User Manual

GSW-3208M1/3216M1/3424M1

L2 Managed GbE Switches

CTC UNION TECHNOLOGIES CO., LTD.

CTC Union Technologies Co., Ltd.
Far Eastern Vienna Technology Center (Neihu Technology Park)
8F, No. 60 Zhouzi St.
Neihu District
Taipei 114
Taiwan
Tel: +886-2-26591021
Fax: +886-2-26275211
Email: sales@ctcu.com
URL: http://www.ctcu.com

GSW-3208M1/3216M1/3424M1 User Manual

8+2, 16+2 and 24+4 Gigabit Ethernet Layer 2 Switches w/SNMP

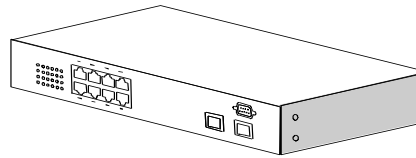
Version 2.0 November 06, 2013 (Updated)

About this manual …

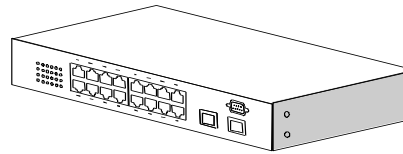
This manual is a general manual for different models of our Gigabit Management Switch. They are similar in operation but have different hardware configurations.

These models are

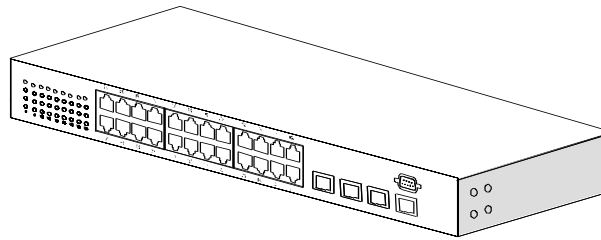
1. **8 * TX + 2 * SFP (10G) ports model**
   This model supports eight TX ports and two extra SFP ports for Gigabit Ethernet connections.



2. **16 * TX + 2 * SFP (18G) ports model**
   This model supports sixteen TX ports and two extra SFP ports for Gigabit Ethernet connections.



3. **24 * TX + 4 * SFP (24G) ports model**
   This model supports twenty-four TX ports and four share SFP ports. Port 21~24 are 1000TX RJ45 port / SFP port optional for Gigabit connection. And they can auto-detect the connection from 1000TX RJ45 port or SFP port.



Contents

1. Introduction

There are three models for the Gigabit Management Switch Series – 8TX+2SFP(10G) model, 16TX+2SFP(18G) model, and 24TX+4SFP(24G) model. This Gigabit Management Switch is a Layer2 Management switch with lots of advanced network functions including VLAN, trunking, spanning tree, mirror port, rate limit, IGMP and port configuration. Console is supported for command-line settings. Web, Telnet, and SNMP interfaces are for remote switch management through network. IEEE 802.1x is supported for port security application. These functions can meet most of the management request for current network.

1.1 Package Contents

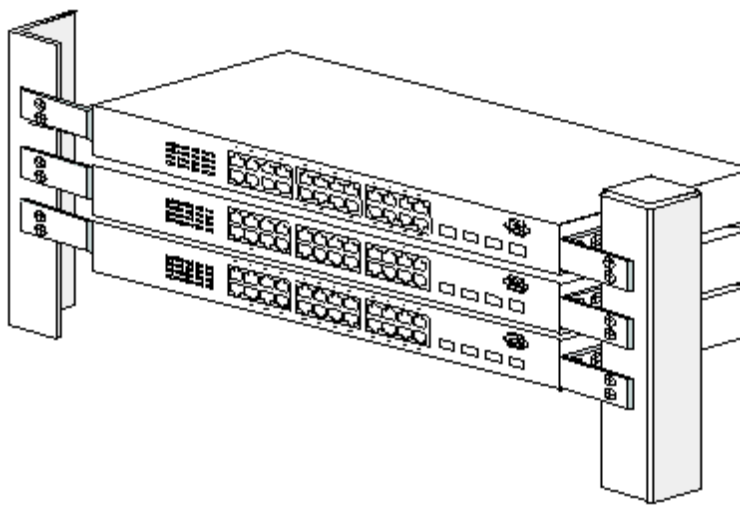
- One Gigabit Management Switch
- One AC power cord (*for AC power model only)
- One console cable
- Two rack-mount kits and screws (*for 24TX+4SFP models only)
- This user's manual

2. Where To Place the Switch

This Switch can be placed on a flat surface (your desk, shelf or table).
Place the Switch at a location with these connection considerations in mind:

- The switch configuration does not break the rules as specified in Section 3.
- The switch is accessible and cables can be connected easily to it.
- The cables connected to the switch are away from sources of electrical interference such as radio, computer monitor, and light fixtures.
- There is sufficient space surrounding the switch to allow for proper ventilation (the switch may not function according to specifications beyond the temperature range of 0 to 50 degrees C).

For 8TX+2SFP/16TX+2SFP/24TX+4SFP model, you can also install the switch on a 19" rack with rack-mount kits as the picture. (Rack-mount kits are option for 8TX+2SFP and 16TX+2SFP models).



<< Rack-Mount Installation >>

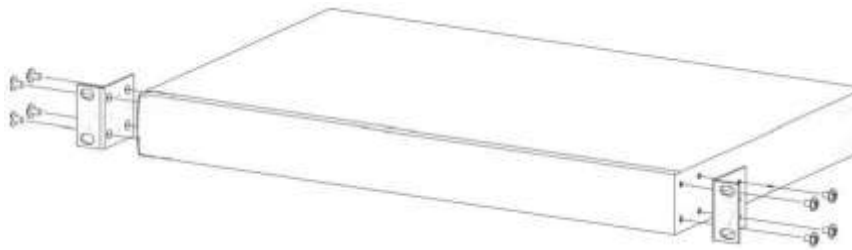
Before rack mounting the switch,please pay attention to the following factors :

1. **Temperature** - Because the temperature in a rack assembly could be higher than the ambient room temperature, check that the rack-environment temperature is within the specified operating temperature range. (Please refer to Product Specifications in the manual.) Air flow is necessary in a rack for temperature stable.
2. **Mechanical Loading** - Do not place any equipment on top of this rack-

mounted switch.

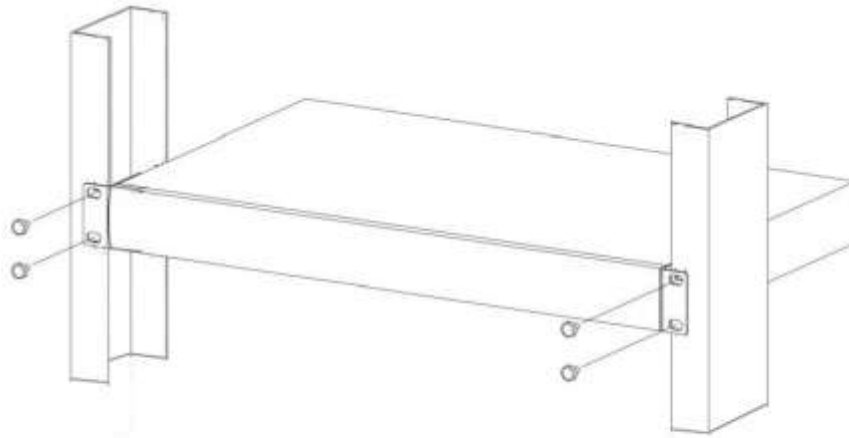
3. **Circuit Overloading** - Be sure that the supply circuit to the rack assembly is not overload after installing this switch.
4. **Grounding** - Rack-mounted equipment should be properly and well grounded. Particular attention should be given to supply connections other than direct connections to the mains.

[Attach Rack-Mount Brackets to the Switch]



1. Position a Rack-Mount Bracket on one side of the Switch.
2. Line up the screw holes on the bracket with the screw holes on the side of the switch.
3. Use a screwdriver to install the M3 flat head screws through the mounting bracket holes into the switch. (There could have two or four screws for one bracket. That depends on the model that installed.)
4. Repeat Step 1~3 to install another bracket to the switch.
5. Now it is ready to mount to a rack.

[Mount the Switch on a Rack]



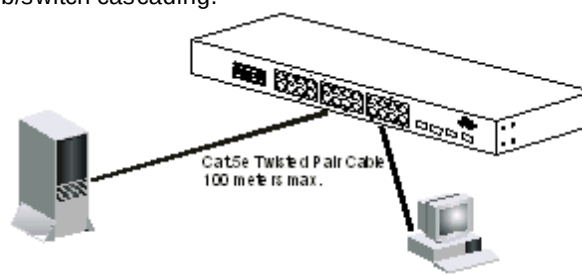
1. Position a bracket that is already attached to the switch on one side of the rack.
2. Line up the screw holes on the bracket with the screw holes on the side of the rack.
3. Use a screwdriver to install the rack screws through the mounting bracket holes into the rack.
4. Repeat Step 1~3 to attach another bracket that is already attached to the switch on another side of the rack.

3. Configure Network Connection

3.1 Connecting Devices to the Switch

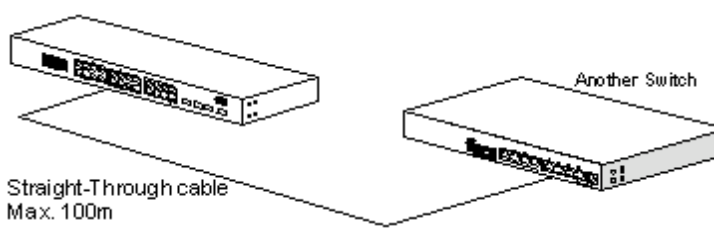
[Connection Guidelines:]

- For 10BaseT connection : Category 3 or 5 twisted-pair Ethernet cable
- For 100BaseTX connection : Category 5 twisted-pair Ethernet cable
- For 1000BaseTX connection: Category 5e or 6 twisted-pair Ethernet cable
- For TX cable connection, always limit the cable distance to 100 meters (328 ft) as defined by IEEE specification
- If your switch has 100/1000BaseSX/LX connections, you can connect long distance fiber optic cable to the switch.
- Because this switch supports **Auto MDI/MDI-X** detection on each TX port, you can use normal straight through cable for both workstation connection and hub/switch cascading.



3.2 Connecting to Another Ethernet Switch/Hub

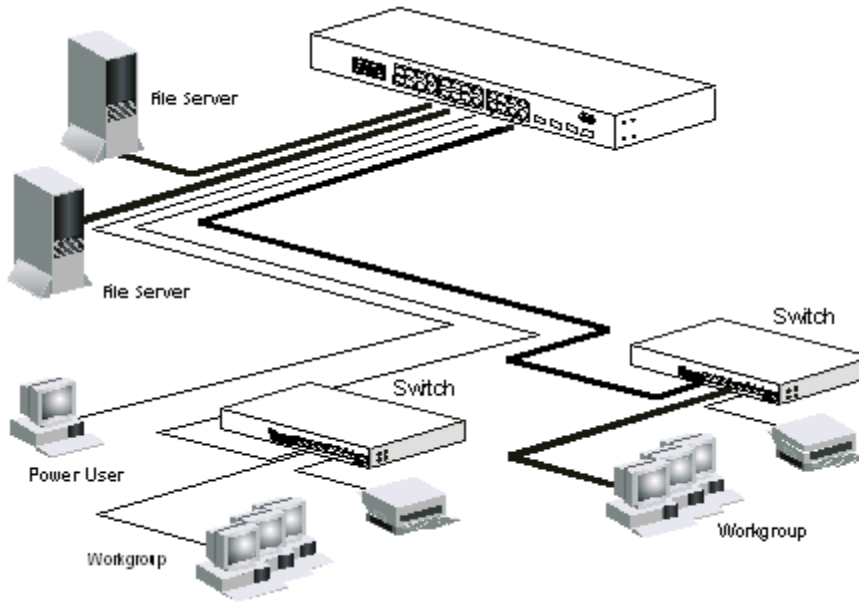
This Switch can be connected to existing 10Mbps / 100Mbps / 1000Mbps hubs/switches. Because all TX ports on the Switch support Auto MDI/MDI-X function, you can connect from any TX port of the Switch to the MDI or MDI-X port of another hub/switch with Straight Through or Crossover cables. If the switches have fiber-optic ports, you can cascade them with fiber optic cable.



3.3 Application

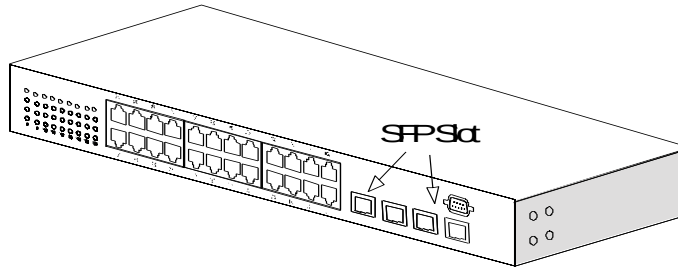
A switch can be used to overcome the hub-to-hub connectivity limitations as well as improve overall network performance. Switches make intelligent decisions about where to send network traffic based on the destination address of the packet. As a result, the switch can significantly reduce unnecessary traffic. The example below demonstrates the switch ability to segment the network. The number of nodes on each segment is reduced thereby minimizing network contention (collisions) and boosting the available bandwidth per port.

With Management function of the switch, network administrator is easy to monitor network status and configure for different applications.



4. Adding Module

This switch supports SFP (for 100/1000SX/LX/… modules) connectors for fiber optic connection. Because the SFP slots support hot-swap function, you can plug/unplug SFP transceiver to/from the SFP slot directly. The switch can auto-detect the fiber optic connection from SFP slot.



Follow the steps for module adding and removing.

[Add SFP Transceiver]

1. Plug in the SFP Transceiver to SFP slot directly.
2. Connect network cable to the SFP Transceiver. If the connected devices are working, the Link/Act LED will be ON.

[Remove SFP Transceiver]

Unplug the SFP Transceiver from SFP slot directly.

5. LEDs Conditions Definition

The LEDs provide useful information about the switch and the status of all individual ports.

[For 8TX+2SFP / 16TX+2SFP / 24TX+4SFP Models]

LED	STATUS	CONDITION
Power	ON	Switch is receiving power.
	OFF	Switch is power OFF.
System	OFF	System is booting.
	Green	System is running.
Link / Act	ON	Port has established a valid link.
	Flashing	Data packets being received or sent.
	Green	The connection speed is 1000Mbps.
	Yellow	The connection speed is 10M or 100Mbps.

6. Manage / Configure the Switch

6.1 Introduction of the management functions

This switch is a L2 Management switch. It supports in-band management function from Http/Telnet/SNMP interfaces. Console is supported for local command-line settings. It supports network configuration functions, like VLAN, Trunking, Port Mirror, QoS, spanning tree and software backup/update. Users can configure these functions for different network applications. The following is a brief introduction about these functions before the detail operation sections.

1. VLAN (Virtual LAN)
   VLAN can divide the switch to several broadcast domains to prevent network traffic between different user groups. This switch supports 802.1Q tag-based VLAN and Port-based VLAN. Users with the same VLAN ID can transfer data to each other. The network traffic will be blocked if they have different VLAN ID. VLAN Stacking function for 802.1Q tag-based VLAN is supported. It allows two VLAN tags in a packet for 802.1Q VLAN tunnelling application through a central network.

2. Trunk
   If two switches are cascaded together, the bottleneck will happen at the cascading connection. If more cables could be used for the cascading connection, it will reduce the bottleneck problem. In normal case, switches will become unstable because of traffic looping when more than one cable is connected between them. If the switches support trunk function, they can treat these cables as one connection between them. The traffic looping will not happen between these cables and the switches will work stable with bigger bandwidth between them.

   Notes: About redundant application
   The trunk connection supports redundant function. If any trunk cable is broken, the traffic going through that cable will be transferred to another trunk cable automatically. For example, if traffic of user port Port 6 is assigned to Port 1 in a Trunk and Port 1 connection breaks, Port 2 will take over the traffic for Port 6 automatically. (It could be used for redundant application.)

3. Spanning Tree Protocol / Rapid Spanning Tree Protocol
   Spanning tree is a protocol to prevent network loop in network topology. If network loop happens, it will cause switches in the network unstable because more and more traffic will loop in the network. If network loop happens, spanning tree protocol will block one connection in the loop

automatically. But it will also cause a period of delay (30 seconds for STP and shorter time for RSTP) if any network connection is changed because of the network topology detection operation of the protocol.
Because there could be more than one switch in the network, users can configure this function for their network spanning tree application.

4. Port Mirror
This switch operates in store-and-forward algorithm so it is not possible to monitor network traffic from another connection port. But the port mirror function can copy packets from some monitored port to another port for network monitor.

5. QoS
For Quality of Service request in a network, packets could be classified to different forwarding priorities. For real-time network traffic (like video, audio), it needs higher priority than normal network traffic. With the definition of packet priority, it could have 8 priority levels (from 0 to 7). This switch supports eight priority level queues on each port. It could be configured for port-based, 802.1P tagged based, or DiffServ of IP packets priority. User can define the mapping of priority values to the priority queues.

6. Static Mac ID in ARL table
The switch can learn the Mac address from user's packets and keep these Mac address in the ARL table for store-and-forward table lookup operation. But these Mac addresses will be deleted from ARL table after some time when users do not send any packets to the switch. This operation is called aging and the time is called aging time. It is about 5 minutes normally (it could be changed by users.) If users want to keep a Mac address always in ARL table on some port, they can assign the Mac address to ARL table. These Mac ID are called Static Mac address. This switch supports static Mac address assignment. *The static Mac address assignment will also limit the Mac address could be used on the assigned port only with the port security configuration function.* For example, assigning "00-00-e2-11-22-33" to Port 5 will always keep this Mac ID alive on Port 5 but also limit this Mac address could work on Port 5 only.

Note: About Static Mac Address Filter-in (port binding) function
There is a Mac Security function for port security. If Mac Table Learning is set to "Secure", only these static Mac addresses can access network through the assigned port. The other Mac addresses will be forbidden for network access through that port. This function can be used for port binding security application. Please refer to Section 6.3 for the details of the Mac address filter-in operation of the switch.

7. Dynamic Mac ID Number Limit

Beside Static Mac ID Limit, there is another Dynamic Mac ID Number Limit function for Mac address security on port. This function can limit the Mac ID number to access network through a port. For example, five Mac ID are allowed for Port 2. That means up to five users are allowed, but don't care who the users are. It is done by "Limit Control" function in "Security - Network" function.

8. IEEE 802.1x Port Security Function

If the 802.1x function is enabled, the switch will act as an authenticator for users accessing network through the switch. It will need a RADIUS server for the authentication function. Users will be asked for username and password before network access. If the RADIUS server authenticates it, the switch will enable the port for network access. This function is very useful for network security application to prevent illegal users access network through the switch.

9. Rate Control

This function can limit the traffic rate for physical ports. The traffic could be ingress traffic or egress traffic. This function can limit the network bandwidth utilization of users.

10. IP Multicast with IGMP Snooping

IP multicast function can forward packets to a group of users connected on different ports. The user group is learned by the switch from packets of IGMP active router with IGMP snooping function. It is often used for video applications

11. MVR (Multicast VLAN Registration)

VLAN function will isolate traffic between VLAN groups. But it will also isolate IP multicast traffic for subscribers in different VLANs. The MVR function allows one multicast VLAN to be shared by subscribers in different VLANs. That can reduce the multicast traffic for VLANs.

12. DHCP Relay & DHCP Option 82

DHCP Relay function will control DHCP requests and forward DHCP requests to the assigned DHCP server. DHCP Option 82 function will add port and switch information to DHCP requests and then send to the assigned DHCP server. Based on those information, DHCP server will assign an IP configuration in the DHCP reply. This is a security function.

13. DHCP Snooping

DHCP Snooping function will assign a trusted port for DHCP server connection, and snoop the DHCP activity between clients and server. This function can prevent illegal DHCP server connection.

14. IP Source Guard

This function can limit the IP address for accessing network from switch port. That can prevent illegal IP problem in network.

15. ACL (Access Control List)

This function is used to define network access control policy - a list of packet filtering rules. The filtering conditions are Layer2 ~ Layer4 - including Mac address, VLAN ID, Ethernet Type, IP address, ARP Packets, ... If conditions are matched, the traffic could be discarded, forwarded, logging or rate limit.

16. LLDP (Link Layer Discover Protocol)

LLDP protocol is used by network devices to advertise their identity, capabilities, and interconnections on a LAN network. This switch can advertise its system information, and show the information of the connected network devices by LLDP protocol.

17. Software Backup/Update

This switch supports backup and update functions for its internal software and its network configuration. It could be done in two ways.

a. From web browser : doing by http protocol and by web browser for run-time code and configuration backup/update.

b. From telnet or console command : doing by tftp protocol for run-time code and configuration backup/update.

6.2 Settings with Console Connection

6.2.1 Basic of the Console Interface

<< Enter Console Interface >>

Please follow the steps to complete the console hardware connection first.

1. Connect from console port of the switch to COM port of PC with the console cable.
2. Start the terminal program of Windows. Create a new connection and select COM port of PC used for the console. Set the configuration of the terminal as **[115200,8,N,1]**. (You can find the terminal program in [Start] -> [Programs] -> [Accessory Programs] -> [Communication] -> [Terminal]. If you cannot find it, please install it from your Windows Installation Disk. Please refer to your Windows user manual for the installation.)
3. Power on the switch.

If everything is correct, the booting screen will appear in the terminal program when the switch is powered on. It will stop at the following screen after some initializing messages.

```
------------------------------------------------------------------------------------------------------------
.....................................................................
.....................................................................


Software Version: 10-P Ver:1.00.00
MAC Address       : 00-00-00-11-22-33
Number of Ports : 10


Username:
------------------------------------------------------------------------------------------------------------
```

<< Previlege Levels for Users >>

There are three previlege levels for users of the switch - administrator, operator, and guest, with previlege level 3, 2, 1. Use “**username**” command in system configure mode under prompt “(config)#” to create users. The system default user is “admin” with password “admin” and previlege level 3.

[administrator level]

The default user name and password is "**admin**" / ”**admin**”. And users with

administrator level could be created with “username” command under “(config)#”. The previlege level is “3” for them.

After login the switch, a prompt “**#**” will be shown. Because this switch supports command-line for console interface, you can press “**?**” to check the command list.
With “**?**” command, you can find the command list as follow.

```
-------------------------------------------------------------------------------------------
# ?
  exit                Exit from current mode
  help                Show available commands
  history             Show a list of previously run commands
  logout              Disconnect
  ping                Ping IPv4 address (ICMPv4 echo) packets to other network nodes
  ping6               Ping IPv6 address (ICMPv6 echo) packets to other network nodes
  quit                Quit commands
  reload              Halts and performs a warm restart
  show                Shows information
  configure           Enter configuration mode
  copy                Copies from one file to another
#
-------------------------------------------------------------------------------------------
```

These are the basic system commands for the switch.

For system configuring, “**configure**” command can enter the configure mode. And the prompt will become ...

```
-------------------------------------------------------------------
# configure
(config)#
-------------------------------------------------------------------
```

In the configure mode, the general configuration of switch can be done. And “exit” command can leave this mode.

If settings for port, “**interface**” command is used. And the prompt will become ...

```
-------------------------------------------------------------------
(config)# interface ethernet 1/5
(config-if)#
-------------------------------------------------------------------
```

“ethernet 1/5” means Ethernet interface 1, port 5. And “exit” command can leave this mode.

“interface” command has another sub-command “**vlan**”. IP address of the

switch can be configured in this mode.

```
-----------------------------------------------------------------
(config)# interface vlan 10
(config-if)#
-----------------------------------------------------------------
```

[operator level]

Users with operator level could be created by administrator with “username” command under “(config)**#**”. The previlege level is “2” for them.

After login the switch, a prompt “**>**” will be shown. Because this switch supports command-line for console interface, you can press “**?**” to check the command list.
With “**?**” command, you can find the command list as follow.

```
-------------------------------------------------------------------------------------------
> ?
  exit                Exit from current mode
  help                Show available commands
  history             Show a list of previously run commands
  logout              Disconnect
  ping                Ping IPv4 address (ICMPv4 echo) packets to other network nodes
  ping6               Ping IPv6 address (ICMPv6 echo) packets to other network nodes
  quit                Quit commands
  reload              Halts and performs a warm restart
  show                Shows information
  copy                Copies from one file to another
>
-------------------------------------------------------------------------------------------
```

These are the basic system commands for the switch.

With operator level, it is allowed to view the switch status and configuration, and run some system maintenance commands.

[guest level]

Users with guest level could be created by administrator with “username” command under “(config)**#**”. The previlege level is “1” for them.

After login the switch, a prompt “**>**” will be shown. With “**?**” command, you can find the command list as follow.

```
-------------------------------------------------------------------------------------------
> ?
```

```
  exit              Exit from current mode
  help              Show available commands
  history           Show a list of previously run commands
  logout            Disconnect
  quit              Quit commands
  show              Show s information
>
```

With guest level, it is allowed to view the switch status and configuration only. No setup/configure commands are supported.

<< Function Keys >>

Here is the function keys for console interface.

[**Tab**] key: this key can help to get the full command keyword with just several beginning letters. For example, "his-Tab" will get the full "history" command word.
[**Esc**] key: this key can use to break message display and go back to command prompt.
[**Up-Arrow**] key: this key can get last input command.
[**Down-Arrow**] key: this key can get next input command.
[**Left-Arrow**]/[**Right-Arrow**] key: the key can move the cursor.
[**Backspace**] key: this key can delete the letter in front of cursor
[**?**] key: this key can get the command list.

<< Command Mode >>

There are four command modes for console interface.

1. General Basic Commands

These are basic commands after login. Users can show switch configuration/status, ping network device, reboot switch, ... The prompt is "**#**" for administrator(users with previlege level 3), and "**>**" for operator(users with previlege level 2) and guest(users with previlege level 1).

2. Configure Mode Commands

With "configure" command, user can enter Configure Mode. Commands in Configuring Mode are for general switch settings. And its prompt is "**(config)#**".

3. Interface Configuring Commands for Port / VLAN Group

If the settings are for ports, it is done with “interface ethernet 1/x” command in configure mode. And the prompt will become “**(config-if)#**”. For example, “interface ethernet 1/5” is for settings on Port 5.

If the settings are for VLAN group, it is done with “interface vlan x” command in configure mode. And the prompt will become “**(config-if)#**”. For example, “interface vlan 100” is for settings on VLAN 100.

4. VLAN Configuring Commands

If the settings are general VLAN settings, it is done with “vlan database” command in configure mode. And its prompt will become “**(config-vlan)#**”.

6.2.2 General Basic Commands

When “admin” / “admin” is used for username/password, the console will enter administrator mode. Enter “?”, command list will be shown.

```
---------------------------------------------------------------------------------------------
# ?
   exit          Exit from current mode
   help          Show available commands
   history       Show a list of previously run commands
   logout        Disconnect
   ping          Ping IPv4 address (ICMPv4 echo) packets to other network nodes
   ping6         Ping IPv6 address (ICMPv6 echo) packets to other network nodes
   quit          Quit commands
   reload        Halts and performs a warm restart
   show          Shows information
   configure     Enter configuration mode
   copy          Copies from one file to another
#
---------------------------------------------------------------------------------------------
```

1. **exit** command
   This command is used to leave current operation mode. It will do logout at this basic command interface.

2. **help** command
   This is a help command and the console will prompt with all available commands.

3. **history** command
   This command will show the history of entering commands.

4. **logout** command
   This is a logout command.

5. **ping** command
   User can use this command to ping another network device to verify the network connection and activity.

Enter “ping ?” at the prompt, the command syntax will be shown.

```
# ping ?
Syntax: ping [-n count] [-l length] [-i ping interval] ip
-n count   : Number of echo requests to send.(1~60)
-l length : Send buffer size, and length (2-1452)
-i          : ping interval (0-30)
ip          : IP address (xxx.xxx.xxx.xxx)
```

For example, “ping 192.168.1.80”.

6. **ping6** command

User can use this command to ping another network device to verify the network connection and activity with IPv6 address.

Enter “ping6 ?” at the prompt, the command syntax will be shown.

```
# ping6 ?
Syntax: ping6 [-n count] [-l length] [-i ping interval] ip
-n count   : Number of echo requests to send.(1~60)
-l length : Send buffer size, and length (2-1452)
-i          : ping interval (0-30)
ip          : IPV6 address For example,fc80::215:c5ff:fe03:4dc7
```

7. **quit** command

This command is used to quit the console interface.

8. **reload** command

This command is used to reset switch. It will halt and perform a warm restart.

Enter “reload” at the prompt, the switch will do warm restart in a fews seconds.

```
# reload
System will reboot in a few seconds
```

9. **show** command

This command is used to show current system information and system configuration.

Enter “show ?” at the prompt, the sub-command list will be shown.

```
# show ?
  aaa                Show AAA service configuration
  acl                Packet Access Control List
  calendar           Date and time information
```

ddmi	Digital Diagnostics Monitoring Interface
dhcp-relay	DHCP Relay Configuration
dot1x	802.1x content
eee	Show eee configuration
history	History information
interface	Interface information
ip	IP information
lacp	LACP statistics
lldp	Show lldp Configuration
log	Log records
loopback-detection	Show loopback detection
mac-address-table	Configuration of the address table
mac-security	MAC Security Configuration
management	Management IP filter
map	Maps priority
mvr	Show MVR Status
ntp	Simple Network Time Protocol configuration
port	Port characteristics
queue	Priority queue information
radius-server	RADIUS server information
running-config	Information on the running configuration
rate-limit	rate-limits
rmon	Rmon
sflow	Sampling flow
snmp	Simple Network Management Protocol statistis
spanning-tree	Spanning-tree configuration
storm-control	Show storm control configuration
system	System information
tacacs-server	TACACS server settings
trunk	Trunk information
users	Show users configuration
version	System hardware and software versions
vlan	Virtual LAN settings

With sub-commands, different configuration settings will be displayed.
More help information for them will be prompted with “show xxxx ?” (xxxx is the sub-command). For example, entering “show port ?” will get the prompt message...

```
# show port ?
  monitor                    Shows the configuration for a mirror port
```

And entering “show port monitor ?” will get next help message...

```
# show port monitor ?
<cr>
```

And entering “show port monitor” will get Port Mirror settings...

```
# show port monitor
```

```
Mirror Configuration:
====================
Mirror Port: Disabled

Port   Mode
----   --------
1      Disabled
2      Disabled
3      Disabled
4      Disabled
5      Disabled
6      Disabled
7      Disabled
8      Disabled
9      Disabled
10     Disabled
CPU    Disabled
```

If the display is more than one console page, “Esc” can be used to break the display.

For the details, please refer to section **6.2.6 Show commands**.

10. **configure** command

This command will change the console interface to configure mode. And the prompt will become “(config)#”. In this mode, administrator can do system configuration of the switch.

The operation of configure mode will be described in next section.

“exit” command can be used to quit this operation mode.

11. **copy** command

This command is used to backup system configuration/firmware to TFTP server, restore system configuration from TFTP server, and update firmware from TFTP server.

```
# copy ?
  config                Copies configuration file
  firmware              Copies run-time firmware
```

copy config running-config tftp <ip address> yyy command is used to backup current switch running configuration to TFTP Server at IP “<ip

address>"(IPv4 or IPv6 address) as file name "yyy" in text format.
copy config tftp running-config <ip address> yyy command is used to restore text configuration file "yyy" from TFTP Server at IP "<ip address>"(IPv4 or IPv6 address).

copy firmware running-firmware tftp <ip address> yyy command is used to backup current running firmware to TFTP Server at IP "<ip address>"(IPv4 or IPv6 address) as file name "yyy" in binary format
copy firmware tftp running-firmware <ip address> yyy command is used to update the running firmware file "yyy" from TFTP Server at IP "<ip address>"(IPv4 or IPv6 address).

6.2.3 Configure Mode Commands

Entering "**configure**" command at console interface, the prompt will become ... "(configure)#".
All the general settings for the switch can be done in this mode.

If the settings are for ports, it is done with "interface" command in configure mode. For example, "interface ethernet 1/5" is for settings on Port 5 and "interface ethernet 1/5,6,10-15" is for settings on Port 5, 6, 10, 11, 12, 13, 14, 15. Please refer to next section for the details of this command.

Enter "?" at the prompt, the sub-command list will be shown.

```
(config)# ?
  exit                 Exit from current mode
  help                 Show available commands
  history              Show a list of previously run commands
  logout               Disconnect
  quit                 Quit commands
  aaa                  AAA Service
  acl                  Access Control List Configuration
  aggregation          Set aggregation mode configuration
  arp-inspection       Set ARP inspection configuration
  default              Restore to factory default setting
  dhcp-relay           Configures DHCP Relay Configuration
  dhcp-snooping        Configures DHCP Snooping Configuration
  dot1x                Configures 802.1x port-based access control
  end                  Exit from configure mode
  hostname             Sets system's network name
  interface            Enters privileged interface configuration
  ip                   Global IP configuration sub commands
  ip-source-guard      IP Source Guard Configuration
  lldp                 LLDP setting
  logging              Modifies message logging facilities
  loopback-detection   Configures loopback detection
  mac-address-table    Configuration of the address table
  mac-security         Configuration of mac security
  management           Specifies management IP filter
  mirror               Configuration of mirror
  mvr                  Multicast VLAN Registration
  no                   Negates a command or sets its defaults
  ntp                  Simple Network Time Protocol configuration
  prompt               Sets system's prompt
```

```
qos                          Configuration of QoS
radius-accounting-server Configures RADIUS Accounting Server
radius-authentication-server Configures RADIUS Authentication Server
rmon                         Configures RMON function
sflow                        Configures sflow function
snmp-server                  Modifies SNMP server parameters
spanning-tree                Configures spanning tree parameters
storm-control                Configures storm control
tacacs-authentication-server Configures TACACS+ Authentication Server
username                     Establishes user name authentication
vlan                         Switch Virtual LAN interface
```

---

1 **exit** command
This command is used to leave current operation mode. Go back to last mode.

2 **help** command
This command is used to show all the available commands in this mode.

3 **history** command
This command is used to show the history of entering commands.

4 **logout** command
This command is used to logout from console interface.

5 **quit** command
This command is used to quit from console interface. It has the same function as logout.

6 **aaa** command
This command is used to set the authentication manner for users of the switch when login by console/telnet/ssh/web. It could be authenticated by local switch, by RADIUS Server, by TACACS+ Server, or no authentication(login is not possible).

Here is the command for the setting.
aaa authentication login console [local|none|radius|tacacs+] command will set the authentication manner for user login from console.

aaa authentication login ssh [local|none|radius|tacacs+] command will set the authentication manner for user login from SSH connection.
aaa authentication login telnet [local|none|radius|tacacs+] command will set the authentication manner for user login from telnet connection.
aaa authentication login web [local|none|radius|tacacs+] command will set the authentication manner for user login from web connection.

And **[local|none|radius|tacacs+]** is authentication method.
- **local**: use the local user database on the switch for authentication.
- **none**: authentication is disabled and login is not possible.
- **radius**: use a remote RADIUS server for authentication.
- **tacacs+**: use a remote TACACS+ server for authentication.

About "**fallback**" sub-command after "radius" and "tacacs+".
Enable fallback to local authentication. If none of the configured authentication servers are alive, the local user database is used for authentication. This is only possible if the Authentication Method is set to a value other than 'none' or 'local'.

RADIUS Server is set by **radius-authentication-server** command for command line interface or set in "AAA" function for web interface.

TACACS+ Server is set by **tacacs-authentication-server** command for command line interface or set in "AAA" function for web interface.

7 **acl** command

This command is used to configure ACL(access control list) function of the switch. For ACL settings, two steps for the settings ...

1). Filtering rule must be defined first. It could be Layer2 ~ Layer4 content of packets - Mac address, VLAN ID, Ethernet Type, IP address, ARP packet, ... Note: More than one filter matching conditions can be set for one rule. And all of these conditions must be matched for this rule to take action.

2). Define the action when packets match the rule - permit or discard or forward to other port, do rate limit, do logging, ...

With "acl ?" command , the sub-commands will be shown.

```
(config)# acl ?
  add                Add or modify Access Control Entry (ACE)
  delete             Delete ACE
  rate-limiter       Rate Limiter Configuration
```

acl add x command can add or modify Access Control Entry (ACE). "**x**" is a

number between 1~256. That is the index of this ACE.
This command will change the prompt to "**(config-ace-x)#**" for ACL setting of this filtering rule. "**x**" is the index number of this rule.

After ACL rules are defined, apply ACL rules to connection ports with "acl" command in port interface configuring mode under prompt "(config-if)#" next.

acl delete x command can delete a Access Control Entry (ACE). "**x**" is a number between 1~256. That is the index of this ACE.

acl rate-limiter x unit kbps rate y
acl rate-limiter x unit pps rate y command can define a rate limiter. Its unit could be by kbps(kilo bit per second) or pps(packet per second). "**x**" is a index number between 1~16 for this rate-limiter. "**y**" is the rate limit number between 0-3276700 for unit pps, or 0, 100, 200, 300, ..., 1000000 for unit kbps.
A rate-limiter can be applied to ACE or port by its index number.

Next, these are the commands for "**acl add x**" command to define a ACL rule - Access Control Entry (ACE). The prompt is "**(config-ace-x)#**"

Enter "?" at the prompt "**(config-ace-x)#**", the commands will be shown.

For example,
(config)# acl add 10
(config-ace-10)# ?

exit	Exit from current mode
help	Show available commands
history	Show a list of previously run commands
logout	Disconnect
quit	Quit commands
action	Specify frames action
destination-mac	Specify destination mac address
frame-type	Select the frame type for this ACE
logging	Specify the logging operation of the ACE
mirror	Specify the mirror operation of the ACE
next_id	Next ACE ID (1-256)
policy	Policy ACE keyword
port	Port list
port-redirect	port copy
rate-limiter	Specify rule's rate
shutdown	Specify the shut down operation of the ACE
source-mac	Specify source mac address
tagged	Specify tagged/untagged frames tagged

tag_prio	VLAN tag priority
vid	Specify vlan id

Here is the details of these sub-commands.

1). **exit** : this command is used to exit the ACL setting.
2). **help** : this command will show all available commands.
3). **history** : this command will list the input command history.
4). **logout** : this command will logout from the command line interface.
5). **quit** : this command will quit from the command line interface.
6). **action** : this command will define the action to premit or deny packets that match this ACL rule.
action permit - The frame that hits this ACE is granted permission for the ACE operation.
action deny - The frame that hits this ACE is dropped.
7). **destination-mac** : this command is used to specify L2 destination Mac address of packet for filter matching.
destination-mac any - No DMAC filter is specified. (DMAC filter status is "don't-care".)
destination-mac xx-xx-xx-xx-xx-xx - Specify the destination MAC filter for this ACE.
8). **frame-type** : this command is used to set Frame Type of packet for filter matching.

```
(config-ace-10)# frame-type ?
  any                 Define Frame to any
  arp                 Define Frame to ARP
  ethernet-type       Ethernet Type: 0x600 - 0xFFFF or 'any' but
excluding 0x800(IPv4) 0x806(ARP) and 0x86DD(IPv6)
  ipv4                Define Frame to IPv4 Frame
```

frame-type any - Any frame can match this ACE.
frame-type arp - Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type.
frame-type ethernet-type - Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal).
frame-type ipv4 - Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type.
9). **logging** : this command is used to specify the logging operation of the ACE. Frames matching the ACE are stored in the System Log. Please note that the System Log memory size and logging rate is limited.
"**logging**" command can enable this function.
10). **mirror** : this command is used to specify the mirror operation of the ACE. Frames matching the ACE are mirrored to the destination mirror port.
"**mirror**" command can enable this function.
11). **next_id** : this command is used to jump to another ACE setting.

"**next_id x**" command can jump to another ACE setting. "**x**" is the ACE index number between 1 to 256.

12). **policy** : this command is used to set the policy number for group of ports to apply this ACE. Policy number of port is defined under port interface prompt with "(config-if)#".

policy y 0xXX command can set a policy number "**y**" (0~255) with bitmask "**0xXX**" (0x00~0xFF). Ports with policy ID in this range will be applied for this ACE.

13). **port** : this command is used to set the ingress ports for which this ACE applies.

port w command can set the ingress Port list for this ACE. "**w**" format is 1/x, 1/x,y,z, 1/x-y, 1/x-y,z for a single port or a group of ports.

14). **port-redirect** : Frames that hit the ACE are redirected to the port number specified here.

port-redirect disable command can disable this function.

port-redirect w command can set the port redirect number. "**w**" format is 1/x, 1/x,y,z, 1/x-y, 1/x-y,z for a single port or a group of ports.

15). **rate-limiter** : Specify the rate limiter for this ACE.

rate-limiter disable command can disable this function.

rate-limiter x command specify the rate limiter for this ACE. "**x**" is the index of rate-limiter with number 1~16.

16). **shutdown** : Specify the port shut down operation of the ACE.

shutdown command can enable this function. If a frame matches the ACE, the ingress port will be disabled.

17). **source-mac** : this command is used to specify L2 source Mac address of packet for filter matching.

source-mac any - No SMAC filter is specified. (SMAC filter status is "don't-care".)

source-mac xx-xx-xx-xx-xx-xx - Specify the source MAC filter for this ACE. A frame that hits this ACE matches this SMAC value.

18). **tagged** : Specify whether frames can hit the action according to the 802.1Q tagged.

tagged any : any value is allowed ("don't-care").

tagged tagged : Tagged frame only.

tagged untagged : Untagged frame only.

19). **tag_prio** : Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority.

tag_prio any : no tag priority is specified (tag priority is "don't-care".)

tag_prio x : A frame that hits this ACE matches this tag priority. "**x**" is the tag priority, allowed number (0~7).

20). **vid** : A frame that hits this ACE matches this VLAN ID value.

vid any : No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".)

vid x : A frame that hits this ACE matches this VLAN ID value. "**x**" is the VLAN ID, allowed number (1~4095).

8 **aggregation** command

This command is used to configure the aggregation hash mode. Frames will go through port in the aggregation connection accroding to the result of hash operation.

aggregation destination_mac_address : The Destination MAC Address can be used to calculate the destination port for the frame.

aggregation ip_address : The IP address can be used to calculate the destination port for the frame.

aggregation source_mac_address : The Source MAC address can be used to calculate the destination port for the frame.

aggregation tcp/udp_port_number : The TCP/UDP port number can be used to calculate the destination port for the frame.

no aggregation : back to default setting.

9 **arp-inspection** command

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

arp-inspection mode command can enable this function. And "**no arp-inspection mode**" can disable it. After enable this function globally, it also need to enable by port with port setup interface under prompt "(config-if)#". Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port.

arp-inspection translation command can translate all dynamic entries to static entries.

Note: Dynamic ARP entry is learned from DHCP request. Before enable ARP Inspection, DHCP Snooping function should be enabled first. Otherwise, static ARP entry should be created for ARP Inspection operation.

10 **default** command

This command is used to restore factory default settings.

default keep-ip command will restore factory default configuration but keep ip address.

11 **dhcp-relay** command

This command is used to configure DHCP Relay function. DHCP Relay is

used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.
The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in stackable switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.
The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address

dhcp-relay information mode command can enable DHCP Option 82 operation. And "**no dhcp-relay information mode**" command can disable it.
When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.
The option 82 circuit ID format as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID(in standalone device it always equal 0, in stackable device it means switch ID). , and the last two characters are the port number. For example, "00030108" means the DHCP message receive form VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal the switch MAC address.

dhcp-relay information policy [drop|keep|replace] command indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' option is invalid when relay information mode is disabled. And "**no dhcp-relay information policy**" command can set it to default. Possible policies are:
drop: Drop the package when a DHCP message that already contains relay information is received.
keep: Keep the original relay information when a DHCP message that already

contains it is received.
replace: Replace the original relay information when a DHCP message that already contains it is received.

dhcp-relay mode command enable the DHCP relay function. And "**no dhcp-relay mode**" command can disable it.
When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.

dhcp-relay server x.x.x.x command can set the DHCP server IP address. "**x.x.x.x**" is the IP address of DHCP server.

dhcp-relay statistics clear command can clear DHCP relay statistics.

12 **dhcp-snooping** command

This command is used to enable DHCP Snooping function. And "**no dhcp-snooping**" command can disable it.

DHCP Snooping is used to block intruder on the untrusted 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.

After DHCP Snooping is enabled, set trusted ports in port configuring interface under prompt "(config-if)#" next. And connect DHCP servers on trusted ports only.

13 **dot1x** command

This command is used configure the general settings of 802.1x function of the switch. Entering "dot1x ?", the sub-commands will be shown.

```
(config)# dot1x ?
  agetime              Time in seconds between check for activity on successfully
authenticated MAC addresses
  eapoltimeout         Set enabledness and parameters of Guest VLAN
  guest_vlan           Max EAP request/identity packet retransmissions
  holdtime             Time in seconds before a MAC-address that failed
authentication gets a new authentication chance
  mode                 Set dot1x enabledness
  radius_qos           Set enabledness of RADIUS-assigned QoS
  radius_vlan          Set enabledness of RADIUS-assigned VLAN
  reauthentication     Set Reauthentication enabledness
  reauthperiod         Set the period between reauthentications
```

dot1x agetime x command is used to set aging time. "**x**" is a number between 10~10000000 in seconds.
This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:
• Single 802.1X
• Multi 802.1X
• MAC-Based Auth.
When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds.
If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries.
For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.
dot1x eapoltimeout x command is used to determine the time for retransmission of Request Identity EAPOL frames. "**x**" is a number between 1~65535 in seconds. This has no effect for MAC-based ports.
dot1x guest_vlan command is used to enable Guest VLAN function. And "**no dot1x guest_vlan**" command is used to disable it. When it is enabled, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. The port setting is configured in port configuring interface under prompt "(config-if)#".
A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. This option is only available for EAPOL-based modes, i.e.:
- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "allow_if_eapol_seen" is disabled.
dot1x guest_vlan vid x command is used to set the VLAN ID of Guest VLAN. "**x**" is a number between 1~4095 for VLAN ID.
dot1x holdtime x command is used to set the Hold Time for 802.1x operation. "**x**" is a number between 10~10000000 for time in seconds.
This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:

• Single 802.1X
• Multi 802.1X
• MAC-Based Auth.

If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified in "AAA") - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication.

In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time.

dot1x mode command is used to eanble 802.1x function. And "**no dot1x mode**" command is used to disable it.

dot1x radius_qos command is used to globally enable RADIUS-server assigning QoS Class functionality. And "**no dot1x radius_qos**" command is used to disable it. When enabled, the individual ports' ditto setting determine whether RADIUS-assigned VLAN is enabled on that port. When disabled, RADIUS-server assigned VLAN is disabled on all ports.

RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature.

dot1x radius_vlan command is used to globally enable RADIUS-server assigned VLAN functionality. And "**no dot1x radius_vlan**" is used to disable it. When enabled, the individual ports' ditto setting determine whether RADIUS-assigned VLAN is enabled on that port. When disabled, RADIUS-server assigned VLAN is disabled on all ports.

RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature.

dot1x reauthentication command is used to enable reauthentication function of 802.1x function. And "**no dot1x reauthentication**" command is used to disable it.

If enabled, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.

For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port.

dot1x reauthperiod x command is used to set the Reauthentication Period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication is enabled. "**x**" is a number in the range 1 to 3600 seconds.

Note:

1. Setting 802.1x function on ports, use “dot1x” command in interface configuring mode.
2. Setting for RADIUS servers, use “radius-accounting-server” and “radius-authentication-server” command.

Please refer to sections for the commands.

14 **end** command

This command is used to exit from configure mode.

15 **hostname** command

This command is used to set the name of the switch in network. This name is also used as the hostname for SNMP agent function of the switch.

16 **interface** command

This command is used to entering **interface configuring mode**. There are two sub-commands for it - one is “ethernet”, it is for port setting, another is “vlan”, it is for VLAN groups characteristics setting.

```
(config)# interface ?
  ethernet        Ethernet port
  vlan            Switch Virtual LAN interface
```

All the port setting commands are put in interface configuring mode - like rate-limit setting, speed-duplex setting, ... And characteristics settings for VLAN groups are also done in interface configuring mode - like IP address assignment.

For example, the console will enter interface configuring mode for Port 5 with “interface ethernet 1/5” command. And the prompt will become ...

```
(config)# interface ethernet 1/5
(config-if)#
```

With “interface ethernet 1/5,6,10-13”, the console will enter interface configuring mode for Port 5, 6, 10, 11, 12, 13. And all the settings will be applied to those ports at the same time.

The description of commands in interface configuring mode is put in Section **6.2.4 Interface Configuring Commands**. Please refer to the section for the details.

17 **ip** command

This command is used to configure some IP-depending functions. Entering "ip ?", the sub-commands will be shown.

```
(config)# ip ?
  default-gateway      Specifies the default gateway
  dns                  Set the DNS server address
  dns-proxy            Setthe IP DNS Proxy mode
  ipv6-default-gateway Specifies the default gateway
  https                HTTPS server configuration
  igmp                 IGMP snooping
  mld                  MLD snooping
  ssh                  Configure ssh server
```

ip default-gateway x.x.x.x command is used to specify the default gateway for IPv4 configuration of the switch. "**x.x.x.x**" is the IP address of the gateway device.

ip ipv6-default-gateway <IPv6 address> is used to specify the default gateway for IPv6 configuration of the switch. "**<IPv6 address>**" is the IP address of the gateway device.

ip dns x.x.x.x command is used to set DNS Server IP address. "**x.x.x.x**" is the IP address.

ip dns-proxy command is used to enable DNS Proxy function. When DNS proxy is enabled, DUT will relay DNS requests to the current configured DNS server on DUT, and reply as a DNS resolver to the client device on the network. "**no dns-proxy**" command is used to disable it.

ip https ... command is used to configure https service of the switch.

Entering "ip https ?", the sub-command will be shown.

```
(config)# ip https ?
  secure-server        Enable secure HTTP server
  automatic-redirect   Automatically redirect web browser to HTTPS
```

ip https secure-server command is used to enable the SSL function of http service (https) of the switch. And **no ip https secure-server** command can be used to disable it.

ip https automatic-redirect command is used to enable HTTPS redirect mode operation. It only significant if HTTPS is enabled.

Automatically redirects web browser to an HTTPS connection when both HTTPS mode and Automatic Redirect are enabled or redirects web browser to an HTTP connection when both are disabled. "**no ip https automatic-redirect**" command can be used to disable it.

ip igmp ... command is used to configure IGMP operation of the switch. Entering "ip igmp snooping ?", the sub-command will be shown.

```
(config)# ip igmp snooping ?
  vlan                 Set Snooping VLAN Configuration
  leave-proxy          Enable  filtering
```

proxy	Set the mode of Proxy
ssm-range	Enable IGMP query function
unregflood	Enable unregister flood function
<cr>	Enable Snooping

ip igmp snooping command is used to enable IGMP function of the switch. And "**no ip igmp snooping**" command can be used to disable it.
ip igmp snooping vlan x ... command is used to configure IGMP settings for the VLAN. "**x**" is VALN ID with number 1~4095.
Entering "ip igmp snooping vlan 10 ?", the sub-command will be shown.
(config)# ip igmp snooping vlan 10 ?

add	Add the snooping VLAN interface
compatibility	Set Compatibility
del	Delete the snooping VLAN interface
parameter-llqi	Set the IPMC Last Listener Query Interval
parameter-qi	Set Query Interval
parameter-qri	Set Query Response Interval
parameter-rv	Set Robustness Variable
parameter-uri	Set Unsolicited Report Interval
querier	Set snooping querier mode for VLAN
state	Set snooping state for VLAN

ip igmp snooping vlan x add command is used to add new IGMP VLAN. The specific IGMP VLAN starts working after the corresponding static VLAN is also created. "**x**" is VALN ID with number 1~4095.
ip igmp snooping vlan x compatibility command is used to set the IGMP operation compatibility mode. Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto.
ip igmp snooping vlan x del command is used to delete a IGMP VLAN. "**x**" is VALN ID with number 1~4095.
ip igmp snooping vlan x parameter-llqi y command is used to set the IPMC Last Listener Query Interval. LLQI (Last Listener Query Interval) is the maximun response time used to calculate the Maximun Respse Code inserted into Specific Queries. It is used to detect the departure of the last listener for a multicast address or source. In IGMP, this term is called LMQI (Last Member Query Interval).
"**x**" is VALN ID with number 1~4095. "**y**" is 0 to 31744 in tenths of seconds.
ip igmp snooping vlan x parameter-qi y command is used to set IGMP Query Interval. The Query Interval is the interval between General Queries sent by the Querier.
"**x**" is VALN ID with number 1~4095. "**y**" is 1 to 31744 in seconds.

ip igmp snooping vlan x parameter-qri y command is used to set IGMP Query Response Interval. Query Response Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.

"**x**" is VALN ID with number 1~4095. "**y**" is 0 to 31744 in tenths of seconds.

ip igmp snooping vlan x parameter-rv y command is use to set Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network.

"**x**" is VALN ID with number 1~4095. "**y**" is 1 to 255 value for Robustness Variable.

ip igmp snooping vlan x parameter-uri y command is used to set Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group.

"**x**" is VALN ID with number 1~4095. "**y**" is 0 to 31744 seconds.

ip igmp snooping vlan x querier command is used to enable IGMP snooping querier operation for the VLAN. And "**no ip igmp snooping vlan x querier**" command is used to disable it.

ip igmp snooping vlan x state command is used to set snooping state for the VLAN.

ip igmp snooping leave-proxy command is used to enable IGMP Leave Proxy. And "**no ip igmp snooping leave-proxy**" command is used to disable it. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

ip igmp snooping proxy command is used to enable IGMP Proxy. And "**no ip igmp snooping proxy**" command is used to disable it. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

ip igmp snooping ssm-range x y command is used to set SSM (Source-Specific Multicast) Range. SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.

"**x**" is prefix. "**y**" is mask with 4~32 for IGMP SSM Range, 8~128 for MLD SSM Range. For example, x/y could be 232.0.0.0/8.

ip igmp snooping unregflood command is used to enable unregistered IPMCv4 traffic flooding. And "**no ip igmp snooping unregflood**" is used to disable it. The flooding control takes effect only when IGMP Snooping is enabled. When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting.

ip mld ... command is used to configure MLD operation of the switch. Entering "ip mld snooping ?", the sub-command will be shown.

```
(config)# ip mld snooping ?
  vlan                  Set Snooping VLAN Configuration
```

leave-proxy	Enable filtering
proxy	Set the mode of Proxy
ssm-range	Enable IGMP query function
unregflood	Enable unregister flood function
<cr>	Enable Snooping

ip mld snooping command is used to enable MLD function of the switch. And "**no ip mld snooping**" command can be used to disable it.

ip mld snooping vlan x ... command is used to configure MLD settings for the VLAN. "**x**" is VALN ID with number 1~4095.

Entering "ip mld snooping vlan 10 ?", the sub-command will be shown.

(config)# ip mld snooping vlan 10 ?

add	Add the snooping VLAN interface
compatibility	Set Compatibility
del	Delete the snooping VLAN interface
parameter-llqi	Set the IPMC Last Listener Query Interval
parameter-qi	Set Query Interval
parameter-qri	Set Query Response Interval
parameter-rv	Set Robustness Variable
parameter-uri	Set Unsolicited Report Interval
querier	Set snooping querier mode for VLAN
state	Set snooping state for VLAN

ip mld snooping vlan x add command is used to add new MLD VLAN. The specific MLD VLAN starts working after the corresponding static VLAN is also created. "**x**" is VALN ID with number 1~4095.

ip mld snooping vlan x compatibility command is used to set the MLD operation compatibility mode. Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selection is MLD-Auto, Forced MLDv1, Forced MLDv2, default compatibility value is MLD-Auto.

ip mld snooping vlan x del command is used to delete a MLD VLAN. "**x**" is VALN ID with number 1~4095.

ip mld snooping vlan x parameter-llqi y command is used to set the IPMC Last Listener Query Interval. LLQI (Last Listener Query Interval) is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages.

"**x**" is VALN ID with number 1~4095. "**y**" is 0 to 31744 in tenths of seconds.

ip mld snooping vlan x parameter-qi y command is used to set the Query Interval. The Query Interval is the interval between General Queries sent

by the Querier.
"**x**" is VALN ID with number 1~4095. "**y**" is 1 to 31744 in seconds.
ip mld snooping vlan x parameter-qri y command is used to set Query Response Interval. Query Response Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.
"**x**" is VALN ID with number 1~4095. "**y**" is 0 to 31744 in tenths of seconds.
ip mld snooping vlan x parameter-rv y command is use to set Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network.
"**x**" is VALN ID with number 1~4095. "**y**" is 1 to 255 value for Robustness Variable.
ip mld snooping vlan x parameter-uri y command is used to set Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address.
"**x**" is VALN ID with number 1~4095. "**y**" is 0 to 31744 seconds.
ip mld snooping vlan x querier command is used to enable MLD snooping querier operation for the VLAN. And "**no ip mld snooping vlan x querier**" command is used to disable it.
ip mld snooping vlan x state command is used to set snooping state for the VLAN.

ip mld snooping leave-proxy command is used to enable MLD Leave Proxy. And "**no ip mld snooping leave-proxy**" command is used to disable it. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
ip mld snooping proxy command is used to enable MLD Proxy. And "**no ip mld snooping proxy**" command is used to disable it. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.
ip mld snooping ssm-range x y command is used to set SSM (Source-Specific Multicast) Range. SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.
"**x**" is prefix. "**y**" is mask with 4~32 for IGMP SSM Range, 8~128 for MLD SSM Range. For example, x/y could be ff3e::/96.
ip mld snooping unregflood command is used to enable unregistered IPMCv6 traffic flooding. And "**no ip mld snooping unregflood**" is used to disable it. The flooding control takes effect only when MLD Snooping is enabled. When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.

ip ssh server command is used to enable SSH function. And "**no ip ssh**

server" command is used to disable it.
SSH is an acronym for Secure SHell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality.

18 **ip-source-guard** command

This command is used to configure IP security function. IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

Note: Dynamic IP Source entry is learned from DHCP request. Before enable IP Source Guard, DHCP Snooping function should be enabled first. Otherwise, static IP Source entry should be created for IP Source Guard operation.

ip-source-guard mode command is used to enable this function globally. And "**no ip-source-guard mode**" is used to disable it globally.
Enabling IP Source Guard on ports is done in port interface configuring mode under prompt "(config-if)#". Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.
ip-source-guard translation command is used to translate all dynamic entries to static entries.

19 **lldp** command

This command is used to configure LLDP function globally. LLDP is an IEEE 802.1ab standard protocol. The Link Layer Discovery Protocol(LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

Entering “lldp ?”, the commands will be listed.

```
(config)# lldp ?
  interval          Specify transmit interval
  tx-hold           Specify hold time multiplier
  tx-delay          Specify delay interval
  reinit-delay      Specify reinit delay
```

lldp interval x command is used to specify transmit interval. The switch periodically transmits LLDP frames to its neighbours for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. “**x**” is the Tx Interval. Valid values are restricted to 5 - 32768 seconds.

lldp tx-hold x command is used to specify hold time multiplier. Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. “**x**” is the Tx hold time multiplier. Valid values are restricted to 2 - 10 times.

lldp tx-delay x command is used to specify delay interval. If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value. “**x**” is the Tx delay Interval. Valid values are restricted to 1 - 8192 seconds.

lldp reinit-delay x command is used to specify reinit delay. When a port is disabled, LLDP is disabled or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, signalling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. “**x**” is the Tx reinit delay. Valid values are restricted to 1 - 10 seconds.

LLDP function is enabled/disabled by port. Information that are carried is also configured by port. It is done in port interface configuring mode under “(config-if)#” prompt.

20 **logging** command

This command is used to configure remote logging function of the switch. When the operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist.

Entering “logging ?”, the sub-commands will be shown.

```
(config)# logging ?
```

log-level	Log level
remote-log	Enable logging to remote host
clear	Clear logging table information

logging log-level x command is used define the log level of events. Indicates what kind of message will send to syslog server. Possible modes are:
0: Info - Send informations, warnings and errors.
1: Warning - Send warnings and errors.
2: Error - Send errors.
The valid value of "**x**" is 0~2.
logging remote-log command is used to configure remote logging function. Entering "logging remote-log ?", the sub-commands will be shown.

```
(config)# logging remote-log ?
  <1-1>                Index
  <cr>
```

logging remote-log command is used to enable the remote logging function. Events will be sent to syslog servers. **no logging remote-log** command is used to disable it.

logging remote-log x host y.y.y.y command is used to set IP address (y.y.y.y) to syslog server index x. One (**x**=1) syslog servers are supported. "**y.y.y.y**" is the IPv4 host address of syslog server. If the switch provides DNS feature, it also can be a host name.

logging clear command is used to clear logging table information.
Entering "logging clear ?", the sub-commands will be shown.

```
(config)# logging clear ?
  <0-2>                Logging level
  <cr>                 All
```

logging clear x command is used to clear level "**x**" logging table information. "**x**" is the logging level with value 0~2.
0: Info - informations, warnings and errors.
1: Warning - warnings and errors.
2: Error - errors.
logging clear command is used to clear all logging table information.

21 **loopback-detection** command

This command is used to configure loopback detection and protection function of the switch globally. If loopback happens on any switch port, packet storm could cause the switch fail to work. With this loopback detection and protection function, port will be shutdown if loopback happens on it. To implement this function, a loop protection PDU will be sent on each port.
Entering "loopback-detection ?", the sub-commands will be shown.

```
(config)# loopback-detection ?
```

mode	Set the Loop Protection to be enabled
shutdown	Set or show the Loop Protection shutdown time
transmit	Set the Loop Protection transmit interval

loopback-detection mode command is used to enable this function globally. And "**no loopback-detection mode**" command is used to disable it globally. Only both loopback-detection function are enabled globally and by port, this function starts to work on those ports.

loopback-detection shutdown x command is used to configure the shoutdown time for those ports that loopback happens on them. That is the period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port).

"**x**" is the shutdown time. Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart).

loopback-detection transmit x command is used to configure the interval between each loop protection PDU sent on each port.

"**x**" is the transmit interval. Valid values are 1 to 10 seconds.

Loopback detection function is also needed to be configured by port. That is done in port configuring interface under prompt "(config-if)#".

22 **mac-address-table** command

This command is used to configure functions for Mac address table of the switch. Entering "mac-address-table ?", the sub-commands will be shown.

```
(config)# mac-address-table ?
  aging-time        Aging time for entries in the address table
  static            Sets MAC address table static information
```

mac-address-table aging-time x command is used to set to aging time of the switch. The valid value of "**x**"(aging time in seconds) is 10-1000000.

mac-address-table aging-time disable command is used to disable the aging operation.

mac-address-table static x-x-x-x-x-x vlan y interface ethernet 1/z command is used to assign a static Mac address "**x-x-x-x-x-x**" to Port "**z**" in VLAN "**y**" of the switch. The static mac address will not be aging out by the switch. The static MAC table can contain 64 entries.

23 **mac-security** command

This command is used to configure the Port Security Limit Control system settings. Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of

the four different actions - None, Trap, Shutdown, Trap & Shutdown.
The Limit Control module utilizes a lower-layer module, Port Security module, which manages MAC addresses learnt on the port.

mac-security aging x command is used to configure the aging time of secured mac address. If the Aging is enabled, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.
"**x**" is the Aging Period and can be set to a number between 10 and 10,000,000 seconds.
To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

mac-security mode command is used to enable the Port Security Limit Control function globally. And "**no mac-security mode**" command is used to disable it. Only both Port Security Limit Control function is enabled globally and by port. It will start to work on those enabled ports.

Port Security Limit Control function is also needed to be configured by port. That is done in port configuring interface under prompt "(config-if)#".

24 **management** command

This command is used to setup the management interface security function. The management interface security function can limit the IP address range / remote interfaces(http,telnet,snmp) for management from network. Different administrators could have different rights to manage this switch. This is for security of this switch management. (Sixteen rules are supported for this function.)

Entering "management ?", the sub-commands will be shown.

```
(config)# management ?
  <1-16>                access id
  enable                Enable the management security function
```

```
(config)# management 1 ?
  ipaddr              Set IP and net mask for a specified set
  protocol            Set protocol for a specified set
```

management enable command is used to enable the management security function. And "**no management enable**" command is used to disable it.

management x ipaddr y.y.y.y z.z.z.z command is used to set the IP address range allowed for this rule. "**x**" is the index of the rule. **y.y.y.y** is the start IP address. **z.z.z.z** is the end IP address. Users in this IP address range will follow this rule for switch management.
management x protocol [http/https | snmp | telnet/ssh] command is used to enable the remote management network protocol for this rule. "**x**" is the index of the rule.

Use "**management x ipaddr y.y.y.y z.z.z.z**" command to create a rule first. Then use "**management x protocol y**" command to assign allowed network protocol for the rule.

no management x command is used to delete a rule that is indexed with "**x**".

25 **mirror** command

This command is used to enable mirror function of the switch. And **no mirror** command can be used to disable mirror function of the switch.

26 **mvr** command

This command is used to configure MVR (Multicast VLAN Registration) function. VLAN function will isolate traffic between VLAN groups. But it will also isolate IP multicast traffic for subscribers in different VLANs. The MVR function allows one multicast VLAN to be shared by subscribers in different VLANs. That can reduce the multicast traffic for VLANs. The MVR feature enables multicast traffic forwarding on the Multicast VLANs. In a multicast television application, a PC or a network television or a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP/MLD report message to Switch A to join the appropriate multicast group address. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.
It is allowed to create at maximum 8 MVR VLANs with corresponding channel settings for each Multicast VLAN. There will be totally at maximum 256 group addresses for channel settings.

** Before configuring MVR function, complete the VLAN setting first
** Using MVR function, you have to enable IGMP snooping function first.

This switch supports eight MVR VLANs. They are referred with their VLAN ID. For any MVR setting, you have to assign the VLAN ID in the command.

Entering "mvr ?", the sub-commands will be shown.

```
(config)# mvr ?
  <1-4095>          Create MVR Multicast VLAN and paramters
  Enabled           Enable the Global MVR
```

mvr enable command is used to enable MVR function. And "**no mvr enable**" command is used to disable it.

Entering "mvr x ?", the sub-commands will be shown. "x" is a VLAN ID with number in 1~4095. For example, "mvr 10 ?".

```
(config)# mvr 10 ?
  llqi          Define the maximun time to wait for IGMP/MLD report memberships on a
                  receiver port before removing the port from multicast group membership
  group         Create a multicast group for MVR VLAN
  mode          Specify the MVR mode of operation
  name          MVR Name is an optional attribute to indicate the name of the specific MVR
                  VLAN
  priority      Specify how the traversed IGMP/MLD control frames will be sent in
                  prioritized manner
  status-clear  Clear MVR operational status
  tagging       Specify whether the traversed IGMP/MLD control frames will be sent as
                  Untagged or Tagged with MVR VID
```

mvr x llqi y command is used to define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. LLQI (Last Listener Query Interval) is the maximun response time used to calculate the Maximun Respse Code inserted into Specific Queries. It is used to detect the departure of the last listener for a multicast address or source. In IGMP, this term is called LMQI (Last Member Query Interval). "**x**" is the Multicast VLAN ID. "**y**" is the time with value in units of tenths of a seconds. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second.

mvr x group yyy start-address <starting IPv4/IPv6 Multicast Group Address> end-address <ending IPv4/IPv6 Multicast Group Address> command is used to create a multicast group for MVR VLAN. "**x**" is the Multicast VLAN ID. "**yyy**" is the name of the Channel of the specific Multicast VLAN. Maximum length of the Channel Name string is 32. Channel Name can only contain alphabets or numbers. Channel name should contain at least one alphabet. And "**no mvr x group**" command is used to delete the channels for Multicast VLAN x. "**x**" is the Multicast VLAN ID.

After MVR VLAN is created, you can assign IP multicast groups (video channels) to the MVR VLAN. And you can assign more than one IP multicast groups (video channels) to one MVR VLAN. For example, "mvr 10 group abc start-address 224.0.0.1 end-address 224.0.0.2".

mvr x mode [compatible | dynamic] command is used to specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports. "**x**" is the Multicast VLAN ID.

mvr x name yyy command is used to create a name for MItuicast VLAN. "**x**" is the Multicast VLAN ID. "**yyy**" is the name of the MVR VLAN. MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 32. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet.

mvr x priority y command is used to specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. "**x**" is the Multicast VLAN ID. "**y**" is the priority with value 0~7.

mvr x status-clear command is used to clear MVR operational status and statistics for MItuicast VLAN "x". "**x**" is the Multicast VLAN ID.

mvr x tagging [tagged | untagged] command is used to specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. "**x**" is the Multicast VLAN ID.

mvr x name yyy command is used to create a MVR VLAN with VLAN ID "**x**" name "**yyy**". "**no mvr x**" command is used to delete a MVR VLAN. "**x**" is the Multicast VLAN ID.

After MVR VLAN is created, source port of IP multicast traffic and receiver ports of subscribers will be assigned next. Assigning source port and receiver port to MVR VLAN is done in "(config-if)#" mode (go with "interface ethernet 1/x" command. "x" is the port number.) Please refer to "mvr" command in Section 6.2.4.1 for the details.

27 **no** command

This command is used to disable a function or restore a setting to factory default of the switch.

```
(config)# no ?
  aaa                AAA Service
  aggregation        Set aggregation mode configuration
  arp-inspection     Set ARP inspection configuration
  dhcp-relay         Configures DHCP Relay Configuration
  dhcp-snooping      Configures DHCP Snooping Configuration
  dot1x              Configures 802.1x port-based access control
```

```
hostname                Sets system's network name
ip                      Global IP configuration sub commands
ip-source-guard         IP Source Guard Configuration
lldp                    LLDP setting
logging                 Modifies message logging facilities
loopback-detection      Configures loopback detection
mac-address-table       Configuration of the address table
mac-security            Configuration of mac security
management              Specifies management IP filter
mirror                  Configuration of mirror
mvr                     Multicast VLAN Registration
ntp                     Simple Network Time Protocol configuration
prompt                  Sets system's prompt
qos                     Configuration of QoS
radius-accounting-server Configures login to RADIUS server
radius-authentication-server Configures login to RADIUS server
rmon                    Configures RMON function
sflow                   Configures sflow function
snmp-server             Modifies SNMP server parameters
spanning-tree           Configures spanning tree parameters
storm-control           Configures TACACS+ Authentication Server
tacacs-authentication-server Configures TACACS+ Authentication Server
username                Sets system's network name
voice-vlan              Voice VLAN Configuration
```

For example,
"**mirror**" command can enable the mirror function and "**no mirror**" command can disable it.
"**ip default-gateway 192.168.1.100**" will set the IP gateway of the switch to 192.168.1.100, and "**no ip default-gateway**" will put it to factory default setting.

28 **ntp** command

This command is used to configure NTP protocol of the switch.
Entering "ntp ?", the sub-commands will be shown.

```
(config)# ntp ?
  client                Accepts time from specified time server
  server                Specified one time server
  zone                  Set time zone
  zone-acronym          Set time zone acronym
  dst                   Config daylight saving time function.
  dst-start-time        Set start time of daylight saving time
  dst-end-time          Set end time of daylight saving time
  dst-offset            Enter the number of minutes to add during Daylight Saving Time
```

ntp client command is used to enable NTP protocol. And **no ntp client** command can be used to disable it.

ntp server x <IP address> command is used to set the IP address of network time server for NTP protocol operation. Up to five time servers is supported. "**x**" is the index(1~5) of time servers. **<IP address>** provides the IPv4 or IPv6 address of a NTP server.

ntp zone x command is used to set the time zone offset. "**x**" is the System Timezone Offset with value -7200~7201 in minutes.

ntp zone-acronym xxx command is used to set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range : Up to 16 alpha-numeric characters and can contain '-', '_' or '.')

ntp dst [disable | non-recurring | recurring] command is used set Daylight Saving Time function operation mode. Daylight Saving Time function will set the clock forward or backward according to the configurations set for a defined Daylight Saving Time duration. "**disable**" will disable Daylight Saving Time function. "**non-recurring**" will set the Daylight Saving Time duration for single time configuration. "**recurring**" will set the Daylight Saving Time duration to repeat the configuration every year.

ntp dst-start-time v/w/x/y/z command is used to set the start time of Daylight Saving Time duration.

- "**v**" is the month number. Its value is 1~12.
- "**w**" is the date number. Its value is 1~31.
- "**x**" is the year number. Its value is 2000-2097.
- "**y**" is the hour number. Its value is 0-23.
- "**z**" is the minute number. Its value is 0-59.

ntp dst-end-time v/w/x/y/z command is used to set the end time of Daylight Saving Time duration.

- "**v**" is the month number. Its value is 1~12.
- "**w**" is the date number. Its value is 1~31.
- "**x**" is the year number. Its value is 2000-2097.
- "**y**" is the hour number. Its value is 0-23.
- "**z**" is the minute number. Its value is 0-59.

ntp dst-offset x command is used to set the number of minutes to add during Daylight Saving Time. "**x**" is a number between 1~1440 in minute.

29 **prompt** command

This command is used to set prompt of command line interface.

prompt xxx command is used to set prompt of command line interface. "**xxx**" is the new prompt string. "**no prompt**" command can set the prompt back to default.

30 **qos** command

This command is used to configure system QoS function of the switch.

Other Port-based QoS settings are configured in port configuring mode under prompt "(config-if)#".

Entering "qos ?", the following sub-commands will be shown.

```
(config)# qos ?
  dscp                 DSCP Configuration
  qcl                  QoS Control List Configuration
```

The first sub-command is for DSCP Configuration. The second sub-command is for QCL(QoS Control List) Configuration.

Entering "qos dscp ?", the following sub-commands will be shown.

```
(config)# qos dscp ?
  classification-map   Set DSCP ingress classification table
  classification-mode  Set DSCP ingress classification mode
  egressremap          Set DSCP egress remap table
  map                  Set DSCP mapping table
  translation          Set global ingress DSCP translation table
  trust                Set w hether a specific DSCP value is trusted
```

qos dscp classification-map x y z command is used to configure the mapping of QoS class and Drop Precedence Level to internal DSCP value. "**x**" is the QoS class with value 0~7. "**y**" is the Drop Precedence Level with value 0~1. "**z**" is the dscp value 0~63.

Frames got a QoS class (either from port default or VLAN Tag or DSCP) then it can map this QoS to internal DSCP. This internal DSCP then can do another egress map to affect the DSCP value when the frame is sent out. It could rewrite the egress DSCP value when Egress Rewrite is not disable.

qos dscp classification-mode x command is used to select the ingress DSCP value for classification mode. "**x**" is the dscp value 0~63.

Select the DSCP value to enable its QoS Class to internal DSCP mapping operation when Ingress Classify is "selected" in port "qos dscp classification" command. And "**no qos dscp classification-mode x**" will deselect the ingress DSCP value for classification mode.

qos dscp egressremap x y z command is used to set DSCP egress remap table. "**x**" is the dscp value 0~63. "**y**" is DPL(Drop Precedence Level) with value 0 or 1. "**z**" is the egress re-map dhcp value (0~63) for ths DPL.

This command is used to set internal DSCP to egress DSCP value remapping for DP level 0 or 1. It takes effect when port "qos dscp egressremark" command is set.

qos dscp map x y z command is used to set DSCP-Based QoS Ingress Classification. "**x**" is the dscp value 0~63. "**y**" is the QoS class with value 0~7. "**z**" is the Drop Precedence Level with value 0~1.

This command can configure the basic DSCP based QoS Ingress

Classification settings. It takes effect for those trusted DSCP values.

qos dscp translation x y command is used to set global ingress DSCP translation table. "**x**" is the DSCP value 0~63 before translation. "**y**" is the DSCP value 0~63 after translation. Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map.

qos dscp trust x command is used to set whether a specific DSCP value is trusted. "**x**" is the dscp value 0~63. It is used to control whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.

Entering "qos qcl ?", the following sub-commands will be shown.

```
(config)# qos qcl ?
  <1-256>                QCE ID
```

Entering "qos qcl x", the prompt will become "**(config-QCE-x)#**" for further Queue Control Entry configuration. "**x**" is the index of this QCE with number 1~256. For example, enter "qos qcl 10".

```
(config)# qos qcl 10
(config-QCE-10)#
```

And ...

```
(config-QCE-10)# ?
  exit                 Exit from current mode
  help                 Show available commands
  history              Show a list of previously run commands
  logout               Disconnect
  quit                 Quit commands
  action               Action Parameters
  ethernet             Port Members
  key                  Key Parameters
  next_id              Next QCE ID
```

1. **exit** command

   This command is used to leave current operation mode. Go back to last mode.

2. **help** command

   This command is used to show all the available commands in this mode.

3. **history** command

   This command is used to show the history of entering commands.

4. **logout** command

This command is used to logout from console interface.

5. **quit** command

This command is used to quit from console interface. It has the same function as logout.

6. **action** command

This command is used to define the QoS action for a frame when this QCE is matched.

```
(config-QCE-10)# action ?
  class                QoS class
  dpl                  DP Level
  dscp                 DSCP
```

action class x command is used to define the QoS class for the action. "**x**" is the QoS class between 0~7.
action dpl x command is used to define the Drop Precedence Level for the action. "**x**" is the Drop Precedence Level with value 0~1.
action dscp x command is used to define the DSCP value for the action. "**x**" is the DSCP value between 0~63.

7. **ethernet** command

This command is used to assign ports to this QCL Entry.
Its format is ...

```
(config-QCE-10)# ethernet ?
  <1-10>           Unit number: format 1/x    1/x,y,z   1/x-y     1/x-y,z
```

8. **key** command

This command is used to define the key parameters for this QCL Entry. The key parameter is the L2 to L4 information of a frame.

```
(config-QCE-10)# key ?
  dmac-type            Destination MAC type
  frame-type           Frame Type
  smac                 Source MAC address
  tag                  Value of Tag field
```

key dmac-type [any | bc | mc | uc] command is used to define the key parameters by destination Mac address type of frames. It could be any(don't care), bc(Broadcast), mc(Multicast), and uc(Unicast) frame.
key frame-type [any | ethernet | ipv4 | ipv6 | llc | snap] command is used to define the key parameters by information in frame type of frames.
It could be ...

- any (don't care)
- Ethernet Type (any / specific type)

- IPv4 (DSCP value / IP-Fragment or not / Protocol - Port Number of TCP, UDP, other / Source IP Address)
- IPv6 (DSCP value / Protocol - Port Number of TCP, UDP, other / Source IP Address)
- LLC (SSAP / DSAP / Control)
- SNAP (PID)

key smac [any | xx-xx-xx] command is used to define the key parameters by the Source MAC address: 24 MS bits (OUI). It could be any(don't care), or some OUI of source MAC address.

key tag [any | tag | untag] command is used to define the key parameters by the tag information of frames.

- any (don't care)
- tag (DEI, PCP, VID)
- untag

9. **next_id** command

This command is used to set the order of this QCL Entry in QCL table.

next_id x command is used to put this QCL Entry after QCL Entry "x". "**x**" is the QCL Entry ID between 1~256.

next_id last command is used to put this QCL Entry as the last entry in QCL table.

The other QoS settings on ports are configured in "(config-if)#" mode (go with "interface ethernet 1/x" command. "x" is the port number.) Please refer to "qos" command in Section 6.2.4.1 for the details.

31 **radius-accounting-server** command

This command is used to configures RADIUS Accounting Server. Up to five RADIUS Accounting Servers are supported. The following is the details of the command.

Configure the server ...

radius-accounting-server x active command is used to activate RADIUS Accounting Server "x". "**x**" is the server index number between 1~5.

radius-accounting-server x host y.y.y.y command is used to assign IP address to RADIUS Accounting Server "x". "**x**" is the server index number between 1~5. "**y.y.y.y**" is a IP address.

radius-accounting-server x key yyy command is used to assign the secret key "yyy" to RADIUS Accounting Server "x". "**x**" is the server index number between 1~5. "**yyy**" is the secret key - up to 29 characters long - shared between the RADIUS Accounting Server and the switch.

radius-accounting-server x port y command is used to assign the UDP port to use on the RADIUS Accounting Server. "**x**" is the server index number between 1~5. "**y**" is the UDP port number between 0~65535. If the port is

set to 0 (zero), the default port (1813) is used.

Configure the operation parameters ...

radius-accounting-server dead-time x command is used to specify Dead Time of Common Servers. "**x**" is the Dead Time with a number between 0 and 3600 seconds.

The Dead Time is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

radius-accounting-server timeout x command is used to specifies Time Out of Common Servers. "**x**" is the Timeout with a number between 3 and 3600 seconds. The Timeout is the maximum time to wait for a reply from a server. If the server does not reply within this time frame, we will consider it to be dead and continue with the next enabled server (if any).

RADIUS servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.

32 **radius-authentication-server** command

This command is used to configures RADIUS Authentication Server. Up to five RADIUS Authentication Servers are supported. The following is the details of the command.

Configure the server ...

radius-authentication-server x active command is used to activate RADIUS Authentication Server "x". "**x**" is the server index number between 1~5.

radius-authentication-server x host y.y.y.y command is used to assign IP address to RADIUS Authentication Server "x". "**x**" is the server index number between 1~5. "**y.y.y.y**" is a IP address.

radius-authentication-server x key yyy command is used to assign the secret key "yyy" to RADIUS Authentication Server "x". "**x**" is the server index number between 1~5. "**yyy**" is the secret key - up to 29 characters long - shared between the RADIUS Authentication Server and the switch.

radius-authentication-server x port y command is used to assign the UDP port to use on the RADIUS Authentication Server. "**x**" is the server index number between 1~5. "**y**" is the UDP port number between 0~65535. If the port is set to 0 (zero), the default port (1812) is used.

Configure the operation parameters ...

radius-authentication-server dead-time x command is used to specify Dead Time of Common Servers. "**x**" is the Dead Time with a number between 0 and 3600 seconds.

The Dead Time is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

radius-authentication-server timeout x command is used to specifies Time Out of Common Servers. "**x**" is the Timeout with a number between 3 and 3600 seconds. The Timeout is the maximum time to wait for a reply from a server.

If the server does not reply within this time frame, we will consider it to be dead and continue with the next enabled server (if any).

RADIUS servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.

33 rmon command

This function is used to configure RMON function of the switch. This switch supports RMON group 1(statistics), 2(history), 3(alarm), 9(event). The following commands are used to configure those RMON groups.

```
(config)# rmon ?
  alarm              Add RMON Alarm entry
  event              Add RMON Event entry
  history            Add RMON Hisotry entry
  statistics         Add RMON Statistics entry
```

Enter "rmon alarm x ?". The commands for configiring parameters for the alarm will be shown. "x" is the index of the entry. The range is from 1 to 65535. For example, entering "rmon alarm 10 ?", the follwing sub-commands will be shown.

```
# rmon alarm 10 ?
  falling-index          Falling event index
  falling-threshold      Falling threshold value
  interval               Indicates the interval in seconds for sampling and
comparing the rising and falling threshold
  rising-index           Rising event index
  rising-threshold       Rising threshold value
  sample-type              The method of sampling
```

startup-alarm	The method of sampling
variable	Indicates the particular variable to be sampled

rmon alarm x falling-index y command is used to set the Falling event index of the alarm. "**x**" is the index of the entry between 1~65535. "**y**" is the Falling event index (1-65535).

rmon alarm x falling-threshold y command is used to set the Falling threshold value of the alarm. "**x**" is the index of the entry between 1~65535. "**y**" is the Falling threshold value (-2147483648-2147483647).

rmon alarm x interval y command is used to indicates the interval in seconds for sampling and comparing the rising and falling threshold. "**x**" is the index of the entry between 1~65535. "**y**" is the interval in seconds between 1~2147483647.

rmon alarm x rising-index y command is used to set the Rising event index of the alarm. "**x**" is the index of the entry between 1~65535. "**y**" is the Rising event index (1-65535).

rmon alarm x rising-threshold y command is used to set the Rising threshold value of the alarm. "**x**" is the index of the entry between 1~65535. "**y**" is the Rising threshold value (-2147483648-2147483647).

rmon alarm x sample-type [absolute | delta] command is use to select the method of sampling the selected variable and calculating the value to be compared against the thresholds. "**x**" is the index of the entry between 1~65535. The possible sample types are ...

- **absolute** : Get the sample directly.
- **delta** : Calculate the difference between samples.

rmon alarm x startup-alarm [falling | rising | risingorfalling] command is used to select the method of sampling the selected variable and calculating the value to be compared against the thresholds. "**x**" is the index of the entry between 1~65535. The possible sample types are ...

- falling : Trigger alarm when the first value is less than the falling threshold.

- **rising** : Trigger alarm when the first value is larger than the rising threshold.
- **risingorfalling** : Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold.

rmon alarm x variable .1.3.6.1.2.1.2.2.1.x.y command is used to indicates the particular variable to be sampled. "**x**" is the index of the entry between 1~65535."**y**" is 10~21. "**z**" is 1~65535.

Enter "rmon event x ?". The commands for configiring parameters for the event will be shown. "x" is the index of the entry. The range is from 1 to 65535. For example, entering "rmon event 10 ?", the follwing sub-commands will be shown.

(config)# rmon event 10 ?

community	Specify the community when trap is sent
desc	Indicates this event, the string length is from 0 to 127
type	Indicates the notification of the event

rmon event x community yyy command is used to specify the community when trap is sent. "**x**" is the index of the entry between 1~65535. "**yyy**" is the community string with length 0~127.

rmon event x desc yyy command is used to indicates this event. "**x**" is the index of the entry between 1~65535. "**yyy**" is a string with length 0~127.

rmon event x type [log | log-trap | none | trap] command is used to indicates the notification of the event. "**x**" is the index of the entry between 1~65535. The possible notification are ...

- **log** : The number of uni-cast packets delivered to a higher-layer protocol.
- **log-trap** : The number of inbound packets that are discarded even the packets are normal.
- **none** : The total number of octets received on the interface, including framing characters.
- **trap** : The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.

Enter "rmon history x ?". The commands for configiring parameters for the history will be shown. "x" is the index of the entry. The range is from 1 to 65535. For example, entering "rmon history 10 ?", the follwing sub-commands will be shown.

```
(config)# rmon history 10 ?
  buckets        Indicates the maximum data entries associated this History control
entry stored in RMON
  data_source    Indicates the port ID which wants to be monitored
  interval       Indicates the interval in seconds for sampling the history statistics data
```

rmon history x buckets y command is used to indicates the maximum data entries associated this History control entry stored in RMON. "**x**" is the index of the entry between 1~65535. "**y**" is the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600.

rmon history x data_source .1.3.6.1.2.1.2.2.1.1.y command is used to Indicates the port ID which wants to be monitored. "**x**" is the index of the entry between 1~65535. "**y**" is the port ID which wants to be monitored.

rmon history x interval y command is used to indicates the interval in seconds for sampling the history statistics data. "**x**" is the index of the entry between 1~65535. "**y**" is the interval in seconds for sampling the history statistics data. The range is from 1 to 3600.

Enter "rmon statistics x ?". The commands for configiring parameters for the statistics will be shown. "x" is the index of the entry. The range is from 1 to

65535. For example, entering “rmon statistics 10 ?”, the follwing sub-commands will be shown.

```
(config)# rmon statistics 10 ?
  data_source          Indicates the port ID which wants to be monitored
```

rmon statistics x data_source .1.3.6.1.2.1.2.2.1.1.y command is used indicates the port ID which wants to be monitored. “**x**” is the index of the entry between 1~65535. “**y**” is the port ID which wants to be monitored.

34 **s-flow** command

sFlow is an industry standard technology for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counters. The sampled packets and counters (referred to as flow samples and counter samples, respectively) are sent as sFlow UDP datagrams to a central network traffic monitoring server. This central server is called an sFlow receiver or sFlow collector. This command is used to configure sFlow function of the switch.

Entering “sflow receiver ?”, the sub-commands will be shown.

```
(config)# sflow receiver ?
  datagramsize          Set the Reciever Data gram length for list of receiver ID
  ip                    Set the sFlow receiver IP for list of receiver ID
  release               Release
  time_out              Set the Receiver Time_out for list of receiver ID
```

sflow receiver datagramsize x command is used to set the Reciever Data gram length for list of receiver ID. “**x**” is 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.

sflow receiver ip <ip address> x command is used to set the sFlow receiver IP and UDP port for list of receiver ID. **<ip address>** is the IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported. “**x**” is the UDP port on which the sFlow receiver listens to sFlow datagrams. Its valid port number is 0~65535. If set to 0 (zero), the default port (6343) is used.

sflow receiver release command is used to release the current owner and disable sFlow sampling.

Basically, sFlow can be configured in two ways: Through local management using the Web/CLI interface or through SNMP. The owner of the current sFlow configuration has possible values as follows:

- If sFlow is currently unconfigured/unclaimed, Owner is <none>.
- If sFlow is currently configured through Web or CLI, Owner is <Configured through local management>.

• If sFlow is currently configured through SNMP, Owner is a string identifying the sFlow receiver.

If sFlow is configured through SNMP, all controls are disabled to avoid inadvertent reconfiguration.

sflow receiver time_out x command is used to set the Receiver Time_out for list of receiver ID. "**x**" is the number of seconds remaining before sampling stops and the current sFlow owner is released. Its valid value is 0~2147483647 in seconds.

sFlow function is enabled by port. And the other sFlow settings on ports are configured in "(config-if)#" mode (go with "interface ethernet 1/x" command. "x" is the port number.) Please refer to "sflow" command in Section 6.2.4.1 for the details.

35 **snmp-server** command

This command is used to configure SNMP function of the switch.

Entering "snmp-server ?", the sub-commands will be shown.

```
(config)# snmp-server ?
  <1-1>                Index of Trap
  community            Defines SNMP community access string
  contact              Sets the system contact string
  enable               Enables SNMP function
  location             Sets the system location string
  snmpv3-access        Sets the snmpv3 community
  snmpv3-community     Sets the snmpv3 community
  snmpv3-group         Sets the snmpv3 group configuration
  snmpv3-user          Sets the snmpv3 user configuration
  snmpv3-view          Sets the snmpv3 view configuration
  version              Sets the snmp version
```

Entering "snmp-server 1 ?" command, the commands for SNMP Trap configuration will be shown.

```
(config)# snmp-server 1 ?
  authentication-failure Trap Community
  community          Trap Community
  enable             Enables this Trap function
  host               Specifies SNMP notification operation recipients
  host-ipv6          Specifies SNMP notification operation recipients (for ipv6 addresss)
  link-up-down       Trap Link-up and Link-down
  version            Trap Version
```

snmp-server x authentication-failure command is used to enable that the SNMP entity is permitted to generate authentication failure traps. "**x**" is the index of the trap 1~1. And "**no snmp-server x authentication-**

failure“ command is used to disable it.

snmp-server x community yyy command is used to set the the community access string when sending SNMP trap packet. “**x**” is the index of the trap 1~1. “**yyy**” is community string with length is 0 to 255, and the allowed content is ASCII characters from 33 to 126.

snmp-server x enable command is used to enabled this SNMP Trap. “**x**” is the index of the trap 1~1. And “**no snmp-server x enable**“ command is used to disable it.

snmp-server x host y.y.y.y command is used to set the SNMP trap IPv4 destination address. “**x**” is the index of the trap 1~1. “**y.y.y.y**” is a IPv4 address.

snmp-server x host-ipv6 <IPv6 address> command is used to set the SNMP trap IPv6 destination address. “**x**” is the index of the trap 1~1. “**<IPv6 address>**” is a IPv6 address.

snmp-server x link-up-down command is used to enable SNMP trap link-up and link-down mode operation. “**x**” is the index of the trap 1~1. And “**no snmp-server x link-up-down**” command is used to disable it.

snmp-server x version [v1 | v2c | v3] command is used to select the SNMP trap supported version. “**x**” is the index of the trap 1~1. The options for SNMP Trap version are SNMP V1(v1), SNMP V2c(v2c), and SNMP V3(v3).

snmp-server community get xxx command is used to set the community string of get command for SNMP operation. “**xxx**” is the community string.

snmp-server community set xxx command is used to set the community string of set command for SNMP operation. “**xxx**” is the community string.

snmp-server contact xxx command is used to set the contact information for this switch. “**xxx**” is the contact information string.

snmp-server enable command is used to enable SNMP function. And “**no snmp-server enable**“ is used to disable it.

snmp-server location xxx command is used to set the location information for this switch. “**xxx**” is the location information string.

snmp-server version [v1 | v2c | v3] command is used to select the SNMP operation version. The options for SNMP version are SNMP V1(v1), SNMP V2c(v2c), and SNMP V3(v3).

The following commands are for SNMP v3 configuration.

snmp-server snmpv3-access group-name xxx security-model [any | v1 | v2c | usm] security-level [authnopriv | authpriv | noauthnopriv] read_view_name yyy write_view_name zzz command is used to create a SNMPv3 access entry. “**xxx**” is a string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. “**yyy**” is the name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is

ASCII characters from 33 to 126. "**zzz**" is the name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. And "**no snmp-server snmpv3-access group-name xxx security-model [any | v1 | v2c | usm] security-level [authnopriv | authpriv | noauthnopriv]**" command is used to delete a SNMPv3 access entry.
About the options for Security Model ...
- **any** : Any security model accepted(v1|v2c|usm)
- **v1** : Reserved for SNMPv1.
- **v2c** : Reserved for SNMPv2c.
- **usm** : User-based Security Model (USM).
About the options for Security Level ...
- **authnopriv** : Authentication and no privacy.
- **authpriv** : Authentication and privacy.
- **noauthnopriv** : No authentication and no privacy.

snmp-server snmpv3-community community xxx source-ip y.y.y.y source-mask z.z.z.z command is used to create a SNMPv3 Community Entry. "**xxx**" is the community access string to permit access to SNMPv3 agent. It is a string with length 1~32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string. "**y.y.y.y**" is the SNMP access source address. "**z.z.z.z**" is the SNMP access source address mask. And "**no snmp-server snmpv3-community community xxx**" command is used to delete a SNMPv3 Community Entry.

snmp-server snmpv3-group security-model [v1 | v2c | usm] security-name xxx group-name yyy command is used to create a SNMPv3 group. "xxx" is a string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. "yyy" is a string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. And "**no snmp-server snmpv3-group security-model [v1 | v2c | usm] security-name xxx**" command is used to delete a SNMPv3 group.
About the options for Security Model ...
- **v1** : Reserved for SNMPv1.
- **v2c** : Reserved for SNMPv2c.
- **usm** : User-based Security Model (USM).

snmp-server snmpv3-user xxx yyy command is used to create a SNMPv3 user with "No Authentication and No Privacy" security level. "**xxx**" is SNMPV3 Engine ID. "**yyy**" is a string identifying the user name that this entry should belong to.
snmp-server snmpv3-user xxx yyy auth [md5 | sha] zzz command is used

to create a SNMPv3 user with “Authentication and No Privacy” security level. “**xxx**” is SNMPV3 Engine ID. “**yyy**” is a string identifying the user name that this entry should belong to. “**zzz**” is a string identifying the authentication password phrase.

snmp-server snmpv3-user xxx yyy auth-priv [md5 | sha] zzz des www command is used to create a SNMPv3 user with “Authentication and Privacy” security level. “**xxx**” is SNMPV3 Engine ID. “**yyy**” is a string identifying the user name that this entry should belong to. “**zzz**” is a string identifying the authentication password phrase. “**www**” is a string identifying the privacy password phrase.

no snmp-server snmpv3-user xxx yyy command is used to delete a SNMPv3 user. “**xxx**” is SNMPV3 Engine ID. “**yyy**” is a string identifying the user name that this entry should belong to.

- SNMPV3 Engine ID is an octet string identifying the engine ID that this entry should belong to. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user.
- User Name is a string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
- Authentication Password is a string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.
- Privacy Password is a string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.

snmp-server snmpv3-view view-name xxx view-type [excluded | included] oid-subtree .yyy command is used to create a SNMPv3 View Entry. “xxx” is a string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. “**.yyy**” is the OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

36 **spanning-tree** command

This command is used to configure spanning tree protocol of the switch. Entering "spanning-tree", the sub-commands will be shown.

```
(config)# spanning-tree ?
  bpdufilter            Set edge port BPDU Filtering
  bpduguard             Set edge port BPDU Guard
  cname                 Set configuration name and revision for MSTI
  forward-delay         Global STA forward time configuration. Range: <4-30 seconds>
  max-age               Global STA maximum age configuration. Range <6-40 seconds>
  max-hop-count         Setthe MSTP Bridge Max Hop Count parameter
  mode                  Select spanning tree operation mode
  msti                  Compatible with old STP
  priority              Specifies spanning tree priority
  recovery              Set edge port error recovery timeout
  transmit-hop-count    Set the STP Bridge Transmit Hold Count parameter
```

spanning-tree bpdufilter command is used to enable that when a port explicitly configured as Edge will transmit and receive BPDUs. And "**no spanning-tree bpdufilter**" is used to disable it.

spanning-tree bpduguard command is used to enable that when a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology. And "**no spanning-tree bpduguard**" command is used to disable it.

spanning-tree cname xxx y command is used to set the Configuration Name and Configuration Revision for MSTI Configuration. "**xxx**" is a string as Configuration Name. It is the name identifying the VLAN to MSTI mapping. Bridges must share the name and revision, as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters. "**y**" is a number between 0~65535 as Configuration Revision. It is the revision of the MSTI configuration named by "**xxx**".

spanning-tree forward-delay x is used to set the global STA forward time configuration. It is the delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). "**x**" is the delay time. Valid values are in the range 4 to 30 seconds.

spanning-tree max-age x command is used to set the global STA maximum age configuration. It is the maximum age of the information transmitted by the Bridge when it is the Root Bridge. "**x**" is the maximum age time. Valid values are in the range 6 to 40 seconds, *and* MaxAge must be <= (FwdDelay-1)*2.

spanning-tree max-hop-count x command is used to set the MSTP Bridge Max Hop Count parameter. This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. "**x**" is the maximum hop count. Valid values are in the range 6 to 40 hops.

spanning-tree mode [mstp | rstp | stp] command is used to select the

operation mode of spanning tree. It could be MSTP, RSTP, or STP.

spanning-tree msti instance x vlan y command is used to add a VLAN to a MSTI. "**x**" is a number between 1~7 to indicate the MSTI. "**y"** is the VLAN ID (1~4094) of the VLAN added to the MSTI. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (i.e. not having any VLANs mapped to it.)

spanning-tree msti priority x y command is used to set the bridge instance priority. "**x**" is a number between 1~7 to indicate the MSTI. "**y**" is the bridge instance priority between 0~61440 in steps of 4096. (For example, "**y**" could be 0, 4096, 8192, 12288, ...) Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a *Bridge Identifier*.

spanning-tree priority x command is used to specify spanning tree priority. "**x**" is a value of spanning-tree priority between 0~61440 in steps of 4096. (For example, "**x**" could be 0, 4096, 8192, 12288, ...) Lower numeric values have better priority. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

spanning-tree recovery x command is used to set edge port error recovery timeout. It is the time to pass before a port in the *error-disabled* state can be enabled. "**x**" is the timeout value. Valid values are between 30 and 86400 seconds (24 hours).

spanning-tree transmit-hop-count x command is used to set the STP Bridge Transmit Hold Count parameter. It is the number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. "**x**" is the Transmit Hold Count. Valid values are in the range 1 to 10 BPDU's per second.

The settings of spanning tree on port are done in "interface" command. The settings here are for bridge only.

37 **storm-control** command

This command is used to set the storm control rate. The packet storms that could be controlled are broadcast, multicast, and unicast flooding traffic. And the rate is counted with packet per second(pps), not bit per second(bps). These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.

storm-control broadcast x command is used to set broadcast flooding traffic suppression rate. "**x**" is the suppression rate in pps(packet per second), and could be 1, 2, 4, 8, ..., 512, 1k, 2k, 4k, ..., 512k, 1024k, 2048k, ..., 32768k.

storm-control multicast x command is used to set multicast flooding traffic suppression rate. "**x**" is the suppression rate in pps(packet per second),

and could be 1, 2, 4, 8, ..., 512, 1k, 2k, 4k, ..., 512k, 1024k, 2048k, ..., 32768k.
storm-control unicast x command is used to set unicast flooding traffic suppression rate. "**x**" is the suppression rate in pps(packet per second), and could be 1, 2, 4, 8, ..., 512, 1k, 2k, 4k, ..., 512k, 1024k, 2048k, ..., 32768k.

38 **tacacs-authentication-server** command

This command is used to configures TACACS+ Authentication Server. Up to five TACACS+ Authentication Servers are supported. The following is the details of the command.

Configure the server ...

tacacs-authentication-server x active command is used to activate TACACS+ Authentication Server "x". "**x**" is the server index number between 1~5.

tacacs-authentication-server x host y.y.y.y command is used to assign IP address to TACACS+ Authentication Server "x". "**x**" is the server index number between 1~5. "**y.y.y.y**" is a IP address.

tacacs-authentication-server x key yyy command is used to assign the secret key "yyy" to TACACS+ Authentication Server "x". "**x**" is the server index number between 1~5. "**yyy**" is the secret key - up to 29 characters long - shared between the TACACS+ Authentication Server and the switch.

tacacs-authentication-server x port y command is used to assign the TCP port to use on the TACACS+ Authentication Server. "**x**" is the server index number between 1~5. "**y**" is the TCP port number between 0~65535. If the port is set to 0 (zero), the default port (49) is used.

Configure the operation parameters ...

tacacs-authentication-server dead-time x command is used to specify Dead Time of Common Servers. "**x**" is the Dead Time with a number between 0~3600 seconds.

The Dead Time is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

tacacs-authentication-server timeout x command is used to specifies Time Out of Common Servers. "**x**" is the Timeout with a number between 3~3600 seconds. The Timeout is the maximum time to wait for a reply from a server. If the server does not reply within this time frame, we will consider it to be dead and continue with the next enabled server (if any).

* RADIUS servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3

subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.

39 **username** command

This command is used to create a user and assign username, password, and privilege_level for him/her.

username xxx yyy z command is used to create a user and assign username, password, and privilege_level. "**xxx**" is the username. The allowed string length is 1 to 31. The valid user name is a combination of letters, numbers and underscores. "**yyy**" is the password. The allowed string length is 0 to 31. "**z**" is the privilege_level. The allowed range is 1~3.

There are three previlege levels for users of the switch - administrator, operator, and guest, with previlege level 3, 2, 1. With administrator level, it is allowed to fully management the switch. With operator level, it is allowed to view the switch status and configuration, and run some system maintenance commands. With guest level, it is allowed to view the switch status and configuration only. No setup/configure commands are supported.

40 **vlan** command

This command is used to enter VLAN configuring mode. And the prompt will become ...

```
(config)# vlan database
(config-vlan)#
```

The operations for VLAN are configured in VLAN configuring mode. Please refer to **6.2.5 VLAN Configuring Commands** section for the details.

41 **voice-vlan** command

This command is used to configure Voice VLAN function. Voice VLAN function can detect IP Phone traffic and assign the traffic to a VLAN with configurable traffic priority automatically.

Enter "voice-vlan ?", the sub-commands will be shown.

```
(config)# voice-vlan ?
  agetime          Indicates the Voice VLAN secure learning aging time
  oui              Specify hold time multiplier
  traffic-class    Indicates the Voice VLAN traffic class
  vlan-id          Indicates the Voice VLAN ID
```

<cr> Enable Voice VLAN mode operation

voice-vlan command is used to enable Voice VLAN function. And "**no voice-lan**" command can be used to disable it.

voice-vlan agetime x command is used to configure the Voice VLAN secure learning aging time. "**x**" is the aging time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval.

voice-vlan oui add xx-xx-xx command is used to add an OUI entry without description. And "**voice-vlan oui add xx-xx-xx yyy**" command is used to add an OUI entry with description. "**xx-xx-xx**" is the telephony OUI address. A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit). "**yyy**" is the description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.

voice-vlan oui clear command is used to clear OUI table. All OUI entries will be deleted.

voice-vlan oui delete xx-xx-xx command is used to delete an OUI entry. "**xx-xx-xx**" is the telephony OUI address. A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).

voice-vlan traffic-class x command is used to configure the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class. "**x**" is the traffic-class with value 0~7.

voice-vlan vlan-id x command is used to set VLAN ID for Voice VLAN. "**x**" is the VLAN ID with value 1~4095.

6.2.4 Interface Configuring Commands

Commands in Configuring Mode are for general switch settings. And its prompt is "(config)#".

The port interface function and VLAN group interface function are set with "interface" command.

```
(config)# interface ?
  ethernet          Ethernet port
  vlan              Switch Virtual LAN interface
```

interface ethernet 1/x command is used to configure settings for **Port x**. Please refer to section **6.2.4.1 Interface Configuring Commands for Port** for the details.
interface vlan x command is used to configure **VLAN Group x** interface ("x" is the VLAN ID). Please refer to section **6.2.4.2 Interface Configuring Commands for VLAN** for the details.

Both commands will change the prompt from "(config)#" to "**(config-if)#**".

Note: The general VLAN settings are done with "**vlan database**" command. Please refer to section **6.2.5 VLAN Configuring Commands** for the details. And **interface vlan x** command is used to assign characteristics to a VLAN interface. For example, assigning IP address to a VLAN interface is done with this command.

6.2.4.1 Interface Configuring Commands for Port

Commands in Configuring Mode are for general switch settings. And its prompt is "(config)#".
If the settings are for ports, it is done with "**interface ethernet 1/x**" command in configure mode. For example, "interface ethernet 1/5" is for settings on Port 5.

Some syntax are supported for port selection.

1. **interface ethernet 1/x** and "**x**" is port number. All the settings after this command will be applied to this port. For example, "interface ethernet 1/5" and all the settings after this command will be applied to Port 5.
2. **interface ethernet 1/x,y,z,...** and "**x**", "**y**", "**z**",.. are port number. All the settings after this command will be applied to these ports. For example, "interface ethernet 1/2,4,7" and the settings after this command will be applied to Port 2, Port 4, and Port 7.
3. **interface ethernet 1/x-y** and "**x**","**y**" are port number. All the settings after

this command will be applied to ports in this range. For example, “interface ethernet 1/4-7” and the settings after this command will be applied to Port 4, Port 5, Port 6, and Port 7. (Port 4~7)

4. **interface ethernet 1/w,x,..,y-z** and “**w**”,”**x**”,”**y**”,”**z**” are port number. All the settings after this command will be applied to those ports. For example, “interface ethernet 1/1,2,4-7” and the settings after this command will be applied to Port 1, Port 2, Port 4, Port 5, Port 6, and Port 7. (Port 4~7)

Entering “interface ethernet 1/5”, and its prompt will become ...

```
(config)# interface ethernet 1/5
(config-if)#
```

Enter “?” at the prompt, the sub-command list will be shown.

```
(config-if)# ?
  exit                  Exit from current mode
  help                  Show available commands
  history               Show a list of previously run commands
  logout                Disconnect
  quit                  Quit commands
  acl                   Access Control List Configuration
  arp-inspection        Set ARP inspection configuration
  channel-group         Adds ports to a trunk
  dhcp-snooping         Configures DHCP Snooping Configuration
  dot1x                 Configures 802.1x port-based access control
  eee                   Set the eee mode
  end                   Exit from interface mode
  excessive             Configure port transmit collision behavior
  flowcontrol           Enables flow control during autoneg
  interface             Enters privileged interface configuration
  ip                    Global IP configuration sub commands
  ip-source-guard       IP Source Guard Configuration
  lacp                  Configures LACP status
  lldp                  Configures lldp
  loopback-detection    Configures loopback detection
  mac-learn             mac learn
  maximum-packet-length Configures the maximum packet length of the port
  mdi/mdi-x             Set MDI crossover
  mvr                   Multicast VLAN Registration
  no                    Negates a command or sets its defaults
  port                  Configures the characteristics of the port
  port-vlan             Configures Port-Based VLAN
  power-control         Decrease energy consumption
  qos                   Configuration of QoS
```

```
  sflow                 configured sFlow samplers
  shutdown              Shuts down the selected interface
  spanning-tree         Specifies spanning tree configuration
  speed                 Configures speed operation
  switchport            Configures switching mode characteristics
  voice-vlan            Voice VLAN Configuration
-------------------------------------------------------------------------------------------
```

1 **exit** command
This command is used to leave current operation mode. Go back to last mode.

2 **help** command
This command is used to show all the available commands in this mode.

3 **history** command
This command is used to show the history of entering commands.

4 **logout** command
This command is used to logout from console interface.

5 **quit** command
This command is used to quit from console interface. It has the same function as logout.

6 **acl** command
This command is used to configure the ACL parameters (ACE) for the interface port(s). These parameters will affect frames received on a port unless the frame matches a specific ACE.
Enter "acl ?". The sub-commands will be shown.

```
(config-if)# acl ?
  action              Select whether forwarding is permitted or denied
  logging             Logging operation of this port
  mirror              Mirror operation of this port
  policy              Select the policy to apply to this port
  port-redirect       Select which port frames are copied on
  rate-limiter        Select which rate limiter to apply on this port
  shutdown            Shut down operation of this port
```

acl action [deny | permit] command is used to select whether forwarding is

permitted ("permit") or denied ("deny") for the interface port(s).

acl logging command is used to enable frames received on the port are stored in the System Log. Please note that the System Log memory size and logging rate is limited. And "**no acl logging**" command is used to disable.

acl mirror command is used to enable that frames received on the port are mirrored. The mirror operation will follow the settings of Mirror function. And "**no acl mirror**" command is used to disable it.

acl policy x command will put the interface port(s) to Policy x group for ACL operation. "**x**" is the Policy ID with value between 0~255.

acl port-redirect [disable | 1/x] command is used to configure traffic redirect operation of the port. It could be disable, or redirect to some other ports. "**1/x**" could be "1/x 1/x,y,z 1/x-y 1/x-y,z" - more than one port. And it can't be set when action is permitted.

acl rate-limiter [disable | x] command is used to configure rate limit function for the interface port(s). "**x**" is the rate limiter ID with value between 1~16.

acl shutdown command is used to enable shutdown function for the interface port(s). If a frame is received on the port, the port will be disabled. And "**no acl shutdown**" command is used to disable it.

7 **arp-inspection** command

This command is used to configure ARP Inspection function for the interface port(s).

Enter "arp-inspection ?". The sub-commands will be shown.

```
(config-if)# arp-inspection ?
  entry                Add ARP inspection static entry
  mode                 Set show the ARP Inspection port mode
```

arp-inspection entry vid x mac yy-yy-yy-yy-yy-yy ip <ip address> command is used to create an static ARP entry for the interface port(s). "**x**" is VLAN ID with value between 1~4095. "**yy-yy-yy-yy-yy-yy**" is allowed Source MAC address in ARP request packets.. **<ip address>** is allowed Source IP address in ARP request packets. And "**no arp-inspection entry vid x mac yy-yy-yy-yy-yy-yy ip <ip address>**" can delete the entry.

arp-inspection mode command is used to enable arp inspection function on the interface port(s). And "**no arp-inspection mode**" command is used to disable it.

Note: Dynamic ARP entry is learned from DHCP request. Before enable ARP Inspection, DHCP Snooping function should be enabled first. Otherwise, static ARP entry should be created for ARP Inspection operation.

8 **channel-group** command

This command is used to add the interface port(s) to a Aggregation Group. This is a static Aggregation Group assignment. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

channel-group x will add the interface port(s) to the trunk group "**x**". "**x**" is the trunk group number, and its valid value is 1-5. And note that aggregation must include 2-10 ports.

no channel-group will remove the interface port(s) from any trunk group.

9 **dhcp-snooping** command

This command is used to configure DHCP Snooping function for the interface port(s). Interface port(s) could be trusted or untrusted for DHCP operation.

dhcp-snooping mode [untrusted | trusted] command is used to set the interface port(s) as trusted or untrusted for source of the DHCP messages.
dhcp-snooping statistics clear command is used to clear DHCP Snooping Port Statistics for the interface port(s).

10 **dot1x** command

This command is used to configure 802.1x function for the interface port(s).
Enter "dot1x ?", the sub-commands will be shown.

```
(config-if)# dot1x ?
  authenticate      Refresh (restart) 802.1X authentication process
  clear             Clear 802.1X statistics
  guest_vlan        Guest VLAN Enabled
  port-control      Needs dot1x-aware client RADIUS server authorization
  radius-qos        RADIUS Assigned QoS Enabled
  radius-vlan       RADIUS Assigned VLAN Enabled
```

dot1x authenticate command is used to schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. This command only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.
This command are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode.
dot1x authenticate now command is used to forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.
This command are only enabled when authentication is globally enabled and

the port's Admin State is in an EAPOL-based or MAC-based mode.
dot1x clear command is used to clear 802.1X statistics for the interface port(s).
dot1x guest_vlan command is used to enable Guest VLAN function for the interface port(s). And "**no dot1x guest_vlan**" command is used to dis able it. Guest VLAN function works when Guest VLAN is both globally enabled and enabled for a given port.
This option is only available for EAPOL-based modes, i.e.:
• Port-based 802.1X
• Single 802.1X
• Multi 802.1X
dot1x port-control [auto | force-authorized | force-unauthorized | mac-based | multi-802.1x | single-802.1x] command is used to select the 802.1X operation mode for the interface port(s).
Here is the details about the operation modes.
- **auto** : Needs dot1x-aware client RADIUS server authorization. This mode will set the port to work as "Port-based 802.1X" mode.
- **force-authorized** : Configures the port to grant access to all clients. In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.
- **force-unauthorized** : Configures the port to deny access to all clients. In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.
- **mac-based** : Configures the port to MAC-based authentication. Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly. When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.
The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user

can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

- **multi-802.1x** : Configures more supplicants can get authenticated on the same port at the same time. Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.

In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port.

The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.

- **single-802.1x** : Configures once a supplicant is successfully authenticated on a port. In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant.

Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

dot1x radius-qos command is used to enable RADIUS-Assigned QoS function. And "**no dot1x radius-qos**" command is used to disable it. When RADIUS-Assigned QoS is both globally enabled and enabled on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-

)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).
This option is only available for single-client modes, i.e.
• Port-based 802.1X
• Single 802.1X
dot1x radius-vlan command is used to enable RADIUS-Assigned VLAN function. And "**no dot1x radius-vlan**" command is used to disable it. When RADIUS-Assigned VLAN is both globally enabled and enabled for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.
If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).
This option is only available for single-client modes, i.e.
• Port-based 802.1X
• Single 802.1X

11 **eee** command

This command is used to configure EEE(Energy Efficient Ethernet, defined in IEEE 802.3az) function for the interface port(s).

eee command is used to enable this function for the interface port(s). And "**no eee**" command is used to disable it.
eee queue-list command is used to select all queues as EEE Urgent Queues. And "**no eee queue-list**" command is used to remove all queues from EEE Urgent Queues. EEE Urgent Queues are Queues set that will activate tranmission of frames as soon as data is available. Otherwise the queue will postpone tranmsission until 3000 bytes are ready to be transmitted.
eee queue-list [x | x,y,z | x-y] command is used to assign queue(s) to EEE Urgent Queues. **[x | x,y,z | x-y]** is the queue number with value 1~8. ("x" for single queue; x,y,z for queue list; x-y for queue range). The original setting will be lost. "**no eee queue-list**" command is used to remove all queues from EEE Urgent Queues List.

12 **end** command

This command is used to exit from interface mode.

```
(config-if)# end
(config)#
```

13 **excessive** command

This command is used to configure the operation when excessive collision happens on half duplex mode.

excessive [discard | restart] command is used to configure the operation when excessive collision happens on half duplex mode.

- **discard** : discard frame after 16 collisions
- **restart** : restart backoff algorithm after 16 collisions

14 **flowcontrol** command

This command is used to enable flow control function of the interface port(s).

flowcontrol command is used to enable flow control function of the interface port(s).

no flowcontrol command is used to disable flow control function of the interface port(s).

15 **interface** command

This command is used to change the interface port(s) for next setup commands.

```
(config-if)# interface ?
  ethernet                  Ethernet port
(config-if)# interface ethernet ?
<1-10>   Unit number: format 1/x     1/x,y,z   1/x-y      1/x-y,z
```

For example,

"(config)# interface ethernet 1/5" will set current setup interface to Port 5 and all the commands will be applied to Port 5.

"(config-if)# interface ethernet 1/6-7" will change current setup interface to Port 6-7 and all the commands will be applied to Port 6-7.

The description of commands in interface configuring mode is put in Section **6.2.4 Interface Configuring Commands**. Please refer to the section for the details.

16 **ip** command

This command is used to configure IGMP/MLD Snooping function for the port(s).

ip igmp snooping fastleave / **ip mld snooping fastleave** command is used to enable fast-leave function for the port(s). And "**no ip igmp snooping fastleave**" / "**no ip mld snooping fastleave**" command is used to disable it.
Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.
ip igmp snooping filtering group_addrress xxx / **ip mld snooping filtering group_addrress xxx** command is used to add a IGMP/MLD filtering group for the port(s). "**xxx**" is a IP Multicast address. And "**no ip igmp snooping filtering group_addrress xxx**" / "**no ip mld snooping filtering group_addrress xxx**" command is used to delete it.
ip igmp snooping router / **ip mld snooping router** command is used to set the port as router port for IGMP/MLD snooping operation. And "**no ip igmp snooping router**" / "**no ip mld snooping router**" command is used to set the port as non-router port. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP/MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
ip igmp snooping throttling [unlimited | x] / **ip mld snooping throttling [unlimited | x]** command is used to limit the number of multicast groups to which a switch port can belong. It could be "**unlimited**" or "**x**" - a value between 1~10.

17 **ip-source-guard** command

This command is used to configure IP Source Guard function for the port(s).

ip-source-guard entry vid x mac yy-yy-yy-yy-yy-yy ip <IP Address> command is used to add a static entry on the port(s) for this function. "**x**" is VLAN ID between 1~4094. "**yy-yy-yy-yy-yy-yy**" is Mac address. And "**no ip-source-guard entry vid x mac yy-yy-yy-yy-yy-yy ip <IP Address>**" command is used to delete the entry.
ip-source-guard limit [unlimited | x] command is used to specify the maximum number of dynamic clients that can be learned on given port. It could be "**unlimited**" or "**x**" with value 0~2. If the port mode is enabled and the value of max dynamic client is equal to 0, it means only allow the IP

packets forwarding that are matched in static entries on the specific port.
ip-source-guard mode command is used to enable this function for the ports. And "**no ip-source-guard mode**" command is used to disable it.

Note: Dynamic IP Source entry is learned from DHCP request. Before enable IP Source Guard, DHCP Snooping function should be enabled first. Otherwise, static IP Source entry should be created for IP Source Guard operation.

18 **lacp** command

This command is used to configure LACP protocol working on the interface port(s).

lacp clear command is used to clear LACP Statistics.
lacp key [auto | specific x] command is used to specify the Key value incurred by the port. The "**auto**" setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the "**specific**" setting, a user-defined value "**x**" with value 1~65535 can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.
lacp mode command is used to enable LACP function on the ports. And "**no lacp mode**" command is used to disable it.
lacp priority x command is used to set LACP Priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.
lacp role [active | passive] command is used to set the role of the ports for LACP operation. The "**active**" will transmit LACP packets each second, while "**passive**" will wait for a LACP packet from a partner (speak if spoken to).
lacp timeout [fast | slow] command is used to configure Timeout to control the period between LACP transmissions. "**fast**" will transmit LACP packets each second, while "**slow**" will wait for 30 seconds before sending a LACP packet.

19 **lldp** command

This command is used to configure LLDP function for the ports.

lldp clear command is used to clear LLDP Statistics.
lldp [disable | **enable | rx-only | tx-only]** command is used to set LLDP operation mode on the ports.
- **disable** : disable LLDP operation on the ports. The switch will not send out LLDP information, and will drop LLDP information received from neighbours.

- **enable** : enable LLDP operation on the ports. The switch will send out LLDP information, and will analyze LLDP information received from neighbours.
- **rx-only** : set the the ports as Receive-Only for LLDP operation. The switch will not send out LLDP information, but LLDP information from neighbour units is analyzed.
- **tx-only** : set the the ports as Transmit-Only for LLDP operation. The switch will drop LLDP information received from neighbours, but will send out LLDP information.

lldp cdp-aware command is used to enable CDP-Aware function. (CDP is an acronym for Cisco Discovery Protocol.) And "**no lldp cdp-aware**" command is used to disable it. The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the port is enabled.

Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbours' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbours' table as shown below.

- CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.
- CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbours table.
- CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.
- CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.
- Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbours' table.

If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbour devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch.

Note: When CDP awareness on a port is disabled the CDP information isn't removed immediately, but gets removed when the hold time is exceeded.

lldp port-description command is used to enable "port description" included in LLDP information transmitted. And "**no lldp port-description**" command is used to disable it.

lldp system-name command is used to enable "system name" included in LLDP information transmitted. And "**no lldp system-name**" command is used to disable it.

lldp system-description command is used to enable "system description" included in LLDP information transmitted. And "**no lldp system-description**" command is used to disable it.

lldp system-capabilities command is used to enable "system capabilities" included in LLDP information transmitted. And "**no lldp system-capabilities**" command is used to disable it.

lldp management-address command is used to enable "management

address" included in LLDP information transmitted. And "**no lldp management-address**" command is used to disable it.

20 **loopback-detection** command

This command is used to configure Loopback Detection for the ports.

loopback-detection action [log | shutdown | shut_log] command is used to configure the action performed when a loop is detected on a port. Valid values are "**shutdown**"(Shutdown Port), "**shut_log**"(Shutdown Port and Log) or "**log**"(Log Only).

loopback-detection mode command is used to enable loopback-detection function on the ports. And "**no loopback-detection mode**" command is used to disable it.

loopback-detection transmit command is used to enable transmit mode for loopback-detection function. And "**no loopback-detection transmit**" command is used to disable it. Transmit mode controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

21 **mac-learn** command

This command is used to configure Mac Address Learning function for the ports.

mac-learn [auto | disable | secure] command is used to set the Mac Address Learning function for the ports.

- **auto** : Learning is done automatically as soon as a frame with unknown SMAC is received.
- **disable** : No learning is done.
- **secure** : Only static MAC entries are learned, all other frames are dropped.

Note: Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

22 **maximum-packet-length** command

This command is used to configure maximum packet length for the ports.

maximum-packet-length x command is used to configure maximum packet length for the ports. "**x**" is the maximum packet length with value 1518~9600.

23 **mdi/mdi-x** command

This command is used to configure MDI/MDI-X mode of port.

mdi/mdi-x [auto | mdi | mdi-x] command is used to configure MDI/MDI-X mode of ports. "mdi" is for Hub/Switch connection. "mdi-x" is for PC device connection. "auto" can auto-detect the connection.

24 **mvr** command

This command is used to configure MVR function for the ports.

mvr immediate-leave command is used to enable fast leave on the ports. And "**no mvr immediate-leave**" command is used to disable it.

mvr vlan x [inactive-port | receiver-port | source-port] command is used set the role of the ports for MVR VLAN "x". "**x**" is MVR VLAN ID with value 1~4094.

- **inactive-port** : The designated port does not participate MVR operations.
- **receiver-port** : Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages.
- **source-port** : Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports. Note: MVR source ports are not recommended to be overlapped with management VLAN ports.

25 **no** command

This command is used to disable a function or restore a setting to factory default of the switch.

```
(config-if)# no ?
  acl                   Access Control List Configuration
  arp-inspection        Set ARP inspection configuration
  channel-group         Adds ports to a trunk
  dhcp-snooping         Configures DHCP Snooping Configuration
  dot1x                 Configures 802.1x port-based access control
  eee                   Set the eee mode
  excessive             Configure port transmit collision behavior
  flow control          Enables flow control during autoneg
  ip                    Global IP configuration sub commands
  ip-source-guard       IP Source Guard Configuration
  lacp                  Configures LACP status
  lldp                  Configures lldp
  loopback-detection    Configures loopback detection
  mac-learn             Configures the maximum packet length of the port
  maximum-packet-length Configures the maximum packet length of the port
  mvr                   Multicast VLAN Registration
```

port	Configures the characteristics of the port
port-vlan	Configures Port-Based VLAN
power-control	Decrease energy consumption
qos	Configuration of QoS
sflow	configured sFlow samplers
shutdown	Shuts down the selected interface
spanning-tree	Specifies spanning tree configuration
speed	Configures speed operation
switchport	Configures switching mode characteristics
voice-vlan	Voice VLAN Configuration

For example,
"**lacp mode**" command can enable the LACP function on the interface port(s) and "**no lacp mode**" command can disable it.
"**maximum-packet-length 2000**" will set the maximum packet size to 2000, and "**no maximum-packet-length**" will put it to factory default setting 9600.

26 **port** command

This command is used to setup monitor function and security function on the interface port(s).

(config-if)# port ?

monitor	Monitors another interface
security	Specifies port security

port monitor ethernet 1/x [disabled | enabled | rx | tx] command is used to add Port x to the monitored port list. And "**no port monitor ethernet 1/x**" command will remove Port x from monitored port list. "**x**" is the monitored port number with format format 1/x, 1/x,y,z, 1/x-y, 1/x-y,z.
- **disabled** : Neither frames transmitted nor frames received are mirrored.
- **enabled** : Frames received and frames transmitted are mirrored on the mirror port.
- **rx** : Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored.
- **tx** : Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored.

port security action [none | shut | trap | trap_shut] command is used to set the action to take when port security is violated.
- **none** : If Limit is reached, no further action.
- **shut** : If Limit is reached, shut down the port.
- **trap** : If Limit is reached, send an SNMP trap.
- **trap_shut** : If Limit is reached, send an SNMP trap & shut down the port.

port security max-mac-count x command is used to set the maximum number of MAC addresses that can be secured on this port. "**x**" is the

maximum number and its valid value is 0-1024. For example, x=5 will allow up to five network devices / PC access network through the interface port(s). If the limit is exceeded, the corresponding action is taken.
The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.
port security mode command is used to enable Limit Control on this port. And "**no port security mode**" command is used to disable it. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect.
port security reopen command is used to reopen a shutdown port that is shuted down by the port security function.

27 **port-vlan** command

This command is used to assign the interface port(s) to a Port-based VLAN.

port-vlan x command will assign the interface port(s) to a Port-based VLAN. "**x**" is the index of the Port-based VLAN with value 1-10. And "**no port-vlan x**" command is used to remove the interface port(s) from a Port-based VLAN.

port-vlan isolation command is used to put the ports to the isolation port group. Memebers in the isolation port group will be isolated to each other even they are in the same VLAN. And "**no port-vlan isolation**" command is used to remove the ports from the isolation port group.

28 **power-control** command

This command is used to configure the power-control function for the interface port(s).

power-control [actiphy | disable | perfectreach | enable] command is used to set the the power savings mode for the interface port(s).
- **actiphy** : Link down power savings enabled.
- **disable** : Disable all power control.
- **perfectreach** : Link up power savings enabled.
- **enable** : Both link up and link down power savings.

29 **qos** command

This command is used to configure QoS function on the interface port(s).

```
(config-if)# qos ?
  classification        QoS Ingress Port Classification
```

dscp	QoS Port DSCP Configuration
policer	QoS Ingress Port Policers
queueshaper	Queue Shaper
scheduler	QoS Egress Port Schedulers
shaper	QoS Egress Port Shapers
tagremarking	QoS Egress Port Tag Remarking

"**qos classification ...**" command is used to configure default QoS Ingress Port Classification on ports.
qos classification class x command is used to set the default QoS class, i.e., the QoS class for frames not classified in any other way on the ports. "**x**" is the default class with value 0~7.
qos classification dpl x command is used to set the default Drop Precedence Level, i.e., the DP level for frames not classified in any other way on the ports. "**x**" is the default DP level with value 0~1.
qos classification dei x command is used to set the default DEI(Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.) for untagged frames on the ports. "**x**" is the default DEI with value 0~1.
qos classification dscp command is used to enable DSCP Based QoS Ingress Port Classification on the ports. And "**no qos classification dscp**" command is used to disable it.
qos classification map w x y z command is used to configure the ingress mapping of the classified (PCP, DEI) to (QoS class, DP level) values when Tag Classification is set to Enabled. "**w**" is pcp value 0~7. "**x**" is DEI value 0~1. "**y**" is QoS class value 0~7. "**z**" is DP level value 0~1.
qos classification pcp x command is used to set the default PCP(Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.) for untagged frames. "**x**" is value between 0~7.
qos classification tag command is used to enable using mapped versions of PCP and DEI for tagged frames. And "**no qos classification tag**" command is used to disable it. If it is disable, default QoS class and DP level is used for tagged frames.

"**qos dscp ...**" command is used to do QoS Port DSCP Configuration.
qos dscp classification [all | none | selected | zero] command is used to set Ingress DSCP values for its QoS class to internal DSCP mapping operation on the ports.
- **all** : Classify all DSCP values for its QoS class to internal DSCP mapping.
- **none** : No Ingress DSCP Classification.
- **selected** : Classify only selected DSCP. It is selected by "qos dscp classification-mode" command in (config)#.
- **zero** : Classify if incoming (or translated if enabled) DSCP is 0.

qos dscp egressremark [enable|remap_dp_aware|remap_dp_unaware] command is used to set DSCP Egress Rewriting operation mode on the

ports.
- **enable** : Rewrite enabled without remapping. The new DSCP value is defined by "qos dscp classification-map" command in (config)#.
- **remap_dp_aware** : Rewrite enabled with remapping. The remapped DSCP value is defined by "qos dscp egressremap" command in (config)#.
- **remap_dp_unaware** : Rewrite enabled with remapping. The remapped DSCP value is defined by "qos dscp egressremap" command with DP level=0 in (config)#.
"**no qos dscp egressremark**" command is used to disable it.
qos dscp translation command is used to enable the Ingress Translation on the ports. And "**no qos dscp translation**" command is used to disable it.

"**qos policer ...**" command is used to configure QoS Ingress Port Policers.
qos policer flowcontrol command is used to enable the port ingress policer flow control function. If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames. And "**no qos policer flowcontrol**" command is used to disable it.
qos policer mode command is used to enable ingress traffic rate policer function on the ports. A policer can limit the bandwidth of received frames. It is located in front of the ingress queue. And "**no qos policer mode**" command is used to disable it.
qos policer rate x command is used to set the port policer rate on the ports. "**x**" is a value between 100-1000000 when the Unit is kbps or fps, 1-3300 when the Unit is Mbps or kfps.
qos policer unit [kbps | fps] command is used to set the port policer rate unit on the ports. It could be "**kbps**" - kilo bit per second, or "**fps**" - frame per second.

"**qos queueshaper ...**" command is used to configure traffic shaping function of transmit queue of the ports.
qos queueshaper mode x command is used to enable traffic shaper on transmit queue "x". "**x**" is queue number with value 0~7. And "**no qos queueshaper mode x**" command is used to disable it.
qos queueshaper excess x command is used to enable that the transmit queue is allowed to use excess bandwidth. "**x**" is queue number with value 0~7. And "**no qos queueshaper excess x**" command is used to disable it.
qos queueshaper rate x y command is used to set traffic shaping rate "y" on transmit queue "x". "**x**" is queue number with value 0~7. "**y**" is traffic rate with value 100~3300000 in unit kbps.

"**qos scheduler ...**" command is used to configure traffic scheduling operation on transmit queue of the ports.
qos scheduler mode [strict | weighted] command is used to set traffic scheduling mode on transmit queue. It could be in "Strict Priority" or in"Weighted".

qos scheduler weight x y command is used to set weighting "y" for transmit queue "x". "**x**" is queue number with value 0~7. "**y**" is weighting with value 1~100. It is for traffic scheduling in Weighted mode.

"**qos shaper ...**" command is used to configure traffic shaper function of the ports.
qos shaper mode command is used to enable traffic shaper function on the ports. And "**no qos shaper mode**" command is used to disable it.
qos shaper rate x command is used to set traffic shaping rate "x" on the ports. "**x**" is traffic rate with value 100~3300000 in unit kbps.

"**qos tagremarking ...**" command is used to configure QoS Egress Port Tag Remarking for the ports.
qos tagremarking dei x command is used to set default DEI(Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.) on the ports when the tag-remarking mode is set to Default. "**x**" is the default DEI with value 0~1.
qos tagremarking map w x y z command is used to set the (QoS class, DP level) to (PCP, DEI) Mapping when the tag-remarking mode is set to Mapped. "**w**" is Qos Class with value 0~7. "**x**" is DP level with value 0~1. "**y**" is PCP with value 0~7. "**z**" is DEI with value 0~1.
qos tagremarking mode [classified | default | mapped] command is used to set the tag-remarking operation mode.
- **classified** : Use classified PCP/DEI values.
- **default** : Use default PCP/DEI values.
- **mapped** : Use mapped versions of QoS class and DP level.

Note: The egress port must be a tagged port for tag remarking operation.
qos tagremarking pcp x command is used to set default PCP(Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame.) on the ports when the tag-remarking mode is set to Default. "**x**" is PCP with value 0~7.

30 **sflow** command

This command is used to configure sflow function of the interface port(s).

sflow counterpoller enable command is used to enable counter poller. And "**no sflow counterpoller enable**" is used to disable it.
sflow counterpoller interval x command is used to set the the interval - in seconds - between counter poller samples. "**x**" is a value between 0~3600 in second.

sflow flowsampler enable command is used to enable flow sampling on this ports. And "**no sflow flowsampler enable**" command is used to disable it.
sflow flowsampler max_hdr-size x command is used to set the maximum

number of bytes that should be copied from a sampled packet to the sFlow datagram. "**x**" is the maximum number with valid range 14~200 bytes. If the maximum datagram size does not take into account the maximum header size, samples may be dropped.
sflow flowsampler sampling-rate x command is used to set the statistical sampling rate for packet sampling. "**x**" is the sampling rate with value 1~4294967295. The sample rate is specified as N to sample on average 1/Nth of the packets transmitted/received on the port. Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable sampling rate.

sflow sampler command is used to clear sflow statistics of the ports.

31 **shutdown** command
This command is used to disable the interface port(s).

shutdown command is used to disable the interface port(s).
no shutdown command is used to enable it.

32 **spanning-tree** command
This command is used to configure spanning tree function on interface port(s).

```
(config-if)# spanning-tree ?
  autoedge          Set the STP autoEdge port
  bpduguard         Set the bpduGuard port
  edge-port         Specifies spanning tree edge port
  mcheck            Set the STP mCheck (Migration Check) variable for ports
  msti              Specifies spanning tree MSTI
  p2p               Set the STP point2point port
  restrictedrole    Set the MSTP restrictedRole port
  restrictedtcn     Set the MSTP restrictedTcn port
  <cr>              Enables the spanning tree
```

spanning-tree autoedge command is used to enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not. "**no spanning-tree autoedge**" command is used to disable it.
spanning-tree bpduguard command is used to enable BPDU Guard function on interface port(s). If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not effect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well. "**no spanning-tree bpduguard**" command is used to disable it.

spanning-tree edge-port command is used to
spanning-tree edge-port command is used to set the operEdge flag should start as set. (The initial operEdge state when a port is initialized). "**no spanning-tree edge-port**" command is used to set the operEdge flag should start as cleared. operEdge flag is an operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having operEdge true) than for other ports.
spanning-tree mcheck command is used to restart the STP Migration Check for the ports. If at any time the switch detects STP BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can use the command to manually re-check the appropriate BPDU format to send on the selected interfaces (i.e., RSTP or STP-compatible).

spanning-tree msti x cost [auto | specific y] command is used to set the the path cost incurred by the ports in MSTI "x". "**x**" is the index of MSTI with value 0~7. "**y**" is cost value in range 1~200000000. The "**auto**" setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values.
spanning-tree msti x port_priority y command is used to set the port priority of the ports in MSTI "x". "**x**" is the index of MSTI with value 0~7. "**y**" is priority value in range 0~240. This can be used to control priority of ports having identical port cost.

spanning-tree p2p [auto | false | true] command is used to set the ponit-to-point connection mode for the ports. If the ports connects to a point-to-point LAN rather than to a shared medium, the ponit-to-point connection mode is true. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

spanning-tree restrictedrole command is used to enable the ports as restricted role in MSTP. If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard. "**no spanning-tree restrictedrole**" command is used to disable it.
spanning-tree restrictedtcn command is used to enable the ports as restricted TCN in MSTP. If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If

set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently. "**no spanning-tree restrictedtcn**" command is used to disable it.

spanning-tree command is used to enable Spanning Tree function on the ports. "**no spanning-tree**" command is used to disable it.

33 **speed** command

This command is used to set the operation speed and duplex mode of the interface port(s).

```
(config-if)# speed ?
  auto              Set port speed to be auto
  10hdx             Set port speed to be 10M hdx
  10fdx             Set port speed to be 10M fdx
  100hdx            Set port speed to be 100M fdx
  100fdx            Set port speed to be 100M fdx
  1000fdx           Set port speed to be 1G fdx
```

speed auto command will set the interface port(s) to auto-negotiation mode.
speed [10hdx | 10fdx] command will set the interface port(s) to 10M speed, full duplex or half duplex.
Speed [100hdx | 100fdx] command will set the interface port(s) to 100M speed, full duplex or half duplex.
speed 1000fdx command will set the interface port(s) to 1000M(gigabit) speed, full duplex.

34 **switchport** command

This command is used to configure VLAN Port Configuration for the interface port(s).

```
(config-if)# switchport ?
  acceptable-frame-types Specifies frame type
  allowed           Configures the VLAN port list
  ingressfilter     Set the port VLAN ingress filter
  mode              Configures the port type
  native            Configures the PVID of the port
  tx_tag            Set the port egress tagging
```

switchport acceptable-frame-types [all | tagged | untagged] command is

used to allow the interface port(s) to accept tagged or untagged frame.
- **all** : The port accepts all frames, tagged or untagged.
- **tagged** : The port accepts only tagged frames.
- **untagged** : The port accepts only untagged frames.

switchport allowed vlan [add x | **remove x | forbidden add x | forbidden remove x]** command will add the interface port(s) to VLAN x, remove the interface port(s) from VLAN x, as forbidden port(s) to VLAV x, not forbidden port(s) to VLAN x. "**x**" is the VLAN ID and its valid value is 2~-4094.

switchport ingressfilter command is used to enable VLAN ingress filter function on the ports. "**no switchport ingressfilter**" command is used to disable it.

switchport mode [c-port | s-custom-port | s-port | unaware] command is used to set Port Type of the ports. "Port Type" defines the port type in the provider bridge(Q-in-Q) model. Customer VLAN has TPID == 0x8100 and Service VLAN has TPID == 0x88A8. For the applications that there is no Q-in-Q support, S-port and S-custom-port could be ignored.
- **c-port** : When a port is setup as C-port, tagged frames will be classified to the VLAN based on this tag of the frames. This is for 802.1Q VLAN trunk.
- **s-custom-port** : When a port is setup as S-custom-port, the TPID in tag of egress frame are always customized TPID as Service VLAN. This is for Q-in-Q uplink connection.
- **s-port** : When a port is setup as S-port, the TPID in tag of egress frame are always 0x88A8 as Service VLAN. This is for Q-in-Q uplink connection.
- **unaware** : When a port is setup as Unaware. Incoming frames will be treated as untagged. Even when an incoming frame is tagged, this tag is treated by the switch as payload. And the frame will be classified to port based VLAN — PVID. This for 802.1Q access connection or Q-in-Q downlink connection. If Port-based VLAN is used, please set ports as "Unaware" with the same PVID.

switchport native vlan [none | x] command is used to assign VLAN ID of the native VLAN for classifying untagged frames on ingress port. "**x**" is the port VLAN ID (PVID) and its valid value is 1~4094. "**none**" is used when this is VLAN trunk port.
When untagged packet is received, PVID of the ingress port will be used as its working VLAN ID. PVID is also used as the VLAN ID for tag adding when untagged packet is translated to tagged packet.
switchport tx_tag [tag_all | untag_all | untag_pvid] command is used to define how frame will be tagged on the egress direction -- when frame is sent out of the switch from this port.
- **tag_all** : this is a tagged egress port. All egress packets are tagged.
- **untag_all** : this is a untagged egress port. All egress packets are

untagged.
- **untag_pvid** : this is a hybrid egress port. All egress packets except the configured PVID will be tagged.

35 **voice-vlan** command

This command is used to configure Voice VLAN function for the interface port(s).

```
(config-if)# voice-vlan ?
  discovery-protocol    Set the Voice VLAN port discovery protocol mode
  port-mode             Set the Voice VLAN port mode
  security              Set the Voice VLAN port security mode
```

voice-vlan discovery-protocol [both | lldp | oui] command is used to set the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process.
Possible discovery protocols are:
- **oui** : Detect telephony device by OUI address.
- **lldp** : Detect telephony device by LLDP.
- **both** : Both OUI and LLDP..

voice-vlan port-mode [auto | disable | force] command is used to set Voice VLAN operation mode on the ports.
- **auto** : Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically.
- **disable** : Disjoin from Voice VLAN.
- **force** : Force join to Voice VLAN.

voice-vlan security command is used to enable security function on the ports. When the security function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. "**no voice-vlan security**" command is used to disable it.

6.2.4.2 Interface Configuring Commands for VLAN

Commands in Configuring Mode are for general switch settings. And its prompt is "(config)#".
If the characteristics are for VLAN group, it is done with "**interface vlan x**" command in configure mode. For example, "interface vlan 100" is for characteristics settings on VLAN 100.

Note: The general VLAN settings are done with "**vlan database**" command. Please refer to section **6.2.5 VLAN Configuring Commands** for the details. And **interface vlan x** command is used to assign characteristics to a VLAN group interface. For example, assigning IP address to a VLAN interface is done with this command.

Entering "interface vlan 100", and its prompt will become ...

```
(config)# interface vlan 100
(config-if)#
```

Enter "?" at the prompt, the sub-command list will be shown.

```
---------------------------------------------------------------------------------------------
(config-if)# ?
  exit                Exit from current mode
  help                Show available commands
  history             Show a list of previously run commands
  logout              Disconnect
  quit                Quit commands
  interface           Enters privileged interface configuration
  ip                  Set the IPv4 setup
  ipv6                Set othe IPv6 setup
  no                  Negates a command or sets its defaults
---------------------------------------------------------------------------------------------
```

1. **exit** command
   This command is used to leave current operation mode. Go back to last mode.

2. **help** command
   This command is used to show all the available commands in this mode.

3. **history** command
   This command is used to show the history of entering commands.

4. **logout** command
   This command is used to logout from console interface.

5. **quit** command
   This command is used to quit from console interface. It has the same function as logout.

6. **interface** command
   This command is used to change to another interface VLAN groups for next setup commands.

```
(config-if)# interface ?
  vlan                Switch Virtual LAN interface
```

   For example,
   "(config-if)**#** interface vlan 100" will change the setup interface to VLAN 100 and all following commands will be applied to VLAN 100.

7. **ip** command
   This command is used to set IP address of the switch on this VLAN interface. And only users in this VLAN can access this switch with the IP address remotely.

```
(config-if)# ip address ?
  dhcp                Dynamic host configuration protocol
  A.B.C.D             IP address
  renew               Renew IP
```

   ip address dhcp command is used to enable DHCP client function. DHCP client function will try to get IP configuration from DHCP server in network. And **no ip address dhcp** command can be used to disable it.
   If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP server does not respond around 35 seconds and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.

   ip address x.x.x.x y.y.y.y command is used to set IP address of the switch on this VLAN. "**x.x.x.x**" is the IP address. "**y.y.y.y**" is the subnet mask.
   For example, "ip address 192.168.1.12 255.255.255.0" will set the IP address of the switch on this VLAN group for remote management.

   ip address renew command is used to refresh the lease time of the IP address got by DHCP. If IP configuration is not got when boot-up, this command will try to get IP configuration again.

8. **ipv6** command

This command is used to set IPv6 address of the switch on this VLAN interface. And only users in this VLAN can access this switch with the IPv6 address remotely.

```
(config-if)# ipv6 address ?
  autoconfig          Set the IPv6 AUTOCONFIG mode
  renew               Renew IP
  <ipv6 address>      IPv6 address For example, fc80::215:c5ff:fe03:4dc7
```

ipv6 address autoconfig command is used to enable IPv6 Auto Configuration function. "**no ipv6 address autoconfig**" command is used to disable it.

If system cannot obtain the stateless address in time, the configured IPv6 settings will be used. The router may delay responding to a router solicitation for a few seconds, the total time needed to complete auto-configuration can be significantly longer.

ipv6 address renew command is used to refresh the the IPv6 address got by IPv6 Auto Configuration function.

ipv6 address <ipv6 address> command is used to set IPv6 adress of the switch on this VLAN. "**<ipv6 address>**" is the IPv6 address.

9. **no** command

This command is used to disable a function or restore a setting to factory default of the switch.

```
(config-if)# no ?
  ip                  Set the IPv4 setup
  ipv6                Set the IPv6 setup
```

For example,

"**ip address dhcp**" command can enable DHCP client function on the VLAN group interface and "**no ip address dhcp**" command can disable it.

6.2.5 VLAN Configuring Commands

Commands in Configuring Mode are for general switch settings. And its prompt is "(config)#".

If the settings are for VLANs, it should enter VLAN configuring mode first by "**vlan database**" command in configure mode. And its prompt will become "**(config-vlan)#**".
Note: If the settings are for some VLAN group (VLAN ID is known), it should enter interface configuring mode for VLAN first by "interface vlan x" command. ("x" is the VLAN ID.) And its prompt is "(config-if)#". It is described in Section 6.2.4.2.

Entering "vlan database", and the prompt will become ...
(config)# vlan database
(config-vlan)#

Enter "?" at the prompt, the sub-command list will be shown.

```
-------------------------------------------------------------------------------------------
(config-vlan)# ?
  exit                Exit from current mode
  help                Show available commands
  history             Show a list of previously run commands
  logout              Disconnect
  quit                Quit commands
  end                 Exit from vlan mode
  no                  Negates a command or sets its defaults
  vlan                Switch Virtual LAN interface
-------------------------------------------------------------------------------------------
```

1 **exit** command
This command is used to leave current operation mode. Go back to last mode.

2 **help** command
This command is used to show all the available commands in this mode.

3 **history** command
This command is used to show the history of entering commands.

4 **logout** command
This command is used to logout from console interface.

5 **quit** command
This command is used to quit from console interface. It has the same function as logout.

6 **end** command
This command is used to exit from VLAN Configuring mode.
(config-vlan)# end
(config)#

7 **no** command
This command is used to disable a function or restore a setting to factory default of the switch.

(config-vlan)# no ?
vlan Switch Virtual LAN interface

For example,
"**no vlan 100**" command will remove VLAN 100.

8 **vlan** command
This command is used to create a 802.1Q VLAN, or set the Custom S-port EtherType for Q-in-Q operation.

vlan x command is used to create a VLAN. "**x**" is the VLAN ID between 1~4094. "**no vlan x**" command is used to delete VLAN "x".
vlan x name yyy command is used to create a VLAN with VLAN ID "x" and VLAN Name "yyy". "**x**" is the VLAN ID between 1~4094. "**yyy**" is a string.

vlan etypecustomsport 0xXXXX command is used to set the Custom S-port EtherType for Q-in-Q operation. "**0xXXXX**" is the EtherType in heximal.

6.2.6 Show Commands

Show command is put in General Basic Commands for viewing system configuration and information.

Enter “show ?” at the prompt, the sub-command list will be shown.

```
---------------------------------------------------------------------------------------------
# show ?
  aaa                   Show AAA service configuration
  acl                   Packet Access Control List
  calendar              Date and time information
  ddmi                  Digital Diagnostics Monitoring Interface
  dhcp-relay            DHCP Relay Configuration
  dot1x                 802.1x content
  eee                   Show eee configuration
  history               History information
  interface             Interface information
  ip                    IP information
  lacp                  LACP statistics
  lldp                  Show lldp Configuration
  log                   Log records
  loopback-detection    Show loopback detection
  mac-address-table     Configuration of the address table
  mac-security          MAC Security Configuration
  management            Management IP filter
  map                   Maps priority
  mvr                   Show MVR Status
  ntp                   Simple Network Time Protocol configuration
  port                  Port characteristics
  queue                 Priority queue information
  radius-server         RADIUS server information
  running-config        Information on the running configuration
  rate-limit            rate-limits
  rmon                  Rmon
  sflow                 Sampling flow
  snmp                  Simple Network Management Protocol statistis
  spanning-tree         Spanning-tree configuration
  storm-control         Show storm control configuration
  system                System information
  tacacs-server         TACACS server settings
  trunk                 Trunk information
  users                 Show users configuration
  version               System hardware and software versions
  vlan                  Virtual LAN settings
---------------------------------------------------------------------------------------------
```

1. **show acl** command
   This command will show ACL settings and status.

```
# show acl ?
  ports                  Show the ACL port configuration
  rate                   Show the ACL rate limiter
  status                 Show ACL status
  <1-256>                show an access list configuration
  <cr>                   show all access list configuration
```

   show acl port command will show ACL port configration.
   For example,

```
# show acl port
ACL Configuration:
==================
```

Port	Policy	Action	Rate L.	Port C.	Mirror	Logging	Shutdown	Counter
1	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	0
2	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	0
3	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	0
4	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	0
5	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	0
6	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	0
7	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	0
8	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	0
9	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	0
10	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	0

Port	State
1	Enabled
2	Enabled
3	Enabled
4	Enabled
5	Enabled
6	Enabled
7	Enabled
8	Enabled
9	Enabled
10	Enabled

   show acl rate command will show ACL rate limiters setting.
   For example,

```
# show acl rate
Rate Limiter     Rate
```

1	1 PPS
2	1 PPS
3	1 PPS
4	1 PPS
5	1 PPS
6	1 PPS
7	1 PPS
8	1 PPS
9	1 PPS
10	1 PPS
11	1 PPS
12	1 PPS
13	1 PPS
14	1 PPS
15	1 PPS
16	1 PPS

show acl status command will show ACL status.
For example,

```
# show acl status
User
----
S    : Static
IPSG: IP Source Guard
IPMC: IPMC
ARPI: ARP Inspection
DHCP: DHCP
LOOP: Loop Protect

User ID   Port     Frame   Action   Rate L.   Port C.   Mirror   CPU     Counter Confl.
---- --   -------  -----   ------   --------  --------  --------  ------  ------- ---
---
S    1    All      Any     Permit   Disabled Disabled Disabled No       29794   No

Number of ACEs: 1
```

- User : the ACL user
- ID : the ACE ID number
- Port : ingress port of the ACE
- Frame : the frame type of the ACE
- Action : action of the ACE
- Rate L. : the rate limiter number of the ACE
- Port C. : the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number.
- Mirror : mirror operation of this ACE.
- CPU : Forward packet that matched the specific ACE to CPU.

- Counter : counter indicates the number of times the ACE was hit by a frame.
- Confl. : the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

show acl x command is used to show an ACE status. "**x**" is the ID of ACE with value 1~256.
For example,

```
# show acl 1
ACE ID          : 1                    Rate Limiter : Disabled
Ingress Port    : All                    Port Redirect: Disabled
                                       Mirror       : Disabled
Policy/Bitmask: Any                     Logging      : Disabled
Type            : User                  Shutdown     : Disabled
Frame Type      : Any                   Counter      : 31393
Action          : Permit

MAC Parameters                         VLAN Parameters
---------------                          ---------------
                                       802.1Q Tagged: Any
                                       VLAN ID      : Any
                                       Tag Priority : Any
```

show acl command will show all ACE status.
For example,

```
# show acl
ID   Type      Port     Policy    Frame  Action Rate L.  Port C.  Mirror    Counter
--   -------   ------   ------    ---- ------ ------  --------  --------  --------  -------
1    User      All      Any       Any    Permit Disabled Disabled Disabled  31741

Number of ACEs: 1
```

2. **show calendar** command
   This command will show current system time.
   For example,

```
# show calendar
System Time      : 2012-01-01T05:09:39+00:00
System Uptime    : 05:09:39
```

3. **show dhcp-relay** command
   This command will show current DHCP Relay settings and status.
   For example,

```
# show dhcp-relay
DHCP Relay Configuration:
=========================
DHCP Relay Mode                  : Disabled
```

```
DHCP Relay Server                : 192.168.1.100
DHCP Relay Information Mode      : Enabled
DHCP Relay Information Policy : Replace

Server Statistics:
------------------
Transmit to Server        :        0    Transmit Error              :        0
Receive from Server       :        0    Receive Missing Agent Option :       0
Receive Missing Circuit ID :       0    Receive Missing Remote ID    :       0
Receive Bad Circuit ID    :        0    Receive Bad Remote ID        :       0

Client Statistics:
--------------------
Transmit to Client    :        0    Transmit Error       :        0
Receive from Client   :        0    Receive Agent Option :        0
Replace Agent Option :         0    Keep Agent Option    :        0
Drop Agent Option     :        0
```

4. **show dot1x** command
   This command is used to show 802.1x configuration and status.

   show dot1x command is used to show current 802.1x Network Access Server Switch Status. For example,

```
# show dot1x
Port   Admin State          Port State           Last Source       Last ID
----   -----------------    ---------------------  -----------------  -----------------
1      Force Unauthorized   Globally Disabled      -                  -
2      Force Unauthorized   Globally Disabled      -                  -
3      Force Unauthorized   Globally Disabled      -                  -
4      Force Unauthorized   Globally Disabled      -                  -
5      Force Unauthorized   Globally Disabled      -                  -
6      Force Unauthorized   Globally Disabled      -                  -
7      Force Unauthorized   Globally Disabled      -                  -
8      Force Unauthorized   Globally Disabled      -                  -
9      Force Unauthorized   Globally Disabled      -                  -
10     Force Unauthorized   Globally Disabled      -                  -
```

   - Last Source : The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.
   - Last ID : The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

   show dot1x configuration command is used to show 802.1x configuration

and status of the switch. For example,

```
# show dot1x configuration
802.1X Configuration:
=====================
Mode                 : Disabled
Reauth.              : Disabled
Reauth. Period       : 3600
EAPOL Timeout        : 30
Age Period           : 300
Hold Time            : 10
RADIUS QoS           : Disabled
RADIUS VLAN          : Disabled
Guest VLAN           : Disabled
Guest VLAN ID        : 1
Max. Reauth Count: 2
Allow Guest VLAN if EAPOL Frame Seen: Disabled
```

show dot1x guest_vlan command is used to show per-port enabledness of Guest VLAN. For example,

```
# show dot1x guest_vlan
          Guest
Port      VLAN          Current
----      -------       -------
1         Disabled
2         Disabled
3         Disabled
4         Disabled
5         Disabled
6         Disabled
7         Disabled
8         Disabled
9         Disabled
10        Disabled
```

show dot1x radius_qos command is used to show per-port enabledness of RADIUS-assigned QoS. For example,

```
# show dot1x radius_qos
         RADIUS
Port     QoS          Current
----     -------      -------
1        Disabled
2        Disabled
3        Disabled
4        Disabled
5        Disabled
6        Disabled
7        Disabled
8        Disabled
```

```
9       Disabled
10      Disabled
```

show dot1x radius_vlan command is used to show per-port enabledness of RADIUS-assigned VLAN. For example,

```
# show dot1x radius_vlan
        RADIUS
Port    VLAN        Current
----    --------    --------
1       Disabled
2       Disabled
3       Disabled
4       Disabled
5       Disabled
6       Disabled
7       Disabled
8       Disabled
9       Disabled
10      Disabled
```

show dot1x statistics command is used to show 802.1X statistics. For example,

```
# show dot1x statistics
Port 1 EAPOL Statistics:
Rx Total:                0    Tx Total:                0
Rx Response/Id:          0    Tx Request/Id:           0
Rx Response:             0    Tx Request:              0
Rx Start:                0
Rx Logoff:               0
Rx Invalid Type:         0
Rx Invalid Length:       0

Port 1 Backend Server Statistics:
Rx Access Challenges:    0    Tx Responses:            0
Rx Other Requests:       0
Rx Auth. Successes:      0
Rx Auth. Failures:       0
---More---
```

5. **show eee** command

This command is used to show EEE (IEEE 802.3az) configuration.

For example,

```
# show eee
EEE Configuration:
==================
Port    Mode        Urgent queues
```

1	Disabled	none
2	Disabled	none
3	Disabled	none
4	Disabled	none
5	Disabled	1
6	Disabled	none
7	Disabled	none
8	Disabled	none
9	N/A	none
10	N/A	none

6. **show history** command

This command is used to show the history of input commands.

```
# show history
  1. config
  2. interface valn 10
  3. ipv6 address state fc80::215:c5ff:fe03:4dc7
  4. exit
  5. show history
```

7. **show interface** command

This command is used to show port information and status.

```
# show interface ?
  counters                Interface counters information
  detailed_counters       Interface detailed counters information
  dualMedia_fiberMode     Show the port speed for fiber ports
  psec                    Port security status
  sfp                     Show the detected sfp type
  status                  Interface status information
  switchport              Interface switchport information
  veriphy                 Run cable diagnostics
```

show interface counters command will show statistics counters for all ports.
show interface counters ethernet 1/x command will show statistics counters for Port x. ("**x**" is the port number).

For example,

```
# show interface counters ethernet 1/5
Port: 1/5
=======================================
Rx Counter                    Statistics
Packets                       0
Octets                        0
```

Errors	0
Drops	0
Filtered	0

==========

Tx Counter	Statistics
Packets	0
Octets	0
Errors	0
Drops	0

show interface detailed_counters command will show detail statistics counters for all ports.

show interface detailed_counters ethernet 1/x command will show detail statistics counters for Port x. ("**x**" is the port number).

For example,

show interface detailed_counters ethernet 1/5

Rx Packets:	0	Tx Packets:	0
Rx Octets:	0	Tx Octets:	0
Rx Unicast:	0	Tx Unicast:	0
Rx Multicast:	0	Tx Multicast:	0
Rx Broadcast:	0	Tx Broadcast:	0
Rx Pause:	0	Tx Pause:	0
Rx 64:	0	Tx 64:	0
Rx 65-127:	0	Tx 65-127:	0
Rx 128-255:	0	Tx 128-255:	0
Rx 256-511:	0	Tx 256-511:	0
Rx 512-1023:	0	Tx 512-1023:	0
Rx 1024-1526:	0	Tx 1024-1526:	0
Rx 1527- :	0	Tx 1527- :	0

show interface psec port command will show MAC addresses learned by port security. For example,

show interface psec port

Port 1:

MAC Address	VID	State	Added	Age/Hold Time

<none>

---More---

show interface psec switch command will show port security status. For example,

show interface psec switch

Users:

L = Limit Control

8 = 802.1X

D = DHCP Snooping

V = Voice VLAN

Port	Users	State	MAC Cnt
1	----	No users	0
2	----	No users	0
3	----	No users	0
4	----	No users	0
5	----	No users	0
6	----	No users	0
7	----	No users	0
8	----	No users	0
9	----	No users	0
10	----	No users	0

show interface sfp command will show the detected sfp type.
For example,
show interface sfp

Port	SFP
1	None
2	None
3	None
4	None
5	None
6	None
7	None
8	None
9	None
10	None

show interface status command will show port configuration.
show interface status
Port Configuration:

Port	State	Mode	Flow Control	MaxFrame	Power	Excessive	Link
1	Enabled	Auto	Disabled	9600	Disabled	Discard	Down
2	Enabled	Auto	Disabled	9600	Disabled	Discard	Down
3	Enabled	Auto	Disabled	9600	Disabled	Discard	Down
4	Enabled	Auto	Disabled	9600	Disabled	Discard	Down
5	Enabled	Auto	Disabled	9600	Disabled	Discard	Down
6	Enabled	Auto	Disabled	9600	Disabled	Discard	Down
7	Enabled	Auto	Disabled	9600	Disabled	Discard	100fdx
8	Enabled	Auto	Disabled	9600	Disabled	Discard	Down
9	Enabled	Auto	Disabled	9600	Disabled	Discard	Down
10	Enabled	Auto	Disabled	9600	Disabled	Discard	Down

show interface switchport command will show VLAN configuration of all ports. For example,

```
#show interface switchport
VLAN Configuration:
==================
Port  PVID  Frame Type  Ingress Filter  Tx Tag      Port Type
----  ----  ----------  --------------  ----------  -------------
1     1     All         Disabled        Untag PVID  Unaware
2     1     All         Disabled        Untag PVID  Unaware
3     1     All         Disabled        Untag PVID  Unaware
4     1     All         Disabled        Untag PVID  Unaware
5     1     All         Disabled        Untag PVID  Unaware
6     1     All         Disabled        Untag PVID  Unaware
7     1     All         Disabled        Untag PVID  Unaware
8     1     All         Disabled        Untag PVID  Unaware
9     1     All         Disabled        Untag PVID  Unaware
10    1     All         Disabled        Untag PVID  Unaware
```

show interface switchport status command will show VLAN Port Configuration Status. For example,

```
# show interface switchport status
Port VLAN User PortType    PVID Frame Type  Ing Filter  Tx Tag      UVID  Conflicts
---- ----------  ----------  ---- ----------  ----------  ----------  ----  ------
---
1    Static      Unaware     1    All         Disabled    Untag This  1
     NAS                                                                 No
     MVR                                                                 No
     Voice VLAN                                                          No
     MSTP                                                                No
     Combined    Unaware     1    All         Disabled    Untag This  1     No
---More---
```

show interface veriphy command will run cable diagnostics. For example,

```
# show interface veriphy
Starting VeriPHY, please wait
Port    Pair A    Length    Pair B    Length    Pair C    Length    Pair D    Length
-----   -------   -------   -------   -------   -------   -------   -------   ------
1       Open      0         Open      0         Open      0         Open      0
2       Open      0         Open      0         Open      0         Open      0
3       Open      0         Open      0         Open      0         Open      0
4       Open      0         Open      0         Open      0         Open      0
5       Open      0         Open      0         Open      0         Open      0
6       Open      0         Open      0         Open      0         Open      0
7       OK        3         OK        3         Open      3         Open      3
8       Open      0         Open      0         Open      0         Open      0
```

8. **show ip** command

This command is used to show switch IP configuration and current ARP Inspection, DHCP Snooping, Http Configuration, IGMP/MLD Snooping, SSH, IP Source Guard,... status and configuration.

```
# show ip ?
  arp                 Address Resolution Protocol
  dhcp                DHCP snooping
  http                Show HTTP configuration
  igmp                IGMP snooping
  interface           Interface information
  mld                 MLD snooping
  ssh                 Secure shell server connections
  verify              IP Source Guard
```

show ip arp inspection command is used to show ARP Inspection configuration and status. For example,

```
# show ip arp inspection
ARP Inspection Configuration:
============================
ARP Inspection Mode : Disabled

Port   Port Mode
----   -----------
1      Disabled
2      Disabled
3      Disabled
4      Disabled
5      Disabled
6      Disabled
7      Disabled
8      Disabled
9      Disabled
10     Disabled

ARP Inspection Entry Table:

Type       Port   VLAN   MAC Address          IP Address
-------    ----   ----   -----------------    -------------
```

show ip dhcp snooping command is used to show DHCP Snooping configuration.

show ip dhcp snooping statistics command is used to show DHCP Snooping statistics.

```
# show ip dhcp snooping
DHCP Snooping Configuration:
============================
```

DHCP Snooping Mode : Disabled

Port	Port Mode
1	trusted
2	trusted
3	trusted
4	trusted
5	trusted
6	trusted
7	trusted
8	trusted
9	trusted
10	trusted

show ip dhcp snooping statistics
Port 1 Statistics:

Rx Discover:	0	Tx Discover:	0
Rx Offer:	0	Tx Offer:	0
Rx Request:	0	Tx Request:	0
Rx Decline:	0	Tx Decline:	0
Rx ACK:	0	Tx ACK:	0
Rx NAK:	0	Tx NAK:	0
Rx Release:	0	Tx Release:	0
Rx Inform:	0	Tx Inform:	0
Rx Lease Query:	0	Tx Lease Query:	0
Rx Lease Unassigned:	0	Tx Lease Unassigned:	0
Rx Lease Unknown:	0	Tx Lease Unknown:	0
Rx Lease Active:	0	Tx Lease Active:	0

---More---

show ip http server secure status commans will show current Http security mode status.

show ip http server secure status
HTTPS Configuration:
==========
HTTPS Mode : Enabled
HTTPS Redirect Mode : Disabled

show ip igmp command will show current IGMP Snooping configuration.

show ip igmp
IGMP Configuration:
==========
IGMP Mode: Disabled
IGMP SSM Range: 232.0.0.0/8
IGMP Leave Proxy: Disabled
IGMP Flooding Control: Enabled

```
IGMP Interface Setting
VID     Compatibility
----      -------------
(Please create IGMP Interfaces)

IGMP Port Status ( Router-Port )
Port    Router      Dynamic Router
----    --------      --------------
1       Disabled    No
---More---
```

show ip interface command will show current switch IP configuration.

```
# show ip interface
IP Configuration:
=================
DHCP Client          : Disabled
IP Address           : 192.168.1.118
IP Mask              : 255.255.255.0
IP Router            : 0.0.0.0
DNS Server           : 0.0.0.0
VLAN ID              : 1
DNS Proxy            : Disabled

IPv6 AUTOCONFIG mode     : Disabled
IPv6 Link-Local Address: fe80::2c0:f9ff:fe66:6699
IPv6 Address             : fc80::215:c5ff:fe03:4dc0
IPv6 Prefix              : 120
IPv6 Router              : ::

Active Configuration for IPv6: (Static w ith Stateless)
IPv6 Address: fe80:2::2c0:f9ff:fe66:6699/64 Scope:Link
Status:UP/RUNNING(Enabled)/MTU 1500/LinkMTU is 1500
IPv6 Address: fc80::215:c5ff:fe03:4dc0/128 Scope:Global
Status:UP/RUNNING(Enabled)/MTU 1500/LinkMTU is 1500
```

show ip mld command will show current MLD Snooping configuration.

```
# show ip mld
MLD Configuration:
==================
MLD Mode: Disabled
MLD SSM Range: ff3e::/96
MLD Leave Proxy: Disabled
MLD Flooding Control: Enabled

MLD Interface Setting
VID     Compatibility
----      -------------
```

(Please create MLD Interfaces)

MLD Port Status (Router-Port)
Port Router Dynamic Router
---- -------- --------------
1 Disabled No
---More---

show ip ssh command will show current SSH settings.
show ip ssh
SSH Configuration:
==========
SSH Mode : Enabled

show ip verify source command will show IP Source Guard configuration.
show ip verify source
IP Source guard Configuration:
==========
IP Source Guard Mode : Enabled
Port Port Mode Dynamic Entry Limit
---- ---------- ----------
1 Disabled unlimited
2 Disabled unlimited
3 Disabled unlimited
4 Disabled unlimited
5 Disabled unlimited
6 Disabled unlimited
7 Disabled unlimited
8 Disabled unlimited
9 Disabled unlimited
10 Disabled unlimited

IP Source Guard Entry Table:
Type Port VLAN IP Address MAC Address
------- ---- ---- ---------- ----------

9. **show lacp** command
This command is used to show current LACP configuration and status of the switch.

show lacp ?
config Show LACP configuration
statistics Show LACP statistics
status Show LACP status

show lacp config command will show current LACP configuration.

```
# show lacp config
LACP Configuration:
===================
System Priority: 32768

Port   Mode       Key    Role    Timeout
----   --------    ----   ------   -------
1      Disabled   Auto   Active   Fast
2      Disabled   Auto   Active   Fast
3      Disabled   Auto   Active   Fast
4      Disabled   Auto   Active   Fast
5      Disabled   Auto   Active   Fast
6      Disabled   Auto   Active   Fast
7      Disabled   Auto   Active   Fast
8      Disabled   Auto   Active   Fast
9      Disabled   Auto   Active   Fast
10     Disabled   Auto   Active   Fast
```

show lacp statistics command will show current LACP statistics.

```
# show lacp statistics
System Priority: 32768

Port   Timeout   Priority Rx Frames   Tx Frames   Rx Unknown   Rx Illegal
----   -------   ------------------   ----------   ----------   ----------
1      Fast      327680               0            0            0
2      Fast      327680               0            0            0
3      Fast      327680               0            0            0
4      Fast      327680               0            0            0
5      Fast      327680               0            0            0
6      Fast      327680               0            0            0
7      Fast      327680               0            0            0
8      Fast      327680               0            0            0
9      Fast      327680               0            0            0
10     Fast      327680               0            0            0
```

show lacp status command will show current LACP status.

```
# show lacp status

Port   Mode       Key    Aggr ID   Partner System ID   Partner Port   Partner Port Prio
----   --------    -----   -------   ------------------   ------------   ------------------
1      Disabled   1      -         -                    -              -
2      Disabled   1      -         -                    -              -
3      Disabled   1      -         -                    -              -
4      Disabled   1      -         -                    -              -
5      Disabled   1      -         -                    -              -
6      Disabled   1      -         -                    -              -
7      Disabled   2      -         -                    -              -
```

8	Disabled	1	-	-	-	-
9	Disabled	1	-	-	-	-
10	Disabled	1	-	-	-	-

10. **show lldp** command

This command is used to show current LLDP configuration and status.

show lldp command will show current LLDP configuration.

```
# show lldp
LLDP Configuration:
==================
Interval      : 30
Hold          : 4
Tx Delay      : 2
Reinit Delay: 2
```

Port	Mode	Port Descr	System Name	System Descr	System Capa	Mgmt Addr	CDP awareness
1	Disabled	Enabled	Enabled	Enabled	Enabled	Enabled	Disabled
2	Disabled	Enabled	Enabled	Enabled	Enabled	Enabled	Disabled
3	Disabled	Enabled	Enabled	Enabled	Enabled	Enabled	Disabled
4	Disabled	Enabled	Enabled	Enabled	Enabled	Enabled	Disabled
5	Disabled	Enabled	Disabled	Enabled	Enabled	Enabled	Disabled
6	Disabled	Enabled	Enabled	Enabled	Enabled	Enabled	Disabled
7	Disabled	Enabled	Enabled	Enabled	Enabled	Enabled	Disabled
8	Disabled	Enabled	Enabled	Enabled	Enabled	Enabled	Disabled
9	Disabled	Enabled	Enabled	Enabled	Enabled	Enabled	Disabled
10	Disabled	Enabled	Enabled	Enabled	Enabled	Enabled	Disabled

show lldp info command will show LLDP neighbor device information.

```
# show lldp info
No LLDP entries found
```

show lldp statistics command will show LLDP statistics.

```
# show lldp statistics
LLDP global counters
Neighbor entries was last changed at 1970-01-01T00:00:00+00:00  (23776 sec. ago).
Total Neighbors Entries Added    0.
Total Neighbors Entries Deleted  0.
Total Neighbors Entries Dropped  0.
Total Neighbors Entries Aged Out 0.

LLDP local counters
        Rx          Tx          Rx          Rx        Rx TLV     Rx TLV     Rx TLV
Port    Frames      Frames      Errors      Discards  Errors     Unknown    Organiz.   Aged
```

1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0

11. **show log** command

This command is used to show current system log and system log configuration.

```
# show log ?
  configuration          logging configuration
  <cr>
```

show log command is used to show current system log content.

For example,

```
# show log
Number of entries:
Info    : 2
Warning: 0
Error   : 0
All     : 2

ID   Level   Time                        Message
---- ------  --------------------------  -------
1    Info    2011-01-01T00:00:00+00:00   Switch just made a cold boot.
2    Info    2011-01-01T00:00:03+00:00   Link up on port 7
```

show log configuration command is used to show current system log configuration.

For example,

```
# show log configuration
System Log Configuration:
=========================
System Log Server Mode      : Disabled
System Log Server Address   :
System Log Level            : Error
```

12. **show loopback-detection** command

This command is used to show Loopback Detection configuration and status.

```
# show loopback-detection ?
  config              Loop protect configuration
  ethernet            Show loop protection port configuration
  status              Show the loop protection status
```

show loopback-detection config command will show Loopback Detection configuration.

```
# show loopback-detection config
Loop Protection Configuration:
==============================
Loop Protection   : Disabled
Transmission Time: 5
Shutdown Time     : 180
```

show loopback-detection ethernet command will show loop protection port configuration.

```
# show loopback-detection ethernet
Port   Mode       Action          Transmit
----   --------   ------------     --------
1      Enabled    Shutdown        Enabled
2      Enabled    Shutdown        Enabled
3      Enabled    Shutdown        Enabled
4      Enabled    Shutdown        Enabled
5      Enabled    Shutdown        Enabled
6      Enabled    Shutdown        Enabled
7      Enabled    Shutdown        Enabled
8      Enabled    Shutdown        Enabled
9      Enabled    Shutdown        Enabled
10     Enabled    Shutdown        Enabled
```

show loopback-detection status command will show the loop protection status.

```
# show loopback-detection status
Port    Action          Transmit   Loops   Status     Loop   Time of Last Loop
----    ------------     --------   --------  --------     ----   ----------------
1       Shutdown        Enabled      0    Down       -      -
2       Shutdown        Enabled      0    Down       -      -
3       Shutdown        Enabled      0    Down       -      -
4       Shutdown        Enabled      0    Down       -      -
5       Shutdown        Enabled      0    Down       -      -
6       Shutdown        Enabled      0    Down       -      -
7       Shutdown        Enabled      0    Up         -      -
8       Shutdown        Enabled      0    Down       -      -
9       Shutdown        Enabled      0    Down       -      -
10      Shutdown        Enabled      0    Down       -      -
```

13. **show mac-address-table** command

This command is used to set Mac address table and configuration about it.

```
# show mac-address-table ?
  aging-time          Aging time for entries in the address table
  address             Address information
  learning            Show the port learn mode
  statistics          Show MAC address table statistics
  <cr>
```

show mac-address-table command will show mac address table content.

For example,

```
# show mac-address-table
Type      VID   MAC Address          Ports
------   ---   -----------------   -----
Dynamic 1      00-00-e2-82-8c-e6   7
Dynamic 1      00-0a-79-b9-a2-c3   7
Dynamic 1      00-0d-87-26-f4-3b   7
Dynamic 1      00-c0-f6-55-09-9b   7
Dynamic 1      00-c0-f6-74-25-01   7
Static   1     00-c0-f9-66-66-99   None,CPU
Static   1     33-33-00-00-00-01   1-8,10,CPU
Static   1     33-33-00-00-00-02   1-8,10,CPU
Static   1     33-33-ff-03-4d-c0   1-8,10,CPU
Static   1     33-33-ff-66-66-99   1-8,10,CPU
Dynamic 1      70-5a-b6-f8-32-ea   7
Static   1     ff-ff-ff-ff-ff-ff   1-10,CPU
Static   10    00-00-00-01-02-03   5
```

show mac-address-table aging-time command will show aging time of mac address table.

For example,

```
# show mac-address-table aging-time
MAC Age Time: 300
```

show mac-address-table address x-x-x-x-x-x command will show the mac address table for mac address “x-x-x-x-x-x”.

For example,

```
# show mac-address-table address 00-00-e2-82-8c-e6
Type      VID    MAC Address          Ports
------      ---     -----------------          -----
Dynamic   1      00-00-e2-82-8c-e6     7
```

show mac-address-table learning command will show the port learn mode.

```
# show mac-address-table learning
```

```
Port   Learning
----   --------
1       Auto
2       Auto
3       Auto
4       Auto
5       Auto
6       Auto
7       Auto
8       Auto
9       Auto
10      Auto
```

show mac-address-table statistics command will show MAC address table statistics.

```
# show mac-address-table statistics
Port   Dynamic Addresses
----   -----------------
1       0
2       0
3       0
4       0
5       0
6       0
7       23
8       0
9       0
10      0

Total Dynamic Addresses: 23
Total Static Addresses : 7
```

14. **show mac-security** command

This command is used to show Port Security Limit Control Configuration. Limit Control allows for limiting the number of users on a given port.

```
# show mac-security
Port Security Limit Control Configuration:
==========================================
Mode         : Disabled
Aging        : Disabled
Age Period: 3600

Port   Mode        Limit   Action              State
----   --------    -----   ----------------    -------------
 1     Disabled      4     None                Disabled
 2     Disabled      4     None                Disabled
 3     Disabled      4     None                Disabled
```

4	Disabled	4	None	Disabled
5	Disabled	4	None	Disabled
6	Disabled	4	None	Disabled
7	Disabled	4	None	Disabled
8	Disabled	4	None	Disabled
9	Disabled	4	None	Disabled
10	Disabled	4	None	Disabled

15. **show management** command

This command is used to show switch management security settings and statistics.

show management command will show Management IP filter settings.

For example,

```
# show management
Access Mgmt Configuration:
==========================
System Access Mode : Disabled
W: WEB/HTTPS
S: SNMP
T: TELNET/SSH

Idx   Start IP Address                End IP Address                  W S T
---   ------------------------------  ------------------------------  - - -
2     192.168.1.100                   192.168.1.200                   N N N
```

show management statistics command will show management security statistics.

```
# show management statistics
Access Management Statistics:
-----------------------------
HTTP      Receive:      0    Allow :      0    Discard:      0
HTTPS     Receive:      0    Allow :      0    Discard:      0
SNMP      Receive:      0    Allow :      0    Discard:      0
TELNET    Receive:      0    Allow :      0    Discard:      0
SSH       Receive:      0    Allow :      0    Discard:      0
```

16. **show map** command

This command is used to show QoS Port Classification and QoS Port Classification Map ((QoS class, DP level) to (PCP, DEI) Mapping if Tag Remarking Mode is “Mapped”.).

```
# show map
QoS Port Classification:
========================
```

```
Port   QoS class   DP level   PCP   DEI   Tag class.
----   ---------   --------    ---   ---   ----------
1      0           0          0     0     Disabled
2      0           0          0     0     Disabled
3      4           0          0     0     Disabled
4      0           0          0     0     Disabled
5      0           0          0     0     Disabled
6      0           0          0     0     Disabled
7      0           0          0     0     Disabled
8      0           0          0     0     Disabled
9      0           0          0     0     Disabled
10     0           0          0     0     Disabled

QoS Port Classification Map:
============================
Port   PCP   DEI   QoS class   DP level
----   ---   ---   ---------    --------
1      0     0     1           0
       0     1     1           1
       1     0     0           0
       1     1     0           1
       2     0     2           0
       2     1     2           1
       3     0     3           0
       3     1     3           1
       4     0     4           0
       4     1     4           1
       5     0     5           0
       5     1     5           1
       6     0     6           0
       6     1     6           1
       7     0     7           0
       7     1     7           1
---More---
```

17. **show mvr** command

This command is used to show MVR configuration and status.

```
# show mvr ?
  config                Show MVR configuration
  group                 Show MVR group addresses
  sfm                   Show SFM (including SSM) related information for MVR
  statistics            Show MVR operational statistics
```

show mvr config command will show MVR configuration.

```
# show mvr config
MVR Configuration:
```

```
==================
MVR Mode: Disabled

MVR Interface Setting
VID     Name                             Mode         Tagging     Priority   LLQI
----    --------------------------------  ----------  --------    --------   -----
10      aaa                              Dynamic      Tagged      0          5
[Port Setting of aaa(VID-10)]
Inactive Port: 1-10
[Channel Setting of aaa(VID-10)]
Name             : aaa
Start Address: 224.0.0.1
End Address    : 224.0.0.10

MVR Immediate Leave Setting
Port    Immediate Leave
----    ---------------
1       Disabled
2       Disabled
3       Disabled
4       Disabled
5       Disabled
6       Disabled
7       Disabled
8       Disabled
9       Disabled
10      Disabled
```

show mvr group command will show MVR Groups.

show mvr sfm command will show SFM (including SSM) related information for MVR.

show mvr statistics command will show MVR statistics.

```
# show mvr statistics
IPv4   Querier    Rx          Tx          Rx          Rx          Rx          Rx
VID    Status     Query       Query       V1 Join     V2 Join     V3 Join     V2 Leave
----    -------    ----------  ----------   ----------  ----------  ----------  ---------
-
10      DISABLE   0           0           0           0           0           0

IPv6   Querier    Rx          Tx          Rx          Rx          Rx
VID    Status     Query       Query       V1 Report   V2 Report   V1 Done
----    -------    ----------  ----------   ----------  ----------  ----------
10      DISABLE   0           0           0           0           0
```

18. **show ntp** command <**>

This command is used to show system time settings of the switch.

```
# show ntp ?
  config                Show NTP configuration
  dst                   Show daylight saving time configuration
  zone                  Show system timezone configuration
```

show ntp config command will show NTP configuration.

```
# show ntp config
NTP Configuration:
==================
NTP Mode : Disabled
Idx    Server IP host address (a.b.c.d) or a host name string
---    ----------------------------------------------------
1      64.90.182.55
2      64.236.96.53
3
4
5
```

show ntp dst command will show daylight saving time configuration.

```
# show ntp dst
System Daylight Saving Time(DST) Configuration:
================================================
Daylight Saving Time Mode : Non-Recurring.
Daylight Saving Time Start Time Settings :
          Week: 0
          Day: 0
        * Month: 1
        * Date: 1
        * Year: 2000
        * Hour: 0
        * Minute: 0
Daylight Saving Time End Time Settings :
          Week: 0
          Day: 0
        * Month: 1
        * Date: 1
        * Year: 2000
        * Hour: 0
        * Minute: 0
Daylight Saving Time Offset : 1 (minutes)
```

* : This symbol indicates the parameter needs to be set the reasonable value.

show ntp zone command will show system timezone configuration.

```
# show ntp zone
System Timezone Configuration:
==============================
Timezone Offset : 5400 ( 540 minutes)
Timezone Acronym : Japan
```

19. **show port** command

This command is used to show port mirror function setting.

show port monitor command is used to show port mirror function setting.

For example,

```
# show port monitor
Mirror Configuration:
=====================
Mirror Port: 5

Port   Mode
----   --------
1      Disabled
2      Disabled
3      Disabled
4      Disabled
5      Disabled
6      Disabled
7      Disabled
8      Disabled
9      Disabled
10     Disabled
CPU    Disabled
```

20. **show queue** command

This command is used to show QCL (Queue Control List) configuration and status.

```
# show queue ?
  status                Show QCL status.
  <cr>
```

show queue command will show QCL configuration.

```
# show queue
QoS QCL:
========
ID   Frame   SMAC     DMAC  VID        PCP  DEI  Class  DP  DSCP  Port
--   -----   -------- ----  ---------  ---  ---  -----  --  ----  -------
10   Any     Any      Any   Any        Any  Any  0      -   -     5
```

Number of QCEs: 1

show queue status command will show QCL status.

```
# show queue status
User          ID  Frame  Class DP DSCP  Conflict  Port
----------    --  -----  ----- -- ------ --------  -------
Static        10  Any    0     -  -      No        5

Number of QCEs: 1
```

21. **show radius-server** command

This command is used to show RADIUS Server configuration and statistics.

show radius-server command will show RADIUS Server configuration.

For example,

```
# show radius-server
Server Timeout    : 15 seconds
Server Dead Time : 300 seconds

RADIUS Authentication Server Configuration:
=========================================
Server  Mode      IP Address      Secret                          Port
------  --------  --------------  ------------------------------  -----
1       Disabled                                                  1812
2       Disabled                                                  1812
3       Disabled                                                  1812
4       Disabled                                                  1812
5       Disabled                                                  1812

RADIUS Accounting Server Configuration:
=====================================
Server  Mode      IP Address      Secret                          Port
------  --------  --------------  ------------------------------  -----
1       Disabled                                                  1813
2       Disabled                                                  1813
3       Disabled                                                  1813
4       Disabled                                                  1813
5       Disabled                                                  1813
```

show radius-server statistics x command will show RADIUS Server statistics. "**x**" is index of RADIUS Server with value 1~5.

22. **show running-config** command

This command is used to show current running configuration of the switch.

For example,

```
# show running-config
!building running-config, please wait.....
!10G
!
……
……

!
!
interface ethernet 1/5
qos tagremarking map 2 1 0 0
exit
!
interface ethernet 1/1-10
switchport allowed vlan add 1
exit
!
interface vlan 1
ip address 192.168.1.118 255.255.255.0
ipv6 address fc80::215:c5ff:fe03:4dc0 120
exit
end
```

23. **show rate-limit** command

This command is used to show Rate Limit configuration of each port.

```
# show rate-limit ethernet

QoS Port Policer:
=================

Port   Parm        Policer
----   --------     ---------
1      Mode        Disabled
       Rate        500 kbps
       Unit        kbps
       Flow Ctl    Disabled
2      Mode        Disabled
       Rate        500 kbps
       Unit        kbps
       Flow Ctl    Disabled
3      Mode        Disabled
       Rate        500 kbps
       Unit        kbps
```

```
        Flow Ctl     Disabled
.............
```

24. **show rmon** command

This command is used to show RMON configuration.

```
# show rmon ?
  alarm                Show RMON alarm entries
  event                Show RMON event entries
  history              Show RMON history entries
  statistics           Show RMON statistics entries
```

show rmon alarm command will show RMON alarm configuration.

```
# show rmon alarm
abc# show rmon alarm
Id      Interval  Alarm Variable              Alarm SampleType
-----   --------- ------------------------    ------------------------
1       30        .1.3.6.1.2.1.2.2.1.10.1     deltaValue

Number of entries: 1
```

show rmon event command will show RMON event configuration.

```
# show rmon event
Id      Description  Type   Community   LastSent
-----   -----------  -----  ----------  ---------
1       abc          none   public      Never

Number of entries: 1
```

show rmon history command will show RMON history configuration.

```
# show rmon history
Id  Data Source                 controlBucketsRequested  controlBucketsGranted  Interval
----- ------------------------------ ----------------------- ----------------------- --
-------
10  .1.3.6.1.2.1.2.2.1.1.10     50                       50                     1800

Number of entries: 1
```

show rmon statistics command will show RMON statistics configuration.

```
# show rmon statistics
Id  Data Source                 etherStatsOctets  etherStatsPkts  therStatsCRCAlignErrors
----- ------------------------------ ------------------ --------------- ----------------------
10  .1.3.6.1.2.1.2.2.1.1.10     0                  0               0

Number of entries: 1
```

25. **sflow** command

This command is used to show sFlow configuration and stauts.

```
# show sflow ?
  counter_poller        Show counter polling interval configuration per port
  flow_sampler          Show flow sampler configuration per port.
  receiver              Show the sFlow receiver
  statistics            Show statistics
```

show sflow counter_poller command will show sFlow counter polling interval configuration per port.

```
# show sflow counter_poller
Counter Poller Configuration:
============================
Port   Interval
----   --------
 8       10
```

show sflow flow_sampler command will show sFlow sampler configuration per port.

```
# show sflow flow_sampler
Flow Sampler Configuration:
===========================
Port   Sampling   Rate   Max Hdr
----   ----------   -------
 8       20         128
```

show sflow receiver command will show sFlow Receiver configuration.

```
# show sflow receiver
Receiver Configuration:
=======================
Owner            : <none>
Receiver         : 0.0.0.0
UDP Port         : 6343
Max. Datagram: 1400 bytes
Time left        : 0 seconds
```

show sflow statistics receiver command will show receiver statistics.

```
# show sflow statistics receiver
Receiver Statistics:
====================
Tx Successes   Tx Errors      Flow Samples   Counter Samples
---------------      ---------------     ---------------       ---------------
         0                0                0                0
```

show sflow statistics samplers command will show per-port statistics.

```
# show sflow statistics samplers
Per-Port Statistics:
====================

No non-zero counters.
```

26. **show snmp** command

This command is used to show SNMP configuration of the switch.

```
# show snmp ?
  access                SNMPv3 access entry
  community             SNMPv3 community entry
  group                 SNMPv3 group entry
  user                  SNMPv3 user entry
  view                  SNMPv3 view entry
  <cr>
```

show snmp command will show SNMP configuration of the switch.

```
# show snmp
SNMP Configuration:
===================
SNMP Mode                          : Enabled
SNMP Version                       : 2c
Read Community                     : public
Write Community                    : private
Trap Mode                          : Disabled
Trap Version                       : 1
Trap Community                     : public
Trap Destination                   : 192.168.1.10
Trap IPv6 Destination              : ::
Trap Authentication Failure        : Disabled
Trap Link-up and Link-down         : Enabled
Trap Inform Mode                   : Enabled
Trap Inform Timeout (seconds)      : 1
Trap Inform Retry Times            : 5
Trap Probe Security Engine ID      : Enabled
Trap Security Engine ID            :
Trap Security Name                 : None

SNMPv3 Engine ID : 800007e5017f000001
```

show snmp access command will show SNMPv3 access entry.

```
# show snmp access
SNMPv3 Accesses Table:
Idx Group Name                     Model   Level          ReadView        WriteView
--- -------------------------------- ----- ---------------------- ---------------- -------------
```

```
--
1    default_ro_group          any    NoAuth, NoPriv   default_view       None
2   default_rw _group          any    NoAuth, NoPriv   default_view       default_view

Number of entries: 2
```

show snmp community command will show SNMPv3 community entry.

```
# show snmp community
SNMPv3 Communities Table:
Idx   Community                    Source IP       Source Mask
---   ---------------------------- ---------------  ---------------
1     public                       0.0.0.0          0.0.0.0
2     private                      0.0.0.0          0.0.0.0
3     yyy                          192.168.1.11     255.255.255.0

Number of entries: 3
```

show snmp group command will show SNMPv3 group entry.

```
# show snmp group
SNMPv3 Groups Table;
Idx Model Security Name             Group Name
---  -----  ------------------------------  ------------------------------
1    v1     public                       default_ro_group
2    v1     private                      default_rw _group
3    v2c    public                       default_ro_group
4    v2c    private                      default_rw _group
5    usm    default_user                 default_rw _group

Number of entries: 5
```

show snmp user command will show SNMPv3 user entry.

```
# show snmp user
SNMPv3 Users Table:
Idx Engine ID   User Name                    Level              Auth    Priv
---  ---------   ------------------------------  --------------  ----    ----
1    Local       default_user                 NoAuth, NoPriv   None   None

Number of entries: 1
```

show snmp view command will show SNMPv3 view entry.

```
# show snmp view
SNMPv3 Views Table:
Idx   View Name                    View Type   OID Subtree
---   ---------------------------- ---------  ------------------------------
1     default_view                  included    .1
2     xxx                           included    .1
3     yyy                           included    .10
```

Number of entries: 3

27. **show spanning-tree** command

This command is used to show spanning tree configuration of the switch.

```
# show spanning-tree ?
  ethernet                Show STP Port configuration
  mst                     Show MSTP configuration
  statistics              Show STP port statistics
  status                  Show STP Bridge status
  <cr>
```

show spanning-tree command will show system spanning tree configuration.

```
# show spanning-tree
STP Configuration:
==================
Protocol Version: MSTP
Max Age           : 20
Forward Delay     : 15
Tx Hold Count     : 2
Max Hop Count     : 20
BPDU Filtering    : Disabled
BPDU Guard        : Disabled
Error Recovery    : Disabled
```

show spanning-tree ethernet command will show port spanning tree configuration.

```
# show spanning-tree ethernet
Port   Mode      AdminEdge   AutoEdge restrRole  restrTcn   bpduGuard   Point2point
----   --------  ----------  -------- ---------  ---------  ----------  ---------
Aggr   Enabled   Disabled    Enabled  Disabled   Disabled   Disabled    Enabled

Port   Mode      AdminEdge   AutoEdge restrRole  restrTcn   bpduGuard   Point2point
----   --------  ----------  -------- ---------  ---------  ----------  ---------
1      Disabled  Disabled    Enabled  Disabled   Disabled   Disabled    Auto
2      Disabled  Disabled    Enabled  Disabled   Disabled   Disabled    Auto
3      Disabled  Disabled    Enabled  Disabled   Disabled   Disabled    Auto
4      Disabled  Disabled    Enabled  Disabled   Disabled   Disabled    Auto
5      Disabled  Disabled    Enabled  Disabled   Disabled   Disabled    Auto
6      Disabled  Disabled    Enabled  Disabled   Disabled   Disabled    Auto
7      Disabled  Disabled    Enabled  Disabled   Disabled   Disabled    Auto
8      Disabled  Disabled    Enabled  Disabled   Disabled   Disabled    Auto
9      Disabled  Disabled    Enabled  Disabled   Disabled   Disabled    Auto
10     Disabled  Disabled    Enabled  Disabled   Disabled   Disabled    Auto
```

show spanning-tree ethernet x command will show port Multi Spanning Tree

configuration. "**x**" is the index of MSTI with value 0~7.

```
# show spanning-tree ethernet 0

MSTI   Port   Path Cost     Priority
----    ----    ----------      --------
CIST   Aggr   Auto          128

MSTI   Port   Path Cost     Priority
----    ----    ----------      --------
CIST   1      Auto          128
CIST   2      Auto          128
CIST   3      Auto          128
CIST   4      Auto          128
CIST   5      Auto          128
CIST   6      Auto          128
CIST   7      Auto          128
CIST   8      Auto          128
CIST   9      Auto          128
CIST   10     Auto          128
```

show spanning-tree mst command will show system MSTP configuration.

```
# show spanning-tree mst
Configuration name: xxx
Configuration rev.: 10

MSTI#   Bridge Priority
-----    ---------------
CIST    32768
MSTI1   32768
MSTI2   32768
MSTI3   32768
MSTI4   32768
MSTI5   32768
MSTI6   32768
MSTI7   32768

MSTI    VLANs mapped to MSTI
----     --------------------
MSTI1   No VLANs mapped
MSTI2   No VLANs mapped
MSTI3   No VLANs mapped
MSTI4   No VLANs mapped
MSTI5   No VLANs mapped
MSTI6   No VLANs mapped
MSTI7   No VLANs mapped
```

show spanning-tree statistics command will show STP port statistics.

```
# show spanning-tree statistics
```

Port Rx_MSTP Tx_MSTP Rx_RSTP Tx_RSTP Rx_STP Tx_STP Rx_TCN Tx_TCN Rx_Ill. Rx_Unk.
--- --- --- --- --- --- --- --- --- --- ---

s**how spanning-tree status x** command will show MSTP Bridge status. "**x**" is the index of MSTI with value 0~7.

```
# show spanning-tree status 0
CIST Bridge STP Status
Bridge ID      : 32768.00-C0-F9-66-66-99
Root ID        : 32768.00-C0-F9-66-66-99
Root Port      : -
Root PathCost: 0
Regional Root: 32768.00-C0-F9-66-66-99
Int. PathCost: 0
Max Hops       : 20
TC Flag        : Steady
TC Count       : 0
TC Last        : -
Port          Port Role          State          Pri   PathCost   Edge   P2P   Uptime
---------     ---------------    ----------     ---   --------   ----   ---   -------------
```

28. **storm-control** command

This command is used to show storm control configuration of the switch.

For example,

```
# show storm-control

QoS Storm Control:
==================
Storm Unicast   : Disabled       1 fps
Storm Multicast: Disabled       1 fps
Storm Broadcast: Disabled       1 fps
```

29. **show system** command

This command is used to show general system information/configuration of the switch.

For example,

```
# show system
System Contact   :
System Name      : abc
System Location :
Software Version: 10-P Ver:1.00.00
```

```
Software Date     : 2012-08-17T14:31:24+08:00
MAC Address       : 00-c0-f9-66-66-99
Number of Ports : 10
Previous Restart: Cold
```

30. **show tacacs-server** command

This command is used to show TACACS+ Authentication Server Configuration.

```
# show tacacs-server
Server Timeout    : 15 seconds
Server Dead Time : 300 seconds

TACACS+ Authentication Server Configuration:
=============================================
Server   Mode        IP Address          Secret                          Port
------   --------    ----------------    ------------------------------          -----
1        Disabled                                                        49
2        Disabled                                                        49
3        Disabled                                                        49
4        Disabled                                                        49
5        Disabled                                                        49
```

31. **show trunk** command

This command is used to show trunk configuration of the switch.

```
# show trunk ?
  all                    Shows all Trunking Group Configuration
  <cr>
```

show trunk command will show system trunk configuration.

```
# show trunk
Aggregation Configuration:
==========================
Aggregation Mode:

SMAC   : Enabled
DMAC   : Disabled
IP     : Enabled
Port   : Enabled
```

show trunk all command will show all Trunking Group Configuration.

```
# show trunk all
Aggr ID   Name      Type     Configured Ports    Aggregated Ports
-------   ------    ------   ----------------    ----------------
```

```
1          LLAG1    Static   1,2                  None
```

32. **show users** command

This command is used to show users configuration.

For example,

```
# show users
Users Configuration:
====================
User Name                        Privilege Level
---------------------------------    ---------------
admin                                3
ad01                                 3
op01                                 2
gu01                                 1
```

33. **show version** command

This command is used to show system version information and model information.

For example,

```
# show version
Software Version: 10-P Ver:1.00.00
Software Date     : 2012-08-17T14:31:24+08:00
Number of Ports : 10
```

34. **show vlan** command

This command is used to show VLAN configuration of the switch.

```
# show vlan  ?
  id                  VLAN interface
  isolation           Isolation VLAN entry
  name                VLAN interface name
  port-based          Port-Based Virtual LAN Configuration
  voice               Show voice VLAN configuration
  <cr>
```

show vlan command is used to show all 802.1Q VLAN settings (VLAN ID, VLAN Name, and Assigned ports).

```
# show vlan
TPID is 0x8888

VID    VLAN Name                        Ports
----   --------------------------------   -----
```

```
1       default                 1-10
10      aaa                     None

VLAN forbidden port list:
========================
VID     VLAN Name               Ports
----    --------------------------------  -----
10      aaa                     2
```

show vlan id x command is used to show VLAN setting of VLAN x. ("**x**" is the VLAN ID).

```
# show vlan  id 10
VID     VLAN Name   User        Ports                                   Conflicts   Conflict_Ports
----    ----------  ----------  --------------------------------------  ----------  ----------
-----
10      aaa         Static      None                                    No          None
                    MVR         None                                    No          None
                    Combined    None                                    No          None

VLAN forbidden port list:
========================
VID     VLAN Name               Ports
----    --------------------------------  -----
10      aaa                     2
```

show vlan isolation command will show port isolation settings.

```
# show vlan isolation
Port    Isolation
----    ---------
1       Disabled
2       Disabled
3       Disabled
4       Disabled
5       Disabled
6       Disabled
7       Disabled
8       Disabled
9       Disabled
10      Disabled
```

show vlan name xxx command will show VLAN setting of VLAN xxx. ("**xxxx**" is the VLAN name).

```
# show vlan name aaa
VID     VLAN Name   User        Ports                                   Conflicts   Conflict_Ports
----    ----------  ----------  --------------------------------------  ----------  ----------
-----
10      aaa         Static      None                                    No          None
                    MVR         None                                    No          None
```

```
                    Combined   None                          No        None

VLAN forbidden port list:
========================
VID     VLAN Name                         Ports
----   --------------------------------   -----
10      aaa                               2
```

show vlan port-based command will show Port-Based VLAN Configuration.

```
# show  vlan port-based
PVLAN ID   Ports
--------       -----
1              1-10
```

show vlan voice command will show Voice VLAN configuration.

```
# show  vlan voice
Voice VLAN Configuration:
========================
Voice VLAN Mode                    : Disabled
Voice VLAN VLAN ID                 : 1000
Voice VLAN Age Time(seconds)   : 86400
Voice VLAN Traffic Class         : 7

Voice VLAN OUI Table:
====================
Telephony OUI   Description
-------------          -----------

Voice VLAN Port Configuration:
=============================
Port   Mode        Security     Discovery Protocol
----    --------       --------       ------------------
1       Disabled   Disabled      OUI
2       Disabled   Disabled      OUI
3       Disabled   Disabled      OUI
4       Disabled   Disabled      OUI
5       Disabled   Disabled      OUI
6       Disabled   Disabled      OUI
7       Disabled   Disabled      OUI
8       Disabled   Disabled      OUI
9       Disabled   Disabled      OUI
10      Disabled   Disabled      OUI
```

6.3 About Telnet and SNMP Management Interfaces

6.3.1 About Telnet Management Interface

If you want to use Telnet to manage the switch from remote site, you have to set the IP/NetMask/Gateway address to the switch first. Then use "**telnet <IP>**" command to connect to the switch. Its operation interface is the same as console interface.

6.3.2 About SNMP Management Interface

If you want to use NMS to management the switch from remote site, you have to set the IP/NetMask/Gateway address to the switch and configure the SNMP setting of the switch first. Then you can use SNMP management program to manage this switch.

This switch supports SNMP v1, v2c, v3 agent function and MIB II(Interface), Bridge MIB, 802.1Q MIB and Private MIB. The default GET community name is "**public**" and SET community name is "**private**".

6.4 Management with Http Connection

Users can manage the switch with Http Web Browser connection. The default IP setting is **192.168.1.1** and NetMask **255.255.255.0**. The default IP Gateway is **192.168.1.254**. Before http connection, IP address configuration of the switch could be changed first.

1 Please follow the instruction in Section 6.2 to complete the console connection.
2 Login in with "**admin**" (password is also "**admin**" by default.)
3 Use "**show ip interface**" command to check IP address of the switch first.
4 If IP address needs to be changed, follow the steps ...
  4.1 Enter "**config**" command, and the prompt will become "(config)#".
  4.2 Enter "**interface vlan 1**" command, and the prompt will become "(config-if)#".
  4.3 Enter "**ip address xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy**" command (**xxx.xxx.xxx.xxx** is the IP address and **yyy.yyy.yyy.yyy** is the netmask) to modify IP address of the switch.
  4.4 Enter "**exit**" command to go back to "(config)#" prompt.
  4.5 If IP Gateway will be set, enter "**ip default-gateway xxx.xxx.xxx.xxx**" command to set the IP gateway of the switch. (**xxx.xxx.xxx.xxx** is the IP address.)
  4.6 Enter "**exit**" command to go back to "#" prompt.
  4.7 Enter "**show ip interface**" to check the IP settings.

After IP address configuration done and the switch is connected to network, users can start Http connection by entering IP address of the switch to the web address line in Web Browser. A login screen will be prompted for user name and password. The default user name and password is "**admin**" / "**admin**". Then the management homepage will appear.

Left part of the homepage is a function list. Users can select one of them for status monitoring or switch configuration.
There are four operation groups in the function list.

1. **Configuration** : this is for switch function configuration.
2. **Monitor** : this is for switch function status and statistics monitor.
3. **Diagnostics** : this is diagnostics functions for switch.
4. **Maintenance** : this is for switch maintenance, like firmware upgrade, configuration backup/restore, system reset, ...

Middle part of homepage is the main operation area for each function.

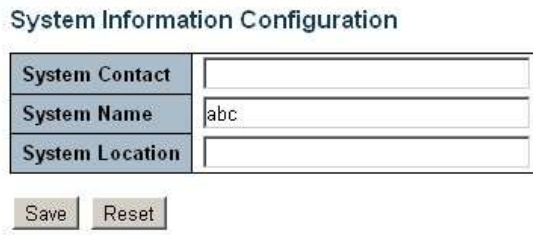
This is Logout. Click it to logout.

This is Help. Click it to get help information for operation.

The details about management with http connection will be shown in the following sub-sections.

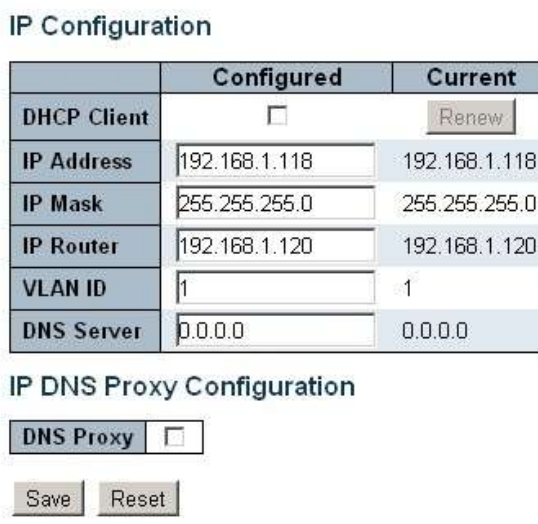
6.4.1 Configuration - System

1). Configuration - System - Information



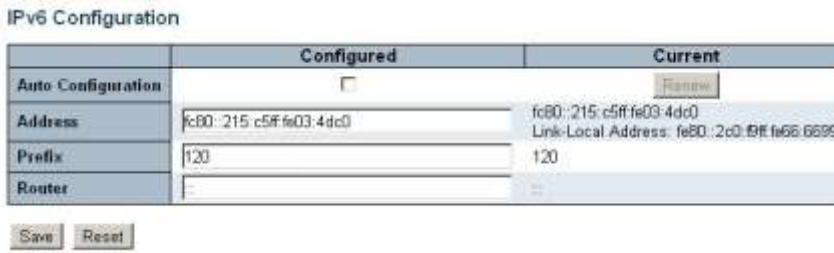
This is used to configure System Name, System Location, and System Contact. The information is also applied to SNMP agent function.

2). Configuration - System - IP



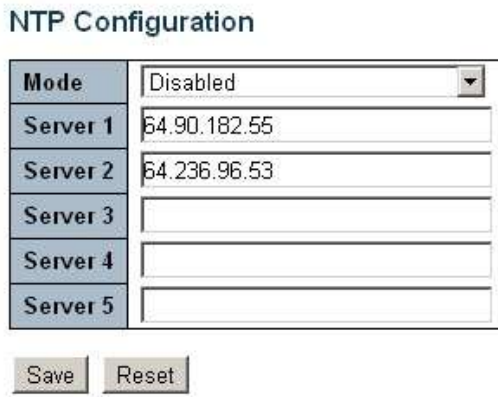
This page is used to setup IP configuration of the switch.
You can enable DHCP client function to get IP configuration from DHCP server automatically. Or, disable DHCP client function and set IP configuration manually.

3). Configuration - System - IPv6



This page is used to setup IPv6 configuration of the switch.
You can enable Auto Configuration function to get IP configuration automatically. Or, disable Auto Configuration function and set IP configuration manually.

4). Configuration - System - NTP



This switch support NTP protocol to get time from Internet time server. For such application, you have to Enable the function and input the IP of Time Server. Then click [Save]
For such application, you have to get the IP of Time Server from your network administrator first.

Then configure “Time Zone” and “Daylight Saving Time” at **Configuration - System - Time** page.

5). Configuration - System - Time

Time Zone Configuration

Time Zone Configuration	
Time Zone	(GMT+09:00) Osaka, Sapporo, Tokyo
Acronym	Japan (0 - 16 characters)

Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Non-Recurring

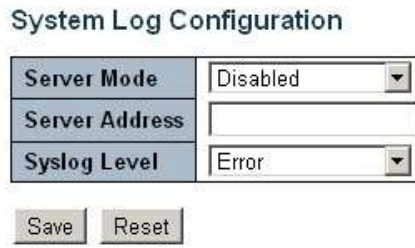
Start Time settings	
Month	Jan
Date	1
Year	2000
Hours	0
Minutes	0
End Time settings	
Month	Jan
Date	1
Year	2000
Hours	0
Minutes	0
Offset settings	
Offset	1 (1 - 1440) Minutes

Save Reset

Refer to your location to configure “Time Zone”.

Daylight Saving Time function will set the system time one-hour early than normal time in a period of time. [Start Time] and [End Time] can be used to set the time period.

6). Configuration - System - Log



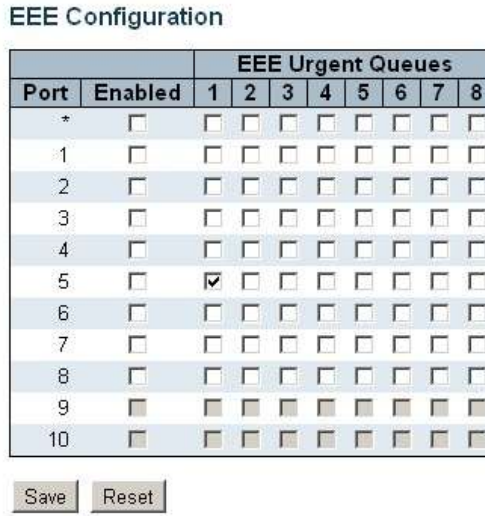
Users can configure Syslog Server here. If this function is enabled, the switch will record events to the Syslog Server.

The **Server Address** is the IPv4 host address of syslog server. If the switch provide DNS feature, it also can be a host name.

The **Syslog Level** indicates what kind of message will send to syslog server. Possible modes are:
- Info: Send informations, warnings and errors.
- Warning: Send warnings and errors.
- Error: Send errors.

6.4.2 Configuration - Power Reduction

1). Configuration - Power Reduction - EEE

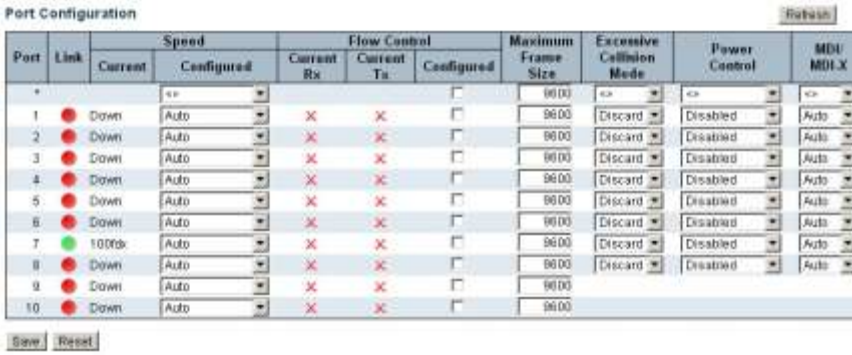


This page is used to configure EEE (Energy Efficient Ethernet) function of the switch for power reduction. It can be enabled by port.

EEE Urgent Queues will activate tranmission of frames as soon as data is available. Otherwise the queue will postpone tranmsission until 3000 bytes are ready to be transmitted.

6.4.3 Configuration - Ports

1). Configuration - Ports



This page is used to configure ports of the switch. And Link status can be found in the page.

Speed can configure the operation speed and duplex mode of ports.
Flow Control can configure the flow control function for full duplex connections.
Excessive Collision Mode can configure the collision function for half duplex connections.

Maximum Frame Size is used to configure the jumbo frame function. And make sure that the connected device can accept such a big packets.

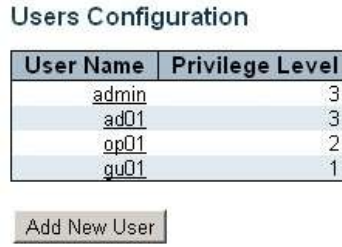
Power Control is used to configure the power control function of ports. It could be ...
- Disabled: All power savings mechanisms disabled.
- ActiPHY: Link down power savings enabled. Less power is used when link down.
- PerfectReach: Link up power savings enabled. Less power is used when short cable.
- Enabled: Both link up and link down power savings enabled.

MDI/MDI-X is used to set the MDI/MDI-X mode of UTP ports. It could be Auto, MDI, or MDI-X. MDI-X is for PC devices connection. MDI is for Hub/Switch connection. Auto can auto-detect the connection.

6.4.4 Configuration - Security

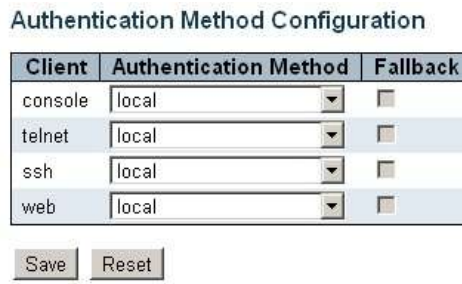
6.4.4.1 Configuration - Security - Switch

1). Configuration - Security - Switch - Users



This page is used to create users for the switch. There are three Privilege Level for users ...
3 - This is for administrator. This user can do every configuration and view every status of the switch.
2- This is for operator. This user can view configuration and status of the switch. And this user can execute maintenance function of the switch.
1 - This for guest. This user can view configuration and status of the switch only.

2). Configuration - Security - Switch - Auth Method



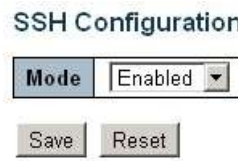
This page is used to configure Authentication Method of the switch for management interface.

The Authentication Method could be ...
- none: authentication is disabled and login is not possible.

- local: use the local user database on the switch for authentication.
- radius: use a remote RADIUS server for authentication.
- tacacs+: use a remote TACACS+ server for authentication.

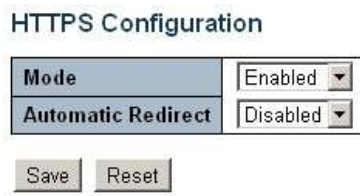
RADIUS server and TACACS+ server are configured in **Configuration - Security - AAA** page.

3). Configuration - Security - Switch - SSH



This page is used to enable SSH function for remote Telnet connection.

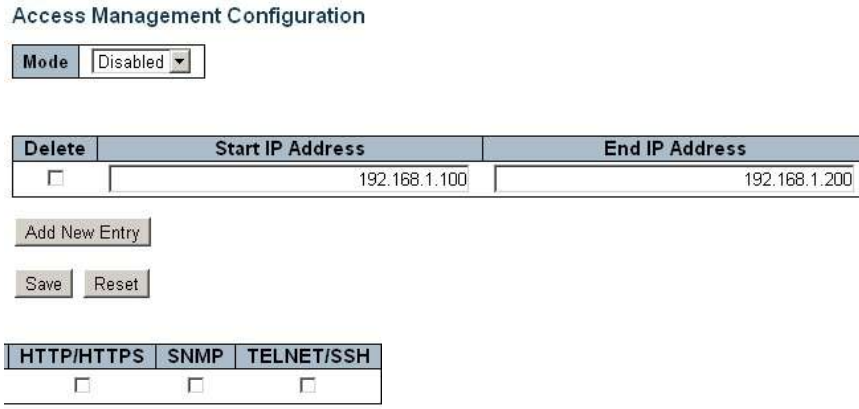
4). Configuration - Security - Switch - HTTPS



This page is used to enable HTTPS security function for remote web connection.

Automatic Redirect automatically redirects web browser to an HTTPS connection when both HTTPS mode and Automatic Redirect are enabled or redirects web browser to an HTTP connection when both are disabled.

5). Configuration - Security - Switch - Access Management



This page is used to configure IP address range that is allowed for remote management. The remote management interface could be HTTP/HTTPS, SNMP, or TELNET/SSH.

6). Configuration - Security - Switch - SNMP

6-1). Configuration - Security - Switch - SNMP - System

SNMP System Configuration

Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	800007e5017f000001

SNMP Trap Configuration

Trap Mode	Disabled
Trap Version	SNMP v1
Trap Community	public
Trap Destination Address	192.168.1.10
Trap Destination IPv6 Address	::
Trap Authentication Failure	Disabled
Trap Link-up and Link-down	Enabled
Trap Inform Mode	Enabled
Trap Inform Timeout (seconds)	1
Trap Inform Retry Times	5

Save Reset

This page is used to configure SNMP System configuration and Trap configuration.

6-2). Configuration - Security - Switch - SNMP - Communities

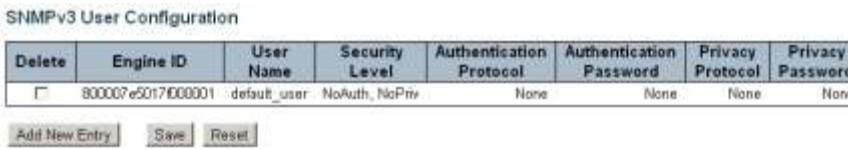
SNMPv3 Community Configuration

Delete	Community	Source IP	Source Mask
☐	public	0.0.0.0	0.0.0.0
☐	private	0.0.0.0	0.0.0.0
☐	yyy	192.168.1.11	255.255.255.0

Add New Entry Save Reset

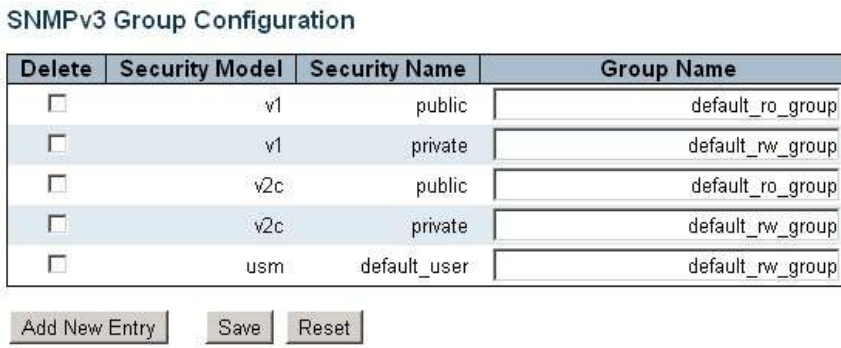
This page is used to configure SNMPv3 Community. Entry could be added or deleted.

6-3). Configuration - Security - Switch - SNMP - Users



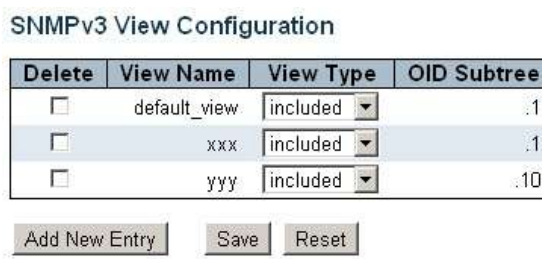
This page is used to configure SNMPv3 User. Entry could be added or deleted.

6-4). Configuration - Security - Switch - SNMP - Groups



This page is used to configure SNMPv3 Group. Entry could be added or deleted.

6-5). Configuration - Security - Switch - SNMP - Views



This page is used to configure SNMPv3 View. Entry could be added or deleted.

6-6). Configuration - Security - Switch - SNMP - Access

SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
☐	default_ro_group	any	NoAuth, NoPriv	default_view	None
☐	default_rw_group	any	NoAuth, NoPriv	default_view	default_view

Add New Entry | Save | Reset

This page is used to configure SNMPv3 Access. Entry could be added or deleted.

7). Configuration - Security - Switch - RMON

7-1). Configuration - Security - Switch - RMON - Statistics

RMON Statistics Configuration

Delete	ID	Data Source
☐	10	.1.3.6.1.2.1.2.2.1.1. 10

Add New Entry | Save | Reset

This page is used to configure RMON Statistics. Entry could be added or deleted.

7-2). Configuration - Security - Switch - RMON - History

RMON History Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
☐	10	.1.3.6.1.2.1.2.2.1.1. 10	1800	50	50

Add New Entry | Save | Reset

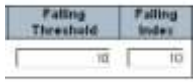
This page is used to configure RMON History. Entry could be added or deleted.

7-3). Configuration - Security - Switch - RMON - Alarm

RMON Alarm Configuration

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index
☐	1	30	.1.3.6.1.2.1.2.2.1. 10.1	Delta	0	RisingOrFalling	20	10

Add New Entry | Save | Reset



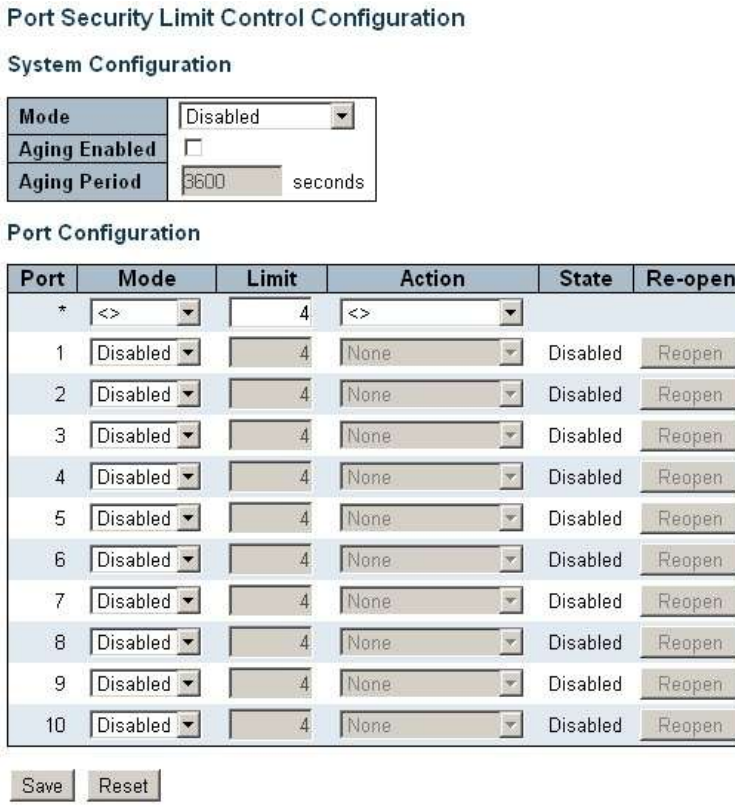
This page is used to configure RMON Alarm. Entry could be added or deleted.

7-4). Configuration - Security - Switch - RMON - Event

This page is used to configure RMON Event. Entry could be added or deleted.

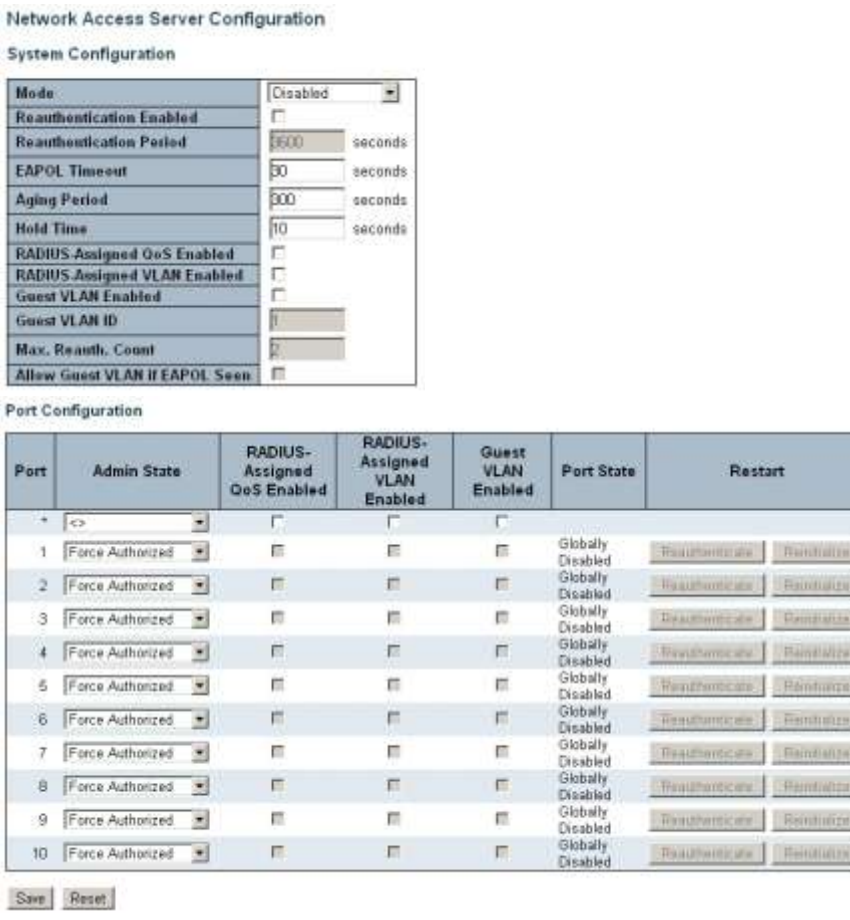
6.4.4.2 Configuration - Security - Network

1). Configuration - Security - Network - Limit Control



This page is used to configure Port Security Limit Control function. Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of the four different actions as described below.

2). Configuration - Security - Network - NAS

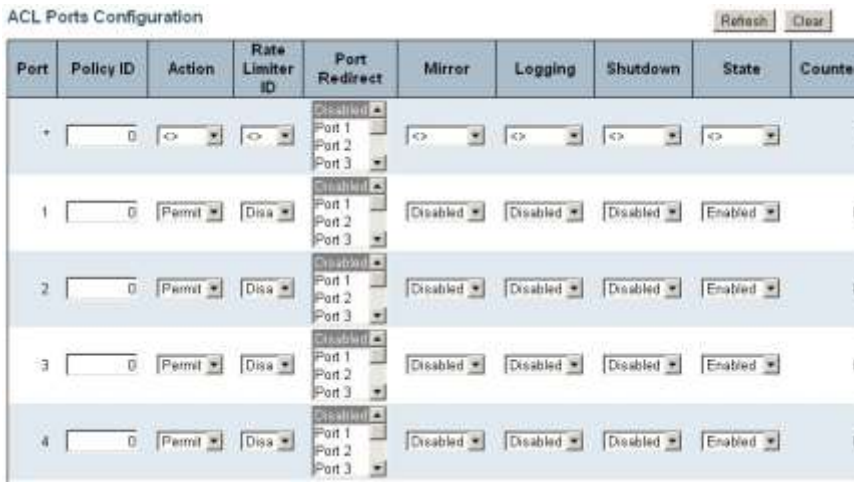


This page is used to configure 802.1x Network Access Control function. Users need to be authenticated first for network access through switch ports. The authentication is processed by RADIUS Server. The details for the operation is configured here.

RADIUS Server is configured in **Configuration - Security - AAA** page.

3). Configuration - Security - Network - ACL

3-1). Configuration - Security - Network - ACL - Ports



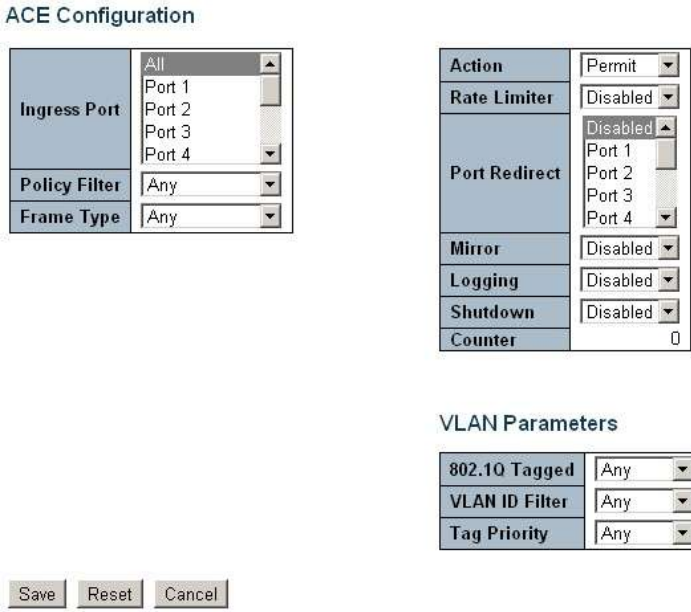
This page is used to configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

3-2). Configuration - Security - Network - ACL - Rate Limiters

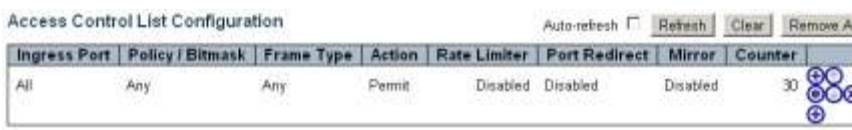
This page is used to define rate limiters. Those Rate Limiters are used for ACL action. The Rate Limiters could be defined by pps (Packet per second) or kbps (kilo bit per second).

3-3). Configuration - Security - Network - ACL - Access Control List

Click “(+)”, the ACE configuration window will be prompted.



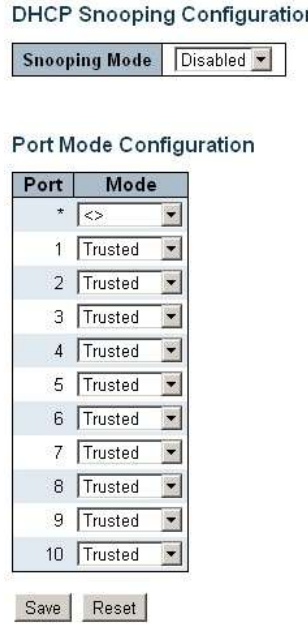
Define the parameters for the ACE and select the action when the parameters are matched. Click [Save] to create the ACE.



Click (+) to add another ACE. Click (e) to edit the ACE. Click (x) to delete the ACE. Click (up-arrow)/(down-arrow) to move the ACE.

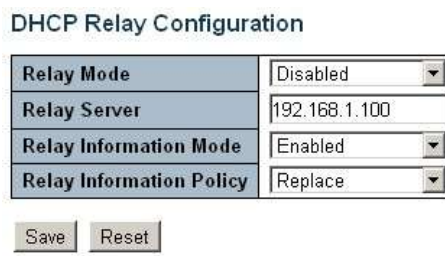
4). Configuration - Security - Network - DHCP

4-1). Configuration - Security - Network - DHCP - Snooping



This page is used to configure DHCP Snooping function. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports. That can prevent illegal DHCP Server connection.

4-2). Configuration - Security - Network - DHCP - Relay



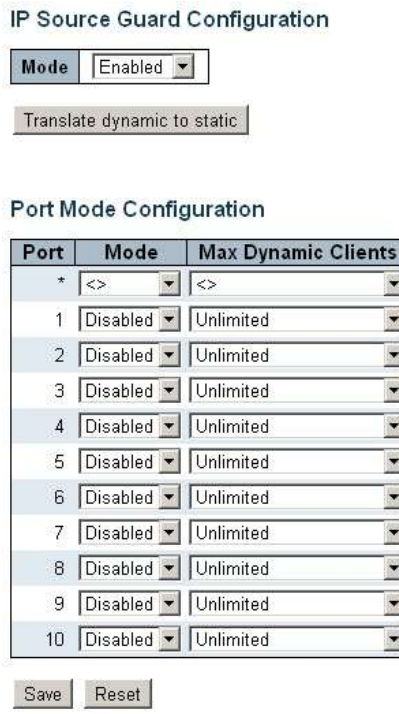
This page is used to configure DHCP Relay and DHCP Option 82 functions.

When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.

When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.
The option 82 circuit ID format as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID(in standalone device it always equal 0, in stackable device it means switch ID).), and the last two characters are the port number. For example, "00030108" means the DHCP message receive form VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal the switch MAC address.
When DHCP relay information mode operation is enabled, if agent receives a DHCP message that already contains relay agent information it will enforce the policy.

5). Configuration - Security - Network - IP Source Guard

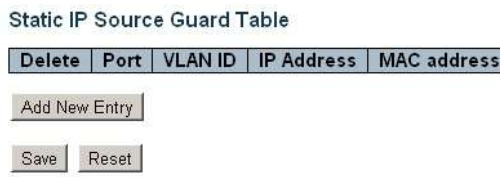
5-1). Configuration - Security - Network - IP Source Guard - Configuration



IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host. This function limit the maximum number of dynamic clients that can be learned on given port.

Note: Dynamic IP Source entry is learned from DHCP request. Before enable IP Source Guard, DHCP Snooping function should be enabled first. Otherwise, static IP Source entry should be created for IP Source Guard operation.

5-2). Configuration - Security - Network - IP Source Guard - Static Table



This page is used to add/delete Static IP Source Entry. A Static IP Source Entry consists of Port, VLAN ID, IP Addtress and Mac address.
This static table is used to prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

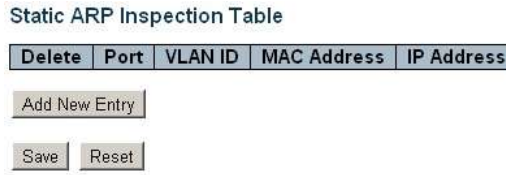
6). Configuration - Security - Network - ARP Inspection

6-1). Configuration - Security - Network - ARP Inspection - Configuration

This page is used to configure ARP Inspection function. ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

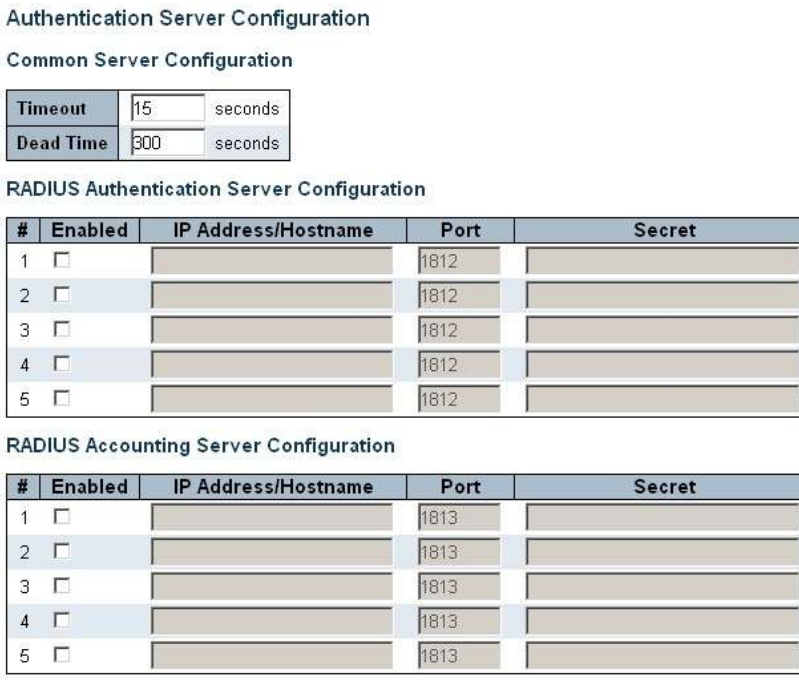
Note: Dynamic ARP entry is learned from DHCP request. Before enable ARP Inspection, DHCP Snooping function should be enabled first. Otherwise, static ARP entry should be created for ARP Inspection operation.

6-2). Configuration - Security - Network - ARP Inspection - Static Table



This page is used to add/delete Static ARP Entry in Static ARP Inspection Table. This table will be used for ARP Inspection security function.

6.4.4.3 Configuration - Security - AAA



TACACS+ Authentication Server Configuration

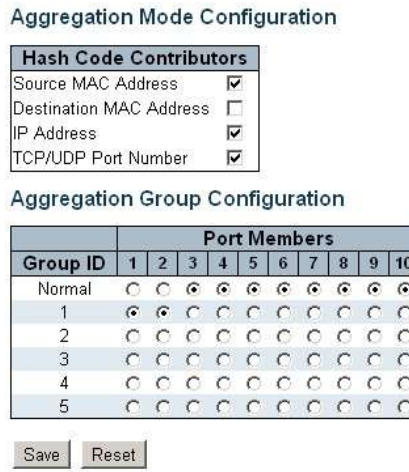
#	Enabled	IP Address/Hostname	Port	Secret
1	☐		49	
2	☐		49	
3	☐		49	
4	☐		49	
5	☐		49	

Save Reset

This page is used to configure RADIUS and TACACS+ Servers.
The settings are used for 802.1x network access and switch user login authentication operations.

6.4.5 Configuration - Aggregation

6.4.5.1 Configuration - Aggregation - Static



This page is used to configure Aggregation Hash Mode and Static Aggregation Group. The Aggregation Hash Mode selects the Hash Code Contributors that can be used to calculate the destination port for the frame.

Up to five Static Aggregation Groups can be used for Aggregation. Assign ports to them for the operation.

6.4.5.2 Configuration - Aggregation - LACP

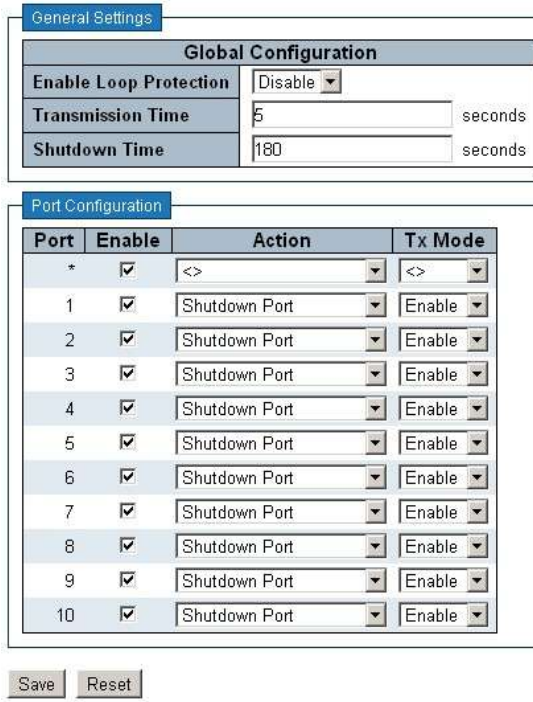
LACP Port Configuration

Port	LACP Enabled	Key		Role	Timeout	Prio
*	☐	<>		<>	<>	32768
1	☐	Auto		Active	Fast	32768
2	☐	Auto		Active	Fast	32768
3	☐	Auto		Active	Fast	32768
4	☐	Auto		Active	Fast	32768
5	☐	Auto		Active	Fast	32768
6	☐	Auto		Active	Fast	32768
7	☐	Auto		Active	Fast	32768
8	☐	Auto		Active	Fast	32768
9	☐	Auto		Active	Fast	32768
10	☐	Auto		Active	Fast	32768

Save Reset

This page is used to configure LACP function for Aggregation operation. LACP is an IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol, allows bundling several physical ports together to form a single logical port. Two switches can create aggregation connection with LACP function.

6.4.6 Configuration - Loop Protection

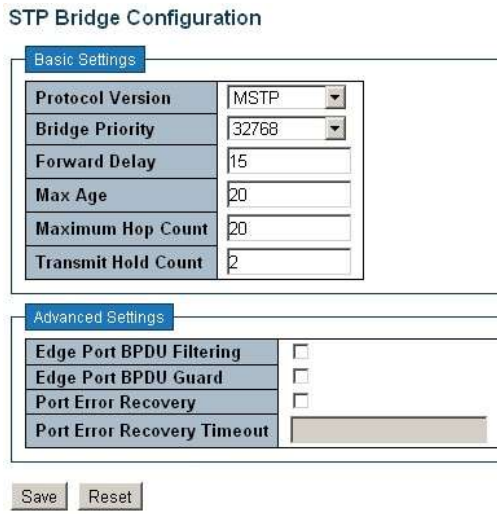


This page is used to configure Loopback Detection function. Loopback on port will cause packet storm in switch.

If Loopback Detection is enabled on ports and Tx Mode is enabled, the port is actively generating loop protection PDU's. If loopback is found, the action could be shutdown port or log it. The shutdown time could be configured for some period.

6.4.7 Configuration - Spanning Tree

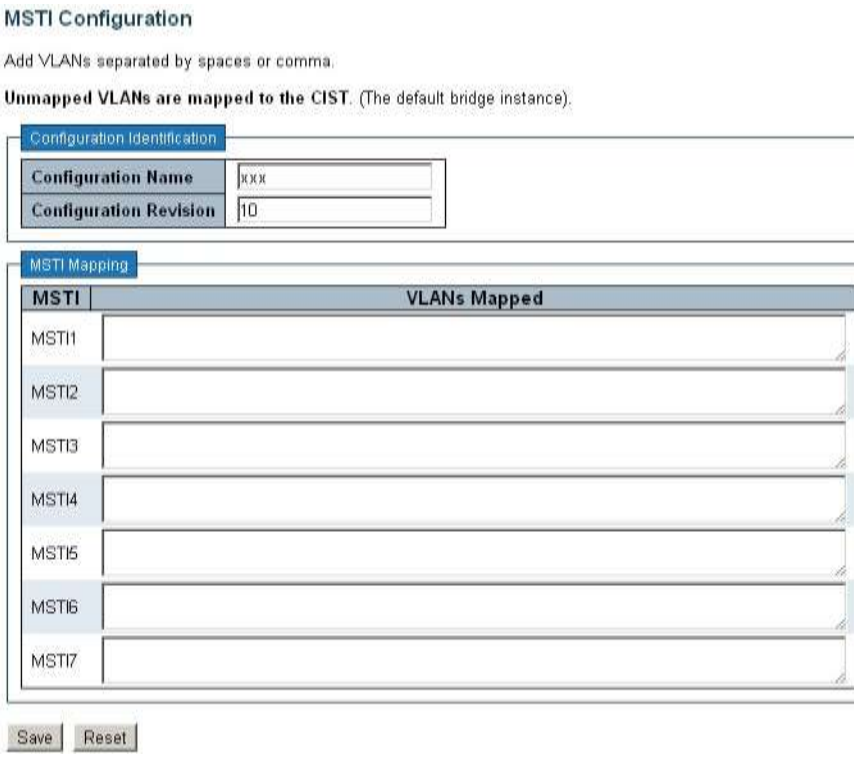
6.4.7.1 Configuration - Spanning Tree - Bridge Settings



This page is used to configure Spanning Tree Bridge configuration.

This switch supports STP(IEEE 802.1D), RSTP(IEEE 802.1w), and MSTP(IEEE 802.1s). It could be selected at Prorocol Version.

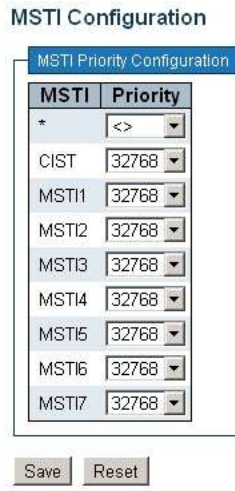
6.4.7.2 Configuration - Spanning Tree - MSTI Mapping



This page is used to configure the mapping between MSTI and VLAN.

Configuration Identification consists of the name and revision to identify the VLAN to MSTI mapping. Bridges must share the name and revision, as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region).

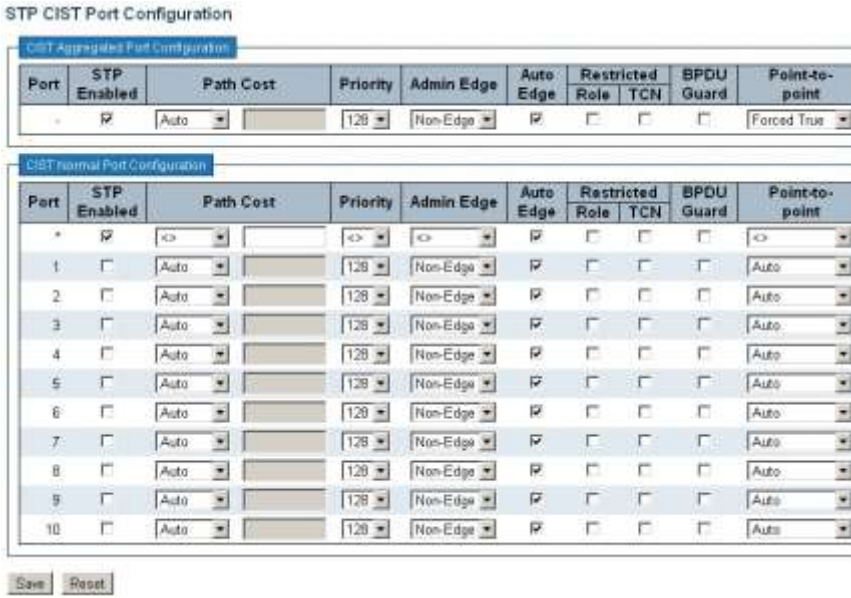
6.4.7.3 Configuration - Spanning Tree - MSTI Priorities



This page is used to configuration MSTI Priority.

Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

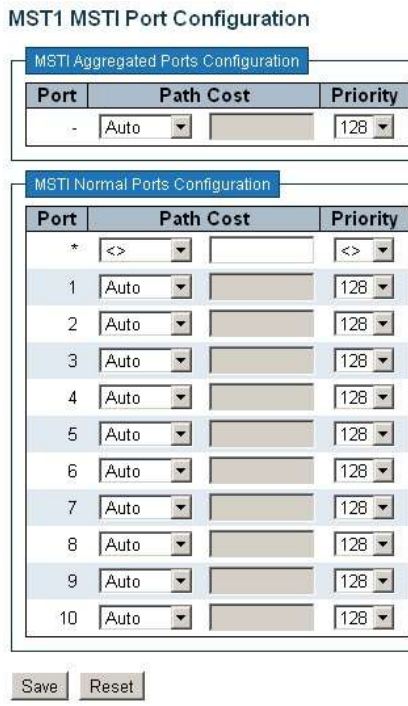
6.4.7.4 Configuration - Spanning Tree - CIST Ports



This page is used to configure Spanning Tree opeartion on Ports.

6.4.7.5 Configuration - Spanning Tree - MSTI Ports

Select the MSTI. Click [Get].
The MSTI Port Configuration will be shown.

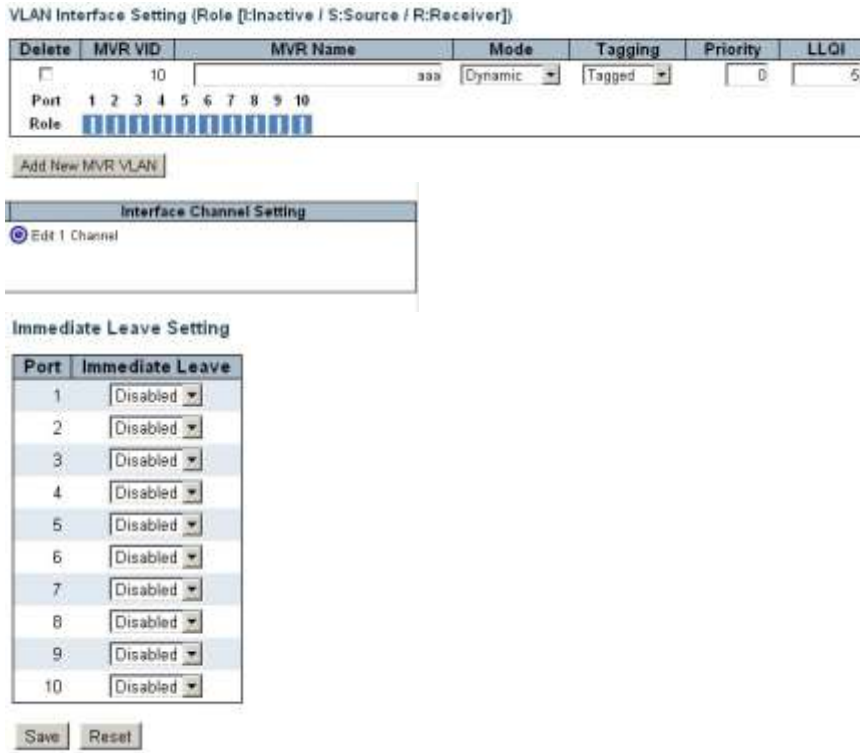


An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

Path Cost controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports.

Priority controls the port priority. This can be used to control priority of ports having identical port cost.

6.4.8 Configuration - MVR



This page is used to configure MVR function. The MVR feature enables multicast traffic forwarding on the Multicast VLANs. In a multicast television application, a PC or a network television or a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP/MLD report message to Switch A to join the appropriate multicast group address. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports. It is allowed to create at maximum 8 MVR VLANs with corresponding channel settings for each Multicast VLAN. There will be totally at maximum 256 group addresses for channel settings.

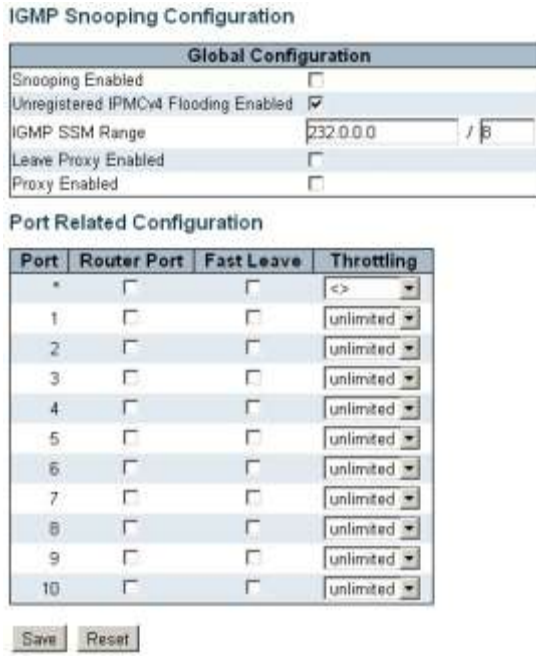
Follow the steps to complete the configuration.

1. Create MVR VLANs and assign ports to the VLANs.
2. Configure the MVR VLAN.
3. Click (e) to assign channels to the VLAN.
4. Enable/Disable Immediate Leave function on Ports.

6.4.9 Configuration - IPMC

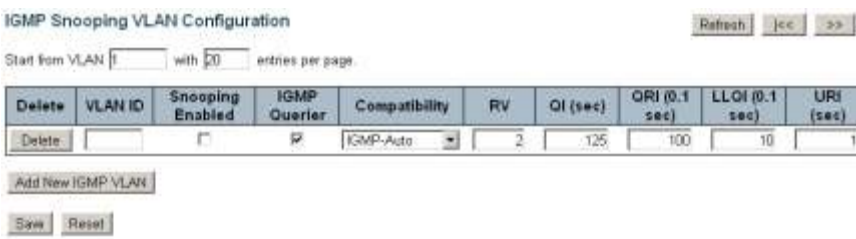
6.4.9.1 Configuration - IPMC - IGMP Snooping

1). Configuration - IPMC - IGMP Snooping - Basic Configuration



This page is used to configure the basic configuration of IGMP Snooping function. Configuration for general settings and port settings can be done here.

2). Configuration - IPMC - IGMP Snooping - VLAN Configuration



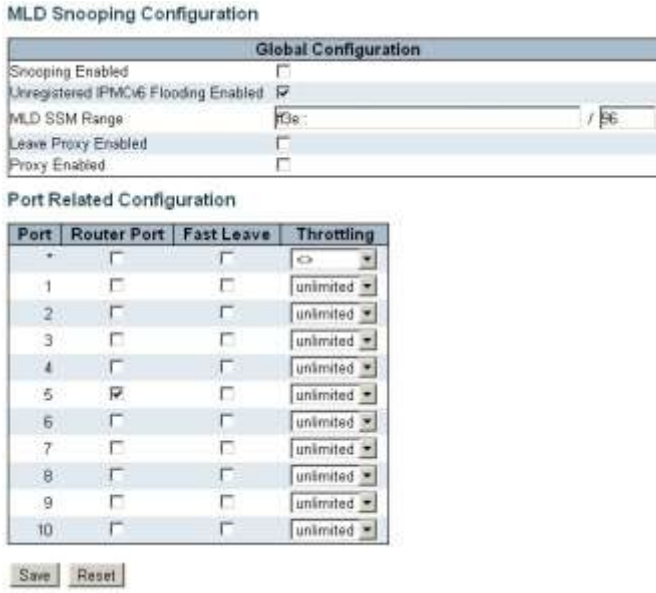
This page is used to maintain the IGMP Snooping VLAN Table. The following functions are supported.
- Add a new IGMP VLAN. Configure it. And Save.
- Edit a IGMP VLAN.
- Delete a IGMP VLAN

3). Configuration - IPMC - IGMP Snooping - Port Group Filtering

This page is used to maintain IGMP Filtering Group on Port. The IP Multicast Group in the table will be filtered on the port.

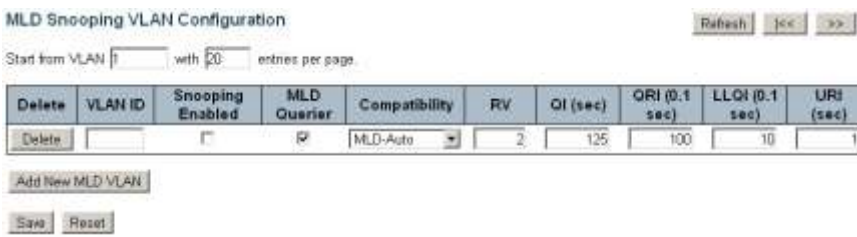
6.4.9.2 Configuration - IPMC - MLD Snooping

1). Configuration - IPMC - MLD Snooping - Basic Configuration



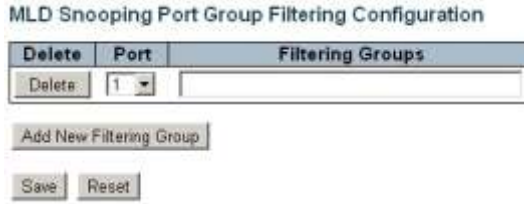
This page is used to configure the basic configuration of MLD Snooping function. Configuration for general settings and port settings can be done here.

2). Configuration - IPMC - MLD Snooping - VLAN Configuration



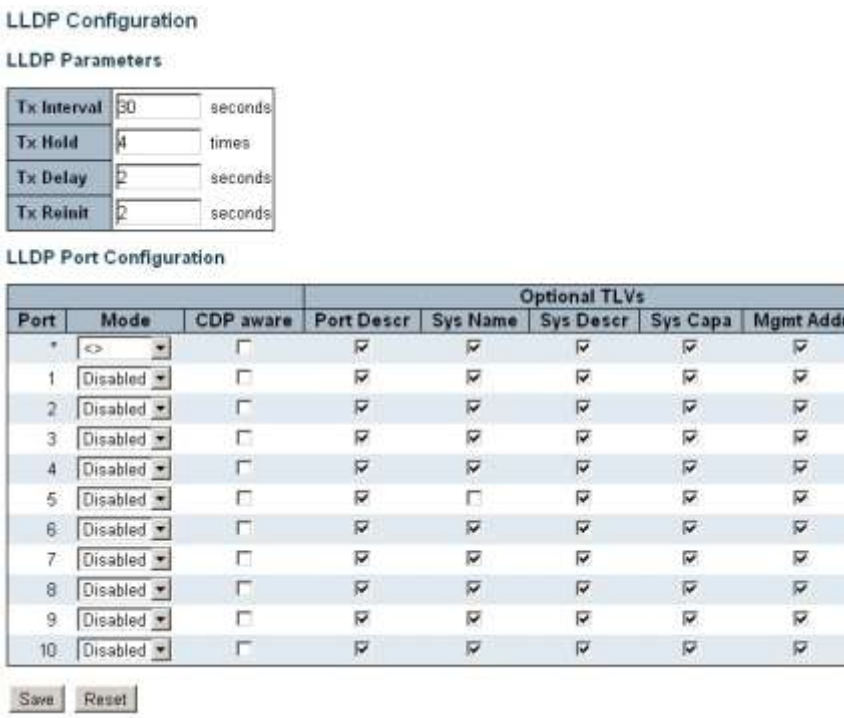
This page is used to maintain the MLD Snooping VLAN Table. The following functions are supported.
- Add a new IGMP VLAN. Configure it. And Save.
- Edit a IGMP VLAN.
- Delete a IGMP VLAN

3). Configuration - IPMC - MLD Snooping - Port Group Filtering



This page is used to maintain MLD Filtering Group on Port. The IP Multicast Group in the table will be filtered on the port.

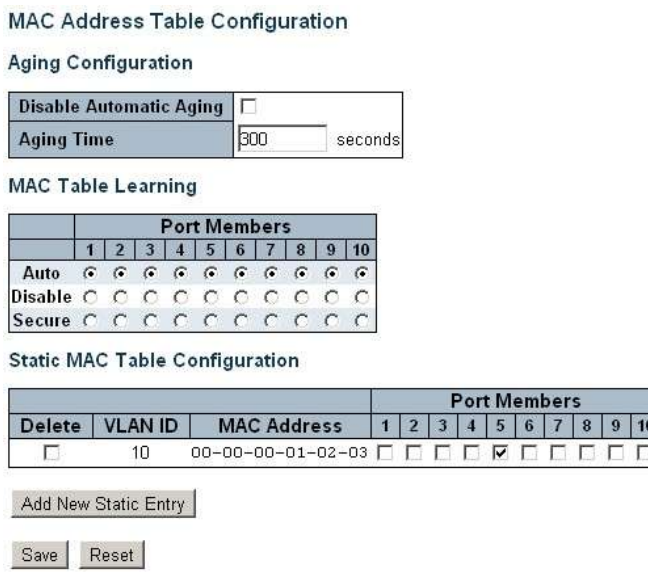
6.4.10 Configuration - LLDP



This page is used to configure LLDP function of the switch. The system general settings and ports settings can be configured.

LLDP is an IEEE 802.1ab standard protocol.
The Link Layer Discovery Protocol(LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

6.4.11 Configuration - MAC Table

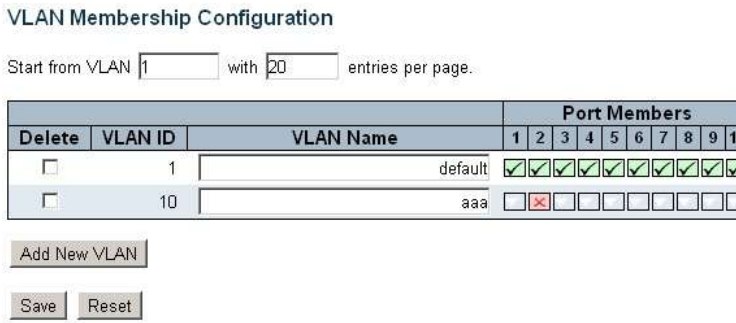


This page is used to configure Mac Table function of the switch.

Aging Time, Mac Address Learning, Static Mac Address can be configured in this function. If Mac Address Learning is set to Secure, only static MAC entries are learned, all other frames are dropped.

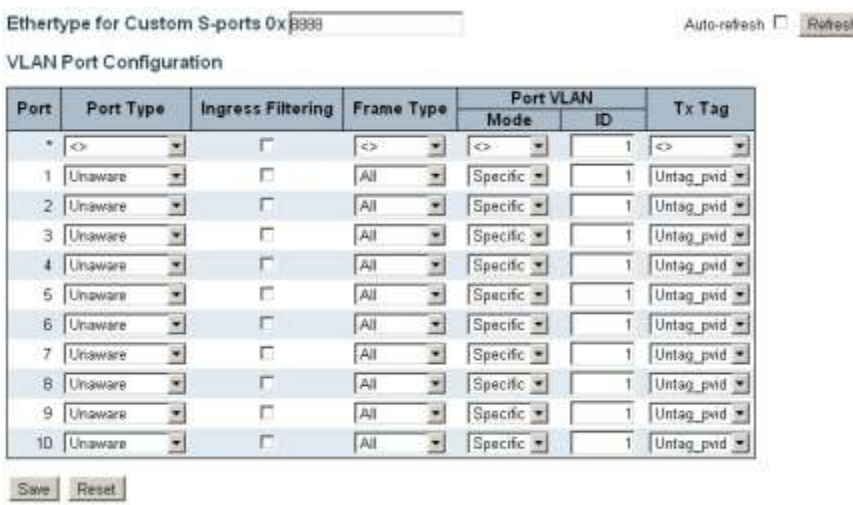
6.4.12 Configuration - VLANs

6.4.12.1 Configuration - VLANs - VLAN Membership



This page is used to maintain 802.1Q VLAN Group.
Add a new VLAN, and assign VLAN ID, VLAN Name, Ports to it.
Edit a VLAN.
Delete a VLAN.

6.4.12.2 Configuration - VLANs - Ports



This page is used to configure 802.1Q VLAN and Q-in-Q function on Ports.

About Port Type ...

- Unaware: When a port is setup as Unaware. Incoming frames will be treated as untagged. Even when an incoming frame is tagged, this tag is treated by the switch as payload. And the frame will be classified to port based VLAN — PVID. This for 802.1Q access connection or Q-in-Q downlink connection. If Port-based VLAN is used, please set ports as “Unaware” with the same PVID.
- C-port: When a port is setup as C-port, tagged frames will be classified to the VLAN based on this tag of the frames. This is for 802.1Q VLAN trunk.
- S-port: When a port is setup as S-port, the TPID in tag of egress frame are always 0x88A8 as Service VLAN. This is for Q-in-Q uplink connection.
- S-custom-port: When a port is setup as S-custom-port, the TPID in tag of egress frame are always customized TPID as Service VLAN. This is for Q-in-Q uplink connection.

About Port VLAN Mode ...

- None: PVID will be ignored. A VLAN tag with the classified VLAN ID is inserted in frames transmitted on the port. This mode is normally used for ports connected to VLAN aware switches as 802.1Q VLAN trunk connection. Tx tag should be set to Untag_pvid when this mode is used.
- Specific: A Port VLAN ID can be configured. Untagged frames received on the port are classified to the Port VLAN ID. If VLAN awareness is disabled(Port Type is Unaware.), all frames received on the port are classified to the Port VLAN ID. If the classified VLAN ID of a frame transmitted on the port is different from the Port VLAN ID, a VLAN tag with the classified VLAN ID is inserted in the frame.

"Tx_Tag" define how frame will be tagged on the egress direction — when frame is sent out of the switch from this port.

About 802.1Q VLAN settings ...
Access: [Port Type]-Unaware, [Port VLAN Mode]-Specific(set PVID), [Tx Tag]-Untag_all.
Trunk: [Port Type]-C-port, [Port VLAN Mode]-None, [Tx Tag]-Untag_pvid.
Hybrid: [Port Type]-Unaware, [Port VLAN Mode]-Specific(set PVID), [Tx Tag]-Untag_pvid.

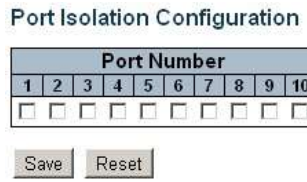
About Q-in-Q settings ...
Uplink: [Port Type]-S-port(or S-custom-port with custom TPID), [Port VLAN Mode]-None, [Tx Tag]-Untag_pvid.
Downlink: [Port Type]-Unaware, [Port VLAN Mode]-Specific(set Service VLAN ID as PVID, remember to create the Service VLAN and put Uplink/Downlink ports in it), [Tx Tag]-Untag_all.

6.4.13 Configuration - Port-Based VLANs

6.4.13.1 Configuration - Port-Based VLANs - PVLAN Membership

This page is used to configure Port-based VLAN. Port-based VLAN can be created, edited, deleted.

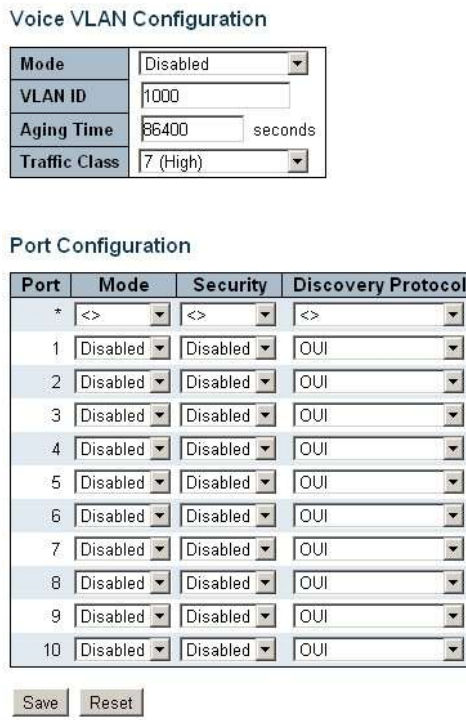
6.4.13.2 Configuration - Port-Based VLANs - Port Isolation



This page is used to configure Port Isolation function. If ports are marked as Isolation, they cannot communicate with each other even they are in the same VLAN.

6.4.14 Configuration - Voice VLAN

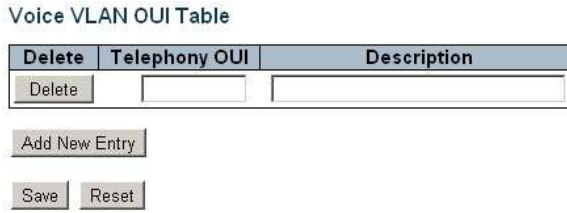
6.4.14.1 Configuration -Voice VLAN - Configuration



This page is used to configure Voice VLAN of the switch. It can configure general system settings and port settings.

If the function is enabled, the switch can auto-detect VoIP traffic and forward the traffic in the Voice VLAN with specific priority. The Voice VLAN port discovery protocol could be by OUI or LLDP. (OUI is the first three bytes of Mac Address.)

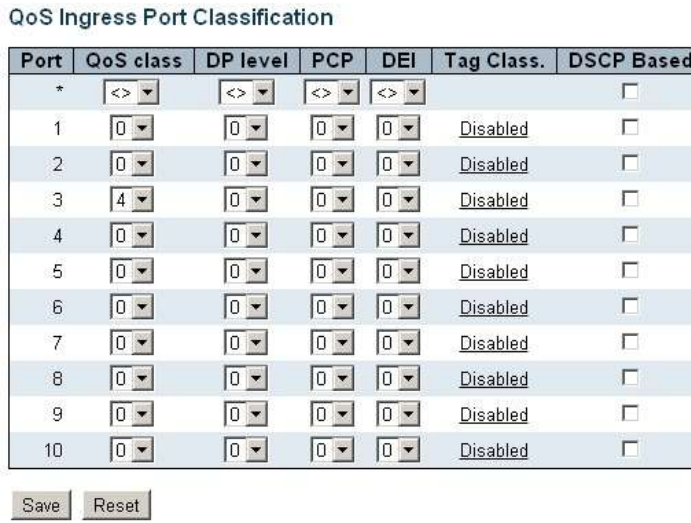
6.4.14.2 Configuration -Voice VLAN - OUI



This page is used to maintain the OUI table for Voice IP traffic. OUI is the first three bytes of Mac Address.

Packets with OUI in the table will be treated as Voice traffic.

6.4.15.1 Configuration - QoS - Port Classification



This page is used to configure the basic QoS Ingress Classification settings for all switch ports. The following parameters could be configured - Default QoS Class, default DP(Drop Precedence) Level, default PCP(Priority Code Point) for untagged frames, default DEI(Drop Eligible Indicator) for untagged frames, default process for tagged frames, DSCP-based QoS.

About tag classification ...
[Tag Class] is used to enable/disable doing QoS by PCP and DEI in 802.1Q tag. Clicking it, a (PCP, DEI) to (QoS class, DP level) mapping setting will be shown. When it is enabled, the ingress tag classification QoS operation of the port will follow the mapping for packet forwarding.

About DSCP classification ...
[DSCP Based] is used to enable/disable doing QoS by DSCP in IP header. Check it, and it is enabled.
For ingress DSCP classification configuration, please refer to [DSCP-Based QoS] page. Check [Trust] in that page, and the DSCP value will work.
For ingress DSCP classification translation configuration, please refer to [DSCP Translation] and [Port DSCP] pages for further settings.
For egress DSCP remarking configuratiin, please refer to [Port DSCP], [DSCP Classification], and [DSCP Translation] pages for further settings.

The QoS class and DP level settings works only when both tag classification and DSCP classification are disabled. The PCP and DEI settings will be applied when untagged packets are translate to tagged packets. When both tag classification and DSCP classification are disabled, QoS class and DP level settings are statically assigned to a port. All frames received on that port will have the same QoS class and DP level. This a Port-based QoS.

6.4.15.2 Configuration - QoS - Port Policing

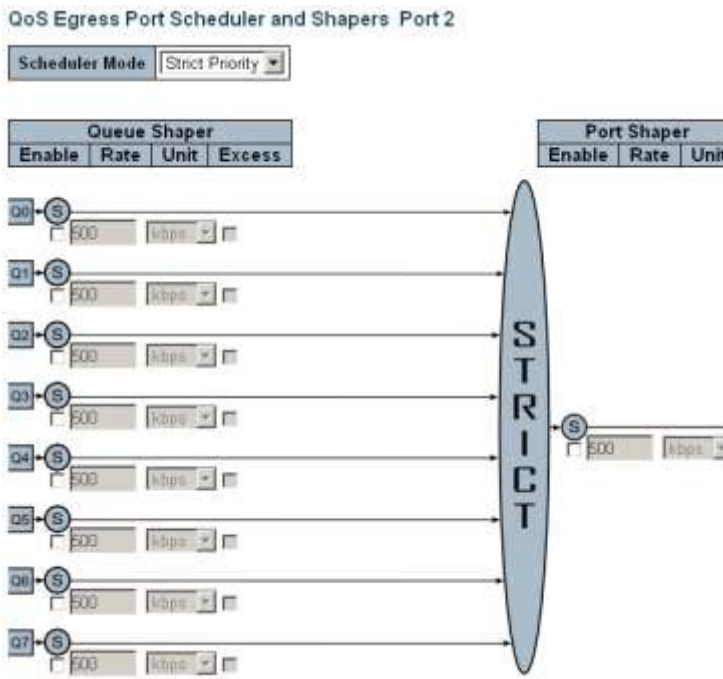
This page is used to configure Port Ingress Rate Limit. If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames when limit rate is reached.

6.4.15.3 Configuration - QoS - Port Scheduler

QoS Egress Port Schedulers

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Weighted	17%	17%	17%	17%	17%	17%
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-

This page will show port egress scheduler mode and weight of each queue. Click Port number to configure its Egress Scheduler. The following page will be shown.



This page is used to configure Egress traffic Scheduler and Egress traffic Shaper on port.

The traffic scheduler could operate in Strict Priority mode or Weighted mode. If in Weighted mode, the weighting of each queue could be configured.

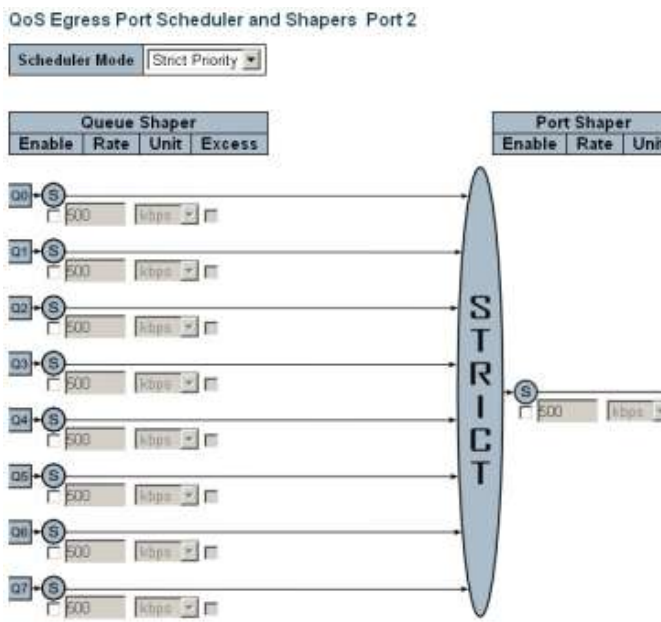
The traffic shaper could operate by queue or by port. Enable by checking it and give a limit value.

6.4.15.4 Configuration - QoS - Port Shaping

QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	10 Mbps	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
10	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

This page will show egress shaper settings of each port and each queue.
Click Port number to configure its Egress Shaper. The following page will be shown.

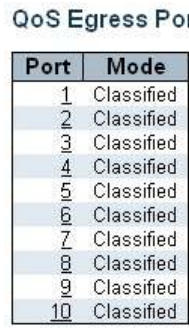


This page is used to configure Egress traffic Scheduler and Egress traffic Shaper on port.

The traffic scheduler could operate in Strict Priority mode or Weighted mode. If in Weighted mode, the weighting of each queue could be configured.

The traffic shaper could operate by queue or by port. Enable by checking it and give a limit value.

6.4.15.5 Configuration - QoS - Port Tag Remarking


QoS Egress Port Tag Remarking

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified

This page is used to show Egress Tag Remarking mode of each port. The mode could be ...
- Classified: Use classified PCP/DEI values.
- Default: Use default PCP/DEI values.
- Mapped: Use mapped versions of QoS class and DP level.

Click Port number to configure the Egress Tag Remarking mode for it. The following page will be shown.

The mode could be ...
- Classified: Use classified PCP/DEI values.
- Default: Use default PCP/DEI values.
- Mapped: Use mapped versions of QoS class and DP level.

Select the mode and configure the parameters for it. When “Default” or “Mapped” is selected, the defaulf/mapped PCP and DEI will applied to the egress tagged packet when the egress port is a tagged port. The original PCP and DEI settings will be remarked by the defaulf/mapped PCP and DEI. Or, the defaulf/mapped PCP and DEI will be applied to out tag for double tagging Q-in-Q applications.

6.4.15.6 Configuration - QoS - Port DSCP

QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	☐	<>	<>
1	☐	Disable	Disable
2	☐	Disable	Disable
3	☐	Disable	Enable
4	☐	Disable	Disable
5	☐	Disable	Disable
6	☐	Disable	Disable
7	☐	Disable	Disable
8	☐	Disable	Disable
9	☐	Disable	Disable
10	☐	Disable	Disable

Save Reset

This page allows you to configure the basic QoS Port DSCP Configuration settings for all switch ports.

You can configure DSCP ingress and egress settings. In Ingress settings you can change ingress translation and classification settings for individual ports. In egress settings, you can configure Rewriting or Remapping for individual ports.

About Ingress Translate ...
The ingress DSCP value can be translated to another DSCP value for QoS operation when “Translate” is checked. The translation mapping is set at [DSCP Translation] page and the translated DSCP value will be used for ingress DSCP QoS operation.

About Ingress Classify ...
The DSCP ingress classify does not mean DSCP to QoS classification. (DSCP

to QoS mapping is done in the [DSCP-Based QoS] page.) Instead Ingress Classify in [Port DSCP] means QoS to internal DSCP mapping. When a QoS class (either from port default or VLAN Tag or DSCP) is gotten, the Ingress Classify can map this QoS class to internal DSCP.
This internal DSCP then can do another egress map to affect the DSCP value when the frame is sent out. The QoS to internal DSCP mapping is set in [DSCP Classification] page, and the mapping will be applied to egress packets when "Egress Rewrite" in [Port DSCP] page is "enable"/"Remap DP Unaware"/"Remap DP Aware". And the original DSCP value is lost.
The Ingress Classify could be ...

- Disable: Disable ingress DSCP QoS class to internal DSCP mapping operation.
- DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0.
- Selected: Classify only selected DSCP for which classification is enabled as specified in [DSCP Translation] page (select by checking "classify").
- All: works for all DSCP values.

About Egress Rewrite ...
This is used to set the DSCP Rewrite for egress packet.

- Disable: No Egress rewrite.
- Enable: Rewrite enabled with settings in [DSCP Classification] page without remapping.
- Remap DP Unaware: Rewrite enabled with remapping "Remap DP0" setting in [DSCP Translation] page from the internal DSCP value.
- Remap DP Aware: Rewrite enabled with remapping "Remap DP0" or "Remap DP1" setting in [DSCP Translation] page from the internal DSCP value.

6.4.15.7 Configuration - QoS - DSCP Based QoS

DSCP-Based QoS Ingress Classification

DSCP	Trust	QoS Class	DPL
*	☐	<>	<>
0 (BE)	☐	0	0
1	☐	0	0
2	☐	0	0
3	☐	0	0
4	☐	0	0
5	☐	0	0
6	☐	0	0

This page is used to configure QoS Ingress Classification for each DSCP value.

Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.

6.4.15.8 Configuration - QoS - DSCP Translation

DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>	☐	<>	<>
0 (BE)	30 (AF33)	☐	0 (BE)	0 (BE)
1	1	☐	1	1
2	2	☐	2	2
3	3	☐	3	3
4	4	☐	4	4
5	5	☐	5	5
6	6	☐	6	6

This page is used to configure the basic QoS DSCP Translation settings for all DSCP values. DSCP translation can be done in Ingress or Egress.

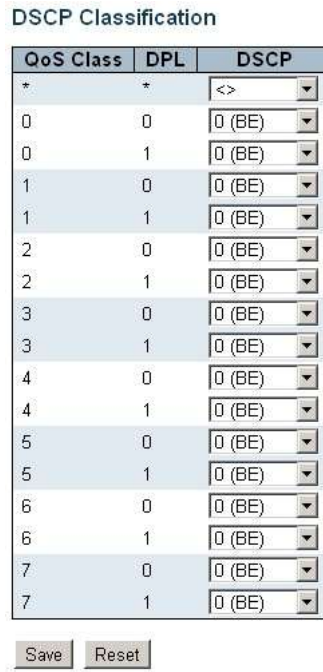
Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two configuration parameters for DSCP Translation -

1. Translate: DSCP at Ingress side can be translated to any of (0-63) DSCP values.

2. Classify: Select the DSCP value to enable its QoS Class to internal DSCP mapping operation when Ingess Classify is “Selected” in [Port DSCP] page.

For Egress, there are the following configurable parameters for Egress side -
1. Remap DP0 Controls the remapping for frames with DP level 0.
2. Remap DP1 Controls the remapping for frames with DP level 1.
The settings are applied to Egress Rewrite in [Port DSCP] page. Please refer to the description about Egress Rewrite in [Port DSCP] page.

6.4.15.9 Configuration - QoS - DSCP Classification



This page is used to configure the mapping of QoS class and Drop Precedence Level to internal DSCP value.

Frames got a QoS class (either from port default or VLAN Tag or DSCP) then it can map this QoS to internal DSCP. This internal DSCP then can do another egress map to affect the DSCP value when the frame is sent out. It could rewrite the egress DSCP value when Egress Rewrite in [Port DSCP] page is not disable. Please refer to the description about Egress Rewrite in [Port DSCP] page.

6.4.15.10 Configuration - QoS - QoS Control List

QoS Control List Configuration

QCE#	Port	Frame Type	SMAC	DMAC	VID	PCP	DEI	Action			
								Class	DPL	DSCP	
10	5	Any	Any	Any	Any	Any	Any	0	Default	Default	

This page is used to configured QCL(QoS Control List). Each QCE consists of packet parameters and QoS action for packets match the parameters. With this function, specific packet traffic could be processed with expected QoS action.

6.4.15.11 Configuration - QoS - Storm Control

Storm Control Configuration

Frame Type	Enable	Rate (pps)
Unicast	☐	1
Multicast	☐	1
Broadcast	☐	1

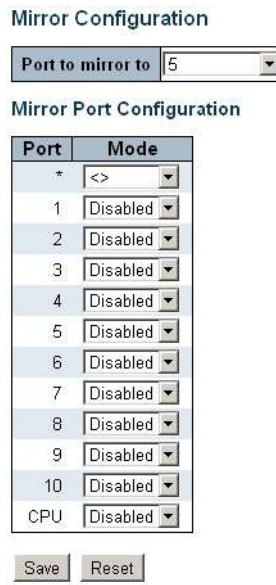
Save Reset

This page is used to configure storm control for the switch.

There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.
The configuration indicates the permitted packet rate for unicast, multicast or broadcast traffic across the switch.

Note: If ports are in management VLAN, Broadcast Storm Control will fail to work.

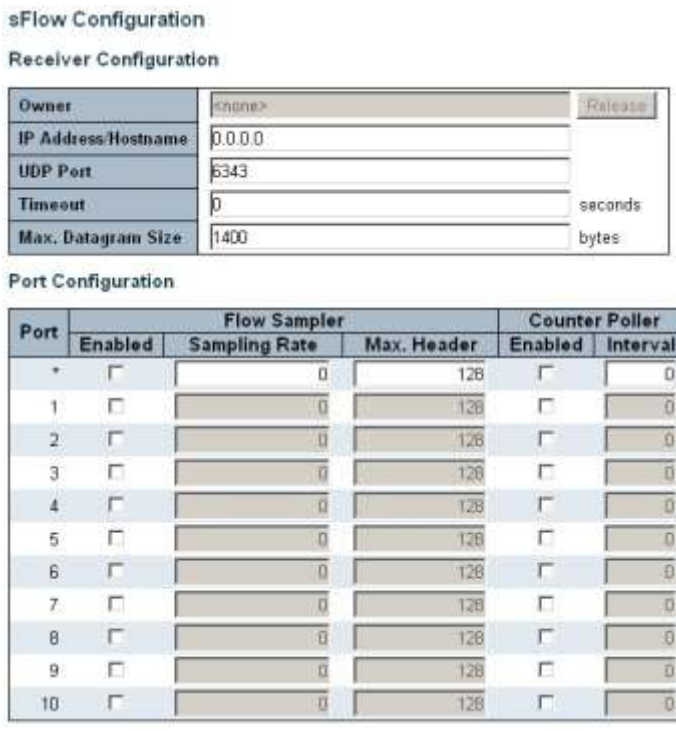
6.4.16 Configuration - Mirroring



This page is used to configure Mirror function of the switch. To debug network problems, selected traffic can be copied, or mirrored, on a mirror port where a frame analyzer can be attached to analyze the frame flow.

The mirror traffic could be transmit packets (egress or destination mirroring), receive packets (ingress or source mirroring), or both. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on the mirror port. Disabled disables mirroring.

6.4.17 Configuration - sFlow



sFlow Configuration

Receiver Configuration

Owner	<none>	Release
IP Address/Hostname	0.0.0.0	
UDP Port	6343	
Timeout	0	seconds
Max. Datagram Size	1400	bytes

Port Configuration

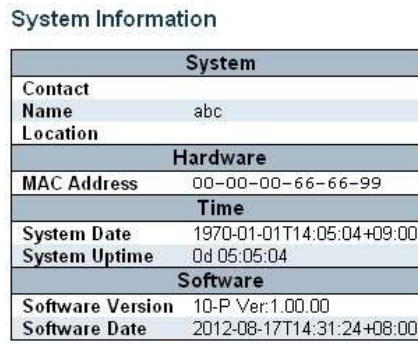
Port	Flow Sampler			Counter Poller	
	Enabled	Sampling Rate	Max. Header	Enabled	Interval
*	☐	0	128	☐	0
1	☐	0	128	☐	0
2	☐	0	128	☐	0
3	☐	0	128	☐	0
4	☐	0	128	☐	0
5	☐	0	128	☐	0
6	☐	0	128	☐	0
7	☐	0	128	☐	0
8	☐	0	128	☐	0
9	☐	0	128	☐	0
10	☐	0	128	☐	0

This page is used to configuring sFlow. The configuration is divided into two parts: Configuration of the sFlow receiver (a.k.a. sFlow collector) and configuration of per-port flow and counter samplers.

sFlow configuration is not persisted to non-volatile memory, which means that a reboot will disable sFlow sampling.

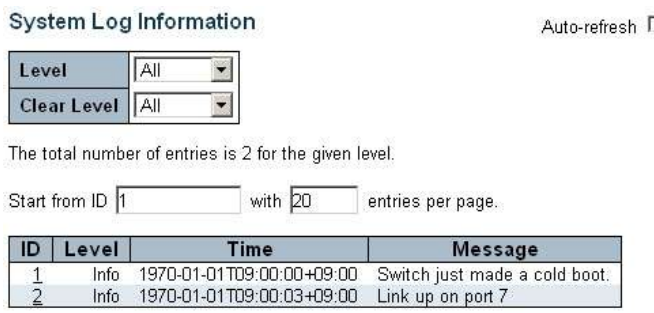
6.4.18 Monitor - System

6.4.18.1 Monitor - System - Information



This page is used to show switch system information.

6.4.18.2 Monitor - System - Log



This page is used to show system log information of the switch.

Level is a filter for showing expected system information.
Clear Level is the level that will be applied for clear operation by clicking [Clear].

Clicking ID will show the details of the log.

6.4.18.3 Monitor - System - Detailed Log

This page is used to show the details of log.
Entering the ID, details of the log will be shown.

6.4.19 Monitor - Port

6.4.19.1 Monitor - Port - State

This page is used to show Port Link status. Clicking port will show its statistics.

6.4.19.2 Monitor - Port - Traffic Overview

Port Statistics Overview

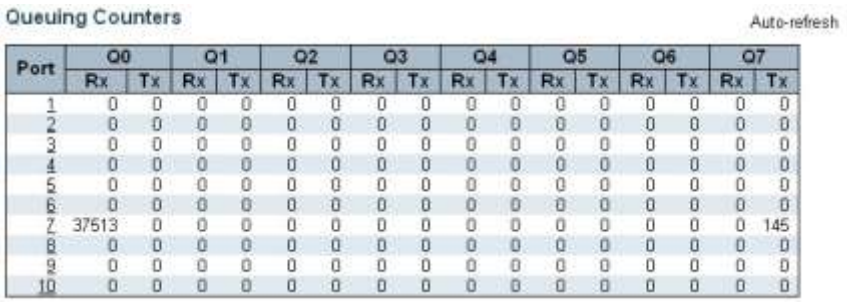
Auto-refresh Refresh Clear

Port	Packets		Bytes		Errors		Drops	
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	36971	135	6832778	26358	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0

Filtered
Received
0
0
0
0
0
0
17477
0
0
0

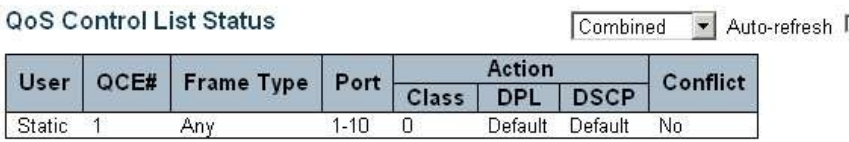
This page is used to show brief statistics of each port.

6.4.19.3 Monitor - Port - QoS Statistics



This page is used to show traffic statistics of queues on each port.
Clicking port will show its statistics.

6.4.19.4 Monitor - Port - QCL Status



This page is used to show the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations.

About Conflict ...
Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

6.4.19.5 Monitor - Port - Detailed Statistics

Detailed Port Statistics Port 7

Port 7 | Auto-refresh | Refresh

Receive Total		Transmit Total	
Rx Packets	39070	Tx Packets	303
Rx Octets	7294595	Tx Octets	82728
Rx Unicast	500	Tx Unicast	292
Rx Multicast	18698	Tx Multicast	8
Rx Broadcast	19972	Tx Broadcast	3
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	14604	Tx 64 Bytes	82
Rx 65-127 Bytes	7695	Tx 65-127 Bytes	25
Rx 128-255 Bytes	3162	Tx 128-255 Bytes	114
Rx 256-511 Bytes	13459	Tx 256-511 Bytes	53
Rx 512-1023 Bytes	129	Tx 512-1023 Bytes	7
Rx 1024-1526 Bytes	1	Tx 1024-1526 Bytes	22
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	39070	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	303
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	18689		

This page is used to show detail statistics of port.
Select the port. And detail statistics of the port will be shown.

6.4.19.6 Monitor - Port - DDMI

DDMI Port 10

Port 10 | Auto-refresh

Serial Info Table	
Status	ok_with_DDM
Vendor	XXX
PartNo	KF231463
SerialNo	09446020
Revision	
DateCode	091030
Transceiver	1000BASE-SX

Ddm Info Table					
Type	AlarmMax	AlarmMin	WarnMax	WarnMin	Current
Temperature(°C)	95.00	-32.00	90.00	-25.00	34.21
Voltage(mV)	3.63	2.97	3.56	3.04	3.27
TxBias(mA)	13.00	2.00	12.00	3.00	7.10
TxPower(mW)	0.79	0.12	0.63	0.14	0.33
RxPower(mW)	1.00	0.02	0.79	0.03	0.00

This page is used to show SFP transceiver information and status if the transceiver supports DDMI (Digital Diagnostics Monitoring Interface) function.

6.4.20 Monitor - Security

6.4.20.1 Monitor - Security - Access Management Statistics

Access Management Statistics

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

This page is used to show management traffic statistics of every interface.

6.4.20.2 Monitor - Security - Network

1-1). Monitor - Security - Network - Port Security - Switch

Port Security Switch Status

User Module Legend

User Module Name	Abbr
Limit Control	L
802.1X	8
DHCP Snooping	D
Voice VLAN	V

Port Status

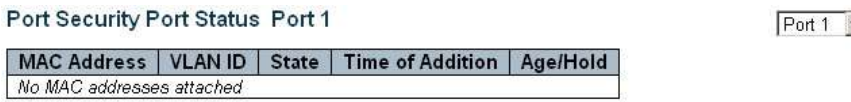
Port	Users	State	MAC Count	
			Current	Limit
1	----	Disabled	-	-
2	----	Disabled	-	-
3	----	Disabled	-	-
4	----	Disabled	-	-
5	----	Disabled	-	-
6	----	Disabled	-	-
7	----	Disabled	-	-
8	----	Disabled	-	-
9	----	Disabled	-	-
10	----	Disabled	-	-

This page is used to show the current state of the port and the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.

State of port could be ...
- Disabled: No user modules are currently using the Port Security service.
- Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.
- Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.
- Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.

Clicking port will show MAC addresses secured by the Port Security module.

1-2). Monitor - Security - Network - Port Security - Port



This page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

About Age/Hold ...
If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin.
If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

2-1). Monitor - Security - Network - NAS - Switch

Network Access Server Switch Status

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled				
2	Force Authorized	Globally Disabled				
3	Force Authorized	Globally Disabled				
4	Force Authorized	Globally Disabled				
5	Force Authorized	Globally Disabled				
6	Force Authorized	Globally Disabled				
7	Force Authorized	Globally Disabled				
8	Force Authorized	Globally Disabled				
9	Force Authorized	Globally Disabled				
10	Force Authorized	Globally Disabled				

This page provides an overview of the current NAS (by 802.1x) port states.

NAS is an acronym for Network Access Server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. The switch implementes NAS by IEEE 802.1X.

Click port to show port state of 802.1x.

2-2). Monitor - Security - Network - NAS - Port

NAS Statistics Port 1

Port 1

Port State

Admin State	Force Authorized
Port State	Globally Disabled

This page is used to show port state of 802.1x.
Select Port. And the Port State of 802.1x will be shown.

3). Monitor - Security - Network - ACL Status

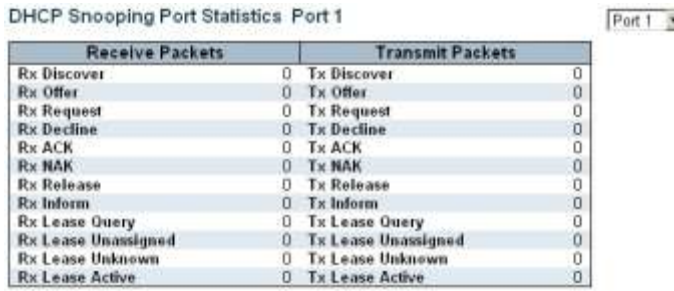
ACL Status

Combined Auto-refresh Refresh

User	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	CPU Once	Counter	Conflict
No entries										

This page is used to show the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations.

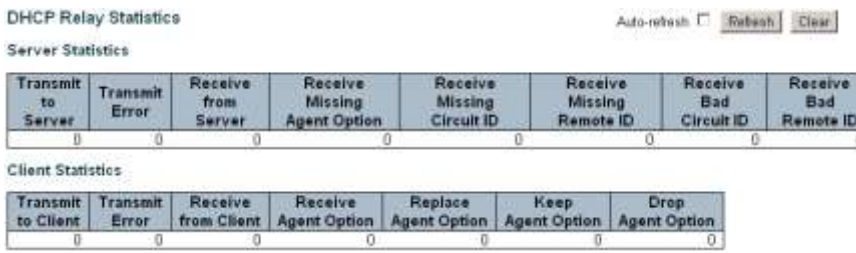
4-1). Monitor - Security - Network - DHCP - Snooping Statistics



This page is used to show DHCP Snooping traffic statistics on port.
Select Port. And the DHCP Snooping traffic statistics on the port will be shown.

The statistics doesn't count the DHCP packets for system DHCP client or DHCP relay mode is enabled

4-2). Monitor - Security - Network - DHCP - Relay Statistics



This page is used to show DHCP Relay statistics.

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.
The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client.

5). Monitor - Security - Network - ARP Inspection

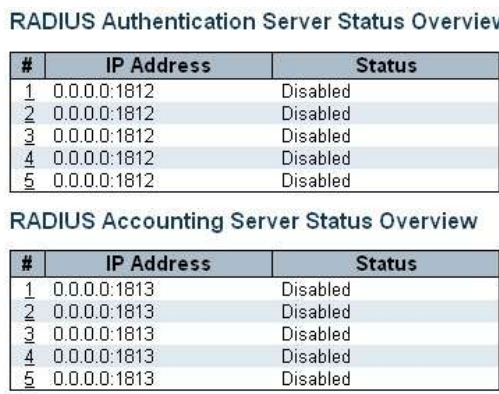
Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

6). Monitor - Security - Network - IP Source Guard

Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.

6.4.20.3 Monitor - Security - AAA

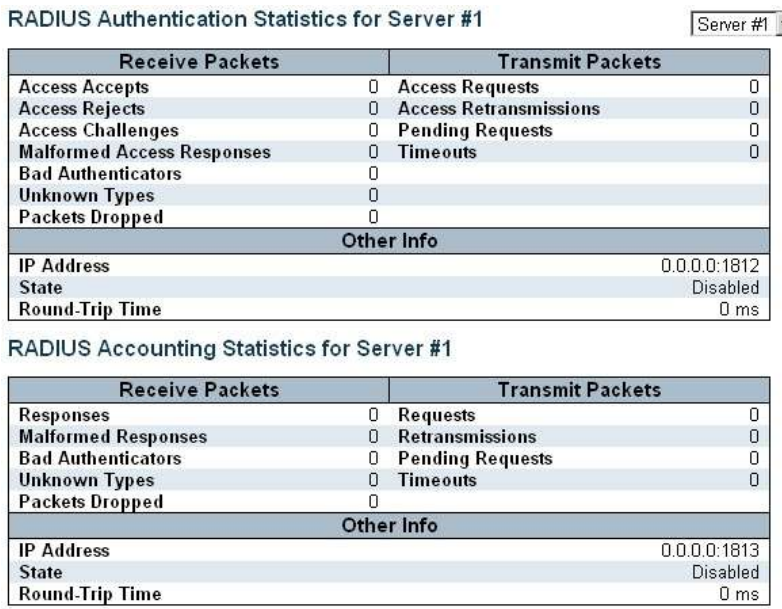
1). Monitor - Security - AAA - RADIUS Overview



This page provides an overview of the status of the RADIUS servers configurable on the Authentication configuration page.

The Status could be ...
- Disabled: The server is disabled.
- Not Ready: The server is enabled, but IP communication is not yet up and running.
- Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.
- Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

2). Monitor - Security - AAA - RADIUS Details



RADIUS Authentication Statistics for Server #1

Server #1

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
IP Address			0.0.0.0:1812
State			Disabled
Round-Trip Time			0 ms

RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address			0.0.0.0:1813
State			Disabled
Round-Trip Time			0 ms

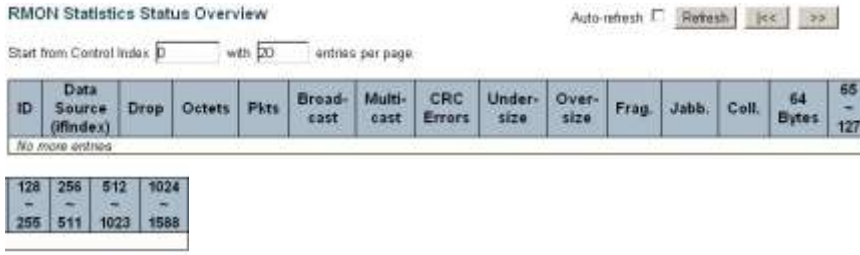
This page provides detailed statistics for a particular RADIUS server.

The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB. Use the server select box to switch between the backend servers to show details for.

6.4.20.4 Monitor - Security - Switch

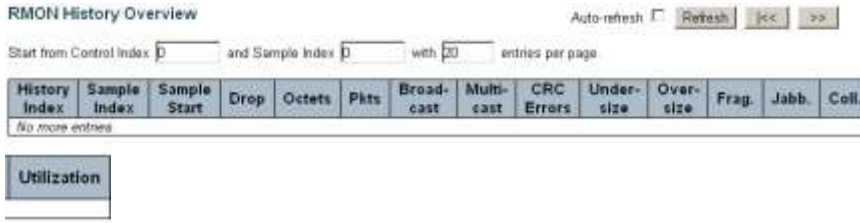
1). Monitor - Security - Switch - RMON

1-1) Monitor - Security - Switch - RMON - Statistics



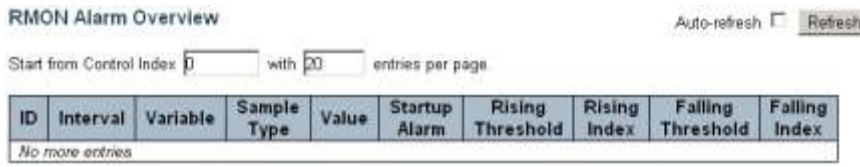
This page provides an overview of RMON Statistics entries.

1-2) Monitor - Security - Switch - RMON - History



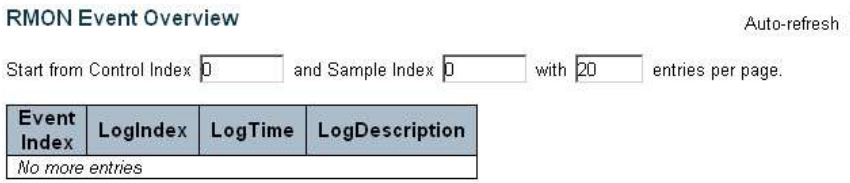
This page provides an overview of RMON History entries.

1-3) Monitor - Security - Switch - RMON - Alarm



This page provides an overview of RMON Alarm entries.

1-4) Monitor - Security - Switch - RMON - Event



This page provides an overview of RMON Event table entries.

6.4.21 Monitor - LACP

6.4.21.1 Monitor - LACP - System Status

LACP System Status

Aggr ID	Partner System ID	Partner Key	Partner Prio	Last Changed	Local Ports
No ports enabled or no existing partners					

This page provides a status overview for all LACP instances.

6.4.21.2 Monitor - LACP - Port Status

LACP Status

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	No	-	-	-	-	-
2	No	-	-	-	-	-
3	No	-	-	-	-	-
4	No	-	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-
7	No	-	-	-	-	-
8	No	-	-	-	-	-
9	No	-	-	-	-	-
10	No	-	-	-	-	-

This page provides a status overview for LACP status for all ports.

6.4.21.3 Monitor - LACP - Port Statistics

LACP Statistics

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0

This page provides an overview for LACP statistics for all ports.

6.4.22 Monitor - Loop Protection

Loop Protection Status

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Down	-	-
2	Shutdown	Enabled	0	Down	-	-
3	Shutdown	Enabled	0	Down	-	-
4	Shutdown	Enabled	0	Down	-	-
5	Shutdown	Enabled	0	Down	-	-
6	Shutdown	Enabled	0	Down	-	-
7	Shutdown	Enabled	0	Up	-	-
8	Shutdown	Enabled	0	Down	-	-
9	Shutdown	Enabled	0	Down	-	-
10	Shutdown	Enabled	0	Down	-	-

This page displays the loop protection port status for ports of the switch.

If loop happens on port, packet storm will be generates from the switch. That will cause serious problem for normal network operation. Loop Protection function can prevent such problem happens on ports.

6.4.23 Monitor - Spanning Tree

6.4.23.1 Monitor - Spanning Tree - Bridge Status

STP Bridges

Auto-refresh ☐

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-C0-F9-66-66-99	32768.00-C0-F9-66-66-99	-	0	Steady	-

This page provides a status overview of all STP bridge instances.

Click CIST or MSTIx, STP Detailed Bridge Status will be shown.

STP Detailed Bridge Status

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	32768.00-00-00-66-66-99
Root ID	32768.00-00-00-66-66-99
Root Cost	0
Root Port	-
Regional Root	32768.00-00-00-66-66-99
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	0
Topology Change Last	-

CIST Ports & Aggregations State

Port	Port ID	Role	State	Path Cost	Edge	Point-to-Point	Uptime
7	128:007	DesignatedPort	Forwarding	200000	Yes	Yes	0d 00:01:26

6.4.23.2 Monitor - Spanning Tree - Port Status

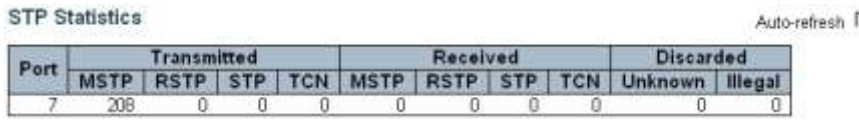
STP Port Status

Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	Disabled	Discarding	-
3	Disabled	Discarding	-
4	Disabled	Discarding	-
5	Disabled	Discarding	-
6	Disabled	Discarding	-
7	DesignatedPort	Forwarding	0d 00:05:09
8	Disabled	Discarding	-
9	Disabled	Discarding	-
10	Disabled	Discarding	-

This page displays the STP CIST port status for physical ports of the switch.

The CIST Role could be AlternatePort, BackupPort, RootPort, DesignatedPort, or Disabled. The CIST State could be Discarding, Learning, or Forwarding.

6.4.23.3 Monitor - Spanning Tree - Port Statistics


STP Statistics

Auto-refresh

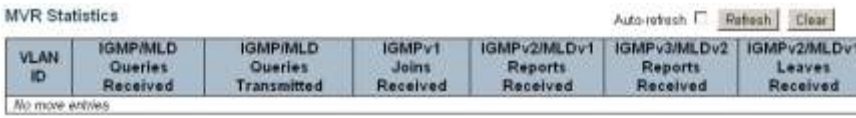
Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
7	208	0	0	0	0	0	0	0	0	0

This page displays the STP port statistics counters of bridge ports in the switch.

- MSTP: The number of MSTP BPDU's received/transmitted on the port.
- RSTP: The number of RSTP BPDU's received/transmitted on the port.
- STP: The number of legacy STP Configuration BPDU's received/transmitted on the port.
- TCN: The number of (legacy) Topology Change Notification BPDU's received /transmitted on the port.
- Discarded Unknown: The number of unknown Spanning Tree BPDU's received (and discarded) on the port.
- Discarded Illegal: The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

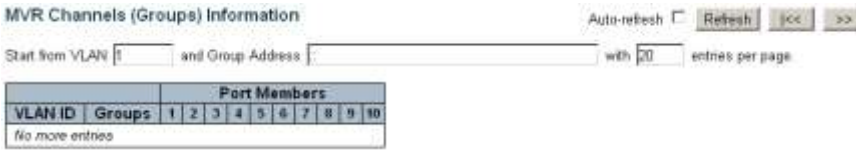
6.4.24 Monitor - MVR

6.4.24.1 Monitor - MVR - Statistics



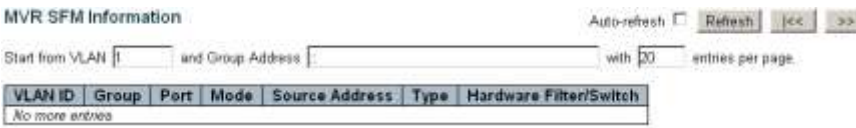
This page provides MVR Statistics information.

6.4.24.2 Monitor - MVR - MVR Channel Groups



Entries in the MVR Channels (Groups) Information Table are shown on this page. The MVR Channels (Groups) Information Table is sorted first by VLAN ID, and then by group.

6.4.24.3 Monitor - MVR - MVR SFM Information

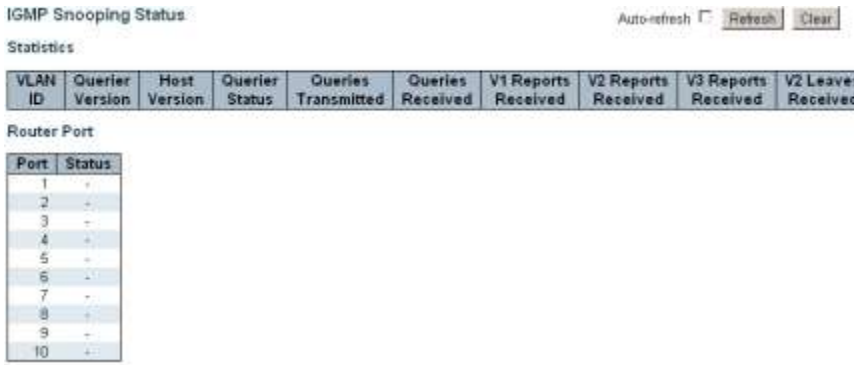


Entries in the MVR SFM Information Table are shown on this page. The MVR SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

6.4.25 Monitor - IPMC

6.4.25.1 Monitor - IPMC - IGMP Snooping

1). Monitor - IPMC - IGMP Snooping - Status



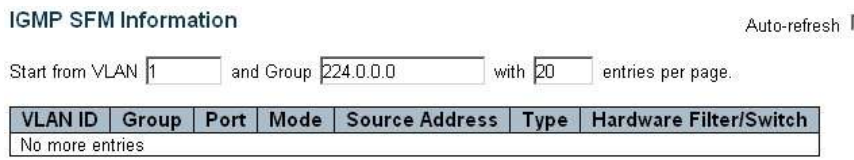
This page provides IGMP Snooping status.

Protocol status and statistics are shown.
Router Port active status is shown.

2). Monitor - IPMC - IGMP Snooping - Groups Information

Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group.

3). Monitor - IPMC - IGMP Snooping - IPv4 SFM Information



Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

6.4.25.2 Monitor - IPMC - MLD Snooping

1). Monitor - IPMC - MLD Snooping - Status

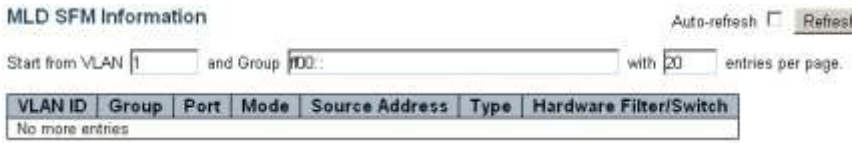
This page provides MLD Snooping status.

Protocol status and statistics are shown.
Router Port active status is shown.

2). Monitor - IPMC - MLD Snooping - Groups Information

Entries in the MLD Group Table are shown on this page. The MLD Group Table is sorted first by VLAN ID, and then by group.

3). Monitor - IPMC - MLD Snooping - IPv6 SFM Information

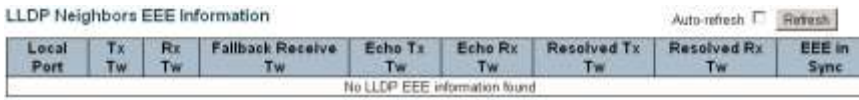


Entries in the MLD SFM Information Table are shown on this page. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

6.4.26.1 Monitor - LLDP - Neighbours

This page provides a status overview for all LLDP neighbours. The displayed table contains a row for each port on which an LLDP neighbour is detected.

6.4.26.2 Monitor - LLDP - EEE



This page provides an overview of EEE information exchanged by LLDP.

By using EEE power savings can be achieved at the expense of traffic latency. This latency occurs due to that the circuits EEE turn off to save power, need time to boot up before sending traffic over the link. This time is called "wakeup time". To achieve minimal latency, devices can use LLDP to exchange information about their respective tx and rx "wakeup time ", as a way to agree upon the minimum wakeup time they need.

6.4.26.3 Monitor - LLDP - Port Statistics

LLDP Global Counters

Auto-refresh ☐ Refresh Clear

Global Counters	
Neighbour entries were last changed	1970-01-01T00:00:00+00:00 (3174 secs. ago)
Total Neighbours Entries Added	0
Total Neighbours Entries Deleted	0
Total Neighbours Entries Dropped	0
Total Neighbours Entries Aged Out	0

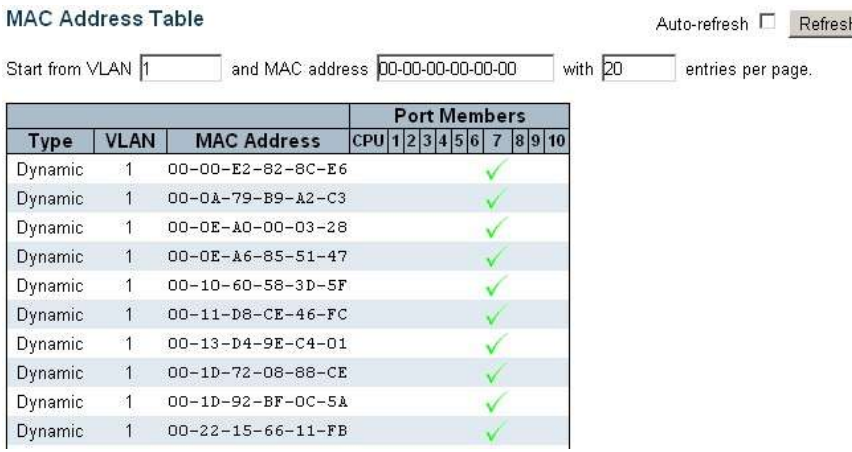
LLDP Statistics Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0

This page provides an overview of all LLDP traffic.

Two types of counters are shown. Global counters are counters that refer to the whole switch, while local counters refer to per port counters for the currently selected switch.

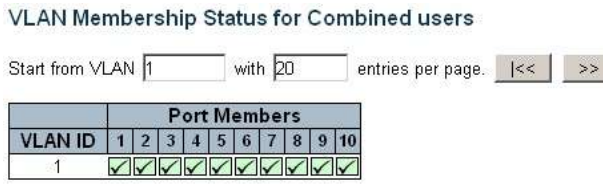
6.4.27 Monitor - MAC Table



Entries in the MAC Table are shown on this page. The MAC Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

6.4.28 Monitor - VLANs

6.4.28.1 Monitor - VLANs - VLAN Membership



This page provides an overview of membership status of VLAN.

6.4.28.2 Monitor - VLANs - VLAN Port

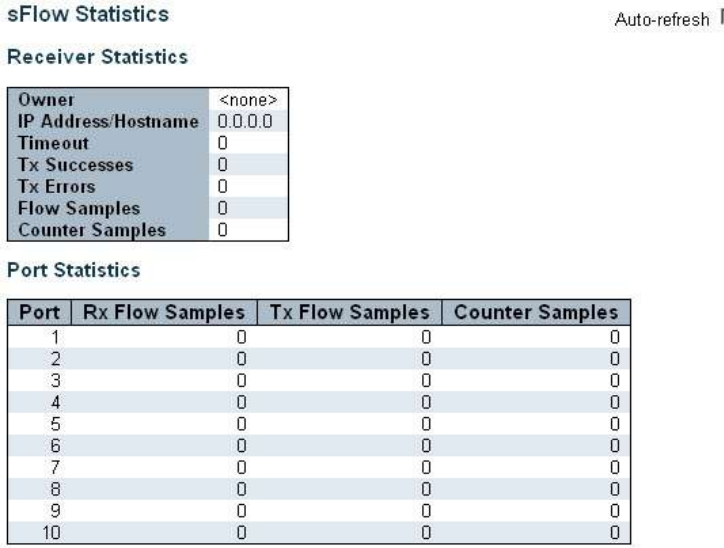
VLAN Port Status for Static user

Static

Port	PVID	Port Type	Ingress Filtering	Frame Type	Tx Tag	UVID	Conflicts
1	1	UnAware	Disabled	All	Untag_this	1	No
2	1	UnAware	Disabled	All	Untag_this	1	No
3	1	UnAware	Disabled	All	Untag_this	1	No
4	1	UnAware	Disabled	All	Untag_this	1	No
5	1	UnAware	Disabled	All	Untag_this	1	No
6	1	UnAware	Disabled	All	Untag_this	1	No
7	1	UnAware	Disabled	All	Untag_this	1	No
8	1	UnAware	Disabled	All	Untag_this	1	No
9	1	UnAware	Disabled	All	Untag_this	1	No
10	1	UnAware	Disabled	All	Untag_this	1	No

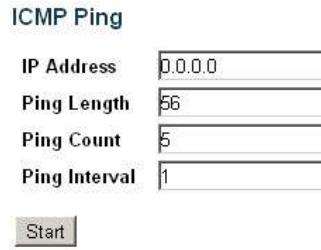
This page provides VLAN Port Status and Setting.

6.4.29 Monitor - sFlow



This page shows receiver and per-port sFlow statistics.

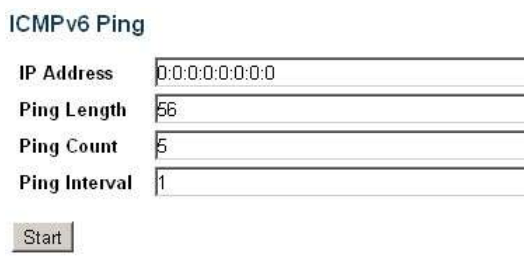
6.4.30 Diagnostics - Ping



This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.

After you click [Start], ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested data space(the ICMP header). The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

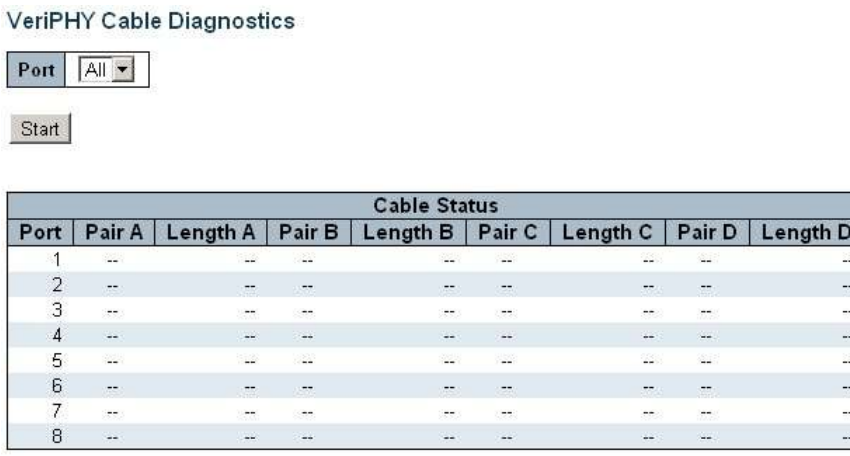
6.4.31 Diagnostics - Ping6



This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

After you click [Start], ICMPv6 packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

6.4.32 Diagnostics - VeriPHY



This page is used for running the VeriPHY Cable Diagnostics for 10/100 and 1G copper ports.

Click [Start] to run the diagnostics. This 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.

6.4.33 Maintenance - Restart Device

You can restart the switch on this page. After restart, the switch will boot normally.

[Yes] : Click to restart device.
[No] : Click to return to the Port State page without restarting.

6.4.34 Maintenance - Factory Defaults

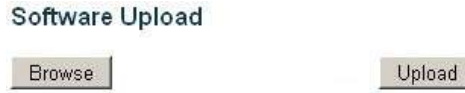
You can reset the configuration of the switch on this page. Only the IP configuration is retained. The new configuration is available immediately, which means that no restart is necessary.

[Yes] : Click to reset the configuration to Factory Defaults.
[No] : Click to return to the Port State page without resetting the configuration.

Note: Restoring factory default can also be performed by making a physical loopback between port 1 and port 2 within the first minute from switch reboot. In the first minute after boot, 'loopback' packets will be transmitted at port 1. If a 'loopback' packet is received at port 2 the switch will do a restore to default

6.4.35 Maintenance - Software

6.4.35.1 Maintenance - Software - Upload



This page facilitates an update of the firmware controlling the switch.

[Browse] to the location of a software image and click **[Upload]**.

After the software image is uploaded, a page announces that the firmware update is initiated. After about 1~2 minutes, the firmware is updated and the switch restarts.

This switch supports firmware image backup function. The old Active Image will become Alternate Image, and the new firmware image will be the Active Image. The Alternate Image can be switched to be Active Image by "Image Select" function to run the old firmware image.

Warning: While the firmware is being updated, Web access appears to be defunct. Do not restart or power off the device at this time or the switch may fail to function afterwards.

6.4.35.2 Maintenance - Software - Image Select

This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.

The web page displays two tables with information about the active and

alternate firmware images.

Note:
1. In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the “Activate Alternate Image” button is also disabled.
2. If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.

6.4.36 Maintenance - Configuration

6.4.36.1 Maintenance - Configuration - Save

You can save the switch configuration. The configuration file is in CLI format.

6.4.36.2 Maintenance - Configuration - Upload

[Browse] to the location of a configuration file and click [Upload].

You can upload the switch configuration. The configuration file is in CLI format.

7. Software Update and Backup

This switch supports software update and configuration backup/update/restore functions. It could be done in two ways.

1. **From web browser**: Doing by http protocol and by web browser. Please refer to the description of "*Maintenance*" function in Section 6.4.35 for Software Update and Section 6.4.36 for Configuration Backup/Restore.

2. **From console/telnet command**: Doing by TFTP protocol and done by "copy" command. Please refer to the description of "*copy*" command in Section 6.2.2.

This switch supports firmware image backup function. The old Active Image will become Alternate Image (backup image), and the new firmware image will be the Active Image. The Alternate Image (backup image) can be switched to be Active Image by "Image Select" function in Web (Maintenance -> Software -> Image Select) to run the old firmware image.

A. Product Hardware Specifications

[8TX+2SFP Model]

Access Method	Ethernet, CSMA/CD
Standards Conformance	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE IEEE 802.3z, IEEE 802.3ab (1000Base)
Communication Rate	10/100/1000Mbps for TX, 100/1000Mbps for SFP Full / Half duplex (auto-negotiation)
MDI/MDIX	Auto-Detect
Indicator Panel	LEDs for each unit : Power, System each port : Link/Act(Green:1000M, Yellow:10/100M)
Number of Ports	8* RJ45 TX, 2* SFP ports (10 GE Ports totally)
Console	D-Sub 9
Dimensions	250 x 117 x 37 mm
Certification	CE Mark, FCC Class A
Temperature	Standard Operating: 0 to 50℃
Humidity	10% to 90% (Non-condensing)
Fan	Fanless
Bridging Function	Filtering, forwarding and learning
Switching Method	Store-and-forward
Address Table	8K entries
Filtering/Forwarding Rate	Line speed
Maximum Packet Size	9600 Bytes
Flow Control	802.3x for full duplex, backpressure for half duplex

[16TX+2SFP Model]

Access Method	Ethernet, CSMA/CD
Standards Conformance	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE IEEE 802.3z, IEEE 802.3ab (1000Base)
Communication Rate	10/100/1000Mbps for TX, 100/1000Mbps for SFP Full / Half duplex (auto-negotiation)
MDI/MDIX	Auto-Detect
Indicator Panel	LEDs for each unit : Power, System each port : Link/Act(Green:1000M, Yellow:10/100M)
Number of Ports	16* RJ45 TX, 2* SFP ports (18 GE Ports totally)
Console	D-Sub 9

Dimensions	250 x 117 x 37 mm
Certification	CE Mark, FCC Class A
Temperature	Standard Operating: 0 to 50℃
Humidity	10% to 90% (Non-condensing)
Fan	Fanless
Bridging Function	Filtering, forwarding and learning
Switching Method	Store-and-forward
Address Table	8K entries
Filtering/Forwarding Rate	Line speed
Maximum Packet Size	9600 Bytes
Flow Control	802.3x for full duplex, backpressure for half duplex

[24TX+4SFP Model]

Access Method	Ethernet, CSMA/CD
Standards Conformance	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE IEEE 802.3z, IEEE 802.3ab (1000Base)
Communication Rate	10/100/1000Mbps for TX, 100/1000Mbps for SFP Full / Half duplex (auto-negotiation)
MDI/MDIX	Auto-Detect
Indicator Panel	LEDs for each unit : Power, System each port : Link/Act(Green:1000M, Yellow:10/100M)
Number of Ports	24* RJ45 TX, 4* SFP ports (24 GE Ports totally)
Console	D-Sub 9
Dimensions	330 x 204 x 43 mm
Certification	CE Mark, FCC Class A
Temperature	Standard Operating: 0 to 50℃
Humidity	10% to 90% (Non-condensing)
Fan	Fanless
Bridging Function	Filtering, forwarding and learning
Switching Method	Store-and-forward
Address Table	8K entries
Filtering/Forwarding Rate	Line speed
Maximum Packet Size	9600 Bytes
Flow Control	802.3x for full duplex, backpressure for half duplex

B. Product Software Specifications

Port Control	Port speed, duplex mode, and flow control Port frame size (1518 - 9600 bytes) Port state (administrative status) Port status (link monitoring) Port statistics (MIB counters) Port VeriPHY (cable diagnostics) Power Control
L2 Switching	Auto MAC address learning/aging and MAC addresses (static) IEEE 802.1Q VLAN, Q-in-Q, Port isolation, Port Based VLAN IEEE 802.1ad Provider Bridge IEEE 802.1D STP/802.1w RSTP/802.1s MSTP IEEE 802.3ad Link Aggregation, static and LACP BPDU guard and restricted role, BPDU transparency DHCP client, DHCP snooping, DHCP option 82 relay ARP inspection Port mirroring IP MAC binding
Layer 2,3 Multicast	IGMP/MLD snooping, (1024 groups) IGMP/MLD throttling, filtering, and leave proxy (Fast Leave /Normal Leave / Immediate Leave) MVR
QoS	8 Priority Queues per Port Port Based priority Scheduler priority QoS Control List Storm control for UC, MC, and BC Policing and shaping per port and per queue DiffServ (RF 2474) remarking Tag remarking
Security	Port-based 802.1X, Single 802.1X, Multiple 802.1X MAC-based authentication, VLAN assignment, QoS assignment, Guest VLAN RADIUS accounting MAC address limit

	TACACS+ Web and CLI authentication and authorization Authorization (3 levels) ACLs for filtering(256 entries), policing, and port copy IP source guard
Synchronization	NTPv4 Client
Power Saving	ActiPHY, PerfectReach Ethernet Energy Efficient power management(EEE)
Management	HTTP server CLI console port Telnet Management access filtering SSHv2 and HTTPS IPv6 Management System Syslog Software download through Web SNMPv1/v2c/v3Agent RMON Group 1, 2, 3, and 9 IEEE 802.1AB-2005 Link Layer Discovery, LLDP Text Configuration download or upload sFlow

C. Compliances

EMI Certification FCC Class A Certification (USA)

Warning: This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A digital device pursuant to Subpart B of Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are required to correct the interference.

CE Mark Declaration of Conformance for EMI and Safety (EEC)

This is to certify that this product complies with ISO/IEC Guide 22 and EN45014. It conforms to the following specifications:

EMC: EN55022:2010:Class A
IEC61000-3-2:2005+A1:2008+A2:2009
IEC61000-3-3:2008
EN55024:2010
IEC61000-4-2:2008
IEC61000-4-3:2006+A1:2007+A2:2010
IEC61000-4-4:2004+A1:2010
IEC61000-4-5:2005
IEC61000-4-6-2008
IEC61000-4-8:2009
IEC61000-4-11:2004

This product complies with the requirements of the Low Voltage Directive 2006/95/EC and the EMC Directive 2004/108/EC.

Warning! Do not plug a phone jack connector into the RJ-45 port. This may damage this device.

D. Warranty

We warrant to the original owner that the product delivered in this package will be free from defects in material and workmanship for a period of warranty time from the date of purchase from us or the authorized reseller. The warranty does not cover the product if it is damaged in the process of being installed. We recommend that you have the company from whom you purchased this product install it.

CTC union®

www.ctcu.com

T +886-2 2659-1021 F +886-2 2659-0237 E sales@ctcu.com