-only.

You can save Start-up Configuration and Running Configuration to your TFTP Server.

Before saving switch's configuration file, a TFTP server is needed.

Step 1	copy <running-config/startup-config> <File_Path>	Saving the current running or start-up configuration to the TFTP server. The <File_Path> must be in this format: tftp://IP_Address_of_TFTP_Server/Configuration_File_Name

【Configuration Example】

copy running-config tftp://192.168.2.33/Running
Building configuration...
% Saving 1195 bytes to TFTP server 192.168.2.33: /Running

Uploading Configuration File from PC to Switch

The following section will guide you to upload previous saved configuration file to the switch.

Before uploading switch's configuration file, a TFTP server is needed.

Step 1	copy <File_Path> <running-config/startup-config>	Upload configuration file from TFTP server to switch. The <File_Path> must be in this format: tftp://IP_Address_of_TFTP_Server/Configuration_File_Name

【Configuration Example】

```
# copy tftp://192.168.2.33/Running startup-config
% Loading /Running from TFTP server 192.168.2.33
% Saving 1195 bytes to flash:startup-config
```

Configuring 802.1X Authentication

Enable 802.1X Authentication

To enable 802.1X port-based authentication, you must enable AAA and specify the authentication method list. A method list describes the sequence and authentication methods to be queried to authenticate a user. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle, the authentication process stops, and no other authentication methods are attempted.

Beginning in privileged EXEC mode, follow these steps to configure the RADIUS server parameters onthe switch. This procedure is required.

Step 1	config terminal	Enter global configuration mode.
Step 2	access management<access_id><access_vid><start_addr> [to <end_addr>] { [web] [snmp] [telnet] | all }	Enable AAA for specified vlan and IP range, service type can be selected.
Step 3	aaa authentication login{ console | telnet | ssh | http } { { local | radius | tacacs } [{ local | radius | tacacs } [{ local | radius | tacacs }]] }	Set the client login type and the authentication methods by priority1~3

To negate the command, use the no aaa authentication login{console | telnet | ssh | http } global configuration command.

【Configuration Example】

<config># access management
<config># access management 1 418 192.168.2.1 all
<config># aaa authentication login telnet radius
<config># no aaa authentication login http

Identifying the RADIUS Server Host

RADIUS security servers are identified by their host name or IP address, host name and specific UDP port numbers, or IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, which enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service— for example, authentication— the second host entry configured acts as the fail-over backup to the first one. The RADIUS host entries are tried in the order that they were configured.

A RADIUS server and the switch use a shared secret text string to encrypt passwords and exchange responses. To configure RADIUS to use the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text (key) string that it shares with the switch. The timeout, retransmission, and encryption key values can be configured globally for all RADIUS servers, on a per-server basis, or in some combination of global and per-server settings. To apply these settings globally to all RADIUS servers communicating with the switch, use the three unique global configuration commands: radius-server timeout, radius-server re-transmit, and radius-server key. To apply these values on a specific RADIUS server, use the radius-server host global configuration command.

Beginning in privileged EXEC mode, follow these steps to configure the RADIUS server parameters on the switch. This procedure is required.

Step 1	config terminal	Enter global configuration mode.
Step 2	radius-server host <host_name> [auth-port <auth_port>] [acct-port <acct_port>] [timeout <seconds>] [retransmit <retries>] [key <key>]	Specify the IP address or host name of the remote RADIUS server host. • (Optional) For auth-port port-number, specify the UDP destination port for authentication requests. • (Optional) For acct-port port-number, specify the UDP destination port for accounting requests. • (Optional) For timeout seconds, specify the time interval that the switch waits for the RADIUS server to reply before retransmitting. The range is 1 to 1000. This setting overrides the radius-server timeout global configuration command setting. If no timeout is set with the radius-server host, the setting of the radius-server timeout global configuration command is used. • (Optional) For retransmit retries, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the radius-server host command, the setting of the radius-server retransmit global configuration command is used. • (Optional) For key string, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server. **Note:** Always configure the key as the last item in the radius-server host command syntax because leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks are part of the key. This key must match the encryption used on the RADIUS daemon. To configure the switch to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that

	each UDP port number is different. The switch software searches for hosts in the order in which you specify them. Set the timeout,retransmit, and encryption key values to use with the specific RADIUShost.

To delete the specified RADIUS server, use the no radius-server host {hostname | ip-address } global configuration command.

【Configuration Example】

<config># radius-server host 192.168.2.173 timeout 5 retransmit 2 key testing123

<config>#no radius-server host 192.168.2.173

Identifying the TACACS+ Server Host and Setting the Authentication Key

You can configure the switch to use a single server or AAA server groups to group existing server hosts for authentication. You can group servers to select a subset of the configured server hosts and use themfor a particular service. The server group is used with a global server-host list and contains the list of IPaddresses of the selected server hosts.

Beginning in privileged EXEC mode, follow these steps to identify the IP host or host maintaining TACACS+ server and optionally set the encryption key:

Step 1	config terminal	Enter global configuration mode.
Step 2	tacacs-server host <host_name> [port <port>] [timeout <seconds>] [key <key>]	Identify the IP host or hosts maintaining a TACACS+ server. Enter thiscommand multiple times to create a list of preferred hosts. The softwaresearches for hosts in the order in which you specify them. • For hostname , specify the name or IP address of the host. • (Optional) For port integer , specify a server port number. The defaultis port 49. The range is 1 to 65535. • (Optional) For timeout integer , specify a time in seconds the switchwaits for a response from the daemon before ittimes out and declaresan error. The default is 5 seconds. The range is 1 to 1000 seconds. • (Optional) For key string , specify the encryption key for encryptingand decrypting all traffic between the switch and the TACACS+daemon. You must configure the same

To delete the specified TACACS+ server, use the no tacacs-server host {hostname | ip-address } globalconfiguration command.

【Configuration Example】

<config># tacacs-server host 192.168.2.175 port 655 timeout 5 key testing456
<config>#no tacacs-server host 192.168.2.175

Configuring RADIUS Authorization for User Privileged Access and Network Services

AAA authorization limits the services available to a user. When AAA authorization is enabled, the switch uses information retrieved from the user's profile, which is in the local user database or on the security server, to configure the user's session. The user is granted access to a requested service only if the information in the user profile allows it.

You can use the aaa authentication global configuration command with the radius keyword to set parameters that restrict a user's network access to privileged EXEC mode.

The aaa authentication exec radius local command sets these authorization parameters:

- Use RADIUS for privileged EXEC access authorization if authentication was performed by using RADIUS.
- Use the local database if authentication was not performed by using RADIUS.

Step 1	config terminal	Enter global configuration mode.
Step 2	aaa authentication login console local	Configure the switch for user local authorization for all network-related service requests.

To disable authorization, use the no aaa authentication login {console | telnet | ssh | http} command

【Configuration Example】

<config># aaa authentication login console radius
<config># aaa authentication login http tacacs

Configuring MSTP

Specifying the MST Region Configuration and Enabling MSTP

For two or more switches to be in the same MST region, they must have the same VLAN-to-instance mapping, the same configuration revision number, and the same name.

A region can have one member or multiple members with the same MST configuration; each member must be capable of processing RSTP BPDUs. There is no limit to the number of MST regions in a network, but each region can support up to 16 spanning-tree instances. You can assign a VLAN to only one spanning-tree instance at a time.

Beginning in privileged EXEC mode, follow these steps to specify the MST region configuration and enable MSTP. This procedure is required.

Step 1	config terminal	Enter global configuration mode.
Step 2	spanning-tree mst <instance-id> vlan <vlan-range>	Map VLANs to an MST instance. • For instance-id, the range is 1 to 15. • For vlan vlan-range, the range is 1 to 4094. When you map VLANs to an MST instance, the mapping is incremental, and the range of VLANs specified is added or removed to the existing ones. To specify a range, use a hyphen; for example, instance 1 vlan 1-63 maps VLANs 1 through 63 to MST instance 1. To specify a series, use a comma; for example, instance 1 vlan 10, 20, 30 maps VLANs 10, 20, and 30 to MST instance 1.
Step3	spanning-tree mst name <Name>	Specify the configuration name. The name string has a maximum length of 32 characters and is case sensitive.
Step 4	spanning-tree mst name <Name> revision <Revision_Version>	Specify the configuration revision number. The range is 0 to 65535.

To return to the default MST region configuration, use the no spanning-tree mst command.

【Configuration Example】

<config># spanning-tree mst 1 vlan 1-2
<config># spanning-tree mst name TEST123 revision 12

Configuring the Root Switch

The switch maintains a spanning-tree instance for the group of VLANs mapped to it. A bridge ID, consisting of the switch priority and the switch MAC address, is associated with each instance. The switch with the lowest bridge ID becomes the root switch for the group of VLANs.

To configure a switch to become the root, use the “spanning-tree mst <instance-id> priority 4096” global configuration command to modify the switch priority from the default value to the lowest value so that the switch becomes the root switch for the specified spanning-tree instance. When you enter this command, the switch checks the switch priorities of the root switches.

Step 1	config terminal	Enter global configuration mode.
Step 2	spanning-tree mst <instance-id> priority 4096	Configure a switch to become the root for the specified VLAN.

To return to the default MST region configuration, use the no spanning-tree mst command.

【Configuration Example】

<config># spanning-tree mst 1 priority 4096

Configuring the Secondary Switch

The switch maintains a spanning-tree instance for the group of VLANs mapped to it. A bridge ID, consisting of the switch priority and the switch MAC address, is associated with each instance. The switch with the lowest bridge ID becomes the root switch for the group of VLANs, and the switch with the second lowest bridge ID becomes the secondary root switch for the group of VLANs.

To configure a switch to become the root, use the “spanning-tree mst <instance-id> priority 8192” global configuration command to modify the switch priority from the default value to the second lowest value so that the switch becomes the secondary root switch for the specified spanning-tree instance. When you enter this command, the switch checks the switch priorities of the root switches.

Step 1	config terminal	Enter global configuration mode.
Step 2	spanning-tree mst <instance-id> priority 8192	Configure a switch to become the secondary root for the specified VLAN.

To return to the default MST region configuration, use the no spanning-tree mst command.

【Configuration Example】

<config># spanning-tree mst 1 priority 8192

Configuring the Port Priority

If a loop occurs, spanning tree uses the port priority when selecting an interface to put into the forwarding state. You can assign higher priority values (lower numerical values) to interfaces that you want selected first and lower priority values (higher numerical values) that you want selected last. If all interfaces have the same priority value, spanning tree puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

Step 1	config terminal	Enter global configuration mode.
Step 2	interface <*/ GigabitEthernet/vlan>	Enter interface configuration mode. • *: All switches or All ports • GigabitEthernet: Enter Gigabit Ethernet Port configuration mode, the port number or port numbters of the switch. • vlan: Enter VLAN configuration mode.
Step 3	spanning-tree mst <instance-id> port-priority <Port_priority>	Configure a port/VLAN to a certain priority. The priority value is a value from 0 to 240.

To return to the default MST region configuration, use the no spanning-tree mst command.

【Configuration Example】

<config># interface *
(config-if)# spanning-tree mst 2 port-priority 1

Configuring the Path Cost

The spanning-tree path cost default value is derived from the media speed of an interface. If a loop occurs, spanning tree uses cost when selecting an interface to put in the forwarding state. You can assign lower cost values to interfaces that you want selected first and higher cost values that you want selected last. If all interfaces have the same cost value, spanning tree puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

Spanning tree uses the cost value when the interface is configured as an access port and uses VLAN port cost values when the interface is configured as a trunk port.

Step 1	config terminal	Enter global configuration mode.
Step 2	interface <*/ GigabitEthernet/vlan>	Enter interface configuration mode. • *: All switches or All ports • GigabitEthernet: Enter Gigabit Ethernet Port configuration mode, the port number or port numbters of the switch. • vlan: Enter VLAN configuration mode.
Step 3	spanning-tree mst <instance-id> cost <Path_cost>	Configure the cost for an interface. If a loop occurs, spanning tree uses the path cost when selecting an interface to place into the forwarding state. A lower path cost represents higher-speed transmission.

To return to the default MST region configuration, use the no spanning-tree mst command.

【Configuration Example】

<config># interface *
(config-if)# spanning-tree mst 2 cost 1

Configuring the Switch Priority of a VLAN

You can configure the switch priority and make it more likely that the switch will be chosen as the root switch.

Step 1	config terminal	Enter global configuration mode.
Step 2	spanning-tree mst <instance-id> priority <Priority_Value>	Configure a MST instance to a set value of priority.
Step 3	spanning-tree mst <instance-id> vlan <VLAN_ID>	Map the MST instance to a VLAN.

To return to the default MST region configuration, use the no spanning-tree mst command.

【Configuration Example】

<config># spanning-tree mst 2 priority 57344
<config># spanning-tree mst 2 vlan 2

Enabling BPDU Guard

The BPDU guard feature can be globally enabled on the switch or can be enabled per interface, but the feature operates with some differences.

This command prevents ports that are in a Port Fast-operational state from sending or receiving BPDUs. The ports still send a few BPDUs at link-up before the switch begins to filter outbound BPDUs. You should globally enable BPDU filtering on a switch so that hosts connected to these ports do not receive BPDUs. If a BPDU is received on a Port Fast-enabled port, the port loses its Port Fast-operational status, and BPDU filtering is disabled.

Step 1	config terminal	Enter global configuration mode.
Step 2	spanning-tree aggregation	Enter spanning tree aggregation configuration mode.
Step 3	spanning-tree bpdu-guard	Enable spanning tree BPDU guard function.

To return to the default MST region configuration, use the no spanning-tree mst command.

【Configuration Example】

(config)# spanning-tree aggregation
(config-stp-aggr)# spanning-tree bpdu-guard

Configuring VLANs

Creating or Modifying an Ethernet VLAN

Each Ethernet VLAN in the VLAN database has a unique, 4-digit ID that can be a number from 1 to 4095. To create a VLAN to be added to the VLAN database, assign a number and name to the VLAN. The following guide will guide you to set access VLAN.

Step 1	config terminal	Enter global configuration mode.
Step 2	interface GigabitEthernet <port_type_list>	Enter port configuration mode. “port_type_list” parameter is in the format of switch_number/port_number. For example, 1/20-24 means port 20~24 of switch 1.
Step3	switchport access vlan <vlan_id>	Set the ports to a port VLAN.

To return to the default VLAN configuration, use the “no switchport access vlan” command in port configuration mode.

【Configuration Example】

configure terminal
(config)# interface GigabitEthernet 1/20-24
(config-if)# switchport access vlan 2

Configure VLAN IP Interface

This switch allows different IP interfaces among different VLANs, which means the configuration web pages can be accessed via different IP addresses in different VLANs.

Step 1	config terminal	Enter global configuration mode.
Step 2	interface vlan <VLAN_ID>	Enter VLAN configuration mode. <VLAN_ID> can be an integer from 1 to 4095
Step3	ip address 192.168.3.1 255.255.255.0	Mapping these ports to a specific MAC address and a specific VLAN ID.

To return to the default VLAN configuration, use the “no switchport vlan mac <mac_ucast> vlan <vlan_id>” command in port configuration mode.

【Configuration Example】

configure terminal
(config)# interface GigabitEthernet 1/20-24
(config-if)# switchport vlan mac 00:01:0c:aa:bb:a9 vlan 2

Configuring SNMP

Disabling the SNMP Agent

SNMP is an application-layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of an SNMP manager, an SNMP agent, and a management information base (MIB). The SNMP manager can be part of a network management system. The agent and MIB reside on the switch. To configure SNMP on the switch, you define the relationship between the manager and the agent.

The SNMP agent contains MIB variables whose values the SNMP manager can request or change. A manager can get a value from an agent or store a value into the agent. The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to a manager's requests to get or set data.

An agent can send unsolicited traps to the manager. Traps are messages alerting the SNMP manager to a condition on the network. Traps can mean improper user authentication, restarts, link status (up or down), MAC address tracking, closing of a TCP connection, loss of connection to a neighbor, or other significant events.

Step 1	config terminal	Enter global configuration mode.
Step 2	no snmp-server	By default, SNMP function is enabled. The "no snmp-server" command can disable SNMP function.

To return to the default VLAN configuration, use the "snmp-server" command in global configuration mode.

【Configuration Example】

configure terminal
(config)# no snmp-server
(config)# snmp-server

Configuring Community Strings

SNMP community strings authenticate access to MIB objects and function as embedded passwords. In order for the NMS to access the switch, the community string definitions on the NMS must match at least one of the three community string definitions on the switch.

A community string can have one of these attributes:

- Read-only (RO)—Gives read access to authorized management stations to all objects in the MIB except the community strings, but does not allow write access
- Read-write (RW)—Gives read and write access to authorized management stations to all objects in the MIB, but does not allow access to the community strings
- Read-write-all—Gives read and write access to authorized management stations to all objects in the MIB, including the community strings

Step 1	config terminal	Enter global configuration mode.
Step 2	snmp-server community v2c <Community_Name> <ro/rw>	Set SNMP version to V2C, and set a read-only or read-write community with the community name of <Community_Name>.

To return to the default VLAN configuration, use the “no snmp-server community v2c <Community_Name> <ro/rw>” command in global configuration mode.

【Configuration Example】

configure terminal
(config)# snmp-server community v2c SNMPTEST rw

Configuring ACLs

Creating a Numbered Standard ACL

Packet filtering can limit network traffic and restrict network use by certain users or devices. ACLs can filter traffic as it passes through a switch and permit or deny packets at specified interfaces. An ACL is a sequential collection of permit and deny conditions that apply to packets. When a packet is received on an interface, the switch compares the fields in the packet against any applied ACLs to verify that the packet has the required permissions to be forwarded, based on the criteria specified in the access lists. The switch tests the packet against the conditions in an access list one by one. The first match determines whether the switch accepts or rejects the packet. Because the switch stops testing conditions after the first match, the order of conditions in the list is critical. If no conditions match, the switch rejects the packet. If there are no restrictions, the switch forwards the packet; otherwise, the switch drops the packet.

You configure access lists on a Layer 2 switch to provide basic security for your network. If you do not configure ACLs, all packets passing through the switch could be allowed onto all parts of the network. You can use ACLs to control which hosts can access different parts of a network or to decide which types of traffic are forwarded or blocked at switch interfaces. For example, you can allow e-mail traffic to be forwarded but not Telnet traffic. ACLs can be configured to block inbound traffic.

An ACL contains an ordered list of access control entries (ACEs). Each ACE specifies permit or deny and a set of conditions the packet must satisfy in order to match the ACE. The meaning of permit or deny depends on the context in which the ACL is used.

The switch supports these types of ACLs on physical interfaces in the inbound direction:

- IP ACLs filter IP, TCP, and UDP traffic.
- Ethernet or MAC ACLs filter Layer 2 traffic.
- MAC extended access lists use source and destination MAC addresses and optional protocol type information for matching operations.
- Standard IP access lists use source addresses for matching operations.
- Extended IP access lists use source and destination addresses and optional protocol type information for matching operations.

The switch examines access lists associated with features configured on a given interface. As packets enter the switch on an interface, ACLs associated with all inbound features configured on that interface are examined.

Beginning in privileged EXEC mode, follow these steps to create a numbered standard IP ACL:

Step 1	config terminal	Enter global configuration mode.
Step 2	access-list ace <Ace_ID : 1-256> action <deny | filter | permit> frame-type <frame_type> sip <source_IP/subnet>	Define a standard IP ACL by using a source address. Enter deny or permit to specify whether to deny or permit access if conditions are matched. The source is the source address of the network or host from which the packet is being sent.

To return to the default VLAN configuration, use the “no access-list ace <AceId : 1-256> action <deny | filter | permit> frame-type <frame_type> sip <source_IP/subnet>” command in global configuration mode.

【Configuration Example】

configure terminal
(config)# no snmp-server
(config)# access-list ace 12 action permit frame-type ipv4 sip 0.0.0.0/24

Creating a Numbered Extended ACL

Although standard ACLs use only source addresses for matching, you can use an extended ACL source and destination addresses for matching operations and optional protocol type information for finer granularity of control. Some protocols also have specific parameters and keywords that apply to that protocol.

These IP protocols are supported on physical interfaces (protocol keywords are in parentheses in bold): Internet Protocol (ip), Transmission Control Protocol (tcp), or User Datagram Protocol (udp).

Step 1	config terminal	Enter global configuration mode.
Step 2	access-list ace < Ace_ID : 1-256> action <deny | filter | permit> frame-type ipv4-tcp dip <Destination_IP/Subnet> sip <Source_IP/Subnet>	Define a standard IP ACL by using a source and a destination. Enter deny or permit to specify whether to deny or permit access if conditions are matched. The source is the source address of the network or host from which the packet is being sent, and the destination is the destination address of the network.

To return to the default VLAN configuration, use the “no access-list ace < Ace_ID : 1-256> action <deny | filter | permit> frame-type ipv4-tcp dip <Destination_IP/Subnet> sip <Source_IP/Subnet>” command in global configuration mode.

【Configuration Example】

configure terminal

(config)# access-list ace 20 action permit frame-type ipv4-tcp dip 192.168.2.30/24 sip 192.168.2.20/24

Creating Named Standard and Extended ACLs

You can identify IP ACLs with an alphanumeric string (a name) rather than a number. You can use named ACLs to configure more IP access lists on a switch than if you use numbered access lists. If you identify your access list with a name rather than a number, the mode and command syntax are slightly different. However, not all commands that use IP access lists accept a named ACL.

Step 1	config terminal	Enter global configuration mode.
Step 2	access-list ace < Ace_ID : 1-256> action <deny | filter | permit> frame-type ipv4-tcp dip <Destination_IP/Subnet> sip <Source_IP/Subnet>	Define a standard IP ACL by using a source and a destination. Enter deny or permit to specify whether to deny or permit access if conditions are matched. The source is the source address of the network or host from which the packet is being sent, and the destination is the destination address of the network.

To return to the default VLAN configuration, use the “no access-list ace < Ace_ID : 1-256> action <deny | filter | permit> frame-type ipv4-tcp dip <Destination_IP/Subnet> sip <Source_IP/Subnet>” command in global configuration mode.

【Configuration Example】

configure terminal

(config)# access-list ace 20 action permit frame-type ipv4-tcp dip 192.168.2.30/24 sip 192.168.2.20/24

CLI Command Reference
The following section is a reference with all the CLI commands.

Command

aaa

Command Syntex

aaa authentication login { console | telnet | ssh | http } { { local | radius | tacacs } [{ local | radius | tacacs } [{ local | radius | tacacs }]] }

Function Description

aaa: Authentication, Authorization and Accounting

Parameter Description

authentication: Authentication
login: Login
console: Configure Console
telnet: Configure Telnet
ssh: Configure SSH
http: Configure HTTP
local: Use local database for authentication
radius: Use RADIUS for authentication
tacacs: Use TACACS+ for authentication
local: Use local database for authentication
radius: Use RADIUS for authentication
tacacs: Use TACACS+ for authentication
local: Use local database for authentication
radius: Use RADIUS for authentication
tacacs: Use TACACS+ for authentication

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

access

Command Syntex

access management <access_id> <access_vid> <start_addr> [to <end_addr>] { [web] [snmp] [telnet] | all }

Function Description

access: Access management

Parameter Description

management: Access management configuration
<access_id>: ID of access management entry
<access_vid>: The VLAN ID for the access management entry
<start_addr>: Start IPv4/IPv6 address
to: End address of the range
<end_addr>: End IPv4/IPv6 address
web: Web service
snmp: SNMP service
telnet: TELNET/SSH service
all: All services

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

access-list ace

Command Syntex

access-list ace [update] <ace_id> [next { <ace_id_next> | last }] [ingress { switch <ingress_switch_id> | switchport { <ingress_switch_port_id> | <ingress_switch_port_list> } | interface { <port_type> <ingress_port_id> | <port_type> [<ingress_port_list>] } | any }] [policy <policy> [policy-bitmask <policy_bitmask>]] [tag { tagged | untagged | any }] [vid { <vid> | any }] [tag-priority { <tag_priority> | 0-1 | 2-3 | 4-5 | 6-7 | 0-3 | 4-7 | any }] [dmac-type { unicast | multicast | broadcast | any }] [frame-type { any | etype [etype-value { <etype_value> | any }] [smac { <etype_smac> | any }] [dmac { <etype_dmac> | any }] | arp [sip { <arp_sip> | any }] [dip { <arp_dip> | any }] [smac { <arp_smac> | any }] [arp-opcode { arp | rarp | other | any }] [arp-flag [arp-request { <arp_flag_request> | any }] [arp-smac { <arp_flag_smac> | any }] [arp-tmac { <arp_flag_tmac> | any }] [arp-len { <arp_flag_len> | any }] [arp-ip { <arp_flag_ip> | any }] [arp-ether { <arp_flag_ether> | any }]] | ipv4 [sip { <sipv4> | any }] [dip { <dipv4> | any }] [ip-protocol { <ipv4_protocol> | any }] [ip-flag [ip-ttl { <ip_flag_ttl> | any }] [ip-options { <ip_flag_options> | any }] [ip-fragment { <ip_flag_fragment> | any }]] | ipv4-icmp [sip { <sipv4_icmp> | any }] [dip { <dipv4_icmp> | any }] [icmp-type { <icmpv4_type> | any }] [icmp-code { <icmpv4_code> | any }] [ip-flag [ip-ttl { <ip_flag_icmp_ttl> | any }] [ip-options { <ip_flag_icmp_options> | any }] [ip-fragment { <ip_flag_icmp_fragment> | any }]] | ipv4-udp [sip { <sipv4_udp> | any }] [dip { <dipv4_udp> | any }] [sport { <sportv4_udp_start> [to <sportv4_udp_end>] | any }] [dport { <dportv4_udp_start> [to <dportv4_udp_end>] | any }] [ip-flag [ip-ttl { <ip_flag_udp_ttl> | any }] [ip-options { <ip_flag_udp_options> | any }] [ip-fragment { <ip_flag_udp_fragment> | any }]] | ipv4-tcp [sip { <sipv4_tcp> | any }] [dip { <dipv4_tcp> | any }] [sport { <sportv4_tcp_start> [to <sportv4_tcp_end>] | any }] [dport { <dportv4_tcp_start> [to <dportv4_tcp_end>] | any }] [ip-flag [ip-ttl { <ip_flag_tcp_ttl> | any }] [ip-options { <ip_flag_tcp_options> | any }] [ip-fragment { <ip_flag_tcp_fragment> | any }]] [tcp-flag [tcp-fin { <tcpv4_flag_fin> | any }] [tcp-syn { <tcpv4_flag_syn> | any }] [tcp-rst { <tcpv4_flag_rst> | any }] [tcp-psh { <tcpv4_flag_psh> | any }] [tcp-ack { <tcpv4_flag_ack> | any }] [tcp-urg { <tcpv4_flag_urg> | any }]] | ipv6 [next-header { <next_header> | any }] [sip { <sipv6> [sip-bitmask <sipv6_bitmask>] | any }] [hop-limit { <hop_limit> | any }] | ipv6-icmp [sip { <sipv6_icmp> [sip-bitmask <sipv6_bitmask_icmp>] | any }] [icmp-type { <icmpv6_type> | any }] [icmp-code { <icmpv6_code> | any }] [hop-limit { <hop_limit_icmp> | any }] | ipv6-udp [sip { <sipv6_udp> [sip-bitmask <sipv6_bitmask_udp>] | any }] [sport { <sportv6_udp_start> [to <sportv6_udp_end>] | any }] [dport { <dportv6_udp_start> [to <dportv6_udp_end>] | any }] [hop-limit { <hop_limit_udp> | any }] | ipv6-tcp [sip { <sipv6_tcp> [sip-bitmask <sipv6_bitmask_tcp>] | any }] [sport { <sportv6_tcp_start> [to <sportv6_tcp_end>] | any }] [dport { <dportv6_tcp_start> [to <dportv6_tcp_end>] | any }] [hop-limit { <hop_limit_tcp> | any }] [tcp-flag [tcp-fin { <tcpv6_flag_fin> | any }] [tcp-syn { <tcpv6_flag_syn> | any }] [tcp-rst { <tcpv6_flag_rst> | any }] [tcp-psh { <tcpv6_flag_psh> | any }] [tcp-ack { <tcpv6_flag_ack> | any }] [tcp-urg { <tcpv6_flag_urg> | any }]] }] [action { permit | deny | filter { switchport <filter_switch_port_list> | interface <port_type> [<fliter_port_list>] } }] [rate-limiter { <rate_limiter_id> | disable }] [evc-policer { <evc_policer_id> | disable }] [mirror [disable]] [logging [disable]] [shutdown [disable]] [lookup [disable]] [{ redirect | port-copy } { switchport { <redirect_switch_port_id> | <redirect_switch_port_list> } | interface { <port_type> <redirect_port_id> | <port_type> [<redirect_port_list>] } | disable }]

Function Description

access-list: Access list

Parameter Description

ace: Access list entry
update: Update an existing ACE
<ace_id>: ACE ID
next: insert the current ACE before the next ACE ID
<ace_id_next>: The next ID
last: Place the current ACE to the end of access list
ingress: Ingress
switch: Switch

<ingress_switch_id>: Switch ID
switchport: Switchport
<ingress_switch_port_id>: Swithport ID
<ingress_switch_port_list>: List of swithport ID
interface: Select an interface to configure
<port_type>: Port type in Fast, Giga or Tengiga ethernet
<ingress_port_id>: Port ID in the format of switch-no/port-no
<port_type>: Port type in Fast, Giga or Tengiga ethernet
<ingress_port_list>: List of Port ID, ex, 1/1,3-5;2/2-4,6
any: Don't-care the ingress interface
policy: Policy
<policy>: Policy ID
policy-bitmask: The bitmask for policy ID
<policy_bitmask>: The value of policy bitmask
tag: Tag
tagged: Tagged
untagged: Untagged
any: Don't-care tagged or untagged
vid: VID field
<vid>: The value of VID field
any: Don't-care the value of VID field
tag-priority: Tag priority
<tag_priority>: The value of tag priority
0-1: The range of tag priority
2-3: The range of tag priority
4-5: The range of tag priority
6-7: The range of tag priority
0-3: The range of tag priority
4-7: The range of tag priority
any: Don't-care the value of tag priority field
dmac-type: The type of destination MAC address
unicast: Unicast destination MAC address
multicast: Multicast destination MAC address
broadcast: Broadcast destination MAC address
any: Don't-care the type of destination MAC address
frame-type: Frame type
any: Don't-care the frame type
etype: Frame type of etype
etype-value: Etype value
<etype_value>: The value of etype field
any: Don't-care the value of etype field
smac: Source MAC address field
<etype_smac>: The value of source MAC address field
any: Don't-care the value of source MAC address field
dmac: Destination MAC address field
<etype_dmac>: The value of destination MAC address field
any: Don't-care the value of destination MAC address field
arp: Frame type of ARP
sip: Source IP address field
<arp_sip>: The value of source IP address field. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action
any: Don't-care the value of source IP address field

dip: Destination IP address field
<arp_dip>: The value of destination IP address field. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action
any: Don't-care the value of destination IP address field
smac: Source MAC address field
<arp_smac>: The value of source MAC address field
any: Don't-care the value of source MAC address field
arp-opcode: ARP/RARP opcode field
arp: ARP opcode
rarp: RARP opcode
other: None ARP/RARP opcode
any: Don't-care the value of ARP/RARP opcode field
arp-flag: ARP flag
arp-request: ARP Request/Reply opcode field
<arp_flag_request>: The value of ARP Request/Reply opcode field
any: Don't-care the value of ARP Request/Reply opcode field
arp-smac: ARP sender hardware address (SHA) field
<arp_flag_smac>: The value of ARP sender hardware address (SHA) field
any: Don't-care the value of ARP sender hardware address (SHA) field
arp-tmac: ARP target hardware address (THA) field
<arp_flag_tmac>: The value of ARP target hardware address (THA) field
any: Don't-care the value of ARP target hardware address (THA) field
arp-len: ARP/RARP hardware address length (HLN) and protocol address length (PLN) field
<arp_flag_len>: The value of ARP/RARP hardware address length (HLN) and protocol address length (PLN) field
any: Don't-care the value of ARP/RARP hardware address length (HLN) and protocol address length (PLN) field
arp-ip: ARP/RARP hardware address space (HRD) field
<arp_flag_ip>: The value of ARP/RARP hardware address space (HRD) field
any: Don't-care the value of ARP/RARP hardware address space (HRD) field
arp-ether: ARP/RARP protocol address space (PRO) field
<arp_flag_ether>: The value of ARP/RARP protocol address space (PRO) field
any: Don't-care the value of ARP/RARP protocol address space (PRO) field
ipv4: Frame type of IPv4
sip: Source IP address field
<sipv4>: The value of source IP address field. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action
any: Don't-care the value of source IP address field
dip: Destination IP address field
<dipv4>: The value of destination IP address field. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action
any: Don't-care the value of destination IP address field
ip-protocol: HELP_ACE_IP_PROTO
<ipv4_protocol>: The value of IPv4 protocol field
any: Don't-care the value of IPv4 protocol field
ip-flag: IP flag
ip-ttl: IPv4 TTL field
<ip_flag_ttl>: The value of IPv4 TTL field
any: Don't-care the value of IPv4 TTL field
ip-options: IPv4 options field
<ip_flag_options>: The value of IPv4 options field
any: Don't-care the value of IPv4 options field
ip-fragment: IPv4 fragment field
<ip_flag_fragment>: The value of IPv4 fragment field

any: Don't-care the value of IPv4 fragment field
ipv4-icmp: Frame type of IPv4 ICMP
sip: Source IP address field
<sipv4_icmp>: The value of source IP address field. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action
any: Don't-care the value of source IP address field
dip: Destination IP address field
<dipv4_icmp>: The value of destination IP address field. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action
any: Don't-care the value of destination IP address field
icmp-type: ICMP type field
<icmpv4_type>: The value of ICMP type field
any: Don't-care the value of ICMP type field
icmp-code: ICMP code field
<icmpv4_code>: The value of ICMP code field
any: Don't-care the value of ICMP code field
ip-flag: IP flag
ip-ttl: IPv4 TTL field
<ip_flag_icmp_ttl>: The value of IPv4 TTL field
any: Don't-care the value of IPv4 TTL field
ip-options: IPv4 options field
<ip_flag_icmp_options>: The value of IPv4 options field
any: Don't-care the value of IPv4 options field
ip-fragment: IPv4 fragment field
<ip_flag_icmp_fragment>: The value of IPv4 fragment field
any: Don't-care the value of IPv4 fragment field
ipv4-udp: Frame type of IPv4 TCP
sip: Source IP address field
<sipv4_udp>: The value of source IP address field. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action
any: Don't-care the value of source IP address field
dip: Destination IP address field
<dipv4_udp>: The value of destination IP address field. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action
any: Don't-care the value of destination IP address field
sport: UDP source port field
<sportv4_udp_start>: The value of UDP source port field
to: Port range
<sportv4_udp_end>: The value of UDP source port field
any: The value of UDP source port field
dport: UDP destination port field
<dportv4_udp_start>: The value of UDP destination port field
to: Port range
<dportv4_udp_end>: The value of UDP destination port field
any: Don't-care the value of UDP destination port field
ip-flag: IP flag
ip-ttl: IPv4 TTL field
<ip_flag_udp_ttl>: The value of IPv4 TTL field
any: Don't-care the value of IPv4 TTL field
ip-options: IPv4 options field
<ip_flag_udp_options>: The value of IPv4 options field
any: Don't-care the value of IPv4 options field
ip-fragment: IPv4 fragment field

<ip_flag_udp_fragment>: The value of IPv4 fragment field
any: Don't-care the value of IPv4 fragment field
ipv4-tcp: Frame type of IPv4 TCP
sip: Source IP address field
<sipv4_tcp>: The value of source IP address field. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action
any: Don't-care the value of source IP address field
dip: Destination IP address field
<dipv4_tcp>: The value of destination IP address field. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action
any: Don't-care the value of destination IP address field
sport: TCP source port field
<sportv4_tcp_start>: The value of TCP source port field
to: Port range
<sportv4_tcp_end>: The value of TCP source port field
any
Don't-care the value of TCP source port field
dport: TCP destination port field
<dportv4_tcp_start>: The value of TCP destination Iport field
to: Port range
<dportv4_tcp_end>: The value of TCP destination Iport field
any: Don't-care the value of TCP destination port field
ip-flag: IP flag
ip-ttl: IPv4 TTL field
<ip_flag_tcp_ttl>: The value of IPv4 TTL field
any: Don't-care the value of IPv4 TTL field
ip-options: IPv4 options field
<ip_flag_tcp_options>: The value of IPv4 options field
any: Don't-care the value of IPv4 options field
ip-fragment: IPv4 fragment field
<ip_flag_tcp_fragment>: The value of IPv4 fragment field
any: Don't-care the value of IPv4 fragment field
tcp-flag: TCP flag
tcp-fin: TCP FIN field
<tcpv4_flag_fin>: The value of TCP FIN field
any: Don't-care the value of TCP FIN field
tcp-syn: TCP SYN field
<tcpv4_flag_syn>: The value of TCP SYN field
any: Don't-care the value of TCP SYN field
tcp-rst: TCP RST field
<tcpv4_flag_rst>: The value of TCP RST field
any: Don't-care the value of TCP RST field
tcp-psh: TCP PSH field
<tcpv4_flag_psh>: The value of TCP PSH field
any: Don't-care the value of TCP PSH field
tcp-ack: TCP ACK field
<tcpv4_flag_ack>: The value of TCP ACK field
any: Don't-care the value of TCP ACK field
tcp-urg: TCP URG field
<tcpv4_flag_urg>: The value of TCP URG field
any: Don't-care the value of TCP URG field
ipv6: Frame type of IPv6
next-header: IPv6 hop limiter field

<next_header>: The value of IPv6 hop limiter field
any: Don't-care the value of IPv6 next header field
sip: Source IP address field
<sipv6>: The value of source IP address field. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action
sip-bitmask: The bitmask for IPv6 source address
<sipv6_bitmask>: The value of IPv6 source address bitmask
any: Don't-care the value of source IP address field
hop-limit: IPv6 hop limiter field
<hop_limit>: The value of IPv6 hop limiter field
any: Don't-care the value of IPv6 hop limiter field
ipv6-icmp: Frame type of IPv6 ICMP
sip: Source IP address field
<sipv6_icmp>: The value of source IP address field. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action
sip-bitmask: The bitmask for IPv6 source address
<sipv6_bitmask_icmp>: The value of IPv6 source address bitmask
any: Don't-care the value of source IP address field
icmp-type: ICMP type field
<icmpv6_type>: The value of ICMP type field
any: Don't-care the value of ICMP type field
icmp-code: ICMP code field
<icmpv6_code>: The value of ICMP code field
any: Don't-care the value of ICMP code field
hop-limit: IPv6 hop limiter field
<hop_limit_icmp>: The value of IPv6 hop limiter field
any: Don't-care the value of IPv6 hop limiter field
ipv6-udp: Frame type of IPv6 UDP
sip: Source IP address field
<sipv6_udp>: The value of source IP address field. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action
sip-bitmask: The bitmask for IPv6 source address
<sipv6_bitmask_udp>: The value of IPv6 source address bitmask
any: Don't-care the value of source IP address field
sport: UDP source port field
<sportv6_udp_start>: The value of UDP source port field
to: Port range
<sportv6_udp_end>: The value of UDP source port field
any: The value of UDP source port field
dport: UDP destination port field
<dportv6_udp_start>: The value of UDP destination port field
to: Port range
<dportv6_udp_end>: The value of UDP destination port field
any: Don't-care the value of UDP destination port field
hop-limit: IPv6 hop limiter field
<hop_limit_udp>: The value of IPv6 hop limiter field
any: Don't-care the value of IPv6 hop limiter field
ipv6-tcp: Frame type of IPv6 TCP
sip: Source IP address field
<sipv6_tcp>: The value of source IP address field. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action
sip-bitmask: The bitmask for IPv6 source address
<sipv6_bitmask_tcp>: The value of IPv6 source address bitmask

any: Don't-care the value of source IP address field
sport: TCP source port field
<sportv6_tcp_start>: The value of TCP source port field
to: Port range
<sportv6_tcp_end>: The value of TCP source port field
any: Don't-care the value of TCP source port field
dport: TCP destination port field
<dportv6_tcp_start>: The value of TCP destination Iport field
to: Port range
<dportv6_tcp_end>: The value of TCP destination Iport field
any: Don't-care the value of TCP destination port field
hop-limit: IPv6 hop limiter field
<hop_limit_tcp>: The value of IPv6 hop limiter field
any: Don't-care the value of IPv6 hop limiter field
tcp-flag: TCP flag
tcp-fin: TCP FIN field
<tcpv6_flag_fin>: The value of TCP FIN field
any: Don't-care the value of TCP FIN field
tcp-syn: TCP SYN field
<tcpv6_flag_syn>: The value of TCP SYN field
any: Don't-care the value of TCP SYN field
tcp-rst: TCP RST field
<tcpv6_flag_rst>: The value of TCP RST field
any: Don't-care the value of TCP RST field
tcp-psh: TCP PSH field
<tcpv6_flag_psh>: The value of TCP PSH field
any: Don't-care the value of TCP PSH field
tcp-ack: TCP ACK field
<tcpv6_flag_ack>: The value of TCP ACK field
any: Don't-care the value of TCP ACK field
tcp-urg: TCP URG field
<tcpv6_flag_urg>: The value of TCP URG field
any: Don't-care the value of TCP URG field
action: Access list action
permit: Permit
deny: Deny
filter: Filter
switchport: Switchport
<filter_switch_port_list>: List of swithport ID
interface: Select an interface to configure
<port_type>: Port type in Fast, Giga or Tengiga ethernet
<fliter_port_list>: List of Port ID, ex, 1/1,3-5;2/2-4,6
rate-limiter: Rate limiter
<rate_limiter_id>: Rate limiter ID
disable: Disable rate-limiter
evc-policer: EVC policer
<evc_policer_id>: EVC policer ID
disable: Disable evc-policer
mirror: Mirror frame to destination mirror port
disable: Disable mirror
logging: Logging frame information. Note: The logging feature only works when the packet length is less than 1518 (without VLAN tags) and the System Log memory size and logging rate is limited.
disable: Disable logging

shutdown: Shutdown incoming port. The shutdown feature only works when the packet length is less than 1518 (without VLAN tags).
disable: Disable shutdown
lookup: Second lookup
disable: Disable second lookup
redirect: Redirect frame to specific port
port-copy: Copy frame to specific port
switchport: Switchport
<redirect_switch_port_id>: Swithport ID
<redirect_switch_port_list>: List of swithport ID
interface: Select an interface to configure
<port_type>: Port type in Fast, Giga or Tengiga ethernet
<redirect_port_id>: Port ID in the format of switch-no/port-no
<port_type>: Port type in Fast, Giga or Tengiga ethernet
<redirect_port_list>: List of Port ID, ex, 1/1,3-5;2/2-4,6
disable: Disable

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

access-list action

Command Syntex

access-list action { permit | deny }

Function Description

access: Access management

Parameter Description

access-list: Access list
action: Access list action
permit: Permit
deny: Deny

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

access-list evc-policer

Command Syntex

access-list evc-policer <evc_policer_id>

Function Description

access: Access management

Parameter Description

access-list: Access list
evc-policer: EVC policer
<evc_policer_id>: EVC policer ID

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

access-list logging

Command Syntex

access-list logging

Function Description

access: Access management

Parameter Description

access-list: Access list
logging: Logging frame information. Note: The logging feature only works when the packet length is less than 1518 (without VLAN tags) and the System Log memory size and logging rate is limited.

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

access-list mirror

Command Syntex

access-list mirror

Function Description

access: Access management

Parameter Description

access-list: Access list
mirror: Mirror frame to destination mirror port

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

access-list policy

Command Syntex

access-list policy <policy_id>

Function Description

access: Access management

Parameter Description

access-list: Access list
policy: Policy
<policy_id>: Policy ID

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

access-list port-state

Command Syntex

access-list port-state

Function Description

access: Access management

Parameter Description

access-list: Access list
port-state: Re-enable shutdown port that was shutdown by access-list module

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

access-list rate-limiter

Command Syntex

access-list rate-limiter <rate_limiter_id>

Function Description

access: Access management

Parameter Description

access-list: Access list
rate-limiter: Rate limiter
<rate_limiter_id>: Rate limiter ID

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

access-list rate-limiter

Command Syntex

access-list rate-limiter <rate_limiter_id>

Function Description

access: Access management

Parameter Description

access-list: Access list
rate-limiter: Rate limiter
<rate_limiter_id>: Rate limiter ID

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

access-list rate-limiter rate_limiter_list

Command Syntex

access-list rate-limiter [<rate_limiter_list>] { pps <pps_rate> | 100pps <pps100_rate> | kpps <kpps_rate> | 100kbps <kpbs100_rate> }

Function Description

access: Access management

Parameter Description

access-list: Access list
rate-limiter: Rate limiter
<rate_limiter_list>: Rate limiter ID
pps: Packets per second
<pps_rate>: Rate value
100pps: 100 packets per second
<pps100_rate>: Rate value
kpps: 1K packets per second
<kpps_rate>: Rate value
100kbps: 100k bits per second
<kpbs100_rate>: Rate value

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

access-list shutdown

Command Syntex

access-list shutdown

Function Description

access: Access management

Parameter Description

access-list: Access list
shutdown: Shutdown incoming port. The shutdown feature only works when the packet length is less than 1518 (without VLAN tags).

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

access-list redirect | port-copy interface

Command Syntex

access-list { redirect | port-copy } interface { <port_type> <port_type_id> | <port_type> [<port_type_list>] }

Function Description

access: Access management

Parameter Description

access-list: Access list
redirect: Redirect frame to specific port
port-copy: Copy frame to specific port
interface: Select an interface to configure
<port_type>: Port type in Fast, Giga or Tengiga ethernet
<port_type_id>: Port ID in the format of switch-no/port-no
<port_type>: Port type in Fast, Giga or Tengiga ethernet
<port_type_list>: List of Port ID, ex, 1/1,3-5;2/2-4,6

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

aggregation group

Command Syntex

aggregation group <v_uint>

Function Description

aggregation: Create an aggregation

Parameter Description

aggregation: Create an aggregation
group: Create an aggregation group
<v_uint>: The aggregation group id

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

aggregation mode

Command Syntex

aggregation mode { [smac] [dmac] [ip] [port] }

Function Description

aggregation: Create an aggregation

Parameter Description

aggregation: Aggregation mode
mode: Traffic distribution mode
smac: Source MAC affects the distribution
dmac: Destination MAC affects the distribution
ip: IP address affects the distribution
port: IP port affects the distribution

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

broadcast

Command Syntex

broadcast <ip>

Function Description

broadcast: Broadcast address in use on the client's subnet

Parameter Description

broadcast: Broadcast address in use on the client's subnet
<ip>: Broadcast IP address

Command Mode/Privilege Level

Command Mode: DHCP Pool Configuration Mode
Privilege level: 13

Command

clear

Command Syntex

clear access management statistics

Function Description

clear: Reset functions

Parameter Description

clear: Reset functions
access: Access management
management: Access management configuration
statistics: Statistics data

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 15

Command

clear access-list

Command Syntex

clear access-list ace statistics

Function Description

clear: Reset functions

Parameter Description

clear: Reset functions
access-list: Access list
ace: Access list entry
statistics: Traffic statistics

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 15

Command

clear ip dhcp detailed statistics

Command Syntex

clear ip dhcp detailed statistics { server | client | snooping | relay | helper | all } [interface <port_type> [<in_port_list>]]

Function Description

clear: Reset functions

Parameter Description

clear: Reset functions
ip: Interface Internet Protocol config commands
dhcp: Dynamic Host Configuration Protocol
detailed: Detailed statistics
statistics: Traffic statistics
server: DHCP server
client: DHCP client
snooping: DHCP snooping
relay: DHCP relay
helper: DHCP normal L2 or L3 forward
all: Clear all DHCP related statistics
interface: Select an interface to configure
<port_type>: Port type in Fast, Giga or Tengiga ethernet
<in_port_list>: List of Port ID, ex, 1/1,3-5;2/2-4,6

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 15

Command

clear ip dhcp relay statistics

Command Syntex

clear ip dhcp relay statistics

Function Description

clear: Reset functions

Parameter Description

clear: Reset functions
ip: Interface Internet Protocol config commands
dhcp: Dynamic Host Configuration Protocol
relay: DHCP relay agent configuration
statistics: Traffic statistics

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 15

Command

clear ip dhcp server binding IP

Command Syntex

clear ip dhcp server binding <ip>

Function Description

clear: Reset functions

Parameter Description

clear: Reset functions
ip: IP protocol
dhcp: Delete items from the DHCP database
server: Miscellaneous DHCP server information
binding: Clear DHCP binding
<ip>: IP address of the binding

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 13

Command

clear ip dhcp server binding

Command Syntex

clear ip dhcp server binding { automatic | manual | expired }

Function Description

clear: Reset functions

Parameter Description

clear: Reset functions
ip: IP protocol
dhcp: Delete items from the DHCP database
server: Miscellaneous DHCP server information
binding: Clear DHCP binding
automatic: Clear automatic bindings to expired bindings
manual: Clear manual bindings to expired bindings
expired: Clear expired bindings for free

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 13

Command

clear ip dhcp server statistics

Command Syntex

clear ip dhcp server statistics

Function Description

clear: Reset functions

Parameter Description

clear: Reset functions
ip: IP protocol
dhcp: Delete items from the DHCP database
server: Miscellaneous DHCP server information
statistics: DHCP server statistics

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 13

Command

clear ip dhcp snooping statistics

Command Syntex

clear ip dhcp snooping statistics [interface <port_type> [<in_port_list>]]

Function Description

clear: Reset functions

Parameter Description

clear: Reset functions
ip: Interface Internet Protocol config commands
dhcp: Dynamic Host Configuration Protocol
snooping: DHCP snooping
statistics: Traffic statistics
interface: Select an interface to configure
<port_type>: Port type in Fast, Giga or Tengiga ethernet
<in_port_list>: List of Port ID, ex, 1/1,3-5;2/2-4,6

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 15

Command

clear ip statistics

Command Syntex

clear ip statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]

Function Description

clear: Reset functions

Parameter Description

clear: Reset functions
ip: Interface Internet Protocol config commands
statistics: Traffic statistics
system: IPv4 system traffic
interface: Select an interface to configure
vlan: IPv4 interface traffic
<v_vlan_list>: VLAN identifier(s): VID
icmp: IPv4 ICMP traffic
icmp-msg: IPv4 ICMP traffic for designated message type
<type>: ICMP message type ranges from 0 to 255

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 15

Command

clear IPv6 neighbors

Command Syntex

clear ipv6 neighbors

Function Description

clear: Reset functions

Parameter Description

clear: Reset functions
ipv6: IPv6 configuration commands
neighbors: IPv6 neighbors

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 15

Command

clear ipv6 statistics

Command Syntex

clear ipv6 statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]

Function Description

clear: Reset functions

Parameter Description

clear: Reset functions
ipv6: IPv6 configuration commands
statistics: Traffic statistics
system: IPv6 system traffic
interface: Select an interface to configure
vlan: IPv6 interface traffic
<v_vlan_list>: VLAN identifier(s): VID
icmp: IPv6 ICMP traffic
icmp-msg: IPv6 ICMP traffic for designated message type
<type>: ICMP message type ranges from 0 to 255

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 15

Command

clear lacp statistics

Command Syntex

clear lacp statistics

Function Description

clear: Reset functions

Parameter Description

clear: Clear LACP statistics
lacp: Clear LACP statistics
statistics: Clear all LACP statistics

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 15

Command

clear lldp statistics

Command Syntex

clear lldp statistics

Function Description

clear: Reset functions

Parameter Description

clear: Clears LLDP statistics.
lldp: Clears LLDP statistics.
statistics: Clears LLDP statistics.

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 0

Command

clear logging

Command Syntex

clear logging [info] [warning] [error] [switch <switch_list>]

Function Description

clear: Reset functions

Parameter Description

clear: Reset functions
logging: Syslog
info: Information
warning: Warning
error: Error
switch: Switch
<switch_list>: List of switch ID, ex, 1,3-5,6

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 15

Command

clear mac address-table

Command Syntex

clear mac address-table

Function Description

clear: Reset functions

Parameter Description

clear: Clear command
mac: MAC Address Table
address-table: Flush MAC Address table

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 15

Command

clear mvr

Command Syntex

clear mvr [vlan <v_vlan_list> | name <mvr_name>] statistics

Function Description

clear: Reset functions

Parameter Description

clear: Reset functions
mvr: Multicast VLAN Registration configuration
vlan: MVR multicast vlan
<v_vlan_list>: MVR multicast VLAN list
name: MVR multicast name
<mvr_name>: MVR multicast VLAN name
statistics: Running MVR protocol counters

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 15

Command

clear spanning-tree

Command Syntex

clear spanning-tree { { statistics [interface <port_type> [<v_port_type_list>]] } | { detected-protocols [interface <port_type> [<v_port_type_list_1>]] } }

Function Description

clear: Reset functions

Parameter Description

clear: Reset functions
spanning-tree: STP Bridge
statistics: STP statistics
interface: Choose port
<port_type>: Port type in Fast, Giga or Tengiga ethernet
<v_port_type_list>: List of Port ID, ex, 1/1,3-5;2/2-4,6
detected-protocols: Set the STP migration check
interface: Choose port
<port_type>: Port type in Fast, Giga or Tengiga ethernet
<v_port_type_list_1>: List of Port ID, ex, 1/1,3-5;2/2-4,6

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 15

Command

clear statistics

Command Syntex

clear statistics [interface] <port_type> [<v_port_type_list>]

Function Description

clear: Reset functions

Parameter Description

clear: Clear
statistics: Clear statistics for one or more given interfaces
interface: Interface
<port_type>: Port type in Fast, Giga or Tengiga ethernet
<v_port_type_list>: List of Port ID, ex, 1/1,3-5;2/2-4,6

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 15

Command

client-identifier

Command Syntex

client-identifier { fqdn <identifier> | mac-address <mac> }

Function Description

client-identifier: Client identifier

Parameter Description

client-identifier: Client identifier
fqdn: FQDN type of client identifier
<identifier>: FQDN in 128 characters
mac-address: MAC address type of client identifier
<mac>: MAC address of client

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 0

Command

client-identifier

Command Syntex

client-identifier { fqdn <identifier> | mac-address <mac> }

Function Description

client-identifier: Client identifier

Parameter Description

client-identifier: Client identifier
fqdn: FQDN type of client identifier
<identifier>: FQDN in 128 characters
mac-address: MAC address type of client identifier
<mac>: MAC address of client

Command Mode/Privilege Level

Command Mode: DHCP Pool Configuration Mode
Privilege level: 13

Command

client-name

Command Syntex

client-name <host_name>

Function Description

client-name: Client host name

Parameter Description

client-name: Client host name
<host_name>: Client hsot name in 32 characters

Command Mode/Privilege Level

Command Mode: DHCP Pool Configuration Mode
Privilege level: 13

Command

clock summer-time

Command Syntex

clock summer-time <word16> date [<start_month_var> <start_date_var> <start_year_var> <start_hour_var> <end_month_var> <end_date_var> <end_year_var> <end_hour_var> [<offset_var>]]

Function Description

clock: Configure time-of-day clock
summer-time: Configure summer (daylight savings) time

Parameter Description

clock: Configure time-of-day clock
summer-time: Configure summer (daylight savings) time
<word16>: name of time zone in summer
date: Configure absolute summer time
<start_month_var>: Month to start
<start_date_var>: Date to start
<start_year_var>: Year to start
<start_hour_var>: Time to start (hh:mm)
<end_month_var>: Month to end
<end_date_var>: Date to end
<end_year_var>: Year to end
<end_hour_var>: Time to end (hh:mm)
<offset_var>: Offset to add in minutes

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 13

Command

clock summer-time

Command Syntex

clock summer-time <word16> recurring [<start_week_var> <start_day_var> <start_month_var> <start_hour_var> <end_week_var> <end_day_var> <end_month_var> <end_hour_var> [<offset_var>]]

Function Description

clock: Configure time-of-day clock
summer-time: Configure summer (daylight savings) time

Parameter Description

clock: Configure time-of-day clock
summer-time: Configure summer (daylight savings) time
<word16>: name of time zone in summer
recurring: Configure recurring summer time
date: Configure absolute summer time
<start_month_var>: Month to start
<start_date_var>: Date to start
<start_year_var>: Year to start
<start_hour_var>: Time to start (hh:mm)
<end_month_var>: Month to end
<end_date_var>: Date to end
<end_year_var>: Year to end
<end_hour_var>: Time to end (hh:mm)
<offset_var>: Offset to add in minutes

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 13

Command

clock timezone

Command Syntex

clock timezone <word_var> <hour_var> [<minute_var>]

Function Description

clock: Configure time-of-day clock

Parameter Description

clock: Configure time-of-day clock
timezone: Configure time zone
<word_var>: name of time zone
<hour_var>: Hours offset from UTC
<minute_var>: Minutes offset from UTC

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 13

Command

configure terminal

Command Syntex

configure terminal

Function Description

configure: Enter configuration mode
terminal: Configure from the terminal

Parameter Description

configure: Enter configuration mode
terminal: Configure from the terminal

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 15

Command

copy

Command Syntex

copy { startup-config | running-config | <source_path> } { startup-config | running-config | <destination_path> } [syntax-check]

Function Description

copy: Copy from source to destination

Parameter Description

copy: Copy from source to destination
startup-config: Startup configuration
running-config: Currently running configuration
<source_path>: File in FLASH or on TFTP server
startup-config: Startup configuration
running-config: Currently running configuration
<destination_path>: File in FLASH or on TFTP server
syntax-check: Perform syntax check on source configuration

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 15

Command

default access-list

Command Syntex

default access-list rate-limiter [<rate_limiter_list>]

Function Description

default: Set a command to its defaults

Parameter Description

default: Set a command to its defaults
access-list: Access list
rate-limiter: Rate limiter
<rate_limiter_list>: Rate limiter ID

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 15

Command

default range

Command Syntex

default range <entry_name>

Function Description

default: Set a command to its defaults

Parameter Description

default: Set a command to its defaults
range: A range of IPv4/IPv6 multicast addresses for the profile
<entry_name>: Range entry name in 16 char's

Command Mode/Privilege Level

Command Mode: IPMC Profile Mode
Privilege level: 15

Command

default range

Command Syntex

default-router <ip> [<ip1> [<ip2> [<ip3>]]]

Function Description

default: Set a command to its defaults

Parameter Description

default-router: Default routers
<ip>: Router's IP address
<ip1>: Router's IP address
<ip2>: Router's IP address
<ip3>: Router's IP address

Command Mode/Privilege Level

Command Mode: DHCP Pool Configuration Mode
Privilege level: 13

Command

delete

Command Syntex

delete <path>

Function Description

delete: Delete one file in flash: file system

Parameter Description

delete: Delete one file in flash: file system
<path>: Name of file to delete

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 15

Command

description

Command Syntex

description <profile_desc>

Function Description

description: Additional description about the profile in 64 char's

Parameter Description

description: Additional description about the profile in 64 char's
<profile_desc>: Description for the designated IPMC filtering profile

Command Mode/Privilege Level

Command Mode: User IPMC Profile Mode
Privilege level: 15

Command

dir

Command Syntex

dir

Function Description

dir: Directory of all files in flash: file system

Parameter Description

dir: Directory of all files in flash: file system

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 15

Command

dns-server

Command Syntex

dns-server <ip> [<ip1> [<ip2> [<ip3>]]]

Function Description

dns-server: DNS servers

Parameter Description

dns-server: DNS servers
<ip>: Server's IP address
<ip1>: Server's IP address
<ip2>: Server's IP address
<ip3>: Server's IP address

Command Mode/Privilege Level

Command Mode: DHCP Pool Configuration Mode
Privilege level: 13

Command

domain-name

Command Syntex

domain-name <domain_name>

Function Description

domain-name: Domain name

Parameter Description

domain-name: Domain name
<domain_name>: Domain name

Command Mode/Privilege Level

Command Mode: DHCP Pool Configuration Mode
Privilege level: 13

Command

do

Command Syntex

do <command>

Function Description

do: To run exec commands in config mode

Parameter Description

do: To run exec commands in config mode
<command>: Exec Command

Command Mode/Privilege Level

Command Mode: DHCP Pool Configuration Mode
Privilege level: 13

Command

dot1x authentication timer inactivity

Command Syntex

dot1x authentication timer inactivity <v_10_to_100000>

Function Description

dot1x: IEEE Standard for port-based Network Access Control

Parameter Description

dot1x: IEEE Standard for port-based Network Access Control
authentication: authentication
timer: timer
inactivity: Time in seconds between check for activity on successfully authenticated MAC addresses.
<v_10_to_100000>: seconds

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

dot1x authentication timer re-authenticate

Command Syntex

dot1x authentication timer re-authenticate <v_1_to_3600>

Function Description

dot1x: IEEE Standard for port-based Network Access Control

Parameter Description

dot1x: IEEE Standard for port-based Network Access Control
authentication: Authentication
timer: timer
re-authenticate: The period between re-authentication attempts in seconds
<v_1_to_3600>: seconds

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

dot1x authentication timer re-authenticate

Command Syntex

dot1x feature { [guest-vlan] [radius-qos] [radius-vlan] }

Function Description

dot1x: IEEE Standard for port-based Network Access Control

Parameter Description

dot1x: IEEE Standard for port-based Network Access Control
feature: Globally enables/disables a dot1x feature functionality
guest-vlan: Globally enables/disables state of guest-vlan
radius-qos: Globally enables/disables state of RADIUS-assigned QoS.
radius-vlan: Globally enables/disables state of RADIUS-assigned VLAN.

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

dot1x guest-vlan

Command Syntex

dot1x guest-vlan

Function Description

dot1x: IEEE Standard for port-based Network Access Control

Parameter Description

dot1x: IEEE Standard for port-based Network Access Control
guest-vlan: Enables/disables guest VLAN

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

dot1x guest-vlan <value>

Command Syntex

dot1x guest-vlan <value>

Function Description

dot1x: IEEE Standard for port-based Network Access Control

Parameter Description

dot1x: IEEE Standard for port-based Network Access Control
guest-vlan: Enables/disables guest VLAN
<value>: Guest VLAN ID used when entering the Guest VLAN.

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

dot1x guest-vlan supplicant

Command Syntex

dot1x guest-vlan supplicant

Function Description

dot1x: IEEE Standard for port-based Network Access Control

Parameter Description

dot1x: IEEE Standard for port-based Network Access Control
guest-vlan: Enables/disables guest VLAN
supplicant: The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port.

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

dot1x initialize

Command Syntex

dot1x initialize [interface <port_type> [<plist>]]

Function Description

dot1x: IEEE Standard for port-based Network Access Control

Parameter Description

dot1x: IEEE Standard for port-based Network Access Control
initialize: Force re-authentication immediately
interface: Interface
<port_type>: Port type in Fast, Giga or Tengiga ethernet
<plist>: List of Port ID, ex, 1/1,3-5;2/2-4,6

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 15

Command

dot1x max-reauth-req

Command Syntex

dot1x max-reauth-req <value>

Function Description

dot1x: IEEE Standard for port-based Network Access Control

Parameter Description

dot1x: IEEE Standard for port-based Network Access Control
max-reauth-req: The number of times a Request Identity EAPOL frame is sent without response before considering entering the Guest VLAN
<value>: number of times

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

dot1x port-control

Command Syntex

dot1x port-control { force-authorized | force-unauthorized | auto | single | multi | mac-based }

Function Description

dot1x: IEEE Standard for port-based Network Access Control

Parameter Description

dot1x: IEEE Standard for port-based Network Access Control
port-control: Sets the port security state.
force-authorized: Port access is allowed
force-unauthorized: Port access is not allowed
auto: Port-based 802.1X Authentication
single: Single Host 802.1X Authentication
multi: Multiple Host 802.1X Authentication
mac-based: Switch authenticates on behalf of the client

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

dot1x radius-vlan

Command Syntex

dot1x radius-vlan

Function Description

dot1x: IEEE Standard for port-based Network Access Control

Parameter Description

dot1x: IEEE Standard for port-based Network Access Control
radius-vlan: Enables/disables per-port state of RADIUS-assigned VLAN.

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

dot1x re-authenticate

Command Syntex

dot1x re-authenticate

Function Description

dot1x: IEEE Standard for port-based Network Access Control

Parameter Description

dot1x: IEEE Standard for port-based Network Access Control
re-authenticate: Refresh (restart) 802.1X authentication process.

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

dot1x re-authentication

Command Syntex

dot1x re-authentication

Function Description

dot1x: IEEE Standard for port-based Network Access Control

Parameter Description

dot1x: IEEE Standard for port-based Network Access Control
re-authentication: Set Re-authentication state

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

dot1x system-auth-control

Command Syntex

dot1x system-auth-control

Function Description

dot1x: IEEE Standard for port-based Network Access Control

Parameter Description

dot1x: IEEE Standard for port-based Network Access Control
system-auth-control: Set the global NAS state

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

dot1x timeout tx-period

Command Syntex

dot1x timeout tx-period <v_1_to_65535>

Function Description

dot1x: IEEE Standard for port-based Network Access Control

Parameter Description

dot1x: IEEE Standard for port-based Network Access Control
timeout: timeout
tx-period: the time between EAPOL retransmissions.
<v_1_to_65535>: seconds

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

duplex

Command Syntex

duplex { half | full | auto [half | full] }

Function Description

duplex: Interface duplex

Parameter Description

duplex: Interface duplex
half: Forced half duplex.
full: Forced full duplex.
auto: Auto negotiation of duplex mode.
half: Advertise half duplex.
full: Advertise full duplex.

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

enable

Command Syntex

enable [<new_priv>]

Function Description

enable: Turn on privileged commands

Parameter Description

enable: Turn on privileged commands
<new_priv>: Choose privileged level

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 0

Command

enable password

Command Syntex

enable password [level <priv>] <password>

Function Description

enable: Turn on privileged commands

Parameter Description

password: Assign the privileged level clear password
level: Set exec level password
<priv>: Level number
<password>: The UNENCRYPTED (cleartext) password

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

enable secret

Command Syntex

enable secret { 0 | 5 } [level <priv>] <password>

Function Description

enable: Turn on privileged commands

Parameter Description

enable: Modify enable password parameters
secret: Assign the privileged level secret
0: Specifies an UNENCRYPTED password will follow
5: Specifies an ENCRYPTED secret will follow
level: Set exec level password
<priv>: Level number
<password>: Password

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

end

Command Syntex

end

Function Description

end: Go back to EXEC mode

Parameter Description

end: Go back to EXEC mode

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 0

Command

end

Command Syntex

end

Function Description

end: Go back to EXEC mode

Parameter Description

end: Go back to EXEC mode

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 0

Command

exit

Command Syntex

exit

Function Description

exit: Exit from current mode

Parameter Description

exit: Exit from current mode

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 0

Command

firmware swap

Command Syntex

firmware swap

Function Description

firmware: Firmware upgrade/swap

Parameter Description

firmware: Firmware upgrade/swap
swap: Swap between Active and Alternate firmware image.

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 15

Command

firmware upgrade

Command Syntex

firmware upgrade <tftpserver_path_file>

Function Description

firmware: Firmware upgrade/swap

Parameter Description

firmware: Firmware upgrade/swap
upgrade: Firmware upgrade
<tftpserver_path_file>: TFTP Server IP address, path and file name for the server containing the new image.

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 15

Command

flowcontrol

Command Syntex

flowcontrol { on | off }

Function Description

flowcontrol: Traffic flow control.

Parameter Description

flowcontrol: Traffic flow control.
on: Enable flow control.
off: Disable flow control.

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

green-ethernet eee

Command Syntex

green-ethernet eee

Function Description

green-ethernet: Green ethernet (Power reduction)

Parameter Description

green-ethernet: Green ethernet (Power reduction)
eee: Powering down of PHYs when there is no traffic.

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

green-ethernet eee optimize-for-power

Command Syntex

green-ethernet eee optimize-for-power

Function Description

green-ethernet: Green ethernet (Power reduction)

Parameter Description

green-ethernet: Green ethernet (Power reduction)
eee: Powering down of PHYs when there is no traffic.
optimize-for-power: Set if EEE shall be optimized for least power comsumption (else optimized for least traffic latency).

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

green-ethernet eee urgent-queues

Command Syntex

green-ethernet eee urgent-queues [<urgent_queue_range_list>]

Function Description

green-ethernet: Green ethernet (Power reduction)

Parameter Description

green-ethernet: Green ethernet (Power reduction)
eee: Powering down of PHYs when there is no traffic.
urgent-queues: Enables EEE urgent queue. An urgent queue means that latency is kept to a minimum for traffic goin to that queue. Note: EEE power savings will be reduced.
<urgent_queue_range_list>: EEE Interface.

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

green-ethernet energy-detect

Command Syntex

green-ethernet energy-detect

Function Description

green-ethernet: Green ethernet (Power reduction)

Parameter Description

green-ethernet: Green ethernet (Power reduction)
energy-detect: Enable power saving for ports with no link partner.

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

green-ethernet short-reach

Command Syntex

green-ethernet short-reach

Function Description

green-ethernet: Green ethernet (Power reduction)

Parameter Description

green-ethernet: Green ethernet (Power reduction)
short-reach: Enable power saving for ports which is connect to link partner with short cable.

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

gvrp

Command Syntex

gvrp

Function Description

gvrp: Enable GVRP feature

Parameter Description

gvrp: Enable GVRP feature

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

hardware-address

Command Syntex

hardware-address <mac>

Function Description

hardware-address: Client hardware address

Parameter Description

hardware-address: Client hardware address
<mac>: Client MAC address

Command Mode/Privilege Level

Command Mode: DHCP Pool Configuration Mode
Privilege level: 13

Command

host

Command Syntex

host <ip> <subnet_mask>

Function Description

hardware-address: Client hardware address

Parameter Description

host: Client IP address and mask
<ip>: Network number
<subnet_mask>: Network mask in dotted-decimal notation, excluding 255.255.255.255

Command Mode/Privilege Level

Command Mode: DHCP Pool Configuration Mode
Privilege level: 13

Command

host <v_ipv6_ucast>

Command Syntex

host <v_ipv6_ucast> [<udp_port>] [traps | informs]

Function Description

hardware-address: Client hardware address

Parameter Description

host: Client IP address and mask
<v_ipv6_ucast>: IP address of SNMP trap host
<udp_port>: UDP port of the trap messges
traps: Send Trap messages to this host
informs: Send Inform messages to this host

Command Mode/Privilege Level

Command Mode: SNMP Server Host Mode
Privilege level: 15

Command

host <v_ipv4_ucast>

Command Syntex

host { <v_ipv4_ucast> | <v_word45> } [<udp_port>] [traps | informs]

Function Description

hardware-address: Client hardware address

Parameter Description

host: Client IP address and mask
<v_ipv4_ucast>: IP address of SNMP trap host
<v_word45>: hostname of SNMP trap host
<udp_port>: UDP port of the trap messges
traps: Send Trap messages to this host
informs: Send Inform messages to this host

Command Mode/Privilege Level

Command Mode: SNMP Server Host Mode
Privilege level: 15

Command

hostname <hostname>

Command Syntex

hostname <hostname>

Function Description

hardware-address: Client hardware address

Parameter Description

host: Client IP address and mask
<hostname>: This system's network name

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

informs retries

Command Syntex

informs retries <retries> timeout <timeout>

Function Description

informs: Send Inform messages to this host

Parameter Description

informs: Send Inform messages to this host
retries: retires inform messages
<retries>: retires times
timeout: timeout parmater
<timeout>: timeout interval

Command Mode/Privilege Level

Command Mode: SNMP Server Host Mode
Privilege level: 15

Command

interface vlan

Command Syntex

interface vlan <vlist>

Function Description

informs: Send Inform messages to this host

Parameter Description

interface: Select an interface to configure
vlan: VLAN interface configurations
<vlist>: List of VLAN interface numbers, 1~4095

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

interface

Command Syntex

interface <port_type> [<plist>]

Function Description

interface: Select an interface to configure

Parameter Description

interface: Select an interface to configure
<port_type>: Port type in Fast, Giga or Tengiga ethernet
<plist>: List of Port ID, ex, 1/1,3-5;2/2-4,6

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ip address

Command Syntex

ip address { { <address> <netmask> } | { dhcp [fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]] } }

Function Description

ip: IPv4 configuration

Parameter Description

ip: IPv4 configuration
address: Address configuraton
<address>: IP address
<netmask>: IP netmask
dhcp: Enable DHCP
fallback: DHCP fallback settings
<fallback_address>: DHCP fallback address
<fallback_netmask>: DHCP fallback netmask
timeout: DHCP fallback timeout
<fallback_timeout>: DHCP fallback timeout in seconds

Command Mode/Privilege Level

Command Mode: VLAN Interface Mode
Privilege level: 15

Command

ip arp inspection

Command Syntex

ip arp inspection

Function Description

ip: IPv4 configuration

Parameter Description

ip: IPv4 configuration
arp: Address Resolution Protocol
inspection: ARP inspection

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 13

Command

ip arp inspection check-vlan

Command Syntex

ip arp inspection check-vlan

Function Description

ip: IPv4 configuration

Parameter Description

ip: IPv4 configuration
arp: Address Resolution Protocol
inspection: ARP inspection
check-vlan: ARP inspection VLAN mode config

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 13

Command

ip arp inspection entry interface

Command Syntex

ip arp inspection entry interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>

Function Description

ip: IPv4 configuration

Parameter Description

ip: IPv4 configuration
arp: Address Resolution Protocol
inspection: ARP inspection
entry: arp inspection entry
interface: arp inspection entry interface config
<port_type>: Port type in Fast, Giga or Tengiga ethernet
<in_port_type_id>: Port ID in the format of switch-no/port-no
<vlan_var>: Select a VLAN id to configure
<mac_var>: Select a MAC address to configure
<ipv4_var>: Select an IP Address to configure

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 13

Command

ip arp inspection logging

Command Syntex

ip arp inspection logging { deny | permit | all }

Function Description

ip: IPv4 configuration

Parameter Description

ip: IPv4 configuration
arp: Address Resolution Protocol
inspection: ARP inspection
logging: ARP inspection logging mode config
deny: log denied entries
permit: log permitted entries
all: log all entries

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 13

Command

ip arp inspection translate

Command Syntex

ip arp inspection translate [interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>]

Function Description

ip: IPv4 configuration

Parameter Description

ip: IPv4 configuration
arp: Address Resolution Protocol
inspection: ARP inspection
translate: arp inspection translate all entries
interface: arp inspection entry interface config
<port_type>: Port type in Fast, Giga or Tengiga ethernet
<in_port_type_id>: Port ID in the format of switch-no/port-no
<vlan_var>: Select a VLAN id to configure
<mac_var>: Select a MAC address to configure
<ipv4_var>: Select an IP Address to configure

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 13

Command

ip arp inspection trust

Command Syntex

ip arp inspection trust

Function Description

ip: IPv4 configuration

Parameter Description

ip: IPv4 configuration
arp: Address Resolution Protocol
inspection: ARP inspection
trust: ARP inspection trust config

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 13

Command

ip arp inspection vlan

Command Syntex

ip arp inspection vlan <in_vlan_list>

Function Description

ip: IPv4 configuration

Parameter Description

ip: IPv4 configuration
arp: Address Resolution Protocol
inspection: ARP inspection
vlan: arp inspection vlan setting
<in_vlan_list>: arp inspection vlan list

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 13

Command

ip arp inspection vlan logging

Command Syntex

ip arp inspection vlan <in_vlan_list> logging { deny | permit | all }

Function Description

ip: IPv4 configuration

Parameter Description

ip: IPv4 configuration
arp: Address Resolution Protocol
inspection: ARP inspection
vlan: arp inspection vlan setting
<in_vlan_list>: arp inspection vlan list
logging: ARP inspection vlan logging mode config
deny: log denied entries
permit: log permitted entries
all: log all entries

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 13

Command

ip dhcp excluded-addres

Command Syntex

ip dhcp excluded-address <low_ip> [<high_ip>]

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
dhcp: Configure DHCP server parameters
excluded-address: Prevent DHCP from assigning certain addresses
<low_ip>: Low IP address
<high_ip>: High IP address

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 13

Command

ip dhcp pool

Command Syntex

ip dhcp pool <pool_name>

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
dhcp: Configure DHCP server parameters
pool: Configure DHCP address pools
<pool_name>: Pool name in 32 characters

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ip dhcp relay

Command Syntex

ip dhcp relay

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
dhcp: Configure DHCP server parameters
relay: DHCP relay agent configuration

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ip dhcp relay information option

Command Syntex

ip dhcp relay information option

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
dhcp: Configure DHCP server parameters
relay: DHCP relay agent configuration
information: DHCP information option(Option 82)
option: DHCP option

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ip dhcp relay information policy

Command Syntex

ip dhcp relay information policy { drop | keep | replace }

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
dhcp: Configure DHCP server parameters
relay: DHCP relay agent configuration
information: DHCP information option(Option 82)
policy: Policy for handling the receiving DHCP packet already include the information option
drop: Drop the package when receive a DHCP message that already contains relay information
keep: Keep the original relay information when receive a DHCP message that already contains it
replace: Replace the original relay information when receive a DHCP message that already contains it

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ip dhcp retry interface vlan

Command Syntex

ip dhcp retry interface vlan <vlan_id>

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
dhcp: Configure DHCP server parameters
retry: Restart the DHCP query process
interface: Interface
vlan: Vlan interface
<vlan_id>: Vlan ID

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 15

Command

ip dhcp server

Command Syntex

ip dhcp server

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
dhcp: Configure DHCP server parameters
server: Enable DHCP server

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 13

Command

ip dhcp snooping

Command Syntex

ip dhcp snooping

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
dhcp: Configure DHCP server parameters
snooping: DHCP snooping

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ip dhcp snooping trust

Command Syntex

ip dhcp snooping trust

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
dhcp: Configure DHCP server parameters
trust: DHCP Snooping trust config

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

ip dns proxy

Command Syntex

ip dns proxy

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
dns: Domain Name System
proxy: DNS proxy service

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ip helper-address

Command Syntex

ip helper-address <v_ipv4_ucast>

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
helper-address: DHCP relay server
<v_ipv4_ucast>: IP address of the DHCP relay server

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ip http secure-redirect

Command Syntex

ip http secure-redirect

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
http: Hypertext Transfer Protocol
secure-redirect: Secure HTTP web redirection

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ip http secure-server

Command Syntex

ip http secure-server

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
http: Hypertext Transfer Protocol
secure-server: Secure HTTP web server

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ip igmp host-proxy

Command Syntex

ip igmp host-proxy [leave-proxy]

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
igmp: Internet Group Management Protocol
host-proxy: IGMP proxy configuration
leave-proxy: IGMP proxy for leave configuration

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ip igmp snooping

Command Syntex

ip igmp snooping

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
igmp: Internet Group Management Protocol
snooping: Snooping IGMP

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ip igmp snooping compatibility

Command Syntex

ip igmp snooping compatibility { auto | v1 | v2 | v3 }

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
igmp: Internet Group Management Protocol
snooping: Snooping IGMP
compatibility: Interface compatibility
auto: Compatible with IGMPv1/IGMPv2/IGMPv3
v1: Forced IGMPv1
v2: Forced IGMPv2
v3: Forced IGMPv3

Command Mode/Privilege Level

Command Mode: VLAN Interface Mode
Privilege level: 15

Command

ip igmp snooping filter

Command Syntex

ip igmp snooping filter <profile_name>

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
igmp: Internet Group Management Protocol
snooping: Snooping IGMP
filter: Access control on IGMP multicast group registration
<profile_name>: Profile name in 16 char's

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

ip igmp snooping immediate-leave

Command Syntex

ip igmp snooping immediate-leave

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
igmp: Internet Group Management Protocol
snooping: Snooping IGMP
immediate-leave: Immediate leave configuration

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

ip igmp snooping last-member-query-interval

Command Syntex

ip igmp snooping last-member-query-interval <ipmc_lmqi>

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
igmp: Internet Group Management Protocol
snooping: Snooping IGMP
last-member-query-interval: Last Member Query Interval in tenths of seconds
<ipmc_lmqi>: 0 - 31744 tenths of seconds

Command Mode/Privilege Level

Command Mode: VLAN Interface Mode
Privilege level: 15

Command

ip igmp snooping max-groups

Command Syntex

ip igmp snooping max-groups <throttling>

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
igmp: Internet Group Management Protocol
snooping: Snooping IGMP
max-groups: IGMP group throttling configuration
<throttling>: Maximun number of IGMP group registration

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

ip igmp snooping mrouter

Command Syntex

ip igmp snooping mrouter

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
igmp: Internet Group Management Protocol
snooping: Snooping IGMP
mrouter: Multicast router port configuration

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

ip igmp snooping priority

Command Syntex

ip igmp snooping priority <cos_priority>

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
igmp: Internet Group Management Protocol
snooping: Snooping IGMP
priority: Interface CoS priority
<cos_priority>: CoS priority ranges from 0 to 7

Command Mode/Privilege Level

Command Mode: VLAN Interface Mode
Privilege level: 15

Command

ip igmp snooping querier

Command Syntex

ip igmp snooping querier { election | address <v_ipv4_ucast> }

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
igmp: Internet Group Management Protocol
snooping: Snooping IGMP
querier: IGMP Querier configuration
election: Act as an IGMP Querier to join Querier-Election
address: IGMP Querier address configuration
<v_ipv4_ucast>: A valid IPv4 unicast address

Command Mode/Privilege Level

Command Mode: VLAN Interface Mode
Privilege level: 15

Command

ip igmp snooping query-interval

Command Syntex

ip igmp snooping query-interval <ipmc_qi>

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
igmp: Internet Group Management Protocol
snooping: Snooping IGMP
query-interval: Query Interval in seconds
<ipmc_qi>: 1 - 31744 seconds

Command Mode/Privilege Level

Command Mode: VLAN Interface Mode
Privilege level: 15

Command

ip igmp snooping query-max-response-time

Command Syntex

ip igmp snooping query-max-response-time <ipmc_qri>

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
igmp: Internet Group Management Protocol
snooping: Snooping IGMP
query-max-response-time: Query Response Interval in tenths of seconds
<ipmc_qri>: 0 - 31744 tenths of seconds

Command Mode/Privilege Level

Command Mode: VLAN Interface Mode
Privilege level: 15

Command

ip igmp snooping robustness-variable

Command Syntex

ip igmp snooping robustness-variable <ipmc_rv>

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
igmp: Internet Group Management Protocol
snooping: Snooping IGMP
robustness-variable: Robustness Variable
<ipmc_rv>: Packet loss tolerance count from 1 to 255

Command Mode/Privilege Level

Command Mode: VLAN Interface Mode
Privilege level: 15

Command

ip igmp snooping unsolicited-report-interval

Command Syntex

ip igmp snooping unsolicited-report-interval <ipmc_uri>

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
igmp: Internet Group Management Protocol
snooping: Snooping IGMP
unsolicited-report-interval: Unsolicited Report Interval in seconds
<ipmc_uri>: 0 - 31744 seconds

Command Mode/Privilege Level

Command Mode: VLAN Interface Mode
Privilege level: 15

Command

ip igmp snooping vlan

Command Syntex

ip igmp snooping vlan <v_vlan_list>

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
igmp: Internet Group Management Protocol
snooping: Snooping IGMP
vlan: IGMP VLAN
<v_vlan_list>: VLAN identifier(s): VID

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ip igmp ssm-range

Command Syntex

ip igmp ssm-range <v_ipv4_mcast> <ipv4_prefix_length>

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
igmp: Internet Group Management Protocol
snooping: Snooping IGMP
ssm-range: IPv4 address range of Source Specific Multicast
<v_ipv4_mcast>: Valid IPv4 multicast address
<ipv4_prefix_length>: Prefix length ranges from 4 to 32

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ip igmp unknown-flooding

Command Syntex

ip igmp unknown-flooding

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
igmp: Internet Group Management Protocol
snooping: Snooping IGMP
unknown-flooding: Flooding unregistered IPv4 multicast traffic

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ip name-server

Command Syntex

ip name-server { <v_ipv4_ucast> | dhcp [interface vlan <v_vlan_id>] }

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
name-server: Domain Name System
<v_ipv4_ucast>: A valid IPv4 unicast address
dhcp: Dynamic Host Configuration Protocol
interface: Select an interface to configure
vlan: VLAN Interface
<v_vlan_id>: VLAN identifier(s): VID

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ip route

Command Syntex

ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
route: Add IP route
<v_ipv4_addr>: Network
<v_ipv4_netmask>: Netmask
<v_ipv4_gw>: Gateway

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ip source binding interface

Command Syntex

ip source binding interface <port_type> <in_port_type_id> <vlan_var> <ipv4_var> <mac_var>

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
source: source command
binding: ip source binding
interface: ip source binding entry interface config
<port_type>: Port type in Fast, Giga or Tengiga ethernet
<in_port_type_id>: Port ID in the format of switch-no/port-no
<vlan_var>: Select a VLAN id to configure
<ipv4_var>: Select an IP Address to configure
<mac_var>: Select a MAC address to configure

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 13

Command

ip ssh

Command Syntex

ip ssh

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
ssh: Secure Shell

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ip verify source

Command Syntex

ip verify source

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
verify: verify command
source: verify source

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 13

Command

ip verify source limit

Command Syntex

ip verify source limit <cnt_var>

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
verify: verify command
source: verify source
limit: limit command
<cnt_var>: the number of limit

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 13

Command

ip verify source translate

Command Syntex

ip verify source translate

Function Description

ip: Interface Internet Protocol config commands

Parameter Description

ip: Interface Internet Protocol config commands
verify: verify command
source: verify source
translate: ip verify source translate all entries

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 13

Command

ipmc profile

Command Syntex

ipmc profile <profile_name>

Function Description

ipmc: IPv4/IPv6 multicast configuration

Parameter Description

ipmc: IPv4/IPv6 multicast configuration
profile: IPMC profile configuration
<profile_name>: Profile name in 16 char's

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ipmc range

Command Syntex

ipmc range <entry_name> { <v_ipv4_mcast> [<v_ipv4_mcast_1>] | <v_ipv6_mcast> [<v_ipv6_mcast_1>] }

Function Description

ipmc: IPv4/IPv6 multicast configuration

Parameter Description

ipmc: IPv4/IPv6 multicast configuration
range: A range of IPv4/IPv6 multicast addresses for the profile
<entry_name>: Range entry name in 16 char's
<v_ipv4_mcast>: Valid IPv4 multicast address
<v_ipv4_mcast_1>: Valid IPv4 multicast address that is not less than start address
<v_ipv6_mcast>: Valid IPv6 multicast address
<v_ipv6_mcast_1>: Valid IPv6 multicast address that is not less than start address

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ipv6 address <subnet>

Command Syntex

ipv6 address <subnet>

Function Description

ipv6: IPv6 configuration commands

Parameter Description

ipv6: IPv6 configuration commands
address: Configure the IPv6 address of an interface
<subnet>: IPv6 prefix x:x::y/z

Command Mode/Privilege Level

Command Mode: VLAN Interface Mode
Privilege level: 15

Command

ipv6 mld host-proxy

Command Syntex

ipv6 mld host-proxy [leave-proxy]

Function Description

ipv6: IPv6 configuration commands

Parameter Description

ipv6: IPv6 configuration commands
mld: Multicasat Listener Discovery
host-proxy: MLD proxy configuration
leave-proxy: MLD proxy for leave configuration

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ipv6 mld snooping

Command Syntex

ipv6 mld snooping

Function Description

ipv6: IPv6 configuration commands

Parameter Description

ipv6: IPv6 configuration commands
mld: Multicasat Listener Discovery
snooping: Snooping MLD

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ipv6 mld snooping compatibility

Command Syntex

ipv6 mld snooping compatibility { auto | v1 | v2 }

Function Description

ipv6: IPv6 configuration commands

Parameter Description

ipv6: IPv6 configuration commands
mld: Multicasat Listener Discovery
snooping: Snooping MLD
compatibility: Interface compatibility
auto: Compatible with MLDv1/MLDv2
v1: Forced MLDv1
v2: Forced MLDv2

Command Mode/Privilege Level

Command Mode: VLAN Interface Mode
Privilege level: 15

Command

ipv6 mld snooping filter

Command Syntex

ipv6 mld snooping filter <profile_name>

Function Description

ipv6: IPv6 configuration commands

Parameter Description

ipv6: IPv6 configuration commands
mld: Multicasat Listener Discovery
snooping: Snooping MLD
filter: Access control on MLD multicast group registration
<profile_name>: Profile name in 16 char's

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

ipv6 mld snooping filter

Command Syntex

ipv6 mld snooping filter <profile_name>

Function Description

ipv6: IPv6 configuration commands

Parameter Description

ipv6: IPv6 configuration commands
mld: Multicasat Listener Discovery
snooping: Snooping MLD
filter: Access control on MLD multicast group registration
<profile_name>: Profile name in 16 char's

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

ipv6 mld snooping immediate-leave

Command Syntex

ipv6 mld snooping immediate-leave

Function Description

ipv6: IPv6 configuration commands

Parameter Description

ipv6: IPv6 configuration commands
mld: Multicasat Listener Discovery
snooping: Snooping MLD
immediate-leave: Immediate leave configuration

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

ipv6 mld snooping last-member-query-interval

Command Syntex

ipv6 mld snooping last-member-query-interval <ipmc_lmqi>

Function Description

ipv6: IPv6 configuration commands

Parameter Description

ipv6: IPv6 configuration commands
mld: Multicasat Listener Discovery
snooping: Snooping MLD
last-member-query-interval: Last Member Query Interval in tenths of seconds
<ipmc_lmqi>: 0 - 31744 tenths of seconds

Command Mode/Privilege Level

Command Mode: VLAN Interface Mode
Privilege level: 15

Command

ipv6 mld snooping max-groups

Command Syntex

ipv6 mld snooping max-groups <throttling>

Function Description

ipv6: IPv6 configuration commands

Parameter Description

ipv6: IPv6 configuration commands
mld: Multicasat Listener Discovery
snooping: Snooping MLD
max-groups: MLD group throttling configuration
<throttling>: Maximun number of MLD group registration

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

ipv6 mld snooping mrouter

Command Syntex

ipv6 mld snooping mrouter

Function Description

ipv6: IPv6 configuration commands

Parameter Description

ipv6: IPv6 configuration commands
mld: Multicasat Listener Discovery
snooping: Snooping MLD
mrouter: Multicast router port configuration

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

ipv6 mld snooping priority

Command Syntex

ipv6 mld snooping priority <cos_priority>

Function Description

ipv6: IPv6 configuration commands

Parameter Description

ipv6: IPv6 configuration commands
mld: Multicasat Listener Discovery
snooping: Snooping MLD
priority: Interface CoS priority
<cos_priority>: CoS priority ranges from 0 to 7

Command Mode/Privilege Level

Command Mode: VLAN Interface Mode
Privilege level: 15

Command

ipv6 mld snooping querier election

Command Syntex

ipv6 mld snooping querier election

Function Description

ipv6: IPv6 configuration commands

Parameter Description

ipv6: IPv6 configuration commands
mld: Multicasat Listener Discovery
snooping: Snooping MLD
querier: MLD Querier configuration
election: Act as a MLD Querier to join Querier-Election

Command Mode/Privilege Level

Command Mode: VLAN Interface Mode
Privilege level: 15

Command

ipv6 mld snooping query-interval

Command Syntex

ipv6 mld snooping query-interval <ipmc_qi>

Function Description

ipv6: IPv6 configuration commands

Parameter Description

ipv6: IPv6 configuration commands
mld: Multicasat Listener Discovery
snooping: Snooping MLD
query-interval: Query Interval in seconds
<ipmc_qi>: 1 - 31744 seconds

Command Mode/Privilege Level

Command Mode: VLAN Interface Mode
Privilege level: 15

Command

ipv6 mld snooping query-max-response-time

Command Syntex

ipv6 mld snooping query-max-response-time <ipmc_qri>

Function Description

ipv6: IPv6 configuration commands

Parameter Description

ipv6: IPv6 configuration commands
mld: Multicasat Listener Discovery
snooping: Snooping MLD
query-max-response-time: Query Response Interval in tenths of seconds
<ipmc_qri>: 0 - 31744 tenths of seconds

Command Mode/Privilege Level

Command Mode: VLAN Interface Mode
Privilege level: 15

Command

ipv6 mld snooping robustness-variable

Command Syntex

ipv6 mld snooping robustness-variable <ipmc_rv>

Function Description

ipv6: IPv6 configuration commands

Parameter Description

ipv6: IPv6 configuration commands
mld: Multicasat Listener Discovery
snooping: Snooping MLD
robustness-variable: Robustness Variable
<ipmc_rv>: Packet loss tolerance count from 1 to 255

Command Mode/Privilege Level

Command Mode: VLAN Interface Mode
Privilege level: 15

Command

ipv6 mld snooping unsolicited-report-interval

Command Syntex

ipv6 mld snooping unsolicited-report-interval <ipmc_uri>

Function Description

ipv6: IPv6 configuration commands

Parameter Description

ipv6: IPv6 configuration commands
mld: Multicasat Listener Discovery
snooping: Snooping MLD
unsolicited-report-interval: Unsolicited Report Interval in seconds
<ipmc_uri>: 0 - 31744 seconds

Command Mode/Privilege Level

Command Mode: VLAN Interface Mode
Privilege level: 15

Command

ipv6 mld snooping vlan

Command Syntex

ipv6 mld snooping vlan <v_vlan_list>

Function Description

ipv6: IPv6 configuration commands

Parameter Description

ipv6: IPv6 configuration commands
mld: Multicasat Listener Discovery
snooping: Snooping MLD
vlan: MLD VLAN
<v_vlan_list>: VLAN identifier(s): VID

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ipv6 mld ssm-range

Command Syntex

ipv6 mld ssm-range <v_ipv6_mcast> <ipv6_prefix_length>

Function Description

ipv6: IPv6 configuration commands

Parameter Description

ipv6: IPv6 configuration commands
mld: Multicasat Listener Discovery
snooping: Snooping MLD
ssm-range: IPv6 address range of Source Specific Multicast
<v_ipv6_mcast>: Valid IPv6 multicast address
<ipv6_prefix_length>: Prefix length ranges from 8 to 128

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ipv6 mld unknown-flooding

Command Syntex

ipv6 mld unknown-flooding

Function Description

ipv6: IPv6 configuration commands

Parameter Description

ipv6: IPv6 configuration commands
mld: Multicasat Listener Discovery
snooping: Snooping MLD
unknown-flooding: Flooding unregistered IPv6 multicast traffic

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ipv6 mtu

Command Syntex

ipv6 mtu <mtubytes>

Function Description

ipv6: IPv6 configuration commands

Parameter Description

ipv6: IPv6 configuration commands
mtu: Maximum transmission unit
<mtubytes>: MTU value in bytes

Command Mode/Privilege Level

Command Mode: VLAN Interface Mode
Privilege level: 15

Command

ipv6 route

Command Syntex

ipv6 route <v_ipv6_subnet> { <v_ipv6_ucast> | interface vlan <v_vlan_id> <v_ipv6_addr> }

Function Description

ipv6: IPv6 configuration commands

Parameter Description

ipv6: IPv6 configuration commands
route: Configure static routes
<v_ipv6_subnet>: IPv6 prefix x:x::y/z
<v_ipv6_ucast>: IPv6 unicast address (except link-local address) of next-hop
interface: Select an interface to configure
vlan: VLAN Interface
<v_vlan_id>: VLAN identifier(s): VID
<v_ipv6_addr>: IPv6 link-local address of next-hop

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

lacp

Command Syntex

lacp

Function Description

ipv6: IPv6 configuration commands

Parameter Description

lacp: Enable LACP on this interface

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

lacp key

Command Syntex

lacp key { <v_1_to_65535> | auto }

Function Description

ipv6: IPv6 configuration commands

Parameter Description

lacp: Enable LACP on this interface
key: Key of the LACP aggregation
<v_1_to_65535>: Key value
auto: Choose a key based on port speed

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

lacp port-priority

Command Syntex

lacp port-priority <v_1_to_65535>

Function Description

ipv6: IPv6 configuration commands

Parameter Description

lacp: Enable LACP on this interface
port-priority: LACP priority of the port
<v_1_to_65535>: Priority value, lower means higher priority

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

lacp role

Command Syntex

lacp role { active | passive }

Function Description

ipv6: IPv6 configuration commands

Parameter Description

lacp: Enable LACP on this interface
role: Active / Passive (speak if spoken to) role
active: Transmit LACP BPDUs continously
passive: Wait for neighbour LACP BPDUs before transmitting

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

lacp system-priority

Command Syntex

lacp system-priority <v_1_to_65535>

Function Description

ipv6: IPv6 configuration commands

Parameter Description

lacp: Enable LACP on this interface
system-priority: System priority
<v_1_to_65535>: Priority value, lower means higher priority

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

lacp timeout

Command Syntex

lacp timeout { fast | slow }

Function Description

ipv6: IPv6 configuration commands

Parameter Description

lacp: Enable LACP on this interface
timeout: The period between BPDU transmissions
fast: Transmit BPDU each second (fast timeout)
slow: Transmit BPDU each 30th second (slow timeout)

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

lease

Command Syntex

lease { <day> [<hour> [<min>]] | infinite }

Function Description

lease: Address lease time

Parameter Description

lease: Address lease time
<day>: Days
<hour>: Hours
<min>: Minutes
infinite: Infinite lease

Command Mode/Privilege Level

Command Mode: DHCP Pool Configuration Mode
Privilege level: 13

Command

lldp cdp-aware

Command Syntex

lldp cdp-aware

Function Description

lldp: LLDP configurations.

Parameter Description

lldp: LLDP configurations.
cdp-aware: Configures if the interface shall be CDP aware (CDP discovery information is added to the LLDP neighbor table)

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

lldp holdtime

Command Syntex

lldp holdtime <val>

Function Description

lldp: LLDP configurations.

Parameter Description

lldp: LLDP configurations.
holdtime: Sets LLDP hold time (The neighbor switch will discarded the LLDP information after \"hold time\" multiplied with \"timer\" seconds).
<val>: 2-10 seconds.

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

lldp med datum

Command Syntex

lldp med datum { wgs84 | nad83-navd88 | nad83-mllw }

Function Description

lldp: LLDP configurations.

Parameter Description

lldp: LLDP configurations.
med: Media Endpoint Discovery.
datum: Datum (geodetic system) type.
wgs84: World Geodetic System 1984
nad83-navd88: North American vertical datum 1983
nad83-mllw: Mean lower low water datum 1983.

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

lldp med fast

Command Syntex

lldp med fast

Function Description

lldp: LLDP configurations.

Parameter Description

lldp: LLDP configurations.
med: Media Endpoint Discovery.
fast: Number of times to repeat LLDP frame transmission at fast start.

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

lldp med location-tlv altitude

Command Syntex

lldp med location-tlv altitude { meters | floors } <v_word11>

Function Description

lldp: LLDP configurations.

Parameter Description

lldp: LLDP configurations.
med: Media Endpoint Discovery.
location-tlv: LLDP-MED Location Type Length Value parameter.
altitude: Altitude parameter.
meters: Specify the altitude in meters.
floors: Specify the altitude in floor.
<v_word11>: Altitude value..

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

lldp med location-tlv civic-addr

Command Syntex

lldp med location-tlv civic-addr { country | state | county | city | district | block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark | additional-info | name | zip-code | building | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code } <v_string250>

Function Description

lldp: LLDP configurations.

Parameter Description

lldp: LLDP configurations.
med: Media Endpoint Discovery.
location-tlv: LLDP-MED Location Type Length Value parameter.
civic-addr: Civic address information and postal information
country: The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.
state: National subdivisions (state, canton, region, province, prefecture).
county: County, parish, gun (Japan), district.
city: City, township, shi (Japan) - Example: Copenhagen.
district: City division, borough, city district, ward, chou (Japan).
block: Neighborhood, block.
street: Street - Example: Poppelvej.
leading-street-direction: Leading street direction - Example: N.
trailing-street-suffix: Trailing street suffix - Example: SW.
street-suffix: Street suffix - Example: Ave, Platz.
house-no: House number - Example: 21.
house-no-suffix: House number suffix - Example: A, 1/2.
landmark: Landmark or vanity address - Example: Columbia University.
additional-info: Additional location info - Example: South Wing.
name: Name (residence and office occupant) - Example: Flemming Jahn.
zip-code: Postal/zip code - Example: 2791.
building: Building (structure) - Example: Low Library.
apartment: Unit (Apartment, suite) - Example: Apt 42.
floor: Floor - Example: 4.
room-number: Room number - Example: 450F.
place-type: Place type - Example: Office.
postal-community-name: Postal community name - Example: Leonia.
p-o-box: Post office box (P.O. BOX) - Example: 12345.
additional-code: Additional code - Example: 1320300003.
<v_string250>: Value for the corresponding selected civic address.

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

lldp med location-tlv elin-addr

Command Syntex

lldp med location-tlv elin-addr <v_word25>

Function Description

lldp: LLDP configurations.

Parameter Description

lldp: LLDP configurations.
med: Media Endpoint Discovery.
location-tlv: LLDP-MED Location Type Length Value parameter.
elin-addr: Emergency Location Identification Number, (e.g. E911 and others), such as defined by TIA or NENA.
<v_word25>: ELIN value

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

lldp med location-tlv latitude

Command Syntex

lldp med location-tlv latitude { north | south } <v_word8>

Function Description

lldp: LLDP configurations.

Parameter Description

lldp: LLDP configurations.
med: Media Endpoint Discovery.
location-tlv: LLDP-MED Location Type Length Value parameter.
latitude: Latitude parameter.
north: Setting latitude direction to north.
south: Setting latitude direction to south.
<v_word8>: Latitude degrees (0.0000-90.0000).

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

lldp med location-tlv longitud

Command Syntex

lldp med location-tlv longitude { west | east } <v_word9>

Function Description

lldp: LLDP configurations.

Parameter Description

lldp: LLDP configurations.
med: Media Endpoint Discovery.
location-tlv: LLDP-MED Location Type Length Value parameter.
longitude: Longitude parameter.
west: Setting longitude direction to west.
east: Setting longitude direction to east.
<v_word9>: Longitude degrees (0.0000-180.0000).

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

lldp med media-vlan policy-list

Command Syntex

lldp med media-vlan policy-list <v_range_list>

Function Description

lldp: LLDP configurations.

Parameter Description

lldp: LLDP configurations.
med: Media Endpoint Discovery.
policy-list: Assignment of policies.
<v_range_list>: Policies to assign to the interface.

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

lldp med media-vlan-policy

Command Syntex

lldp med media-vlan-policy <policy_index> { voice | voice-signaling | guest-voice-signaling | guest-voice | softphone-voice | video-conferencing | streaming-video | video-signaling } { tagged <v_vlan_id> | untagged } [l2-priority <v_0_to_7>] [dscp <v_0_to_63>]

Function Description

lldp: LLDP configurations.

Parameter Description

lldp: LLDP configurations.
med: Media Endpoint Discovery.
media-vlan-policy: Use the media-vlan-policy to create a policy, which can be assigned to an interface.
<policy_index>: Policy id for the policy which is created.
voice: Create a voice policy.
voice-signaling: Create a voice signaling policy.
guest-voice-signaling: Create a guest voice signaling policy.
guest-voice: Create a guest voice policy.
softphone-voice: Create a softphone voice policy.
video-conferencing: Create a video conferencing policy.
streaming-video: Create a streaming video policy.
video-signaling: Create a video signaling policy.
tagged: The policy uses tagged frames.
<v_vlan_id>: The VLAN the policy uses tagged frames.
untagged: The policy uses un-tagged frames.
l2-priority: Layer 2 priority.
<v_0_to_7>: Priority 0-7
dscp: Differentiated Services Code Point.
<v_0_to_63>: DSCP value 0-63.

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

lldp med transmit-tlv

Command Syntex

lldp med transmit-tlv [capabilities] [location] [network-policy]

Function Description

lldp: LLDP configurations.

Parameter Description

lldp: LLDP configurations.
med: Media Endpoint Discovery.
transmit-tlv: LLDP-MED Location Type Length Value parameter.
capabilities: Enable transmission of the optional capabilities TLV.
location: Enable transmission of the optional location TLV.
network-policy: Enable transmission of the optional network-policy TLV.

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

lldp receive

Command Syntex

lldp receive

Function Description

lldp: LLDP configurations.

Parameter Description

lldp: LLDP configurations.
receive: Enable/Disable decoding of received LLDP frames.

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

lldp reinit

Command Syntex

lldp reinit <val>

Function Description

lldp: LLDP configurations.

Parameter Description

lldp: LLDP configurations.
reinit: LLDP tx reinitialization delay in seconds.
<val>: 1-10 seconds.

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

lldp timer

Command Syntex

lldp timer <val>

Function Description

lldp: LLDP configurations.

Parameter Description

lldp: LLDP configurations.
timer: Sets LLDP TX interval (The time between each LLDP frame transmitted in seconds).
<val>: 5-32768 seconds.

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

lldp tlv-select

Command Syntex

lldp tlv-select { management-address | port-description | system-capabilities | system-description | system-name }

Function Description

lldp: LLDP configurations.

Parameter Description

lldp: LLDP configurations.
tlv-select: Which optional TLVs to transmit.
management-address: Enable/Disable transmission of management address.
port-description: Enable/Disable transmission of port description.
system-capabilities: Enable/Disable transmission of system capabilities.
system-description: Enable/Disable transmission of system description.
system-name: Enable/Disable transmission of system name.

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

lldp transmission-delay

Command Syntex

lldp transmission-delay <val>

Function Description

lldp: LLDP configurations.

Parameter Description

lldp: LLDP configurations.
transmission-delay: Sets LLDP transmision-delay. LLDP transmission delay (the amount of time that the transmission of LLDP frames will delayed after LLDP configuration has changed) in seconds.)
<val>: 1-8192 seconds.

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

lldp transmit

Command Syntex

lldp transmit

Function Description

lldp: LLDP configurations.

Parameter Description

lldp: LLDP configurations.
transmit: Enable/Disabled transmision of LLDP frames.

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

location

Command Syntex

location <location>

Function Description

location: Enter terminal location description

Parameter Description

location: Enter terminal location description
<location>: One text line describing the terminal's location in 32 char's

Command Mode/Privilege Level

Command Mode: Line Configuration Mode
Privilege level: 15

Command

logging host

Command Syntex

logging host <v_word45>

Function Description

logging: Syslog

Parameter Description

logging: Syslog
host: host
<v_word45>: Domain name of the log server

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

logging level

Command Syntex

logging level { info | warning | error }

Function Description

logging: Syslog

Parameter Description

logging: Syslog
level: level
info: Information
warning: Warning
error: Error

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

logging on

Command Syntex

logging on

Function Description

logging: Syslog

Parameter Description

logging: Syslog
on: Enable syslog server

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

logout

Command Syntex

logout

Function Description

logout: Exit from EXEC mode

Parameter Description

logout: Exit from EXEC mode

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 0

Command

loop-protect

Command Syntex

loop-protect

Function Description

loop-protect: Loop protection configuration

Parameter Description

loop-protect: Loop protection configuration

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

loop-protect action

Command Syntex

loop-protect action { [shutdown] [log] }

Function Description

loop-protect: Loop protection configuration

Parameter Description

loop-protect: Loop protection configuration
action: Action if loop detected
shutdown: Shutdown port
log: Generate log

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

loop-protect shutdown-time

Command Syntex

loop-protect shutdown-time <t>

Function Description

loop-protect: Loop protection configuration

Parameter Description

loop-protect: Loop protection configuration
shutdown-time: Loop protection shutdown time interval
<t>: Shutdown time in second

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

loop-protect transmit-time

Command Syntex

loop-protect transmit-time <t>

Function Description

loop-protect: Loop protection configuration

Parameter Description

loop-protect: Loop protection configuration
transmit-time: Loop protection transmit time interval
<t>: Transmit time in second

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

loop-protect tx-mode

Command Syntex

loop-protect tx-mode

Function Description

loop-protect: Loop protection configuration

Parameter Description

loop-protect: Loop protection configuration
tx-mode: Actively generate PDUs

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

mac address-table aging-time

Command Syntex

mac address-table aging-time <v_0_10_to_1000000>

Function Description

mac: Mac Address Table

Parameter Description

mac: Mac Address Table
address-table: Mac Address Table
aging-time: Mac address aging time
<v_0_10_to_1000000>: Aging time in seconds, 0 disables aging

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

mac address-table learning

Command Syntex

mac address-table learning [secure]

Function Description

mac: Mac Address Table

Parameter Description

mac: Mac Address Table
address-table: MAC table configuration
learning: Port learning mode
secure: Port Secure mode

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

mac address-table static

Command Syntex

mac address-table static <v_mac_addr> vlan <v_vlan_id> interface <port_type> [<v_port_type_list>]

Function Description

mac: Mac Address Table

Parameter Description

mac: Mac Address Table
address-table: MAC table configuration
static: Static MAC address
<v_mac_addr>: 48 bit MAC address: xx:xx:xx:xx:xx:xx
vlan: VLAN keyword
<v_vlan_id>: VLAN IDs 1-4095
interface: Select an interface to configure
<port_type>: Port type in Fast, Giga or Tengiga ethernet
<v_port_type_list>: List of Port ID, ex, 1/1,3-5;2/2-4,6

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

media-type

Command Syntex

media-type { rj45 | sfp | dual }

Function Description

media-type: Media type.

Parameter Description

media-type: Media type.
rj45: rj45 interface (copper interface).
sfp: sfp interface (fiber interface).
dual: Dual media interface (cu & fiber interface).

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

monitor destination interface

Command Syntex

monitor destination interface

Function Description

monitor: Set monitor configuration.

Parameter Description

monitor: Set monitor configuration.
destination: The destination port. That is the port that trafficed should be mirrored to.
interface: Interface to mirror traffic to.

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

mtu

Command Syntex

mtu <max_length> }

Function Description

mtu: Maximum transmission unit

Parameter Description

mtu: Maximum transmission unit
<max_length>: Maximum frame size in bytes.

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

mvr

Command Syntex

mvr

Function Description

mvr: Multicast VLAN Registration configuration

Parameter Description

mvr: Multicast VLAN Registration configuration

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

mvr immediate-leave

Command Syntex

mvr immediate-leave

Function Description

mvr: Multicast VLAN Registration configuration

Parameter Description

mvr: Multicast VLAN Registration configuration
immediate-leave: Immediate leave configuration

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

mvr name/channel

Command Syntex

mvr name <mvr_name> channel <profile_name>

Function Description

mvr: Multicast VLAN Registration configuration

Parameter Description

mvr: Multicast VLAN Registration configuration
name: MVR multicast name
<mvr_name>: MVR multicast VLAN name
channel: MVR channel configuration
<profile_name>: Profile name in 16 char's

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

mvr name/frame priority

Command Syntex

mvr name <mvr_name> frame priority <cos_priority>

Function Description

mvr: Multicast VLAN Registration configuration

Parameter Description

mvr: Multicast VLAN Registration configuration
name: MVR multicast name
<mvr_name>: MVR multicast VLAN name
frame: MVR control frame in TX
priority: Interface CoS priority
<cos_priority>: CoS priority ranges from 0 to 7

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

mvr name/frame tagged

Command Syntex

mvr name <mvr_name> frame tagged

Function Description

mvr: Multicast VLAN Registration configuration

Parameter Description

mvr: Multicast VLAN Registration configuration
name: MVR multicast name
<mvr_name>: MVR multicast VLAN name
frame: MVR control frame in TX
frame: MVR control frame in TX
tagged: Tagged IGMP/MLD frames will be sent

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

mvr name/igmp-address

Command Syntex

mvr name <mvr_name> igmp-address <v_ipv4_ucast>

Function Description

mvr: Multicast VLAN Registration configuration

Parameter Description

mvr: Multicast VLAN Registration configuration
name: MVR multicast name
<mvr_name>: MVR multicast VLAN name
igmp-address: MVR address configuration used in IGMP
<v_ipv4_ucast>: A valid IPv4 unicast address

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

mvr name/last-member-query-interval

Command Syntex

mvr name <mvr_name> last-member-query-interval <ipmc_lmqi>

Function Description

mvr: Multicast VLAN Registration configuration

Parameter Description

mvr: Multicast VLAN Registration configuration
name: MVR multicast name
<mvr_name>: MVR multicast VLAN name
last-member-query-interval: Last Member Query Interval in tenths of seconds
<ipmc_lmqi>: 0 - 31744 tenths of seconds

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

mvr name/mode

Command Syntex

mvr name <mvr_name> mode { dynamic | compatible }

Function Description

mvr: Multicast VLAN Registration configuration

Parameter Description

mvr: Multicast VLAN Registration configuration
name: MVR multicast name
<mvr_name>: MVR multicast VLAN name
mode: MVR mode of operation
dynamic: Dynamic MVR operation mode
compatible: Compatible MVR operation mode

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

mvr name/type

Command Syntex

mvr name <mvr_name> type { source | receiver }

Function Description

mvr: Multicast VLAN Registration configuration

Parameter Description

mvr: Multicast VLAN Registration configuration
name: MVR multicast name
<mvr_name>: MVR multicast VLAN name
type: MVR port role configuration
source: MVR source port
receiver: MVR receiver port

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

mvr vlan

Command Syntex

mvr vlan <v_vlan_list> [name <mvr_name>]

Function Description

mvr: Multicast VLAN Registration configuration

Parameter Description

mvr: Multicast VLAN Registration configuration
vlan: MVR multicast vlan
<v_vlan_list>: MVR multicast VLAN list
name: MVR multicast name
<mvr_name>: MVR multicast VLAN name

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

mvr vlan/channel

Command Syntex

mvr vlan <v_vlan_list> channel <profile_name>

Function Description

mvr: Multicast VLAN Registration configuration

Parameter Description

mvr: Multicast VLAN Registration configuration
vlan: MVR multicast vlan
<v_vlan_list>: MVR multicast VLAN list
channel: MVR channel configuration
<profile_name>: Profile name in 16 char's

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

mvr vlan/frame priority

Command Syntex

mvr vlan <v_vlan_list> frame priority <cos_priority>

Function Description

mvr: Multicast VLAN Registration configuration

Parameter Description

mvr: Multicast VLAN Registration configuration
vlan: MVR multicast vlan
<v_vlan_list>: MVR multicast VLAN list
frame: MVR control frame in TX
priority: Interface CoS priority
<cos_priority>: CoS priority ranges from 0 to 7

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

mvr vlan/frame tagged

Command Syntex

mvr vlan <v_vlan_list> frame tagged

Function Description

mvr: Multicast VLAN Registration configuration

Parameter Description

mvr: Multicast VLAN Registration configuration
vlan: MVR multicast vlan
<v_vlan_list>: MVR multicast VLAN list
frame: MVR control frame in TX
tagged: Tagged IGMP/MLD frames will be sent

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

mvr vlan/igmp-address

Command Syntex

mvr vlan <v_vlan_list> igmp-address <v_ipv4_ucast>

Function Description

mvr: Multicast VLAN Registration configuration

Parameter Description

mvr: Multicast VLAN Registration configuration
vlan: MVR multicast vlan
<v_vlan_list>: MVR multicast VLAN list
igmp-address: MVR address configuration used in IGMP
<v_ipv4_ucast>: A valid IPv4 unicast address

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

mvr vlan/ last-member-query-interval

Command Syntex

mvr vlan <v_vlan_list> last-member-query-interval <ipmc_lmqi>

Function Description

mvr: Multicast VLAN Registration configuration

Parameter Description

mvr: Multicast VLAN Registration configuration
vlan: MVR multicast vlan
<v_vlan_list>: MVR multicast VLAN list
last-member-query-interval: Last Member Query Interval in tenths of seconds
<ipmc_lmqi>: 0 - 31744 tenths of seconds

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

mvr vlan/ mode

Command Syntex

mvr vlan <v_vlan_list> mode { dynamic | compatible }

Function Description

mvr: Multicast VLAN Registration configuration

Parameter Description

mvr: Multicast VLAN Registration configuration
vlan: MVR multicast vlan
<v_vlan_list>: MVR multicast VLAN list
mode: MVR mode of operation
dynamic: Dynamic MVR operation mode
compatible: Compatible MVR operation mode

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

mvr vlan/type

Command Syntex

mvr vlan <v_vlan_list> type { source | receiver }

Function Description

mvr: Multicast VLAN Registration configuration

Parameter Description

mvr: Multicast VLAN Registration configuration
vlan: MVR multicast vlan
<v_vlan_list>: MVR multicast VLAN list
type: MVR port role configuration
source: MVR source port
receiver: MVR receiver port

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

netbios-name-server

Command Syntex

netbios-name-server <ip> [<ip1> [<ip2> [<ip3>]]]

Function Description

netbios-name-server: NetBIOS (WINS) name servers

Parameter Description

netbios-name-server: NetBIOS (WINS) name servers
<ip>: Server's IP address
<ip1>: Server's IP address
<ip2>: Server's IP address
<ip3>: Server's IP address

Command Mode/Privilege Level

Command Mode: DHCP Pool Configuration Mode
Privilege level: 13

Command

netbios-node-type

Command Syntex

netbios-node-type { b-node | h-node | m-node | p-node }

Function Description

netbios-node-type: NetBIOS node type

Parameter Description

netbios-node-type: NetBIOS node type
b-node: Broadcast node
h-node: Hybrid node
m-node: Mixed node
p-node: Peer-to-peer node

Command Mode/Privilege Level

Command Mode: DHCP Pool Configuration Mode
Privilege level: 13

Command

netbios-scope

Command Syntex

netbios-scope <netbios_scope>

Function Description

netbios-scope: NetBIOS scope

Parameter Description

netbios-scope: NetBIOS scope
<netbios_scope>: Netbios scope identifier, in 128 characters

Command Mode/Privilege Level

Command Mode: DHCP Pool Configuration Mode
Privilege level: 13

Command

network

Command Syntex

network <ip> <subnet_mask>

Function Description

netbios-scope: NetBIOS scope

Parameter Description

network: Network number and mask
<ip>: Network number
<subnet_mask>: Network mask in dotted-decimal notation, excluding 255.255.255.255

Command Mode/Privilege Level

Command Mode: DHCP Pool Configuration Mode
Privilege level: 13

Command

nis-domain-name

Command Syntex

nis-domain-name <domain_name>

Function Description

nis-domain-name: NIS domain name

Parameter Description

nis-domain-name: NIS domain name
<domain_name>: NIS domain name

Command Mode/Privilege Level

Command Mode: DHCP Pool Configuration Mode
Privilege level: 13

Command

nis-server

Command Syntex

nis-server <ip> [<ip1> [<ip2> [<ip3>]]]

Function Description

nis-server: Network information servers

Parameter Description

nis-server: Network information servers
<ip>: Server's IP address
<ip1>: Server's IP address
<ip2>: Server's IP address
<ip3>: Server's IP address

Command Mode/Privilege Level

Command Mode: DHCP Pool Configuration Mode
Privilege level: 13

Command

no

Command Syntex

no

Function Description

no: Negate a command or set its defaults

Parameter Description

no: Negate a command or set its defaults

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

no

Command Syntex

no

Function Description

no: Negate a command or set its defaults

Parameter Description

no: Negate a command or set its defaults

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ntp

Command Syntex

ntp

Function Description

ntp: Configure NTP

Parameter Description

ntp: Configure NTP

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 13

Command

ntp server

Command Syntex

ntp server <index_var> ip-address { <ipv4_var> | <ipv6_var> | <name_var> }

Function Description

ntp: Configure NTP

Parameter Description

ntp: Configure NTP
server: Configure NTP server
<index_var>: index number
ip-address: ip address
<ipv4_var>: ipv4 address
<ipv6_var>: ipv6 address
<name_var>: domain name

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 13

Command

ntp-server

Command Syntex

ntp-server <ip> [<ip1> [<ip2> [<ip3>]]]

Function Description

ntp-server: NTP servers

Parameter Description

ntp-server: NTP servers
<ip>: Server's IP address
<ip1>: Server's IP address
<ip2>: Server's IP address
<ip3>: Server's IP address

Command Mode/Privilege Level

Command Mode: DHCP Pool Configuration Mode
Privilege level: 13

Command

password encrypted

Command Syntex

password encrypted <encry_password>

Function Description

password: Specify the password for the administrator

Parameter Description

password: Specify the password for the administrator
encrypted: Specifies an ENCRYPTED password will follow
<encry_password>: The ENCRYPTED (hidden) user password. Notice the ENCRYPTED password will be decoded by system internally. You cannot directly use it as same as the Plain Text and it is not human-readable text normally.

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

password none

Command Syntex

password none

Function Description

password: Specify the password for the administrator

Parameter Description

password: Specify the password for the administrator
none: NULL password

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

password unencrypted

Command Syntex

password unencrypted <password>

Function Description

password: Specify the password for the administrator

Parameter Description

password: Specify the password for the administrator
unencrypted: Specifies an UNENCRYPTED password will follow
<password>: The UNENCRYPTED (Plain Text) user password. Any printable characters including space is accepted. Notice that you have no change to get the Plain Text password after this command. The system will always display the ENCRYPTED password.

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

ping ip

Command Syntex

ping ip <v_ip_addr> [repeat <count>] [size <size>] [interval <seconds>]

Function Description

ping: Send ICMP echo messages

Parameter Description

ping: Send ICMP echo messages
ip: IP (ICMP) echo
<v_ip_addr>: ICMP destination address
repeat: Specify repeat count
<count>: 1-60; Default is 5
size: Specify datagram size
<size>: 2-1452; Default is 56 (excluding MAC, IP and ICMP headers)
interval: Specify repeat interval
<seconds>: 0-30; Default is 0

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 0

Command

ping ipv6

Command Syntex

ping ipv6 <v_ipv6_addr> [repeat <count>] [size <size>] [interval <seconds>] [interface vlan <v_vlan_id>]

Function Description

ping: Send ICMP echo messages

Parameter Description

ping: Send ICMP echo messages
ipv6: IPv6 (ICMPv6) echo
<v_ipv6_addr>: ICMPv6 destination address
repeat: Specify repeat count
<count>: 1-60; Default is 5
size: Specify datagram size
<size>: 2-1452; Default is 56 (excluding MAC, IP and ICMP headers)
interval: Specify repeat interval
<seconds>: 0-30; Default is 0
interface: Select an interface to configure
vlan: VLAN Interface
<v_vlan_id>: VLAN identifier(s): VID

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 0

Command

poe management mode

Command Syntex

poe management mode { class-consumption | class-reserved-power | allocation-consumption | allocation-reserved-power | lldp-consumption | lldp-reserved-power }

Function Description

poe: Power Over Ethernet.

Parameter Description

poe: Power Over Ethernet.
management: Use management mode to configure PoE power management method.
mode: mode
class-consumption: Max. port power determined by class, and power is managed according to power consumption.
class-reserved-power: Max. port power determined by class, and power is managed according to reserved power.
allocation-consumption: Max. port power determined by allocated, and power is managed according to power consumption.
allocation-reserved-power: Max. port power determined by alocated, and power is managed according to reserved power.
lldp-consumption: Max. port power determined by LLDP Media protocol, and power is managed according to power consumption.
lldp-reserved-power: Max. port power determined by LLDP Media protocol, and power is managed according to reserved power.

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

poe mode

Command Syntex

poe mode { standard | plus }

Function Description

poe: Power Over Ethernet.

Parameter Description

poe: Power Over Ethernet.
mode: PoE mode.
standard: Set mode to PoE (Maximum power 15.4 W)
plus: Set mode to PoE+ (Maximum power 30.0 W)

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

poe power limit

Command Syntex

poe power limit { <v_word9> }

Function Description

poe: Power Over Ethernet.

Parameter Description

poe: Power Over Ethernet.
power: Setting maximum power for port in allocation mode.
limit: The maximum power.
<v_word9>: Maximum power for the interface (0-15.4 Watt for PoE standard mode, 0-30.0 Watt for PoE plus mode)

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

poe priority

Command Syntex

poe priority { low | high | critical }

Function Description

poe: Power Over Ethernet.

Parameter Description

poe: Power Over Ethernet.
priority: Interface priority.
low: Set priority to low.
high: Set priority to high.
critical: Set priority to critical.

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

poe supply sid

Command Syntex

poe supply sid <v_1_to_16> <v_1_to_2000>

Function Description

poe: Power Over Ethernet.

Parameter Description

poe: Power Over Ethernet.
supply: Use poe supply to specify the maximum power the power supply can deliver.
sid: runtime, see poe_icli_functions.c
<v_1_to_16>: runtime, see poe_icli_functions.c
<v_1_to_2000>: Maximum power the power supply can deliver.

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

port-security

Command Syntex

port-security

Function Description

port-security: Enable/disable port security per interface.

Parameter Description

port-security: Enable/disable port security per interface.

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

port-security aging time

Command Syntex

port-security aging time <v_10_to_10000000>

Function Description

port-security: Enable/disable port security per interface.

Parameter Description

port-security: Port security (psec limit)
aging: Time in seconds between check for activity on learned MAC addresses.
time: Time in seconds between check for activity on learned MAC addresses.
<v_10_to_10000000>: seconds

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

port-security maximum

Command Syntex

port-security maximum [<v_1_to_1024>]

Function Description

port-security: Enable/disable port security per interface.

Parameter Description

port-security: Port security (psec limit)
maximum: Miximum number of MAC addresses that can be learned on this set of interfaces.
<v_1_to_1024>: Number of addresses

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

privilege level

Command Syntex

privilege level <privileged_level>

Function Description

privilege: Change privilege level for line

Parameter Description

privilege: Change privilege level for line
level: Assign default privilege level for line
<privileged_level>: Default privilege level for line

Command Mode/Privilege Level

Command Mode: Line Configuration Mode
Privilege level: 15

Command

privilege

Command Syntex

privilege { exec | configure | config-vlan | line | interface | if-vlan | ipmc-profile | snmps-host | stp-aggr | dhcp-pool | rfc2544-profile } level <privilege> <cmd>

Function Description

privilege: Change privilege level for line

Parameter Description

privilege: Change privilege level for line
exec: Exec mode
configure: Global configuration mode
config-vlan: VLAN Configuration Mode
line: Line configuration mode
interface: Port List Interface Mode
if-vlan: VLAN Interface Mode
ipmc-profile: IPMC Profile Mode
snmps-host: SNMP Server Host Mode
stp-aggr: STP Aggregation Mode
dhcp-pool: DHCP Pool Configuration Mode
rfc2544-profile: RFC2544 Profile Mode
level: Set privilege level of command
<privilege>: Privilege level
<cmd>: Initial valid words and literals of the command to modify, in 128 char's

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

pvlan

Command Syntex

pvlan <pvlan_list>

Function Description

pvlan: Private VLAN

Parameter Description

pvlan: Private VLAN
<pvlan_list>: list of PVLANs. Range is from 1 to number of ports.

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 13

Command

pvlan isolation

Command Syntex

pvlan isolation

Function Description

pvlan: Private VLAN

Parameter Description

pvlan: Private VLAN
isolation: Port isolation

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 13

Command

qos cos <cos>

Command Syntex

qos cos <cos>

Function Description

qos: Quality of Service

Parameter Description

qos: Quality of Service
cos: Class of service configuration
<cos>: Specific class of service

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

qos map dscp-cos

Command Syntex

qos map dscp-cos { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } cos <cos> dpl <dpl>

Function Description

qos: Quality of Service

Parameter Description

qos: Quality of Service
map: Global QoS Map/Table
dscp-cos: Map for dscp to cos
<dscp_num>: Specific DSCP or range
be: Default PHB(DSCP 0) for best effort traffic
af11: Assured Forwarding PHB AF11(DSCP 10)
af12: Assured Forwarding PHB AF12(DSCP 12)
af13: Assured Forwarding PHB AF13(DSCP 14)
af21: Assured Forwarding PHB AF21(DSCP 18)
af22: Assured Forwarding PHB AF22(DSCP 20)
af23: Assured Forwarding PHB AF23(DSCP 22)
af31: Assured Forwarding PHB AF31(DSCP 26)
af32: Assured Forwarding PHB AF32(DSCP 28)
af33: Assured Forwarding PHB AF33(DSCP 30)
af41: Assured Forwarding PHB AF41(DSCP 34)
af42: Assured Forwarding PHB AF42(DSCP 36)
af43: Assured Forwarding PHB AF43(DSCP 38)
cs1: Class Selector PHB CS1 precedence 1(DSCP 8)
cs2: Class Selector PHB CS2 precedence 2(DSCP 16)
cs3: Class Selector PHB CS3 precedence 3(DSCP 24)
cs4: Class Selector PHB CS4 precedence 4(DSCP 32)
cs5: Class Selector PHB CS5 precedence 5(DSCP 40)
cs6: Class Selector PHB CS6 precedence 6(DSCP 48)
cs7: Class Selector PHB CS7 precedence 7(DSCP 56)
ef: Expedited Forwarding PHB(DSCP 46)
va: Voice Admit PHB(DSCP 44)
cos: Specify class of service
<cos>: Specific class of service
dpl: Specify drop precedence level
<dpl>: Specific drop precedence level

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

radius-server deadtime

Command Syntex

radius-server deadtime <minutes>

Function Description

radius-server: Configure RADIUS

Parameter Description

radius-server: Configure RADIUS
deadtime: Time to stop using a RADIUS server that doesn't respond
<minutes>: Time in minutes

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

radius-server host

Command Syntex

radius-server host <host_name> [auth-port <auth_port>] [acct-port <acct_port>] [timeout <seconds>] [retransmit <retries>] [key <key>]

Function Description

radius-server: Configure RADIUS

Parameter Description

radius-server: Configure RADIUS
host: Specify a RADIUS server
<host_name>: Hostname or IP address
auth-port: UDP port for RADIUS authentication server
<auth_port>: UDP port number
acct-port: UDP port for RADIUS accounting server
<acct_port>: UDP port number
timeout: Time to wait for this RADIUS server to reply (overrides default)
<seconds>: Wait time in seconds
retransmit: Specify the number of retries to active server (overrides default)
<retries>: Number of retries for a transaction
key: Server specific key (overrides default)
<key>: The shared key

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

radius-server key

Command Syntex

radius-server key <key>

Function Description

radius-server: Configure RADIUS

Parameter Description

radius-server: Configure RADIUS
key: Set RADIUS encryption key
<key>: The shared key

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

radius-server retransmit

Command Syntex

radius-server retransmit <retries>

Function Description

radius-server: Configure RADIUS

Parameter Description

radius-server: Configure RADIUS
retransmit: Specify the number of retries to active server
<retries>: Number of retries for a transaction

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

radius-server timeout

Command Syntex

radius-server timeout <seconds>

Function Description

radius-server: Configure RADIUS

Parameter Description

radius-server: Configure RADIUS
timeout: Time to wait for a RADIUS server to reply
<seconds>: Wait time in seconds

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

range

Command Syntex

range <entry_name> { permit | deny } [log] [next <next_entry>]

Function Description

range: A range of IPv4/IPv6 multicast addresses for the profile

Parameter Description

range: A range of IPv4/IPv6 multicast addresses for the profile
<entry_name>: Range entry name in 16 char's
permit: Permit matching addresses
deny: Deny matching addresses
log: Log when matching
next: Specify next entry used in profile; Default: Add entry last
<next_entry>: Range entry name in 16 char's

Command Mode/Privilege Level

Command Mode: IPMC Profile Mode
Privilege level: 15

Command

reload

Command Syntex

reload { { { cold | warm } [sid <usid>] } | { defaults [keep-ip] } }

Function Description

reload: Reload system.

Parameter Description

reload: Reload system.
cold: Reload cold.
warm: Reload warm (CPU restart only).
sid: Specific stack switch to reload.
<usid>: Stack switch ID.
defaults: Reload defaults without rebooting.
keep-ip: Attempt to keep VLAN1 IP setup.

Command Mode/Privilege Level

Command Mode: User EXEC Mode
Privilege level: 15

Command

rfc2544 profile

Command Syntex

rfc2544 profile <profile_name>

Function Description

rfc2544: RFC2544 performance tests

Parameter Description

rfc2544: RFC2544 performance tests
profile: RFC2544 profile configuration
<profile_name>: Profile name up to 32 characters long

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

rmon alarm

Command Syntex

rmon alarm <id> <oid_str> <interval> { absolute | delta } rising-threshold <rising_threshold> [<rising_event_id>] falling-threshold <falling_threshold> [<falling_event_id>] { [rising | falling | both] }

Function Description

rmon: Remote Monitoring

Parameter Description

rmon: Remote Monitoring
alarm: Configure an RMON alarm
<id>: Alarm entry ID
<oid_str>: MIB object to monitor
<interval>: Sample interval
absolute: Test each sample directly
delta: Test delta between samples
rising-threshold: Configure the rising threshold
<rising_threshold>: rising threshold value
<rising_event_id>: Event to fire on rising threshold crossing
falling-threshold: Configure the falling threshold
<falling_threshold>: falling threshold value
<falling_event_id>: Event to fire on falling threshold crossing
rising: Trigger alarm when the first value is larger than the rising threshold
falling: Trigger alarm when the first value is less than the falling threshold
both: Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default)

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

rmon alarm

Command Syntex

rmon alarm <id> { ifInOctets | ifInUcastPkts | ifInNUcastPkts | ifInDiscards | ifInErrors | ifInUnknownProtos | ifOutOctets | ifOutUcastPkts | ifOutNUcastPkts | ifOutDiscards | ifOutErrors } <ifIndex> <interval> { absolute | delta } rising-threshold <rising_threshold> [<rising_event_id>] falling-threshold <falling_threshold> [<falling_event_id>] { [rising | falling | both] }

Function Description

rmon: Remote Monitoring

Parameter Description

alarm: Configure an RMON alarm
<id>: Alarm entry ID
ifInOctets: The total number of octets received on the interface, including framing characters
ifInUcastPkts: The number of uni-cast packets delivered to a higher-layer protocol
ifInNUcastPkts: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol
ifInDiscards: The number of inbound packets that are discarded even the packets are normal
ifInErrors: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol
ifInUnknownProtos: The number of the inbound packets that were discarded because of the unknown or un-support protocol
ifOutOctets: The number of octets transmitted out of the interface , including framing characters
ifOutUcastPkts: The number of uni-cast packets that request to transmit
ifOutNUcastPkts: The number of broad-cast and multi-cast packets that request to transmit
ifOutDiscards: The number of outbound packets that are discarded event the packets is normal
ifOutErrors: The The number of outbound packets that could not be transmitted because of errors
<ifIndex>: ifIndex
<interval>: Sample interval
absolute: Test each sample directly
delta: Test delta between samples
rising-threshold: Configure the rising threshold
<rising_threshold>: rising threshold value
<rising_event_id>: Event to fire on rising threshold crossing
falling-threshold: Configure the falling threshold
<falling_threshold>: falling threshold value
<falling_event_id>: Event to fire on falling threshold crossing
rising: Trigger alarm when the first value is larger than the rising threshold
falling: Trigger alarm when the first value is less than the falling threshold
both: Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default)

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

rmon collection history

Command Syntex

rmon collection history <id> [buckets <buckets>] [interval <interval>]

Function Description

rmon: Remote Monitoring

Parameter Description

rmon: Configure Remote Monitoring on an interface
collection: Configure Remote Monitoring Collection on an interface
history: Configure history
<id>: History entry ID
buckets: Requested buckets of intervals. Default is 50 buckets
<buckets>: Requested buckets of intervals
interval: Interval to sample data for each bucket. Default is 1800 seconds
<interval>: Interval in seconds to sample data for each bucket

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

rmon collection stats

Command Syntex

rmon collection stats <id>

Function Description

rmon: Remote Monitoring

Parameter Description

rmon: Configure Remote Monitoring on an interface
collection: Configure Remote Monitoring Collection on an interface
stats: Configure statistics
<id>: Statistics entry ID

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

rmon event

Command Syntex

rmon event <id> [log] [trap <community>] { [description <description>] }

Function Description

rmon: Remote Monitoring

Parameter Description

rmon: Configure Remote Monitoring on an interface
event: Configure an RMON event
<id>: Event entry ID
log: Generate RMON log when the event fires
trap: Generate SNMP trap when the event fires
<community>: SNMP community string
description: Specify a description of the event
<description>: Event description

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

sflow

Command Syntex

sflow [<sampler_idx_list>]

Function Description

sflow: Enables/disables flow sampling on this port.

Parameter Description

sflow: Enables/disables flow sampling on this port.
<sampler_idx_list>: Sampler instance

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

sflow agent-ip

Command Syntex

sflow agent-ip { ipv4 <v_ipv4_addr> | ipv6 <v_ipv6_addr> }

Function Description

sflow: Enables/disables flow sampling on this port.

Parameter Description

sflow: Enables/disables flow sampling on this port.
agent-ip: The agent IP address used as agent-address in UDP datagrams. Defaults to IPv4 loopback address.

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

sflow collector-address

Command Syntex

sflow collector-address [receiver <rcvr_idx_list>] [<host_name>]

Function Description

sflow: Enables/disables flow sampling on this port.

Parameter Description

sflow: Enables/disables flow sampling on this port.
collector-address: Collector address
receiver: runtime, see sflow_icli_functions.c
<rcvr_idx_list>: runtime, see sflow_icli_functions.c
<host_name>: runtime, see sflow_icli_functions.c

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

sflow collector-port

Command Syntex

sflow collector-port [receiver <rcvr_idx_list>] <collector_port>

Function Description

sflow: Enables/disables flow sampling on this port.

Parameter Description

sflow: Enables/disables flow sampling on this port.
collector-port: Collector UDP port
receiver: runtime, see sflow_icli_functions.c
<rcvr_idx_list>: runtime, see sflow_icli_functions.c
<collector_port>: Port number

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

sflow counter-poll-interval

Command Syntex

sflow counter-poll-interval [sampler <sampler_idx_list>] [<poll_interval>]

Function Description

sflow: Enables/disables flow sampling on this port.

Parameter Description

sflow: Enables/disables flow sampling on this port.
counter-poll-interval: The interval - in seconds - between counter poller samples.
sampler: sampler
<sampler_idx_list>: Sampler instance
<poll_interval>: seconds

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

sflow max-datagram-size

Command Syntex

sflow max-datagram-size [receiver <rcvr_idx_list>] <datagram_size>

Function Description

sflow: Enables/disables flow sampling on this port.

Parameter Description

sflow: Enables/disables flow sampling on this port.
max-datagram-size: Maximum datagram size.
receiver: receiver
<rcvr_idx_list>: receiver list
<datagram_size>: bytes

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

sflow max-sampling-size

Command Syntex

sflow max-sampling-size [sampler <sampler_idx_list>] [<max_sampling_size>]

Function Description

sflow: Enables/disables flow sampling on this port.

Parameter Description

sflow: Enables/disables flow sampling on this port.
max-sampling-size: Specifies the maximum number of bytes to transmit per flow sample.
sampler: sampler
<sampler_idx_list>: Sampler instance
<max_sampling_size>: bytes

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

sflow sampling-rate

Command Syntex

sflow sampling-rate [sampler <sampler_idx_list>] [<sampling_rate>]

Function Description

sflow: Enables/disables flow sampling on this port.

Parameter Description

sflow: Enables/disables flow sampling on this port.
sampling-rate: Specifies the statistical sampling rate. The sample rate is specified as N to sample 1/Nth of the packets n the monitored flows. There are no restrictions on the value, but the switch will adjust it to the closest possible sampling rate.
sampler: sampler
<sampler_idx_list>: Sampler instance
<sampling_rate>: Sampling rate

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

sflow timeout

Command Syntex

sflow timeout [receiver <rcvr_idx_list>] <timeout>

Function Description

sflow: Enables/disables flow sampling on this port.

Parameter Description

sflow: Enables/disables flow sampling on this port.
timeout: Receiver timeout measured in seconds. The switch decrements the timeout once per second, and as long as it is non-zero, the receiver receives samples. Once the timeout reaches 0, the receiver and all its configuration is reset to defaults.
receiver: runtime, see sflow_icli_functions.c
<rcvr_idx_list>: runtime, see sflow_icli_functions.c
<timeout>: Number of seconds.

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

sflow timeout

Command Syntex

sflow timeout [receiver <rcvr_idx_list>] <timeout>

Function Description

sflow: Enables/disables flow sampling on this port.

Parameter Description

sflow: Enables/disables flow sampling on this port.
timeout: Receiver timeout measured in seconds. The switch decrements the timeout once per second, and as long as it is non-zero, the receiver receives samples. Once the timeout reaches 0, the receiver and all its configuration is reset to defaults.
receiver: runtime, see sflow_icli_functions.c
<rcvr_idx_list>: runtime, see sflow_icli_functions.c
<timeout>: Number of seconds.

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

snmp-server

Command Syntex

snmp-server

Function Description

snmp-server: Enable SNMP server

Parameter Description

snmp-server: Enable SNMP server

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 13

Command

snmp-server access

Command Syntex

snmp-server access <group_name> model { v1 | v2c | v3 | any } level { auth | noauth | priv } [read <view_name>] [write <write_name>]

Function Description

snmp-server: Enable SNMP server

Parameter Description

snmp-server: Enable SNMP server
access: access configuration
<group_name>: group name
model: security model
v1: v1 security model
v2c: v2c security model
v3: v3 security model
any: any security model
level: security level
auth: authNoPriv Security Level
noauth: noAuthNoPriv Security Level
priv: authPriv Security Level
read: specify a read view for the group
<view_name>: read view name
write: specify a write view for the group
<write_name>: write view name

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

snmp-server community v2c

Command Syntex

snmp-server community v2c <comm> [ro | rw]

Function Description

snmp-server: Enable SNMP server

Parameter Description

snmp-server: Enable SNMP server
community: Set the SNMP community
v2c: SNMPv2c
<comm>: Community word
ro: Read only
rw: Read write

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

snmp-server community v3

Command Syntex

snmp-server community v3 <v3_comm> [<v_ipv4_addr> <v_ipv4_netmask>]

Function Description

snmp-server: Enable SNMP server

Parameter Description

snmp-server: Enable SNMP server
community: Set the SNMP community
v3: SNMPv3
<v3_comm>: Community word
<v_ipv4_addr>: IPv4 address
<v_ipv4_netmask>: IPv4 netmask

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

snmp-server contact

Command Syntex

snmp-server contact <v_line255>

Function Description

snmp-server: Enable SNMP server

Parameter Description

snmp-server: Enable SNMP server
contact: Set the SNMP server's contact string
<v_line255>: contact string

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

snmp-server engine-id local

Command Syntex

snmp-server engine-id local <engineID>

Function Description

snmp-server: Enable SNMP server

Parameter Description

snmp-server: Enable SNMP server
engine-id: Set SNMP engine ID
local: Set SNMP local engine ID
<engineID>: local engine ID

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 13

Command

snmp-server host

Command Syntex

snmp-server host <conf_name>

Function Description

snmp-server: Enable SNMP server

Parameter Description

snmp-server: Enable SNMP server
host: Set SNMP host's configurations
<conf_name>: Name of the host configuration

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

snmp-server host/traps

Command Syntex

snmp-server host <conf_name> traps [linkup] [linkdown] [lldp]

Function Description

snmp-server: Enable SNMP server

Parameter Description

snmp-server: Enable SNMP server
host: Set SNMP host's configurations
<conf_name>: Name of the host configuration
traps: Enable traps
linkup: Link up event
linkdown: Link down event
lldp: LLDP event

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

snmp-server location

Command Syntex

snmp-server location <v_line255>

Function Description

snmp-server: Enable SNMP server

Parameter Description

snmp-server: Enable SNMP server
location: Set the SNMP server's location string
<v_line255>: location string

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

snmp-server security-to-group model

Command Syntex

snmp-server security-to-group model { v1 | v2c | v3 } name <security_name> group <group_name>

Function Description

snmp-server: Enable SNMP server

Parameter Description

snmp-server: Enable SNMP server
security-to-group: security-to-group configuration
model: security model
v1: v1 security model
v2c: v2c security model
v3: v3 security model
name: security user
<security_name>: security user name
group: security group
<group_name>: security group name

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

snmp-server trap

Command Syntex

snmp-server trap

Function Description

snmp-server: Enable SNMP server

Parameter Description

snmp-server: Enable SNMP server
trap: Set trap's configurations

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

snmp-server user/engine-id

Command Syntex

snmp-server user <username> engine-id <engineID> [{ md5 <md5_passwd> | sha <sha_passwd> } [priv { des | aes } <priv_passwd>]]

Function Description

snmp-server: Enable SNMP server

Parameter Description

snmp-server: Enable SNMP server
user: Set the SNMPv3 user's configurations
<username>: Username
engine-id: engine ID
<engineID>: Engine ID octet string
md5: Set MD5 protocol
<md5_passwd>: MD5 password
sha: Set SHA protocol
<sha_passwd>: SHA password
priv: Set Privacy
des: Set DES protocol
aes: Set AES protocol
<priv_passwd>: Set privacy password

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

snmp-server version

Command Syntex

snmp-server version { v1 | v2c | v3 }

Function Description

snmp-server: Enable SNMP server

Parameter Description

snmp-server: Enable SNMP server
version: Set the SNMP server's version
v1: SNMPv1
v2c: SNMPv2c
v3SNMPv3

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

snmp-server view

Command Syntex

snmp-server view <view_name> <oid_subtree> { include | exclude }

Function Description

snmp-server: Enable SNMP server

Parameter Description

snmp-server: Enable SNMP server
view: MIB view configuration
<view_name>: MIB view name
<oid_subtree>: MIB view OID
include: Ixcluded type from the view
exclude: Excluded type from the view

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

spanning-tree

Command Syntex

spanning-tree

Function Description

spanning-tree: Enable/disable STP on this interface

Parameter Description

spanning-tree: Enable/disable STP on this interface

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

spanning-tree aggregation

Command Syntex

spanning-tree aggregation

Function Description

spanning-tree: Enable/disable STP on this interface

Parameter Description

spanning-tree: Enable/disable STP on this interface
aggregation: Aggregation mode

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

spanning-tree bpdu-guard

Command Syntex

spanning-tree bpdu-guard

Function Description

spanning-tree: Enable/disable STP on this interface

Parameter Description

spanning-tree: Enable/disable STP on this interface
bpdu-guard: Enable/disable BPDU guard

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

spanning-tree edge

Command Syntex

spanning-tree edge

Function Description

spanning-tree: Enable/disable STP on this interface

Parameter Description

spanning-tree: Enable/disable STP on this interface
edge: Edge port

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

spanning-tree edge bpdu-filter

Command Syntex

spanning-tree edge bpdu-filter

Function Description

spanning-tree: Enable/disable STP on this interface

Parameter Description

spanning-tree: Enable/disable STP on this interface
edge: Edge port
bpdu-filter: Enable BPDU filter (stop BPDU tx/rx)

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

spanning-tree link-type

Command Syntex

spanning-tree link-type { point-to-point | shared | auto }

Function Description

spanning-tree: Enable/disable STP on this interface

Parameter Description

spanning-tree: Enable/disable STP on this interface
link-type: Port link-type
point-to-point: Forced to point-to-point
shared: Forced to Shared
auto: Auto detect

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

spanning-tree mode

Command Syntex

spanning-tree mode { stp | rstp | mstp }

Function Description

spanning-tree: Enable/disable STP on this interface

Parameter Description

spanning-tree: Enable/disable STP on this interface
mode: STP protocol mode
stp: 802.1D Spanning Tree
rstp: Rabid Spanning Tree (802.1w)
mstp: Multiple Spanning Tree (802.1s)

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

spanning-tree mst

Command Syntex

spanning-tree mst <instance> cost { <cost> | auto }

Function Description

spanning-tree: Enable/disable STP on this interface

Parameter Description

spanning-tree: Enable/disable STP on this interface
mst: STP bridge instance
<instance>: instance 0-7 (CIST=0, MST2=1...)
cost: STP Cost of this port
<cost>: Cost range
auto: Use auto cost

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

spanning-tree mst/port-priority

Command Syntex

spanning-tree mst <instance> port-priority <prio>

Function Description

spanning-tree: Enable/disable STP on this interface

Parameter Description

spanning-tree: Enable/disable STP on this interface
mst: STP bridge instance
<instance>: instance 0-7 (CIST=0, MST2=1...)
port-priority: STP priority of this port
<prio>: Range (lower higher priority)

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

spanning-tree mst/priority

Command Syntex

spanning-tree mst <instance> priority <prio>

Function Description

spanning-tree: Enable/disable STP on this interface

Parameter Description

spanning-tree: Enable/disable STP on this interface
mst: STP bridge instance
<instance>: instance 0-7 (CIST=0, MST2=1...)
priority: Priority of the instance
<prio>: Range in seconds

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

spanning-tree mst/vlan

Command Syntex

spanning-tree mst <instance> vlan <v_vlan_list>

Function Description

spanning-tree: Enable/disable STP on this interface

Parameter Description

spanning-tree: Enable/disable STP on this interface
mst: STP bridge instance
<instance>: instance 0-7 (CIST=0, MST2=1...)
vlan: VLAN keyword
<v_vlan_list>: Range of VLANs

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

spanning-tree mst forward-time

Command Syntex

spanning-tree mst forward-time <fwdtime>

Function Description

spanning-tree: Enable/disable STP on this interface

Parameter Description

spanning-tree: Enable/disable STP on this interface
mst: STP bridge instance
forward-time: Delay between port states
<fwdtime>: Range in seconds

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

spanning-tree mst max-hops

Command Syntex

spanning-tree mst max-hops <maxhops>

Function Description

spanning-tree: Enable/disable STP on this interface

Parameter Description

spanning-tree: Enable/disable STP on this interface
mst: STP bridge instance
max-hops: MSTP bridge max hop count
<maxhops>: Hop count range

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

spanning-tree mst name/revision

Command Syntex

spanning-tree mst name <name> revision <v_0_to_65535>

Function Description

spanning-tree: Enable/disable STP on this interface

Parameter Description

spanning-tree: Enable/disable STP on this interface
mst: STP bridge instance
name: Name keyword
<name>: Name of the bridge
revision: Revision keyword
<v_0_to_65535>: Revision number

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

spanning-tree recovery interval

Command Syntex

spanning-tree recovery interval <interval>

Function Description

spanning-tree: Enable/disable STP on this interface

Parameter Description

spanning-tree: Enable/disable STP on this interface
recovery: The error recovery timeout
interval: The interval
<interval>: Range in seconds

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

spanning-tree restricted-role

Command Syntex

spanning-tree restricted-role

Function Description

spanning-tree: Enable/disable STP on this interface

Parameter Description

spanning-tree: Enable/disable STP on this interface
restricted-role: Port role is restricted (never root port)

Command Mode/Privilege Level

Command Mode: STP Aggregation Mode
Privilege level: 15

Command

spanning-tree restricted-tcn

Command Syntex

spanning-tree restricted-tcn

Function Description

spanning-tree: Enable/disable STP on this interface

Parameter Description

spanning-tree: Enable/disable STP on this interface
restricted-tcn: Restrict topology change notifications

Command Mode/Privilege Level

Command Mode: STP Aggregation Mode
Privilege level: 15

Command

spanning-tree transmit hold-count

Command Syntex

spanning-tree transmit hold-count <holdcount>

Function Description

spanning-tree: Enable/disable STP on this interface

Parameter Description

spanning-tree: Enable/disable STP on this interface
transmit: BPDUs to transmit
hold-count: Max number of transmit BPDUs per sec
<holdcount>: 1-10 per sec, 6 is default

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

speed

Command Syntex

speed { 10g | 2500 | 1000 | 100 | 10 | auto { [10] [100] [1000] } }

Function Description

speed: Configures interface speed. If you use 10, 100, or 1000 keywords with the auto keyword the port will only advertise the specified speeds.

Parameter Description

speed: Configures interface speed. If you use 10, 100, or 1000 keywords with the auto keyword the port will only advertise the specified speeds.
10g: 10Gbps
2500: 2.5Gbps
1000: 1Gbps
100: 100Mbps
10: 10Mbps
auto: Auto negotiation
10: 10Mbps
100: 100Mbps
1000: 1Gbps

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

switchport access vlan

Command Syntex

switchport access vlan <pvid>

Function Description

switchport: Set switching mode characteristics

Parameter Description

switchport: Set switching mode characteristics
access: Set access mode characteristics of the interface
vlan: Set VLAN when interface is in access mode
<pvid>: VLAN ID of the VLAN when this port is in access mode

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 13

Command

switchport forbidden vlan

Command Syntex

switchport forbidden vlan { add | remove } <vlan_list>

Function Description

switchport: Set switching mode characteristics

Parameter Description

switchport: Set switching mode characteristics
forbidden: Adds or removes forbidden VLANs from the current list of forbidden VLANs
vlan: Add or modify VLAN entry in forbidden table.
add: Add to existing list.
remove: Remove from existing list.
<vlan_list>: VLAN IDs

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

switchport hybrid acceptable-frame-type

Command Syntex

switchport hybrid acceptable-frame-type { all | tagged | untagged }

Function Description

switchport: Set switching mode characteristics

Parameter Description

switchport: Set switching mode characteristics
hybrid: Set hybrid characteristics of the interface
acceptable-frame-type: Set acceptable frame type on a port
all: Allow all frames
tagged: Allow only tagged frames
untagged: Allow only untagged frames

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 13

Command

switchport hybrid allowed vlan

Command Syntex

switchport hybrid allowed vlan { all | none | [add | remove | except] <vlan_list> }

Function Description

switchport: Set switching mode characteristics

Parameter Description

switchport: Set switching mode characteristics
hybrid: Set hybrid characteristics of the interface
allowed: Set allowed VLAN characteristics when interface is in hybrid mode
vlan: Set allowed VLANs when interface is in hybrid mode
all: All VLANs
none: No VLANs
add: Add VLANs to the current list
remove: Remove VLANs from the current list
except: All VLANs except the following
<vlan_list>: VLAN IDs of the allowed VLANs when this port is in hybrid mode

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 13

Command

switchport hybrid egress-tag

Command Syntex

switchport hybrid egress-tag { none | all [except-native] }

Function Description

switchport: Set switching mode characteristics

Parameter Description

switchport: Set switching mode characteristics
hybrid: Set hybrid characteristics of the interface
egress-tag: Egress VLAN tagging configuration
none: No egress tagging
all: Tag all frames
except-native: Tag all frames except frames classified to native VLAN of the hybrid port

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 13

Command

switchport hybrid ingress-filtering

Command Syntex

switchport hybrid ingress-filtering

Function Description

switchport: Set switching mode characteristics

Parameter Description

switchport: Set switching mode characteristics
hybrid: Set hybrid characteristics of the interface
ingress-filtering: VLAN Ingress filter configuration

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 13

Command

switchport hybrid native vlan

Command Syntex

switchport hybrid native vlan <pvid>

Function Description

switchport: Set switching mode characteristics

Parameter Description

switchport: Set switching mode characteristics
hybrid: Set hybrid characteristics of the interface
native: Set native VLAN
vlan: Set native VLAN when interface is in hybrid mode
<pvid>: VLAN ID of the native VLAN when this port is in hybrid mode

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 13

Command

switchport hybrid port-type

Command Syntex

switchport hybrid port-type { unaware | c-port | s-port | s-custom-port }

Function Description

switchport: Set switching mode characteristics

Parameter Description

switchport: Set switching mode characteristics
hybrid: Set hybrid characteristics of the interface
port-type: Set port type
unaware: Port in not aware of VLAN tags.
c-port: Customer port
s-port: Provider port
s-custom-port: Custom Provider port

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 13

Command

switchport mode

Command Syntex

switchport mode { access | trunk | hybrid }

Function Description

switchport: Set switching mode characteristics

Parameter Description

switchport: Set switching mode characteristics
mode: Set mode of the interface
access: Set mode to ACCESS unconditionally
trunk: Set mode to TRUNK unconditionally
hybrid: Set mode to HYBRID unconditionally

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 13

Command

switchport trunk allowed vlan

Command Syntex

switchport trunk allowed vlan { all | none | [add | remove | except] <vlan_list> }

Function Description

switchport: Set switching mode characteristics

Parameter Description

switchport: Set switching mode characteristics
trunk: Set trunk mode characteristics of the interface
allowed: Set allowed VLAN characteristics when interface is in trunk mode
vlan: Set allowed VLANs when interface is in trunk mode
all: All VLANs
none: No VLANs
add: Add VLANs to the current list
remove: Remove VLANs from the current list
except: All VLANs except the following
<vlan_list>: VLAN IDs of the allowed VLANs when this port is in trunk mode

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 13

Command

switchport trunk native vlan

Command Syntex

switchport trunk native vlan <pvid>

Function Description

switchport: Set switching mode characteristics

Parameter Description

switchport: Set switching mode characteristics
trunk: Set trunk mode characteristics of the interface
native: Set native VLAN
vlan: Set native VLAN when interface is in trunk mode
<pvid>: VLAN ID of the native VLAN when this port is in trunk mode

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 13

Command

switchport trunk vlan tag native

Command Syntex

switchport trunk vlan tag native

Function Description

switchport: Set switching mode characteristics

Parameter Description

switchport: Set switching mode characteristics
trunk: Set trunk mode characteristics of the interface
vlan: Vlan commands
tag: tag parameters
native: tag native vlan

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 13

Command

switchport vlan ip-subnet id

Command Syntex

switchport vlan ip-subnet id <vce_id> <ipv4> vlan <vid>

Function Description

switchport: Set switching mode characteristics

Parameter Description

switchport: Set switching mode characteristics
vlan: VLAN commands
ip-subnet: VCL IP Subnet-based VLAN configuration.
id: id keyword
<vce_id>: Unique VCE ID for each VCL entry (1-128)
<ipv4>: Source IP address and mask (Format: xx.xx.xx.xx/mm.mm.mm.mm).
vlan: vlan keyword
<vid>: VLAN ID required for the group to VLAN mapping (Range: 1-4095)

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 13

Command

switchport vlan mac

Command Syntex

switchport vlan mac <mac_addr> vlan <vid>

Function Description

switchport: Set switching mode characteristics

Parameter Description

switchport: Set switching mode characteristics
vlan: VLAN commands
mac: MAC-based VLAN commands
<mac_addr>: 48 bit unicast MAC address: xx:xx:xx:xx:xx:xx
vlan: vlan keyword
<vid>: VLAN ID required for the group to VLAN mapping (Range: 1-4095)

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 13

Command

switchport vlan protocol gr

Command Syntex

switchport vlan protocol group <grp_id> vlan <vid>

Function Description

switchport: Set switching mode characteristics

Parameter Description

switchport: Set switching mode characteristics
vlan: VLAN commands
protocol: Protocol-based VLAN commands
group: Protocol-based VLAN group commands
<grp_id>: Group Name (Range: 1 - 16 characters)
vlan: vlan keyword
<vid>: VLAN ID required for the group to VLAN mapping (Range: 1-4095)

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 13

Command

switchport voice vlan discovery-protocol

Command Syntex

switchport voice vlan discovery-protocol { oui | lldp | both }

Function Description

switchport: Set switching mode characteristics

Parameter Description

switchport: Set switching mode characteristics
voice: Voice appliance attributes
vlan: Vlan for voice traffic
discovery-protocol: Set Voice VLAN port discovery protocol
oui: Detect telephony device by OUI address
lldp: Detect telephony device by LLDP
both: Detect telephony device by OUI address and LLDP

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

switchport voice vlan mode

Command Syntex

switchport voice vlan mode { auto | force | disable }

Function Description

switchport: Set switching mode characteristics

Parameter Description

switchport: Set switching mode characteristics
voice: Voice appliance attributes
vlan: Vlan for voice traffic
mode: Set Voice VLAN port mode
auto: Enable auto detect mode
force: Force to join Voice VLAN
disable: disjoin Voice VLAN

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

switchport voice vlan security

Command Syntex

switchport voice vlan security

Function Description

switchport: Set switching mode characteristics

Parameter Description

switchport: Set switching mode characteristics
voice: Voice appliance attributes
vlan: Vlan for voice traffic
security: Enable Voice VLAN port security mode

Command Mode/Privilege Level

Command Mode: Port List Interface Mode
Privilege level: 15

Command

tacacs-server deadtime

Command Syntex

tacacs-server deadtime <minutes>

Function Description

tacacs-server: Configure TACACS+

Parameter Description

tacacs-server: Configure TACACS+
deadtime: Time to stop using a TACACS+ server that doesn't respond
<minutes>: Time in minutes

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

tacacs-server host

Command Syntex

tacacs-server host <host_name> [port <port>] [timeout <seconds>] [key <key>]

Function Description

tacacs-server: Configure TACACS+

Parameter Description

tacacs-server: Configure TACACS+
host: Specify a TACACS+ server
<host_name>: Hostname or IP address
port: TCP port for TACACS+ server
<port>: TCP port number
timeout: Time to wait for this TACACS+ server to reply (overrides default)
<seconds>: Wait time in seconds
key: Server specific key (overrides default)
<key>: The shared key

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

tacacs-server key

Command Syntex

tacacs-server key <key>

Function Description

tacacs-server: Configure TACACS+

Parameter Description

tacacs-server: Configure TACACS+
key: Set TACACS+ encryption key
<key>: The shared key

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

tacacs-server timeout

Command Syntex

tacacs-server timeout <seconds>

Function Description

tacacs-server: Configure TACACS+

Parameter Description

tacacs-server: Configure TACACS+
timeout: Time to wait for a TACACS+ server to reply
<seconds>: Wait time in seconds

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

traps

Command Syntex

traps [aaa authentication] [system [coldstart] [warmstart]] [switch [stp] [rmon]]

Function Description

traps: trap event configuration

Parameter Description

traps: trap event configuration
aaa: AAA event group
authentication: Authentication fail event
system: System event group
coldstart: Cold start event
warmstart: Warm start event
switch: Switch event group
stp: STP event
rmon: RMON event

Command Mode/Privilege Level

Command Mode: SNMP Server Host Mode
Privilege level: 15

Command

upnp

Command Syntex

upnp

Function Description

upnp: Set UPnP's configurations

Parameter Description

upnp: Set UPnP's configurations

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

upnp advertising-duration

Command Syntex

upnp advertising-duration <v_100_to_86400>

Function Description

upnp: Set UPnP's configurations

Parameter Description

upnp: Set UPnP's configurations
advertising-duration: Set advertising duration
<v_100_to_86400>: advertising duration

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

upnp ttl

Command Syntex

upnp ttl <v_1_to_255>

Function Description

upnp: Set UPnP's configurations

Parameter Description

upnp: Set UPnP's configurations
ttl: Set TTL value
<v_1_to_255>: TTL value

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

username privilege/password encrypted

Command Syntex

username <username> privilege <priv> password encrypted <encry_password>

Function Description

username: Establish User Name Authentication

Parameter Description

username: Establish User Name Authentication
<username>: User name allows letters, numbers and underscores
privilege: Set user privilege level
<priv>: User privilege level
password: Specify the password for the user
encrypted: Specifies an ENCRYPTED password will follow
<encry_password>: The ENCRYPTED (hidden) user password. Notice the ENCRYPTED password will be decoded by system internally. You cannot directly use it as same as the Plain Text and it is not human-readable text normally.

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

username privilege/password none

Command Syntex

username <username> privilege <priv> password none

Function Description

username: Establish User Name Authentication

Parameter Description

username: Establish User Name Authentication
<username>: User name allows letters, numbers and underscores
privilege: Set user privilege level
<priv>: User privilege level
password: Specify the password for the user
none: NULL password

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

username privilege/password unencrypted

Command Syntex

username <username> privilege <priv> password unencrypted <password>

Function Description

username: Establish User Name Authentication

Parameter Description

username: Establish User Name Authentication
<username>: User name allows letters, numbers and underscores
privilege: Set user privilege level
<priv>: User privilege level
password: Specify the password for the user
unencrypted: Specifies an UNENCRYPTED password will follow
<password>: The UNENCRYPTED (Plain Text) user password. Any printable characters including space is accepted. Notice that you have no chance to get the Plain Text password after this command. The system will always display the ENCRYPTED password.

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

version

Command Syntex

version { v1 [<v1_comm>] | v2 [<v2_comm>] | v3 [probe | engineID <v_word10_to_32>] [<securtyname>] }

Function Description

version: Set SNMP trap version

Parameter Description

version: Set SNMP trap version
v1: SNMP trap version 1
<v1_comm>: SNMP trap community
v2: SNMP trap version 2
<v2_comm>: SNMP trap community
v3: SNMP trap version 3
probe: Probe trap server's engine ID
engineID: Configure trap server's engine ID
<v_word10_to_32>: trap server's engine ID
<securtyname>: seucrity name

Command Mode/Privilege Level

Command Mode: SNMP Server Host Mode
Privilege level: 15

Command

vlan

Command Syntex

vlan <vlist>

Function Description

vlan: VLAN commands

Parameter Description

vlan: VLAN commands
<vlist>: ISL VLAN IDs 1~4095

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

vlan ethertype s-custom-port

Command Syntex

vlan ethertype s-custom-port <etype>

Function Description

vlan: VLAN commands

Parameter Description

vlan: VLAN commands
ethertype: Ether type for Custom S-ports
s-custom-port: Custom S-ports configuration
<etype>: Ethertype (Range: 0x0600-0xffff)

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 13

Command

vlan protocol

Command Syntex

vlan protocol { { eth2 { <etype> | arp | ip | ipx | at } } | { snap { <oui> | rfc-1042 | snap-8021h } <pid> } | { llc <dsap> <ssap> } } group <grp_id>

Function Description

vlan: VLAN commands

Parameter Description

vlan: VLAN commands
protocol: Protocol-based VLAN commands
eth2: Ethernet-based VLAN commands
<etype>: Ether Type(Range: 0x600 - 0xFFFF)
arp: Ether Type is ARP
ip: Ether Type is IP
ipx: Ether Type is IPX
at: Ether Type is AppleTalk
snap: SNAP-based VLAN group
<oui>: SNAP OUI (Range 0x000000 - 0XFFFFFF)
rfc-1042: SNAP OUI is rfc-1042
snap-8021h: SNAP OUI is 8021h
<pid>: PID (Range: 0x0 - 0xFFFF)
llc: LLC-based VLAN group
<dsap>: DSAP (Range: 0x00 - 0xFF)
<ssap>: SSAP (Range: 0x00 - 0xFF)
group: Protocol-based VLAN group commands
<grp_id>: Group Name (Range: 1 - 16 characters)

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 13

Command

voice vlan

Command Syntex

voice vlan

Function Description

voice: Voice appliance attributes

Parameter Description

voice: Voice appliance attributes
vlan: Vlan for voice traffic

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

voice vlan aging-time

Command Syntex

voice vlan aging-time <aging_time>

Function Description

voice: Voice appliance attributes

Parameter Description

voice: Voice appliance attributes
vlan: Vlan for voice traffic
aging-time: Set secure learning aging time
<aging_time>: Aging time, 10-10000000 seconds

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

voice vlan class

Command Syntex

voice vlan class { <traffic_class> | low | normal | medium | high }

Function Description

voice: Voice appliance attributes

Parameter Description

voice: Voice appliance attributes
vlan: Vlan for voice traffic
class: Set traffic class
<traffic_class>: Traffic class value
low: Traffic class low (0)
normal: Traffic class normal (1)
medium: Traffic class medium (2)
high: Traffic class high (3)

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

voice vlan oui

Command Syntex

voice vlan oui <oui> [description <description>]

Function Description

voice: Voice appliance attributes

Parameter Description

voice: Voice appliance attributes
vlan: Vlan for voice traffic
oui: OUI configuration
<oui>: OUI value
description: Set description for the OUI
<description>: Description line

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15

Command

voice vlan oui

Command Syntex

voice vlan vid <vid>

Function Description

voice: Voice appliance attributes

Parameter Description

voice: Voice appliance attributes
vlan: Vlan for voice traffic
vid: Set VLAN ID
<vid>: VLAN ID, 1-4095

Command Mode/Privilege Level

Command Mode: Global Configuration Mode
Privilege level: 15