# User Manual

# GSW-3420FM

## 20 X 100/1000Base-X SFP slots + 4 X GbE combo ports (10/100/1000Base-T or 1000Base-X) L2 managed Ethernet Switch

CTC UNION TECHNOLOGIES CO., LTD.

**LEGAL**

The information in this publication has been carefully checked and is believed to be entirely accurate at the time of publication. CTC Union Technologies assumes no responsibility, however, for possible errors or omissions, or for any consequences resulting from the use of the information contained herein. CTC Union Technologies reserves the right to make changes in its products or product specifications with the intent to improve function or design at any time and without notice and is not required to update this documentation to reflect such changes.

CTC Union Technologies makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does CTC Union assume any liability arising out of the application or use of any product and specifically disclaims any and all liability, including without limitation any consequential or incidental damages.

CTC Union products are not designed, intended, or authorized for use in systems or applications intended to support or sustain life, or for any other application in which the failure of the product could create a situation where personal injury or death may occur. Should the Buyer purchase or use a CTC Union product for any such unintended or unauthorized application, the Buyer shall indemnify and hold CTC Union Technologies and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, expenses, and reasonable attorney fees arising out of, either directly or indirectly, any claim of personal injury or death that may be associated with such unintended or unauthorized use, even if such claim alleges that CTC Union Technologies was negligent regarding the design or manufacture of said product.

**WARNING:**

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual may cause harmful interference in which case the user will be required to correct the interference at his own expense. NOTICE: (1) The changes or modifications not expressively approved by the party responsible for compliance could void the user's authority to operate the equipment. (2) Shielded interface cables and AC power cord, if any, must be used in order to comply with the emission limits.

**CISPR PUB.22 Class A COMPLIANCE:**

This device complies with EMC directive of the European Community and meets or exceeds the following technical standard. EN 55022 - Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment. This device complies with CISPR Class A.

**WARNING:**

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

**CE NOTICE**

Marking by the symbol CE indicates compliance of this equipment to the EMC directive of the European Community. Such marking is indicative that this equipment meets or exceeds the following technical standards: EN 55022:2006+A1:2007, Class A, EN55024:2010, and EN60950-1:2006

**Version 1.0**

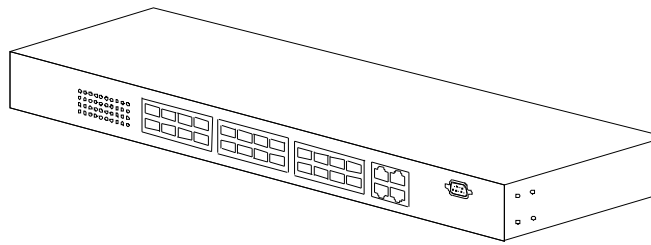
**December 2013**

About this manual …

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

These models are

1. **24 * SFP + 4 * TX(combo) ports model**
   This model supports twenty-four SFP ports and four share TX 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

This Gigabit Management Fiber Optic Switch is a Layer 2 Management switch with lots of advanced network functions. Console is supported for command-line settings. Web, Telnet, and SNMP interfaces are for remote switch management through network. These functions can meet most of the management request for current network.

## 1.1 Package Contents

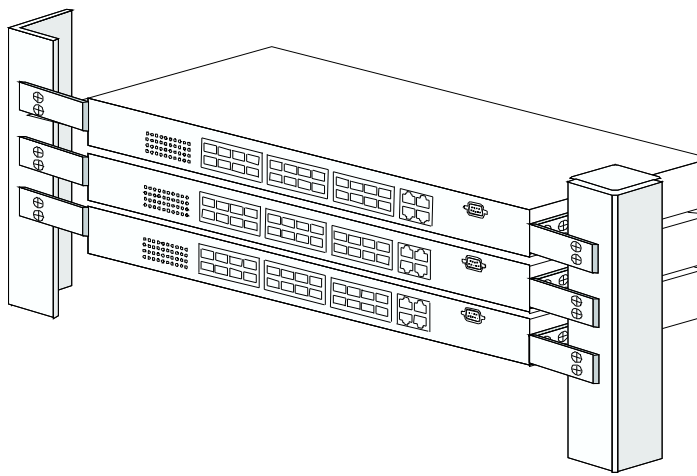
- One Gigabit Management Fiber Optic Switch
- One AC power cord (*for AC power model only)
- One console cable
- Two rack-mount kits and screws
- This user's manual

# 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).

You can install the switch on a 19" rack with rack-mount kits as the picture.

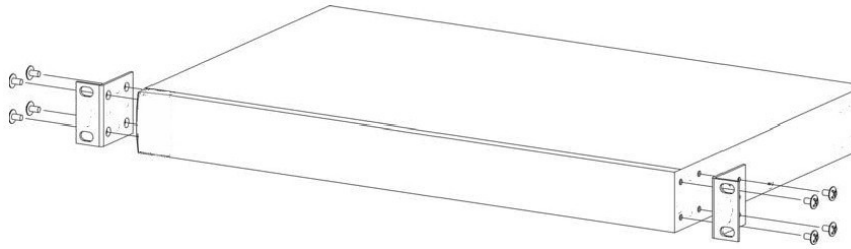


**<< Rack-Mount Installation >>**

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

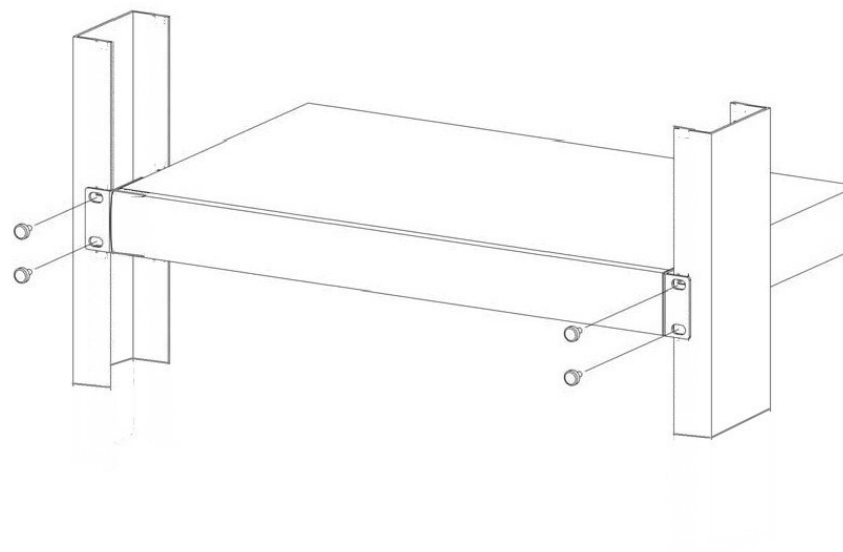
1. **Temperature** - Because the temperature in a rack assembly could be higher than the ambient room temperature, check that the rack-environment temperature is within the specified operating temperature range. (Please refer to Product Specifications in the manual.) Air flow is necessary in a rack for 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.

## << Safety Note for Installation >>

1. The switch shall be operated only in horizontal position.

2. If the switch works in locations, where IT power distribution system is used, double pole fusing is required in building installation.

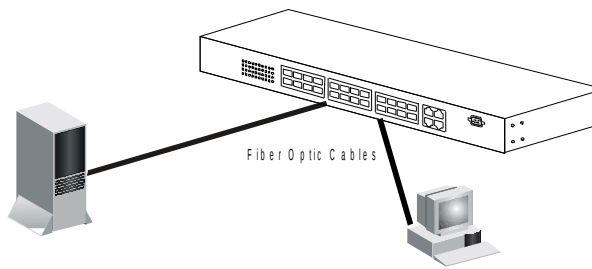
3. A LAN or LAN segment, with all its associated interconnected equipment, shall be entirely contained within a single low-voltage power distribution and within a single building. The LAN is considered to be in an "environment A" according IEEE802.3 or "environment 0" according IEC TR 62102, respectively. Never make direct electrical connection to TNV-circuits (Telephone Network) or WAN (Wide Area Network).

# 3. Configure Network Connection

## 3.1 Connecting Devices to the Switch

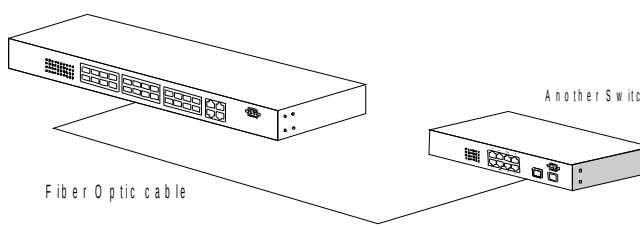
[ Connection Guidelines: ]

- 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
- For 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.



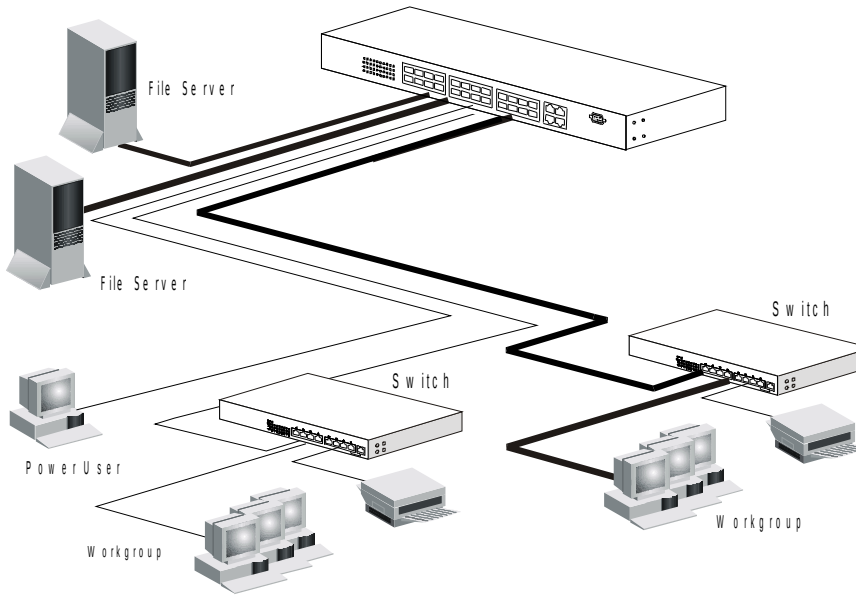

## 3.2 Connecting to Another Ethernet Switch/Hub

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

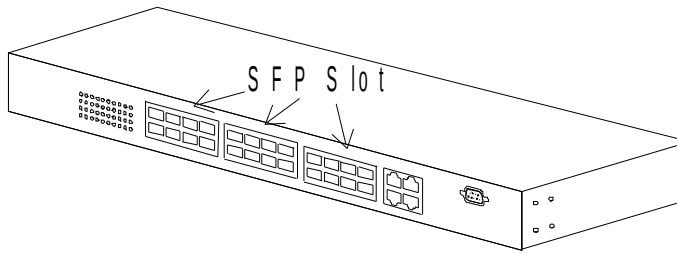
A switch can be used to overcome the hub-to-hub connectivity limitations as well as improve overall network performance. Switches make intelligent decisions about where to send network traffic based on the destination address of the packet. As a result, the switch can significantly reduce unnecessary 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

## 4.1 Adding SFP 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.

## 4.2 Adding DC Power Module

This switch supports AC/DC dual power inputs. The DC power module could be not installed when the switch is shipped. And the DC power module can be installed with the following steps.

1. Power OFF the switch first.
2. Remove the DC power module slot cover at rear side of the switch.
3. Plug in the DC power module.
4. Fix it to switch with screws.
5. Connection AC/DC power to the switch.

If both AC and DC powers are connected to the switch, AC power has higher priority to deliver power to switch. DC power will deliver power to switch when AC power is not available.

# 5. LEDs Conditions Definition

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

[ For 24 GE Model ]

| LED | STATUS | CONDITION |
|---|---|---|
| **Power** | ON | Switch is receiving power. |
| | OFF | Switch is power OFF. |
| **System** | Yellow | System is running power on diagnostic. |
| | Green | System is booting or 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. Management Connection

## 6.1 Console Interface and Command Line Brief

### 6.1.1 Console Interface Connection

**<< 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.

```
--------------------------------------------------------------------------------------------------------
+M25PXX : Init device with JEDEC ID 0xC22018.
Jaguar-1 board detected (VSC7460 Rev. B).

.....
.....
RedBoot> fis load -d managed
Image loaded from 0x80040000-0x809903e4
RedBoot> go

press ENTER to get started
--------------------------------------------------------------------------------------------------------
```

Press <ENTER>, and Username and Password will be asked. "**admin**" / "**admin**" is the default Username and Password for the switch.

### 6.1.2 Command Line Brief

**<< Previlege Levels for Users >>**
There are fifteen previlege levels for users of the switch. 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 15.

**[ user previlege level ]**
The default user name and password is "**admin**" / "**admin**" with previlege level 15. And users with different previlege level could be created with "username"

command under "(config)#". Users with different previlege levels will have different access rights for functions of the switch. Please refer to Privilege Level Configuration of the switch.

**[ command line level ]**
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.

```
---------------------------------------------------------------------------------------------
# ?
   clear       Reset functions
   configure    Enter configuration mode
   copy        Copy from source to destination
   delete      Delete one file in flash: file system
   dir         Directory of all files in flash: file system
   disable      Turn off privileged commands
   do          To run exec commands in config mode
   dot1x       IEEE Standard for port-based Network Access Control
   enable       Turn on privileged commands
   exit        Exit from EXEC mode
   firmware     Firmware upgrade/swap
   help        Description of the interactive help system
   logout      Exit from EXEC mode
   more        Display file
   no          Negate a command or set its defaults
   ping        Send ICMP echo messages
   reload      Reload system.
   send        Send a message to other tty lines
   show        Show running system information
   terminal    Set terminal line parameters
#
---------------------------------------------------------------------------------------------
```

These are the basic system commands for the switch.

For system configuring, "**configure terminal**" 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 GigabitEthernet 1/5
(config-if)#
-------------------------------------------------------------------
```

"GigabitEthernet 1/5" means Gigabit 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-vlan)#
-------------------------------------------------------------------
```

**<< 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 "**#**".

2. **Configure Mode Commands**
   With "configure terminal" 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 GigabitEthernet 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-vlan)#**". 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 x" command in configure mode. And its prompt will become "**(config-vlan)#**".

**<< Save Configuration >>**
Remember to do save after configuration is done with the following command.
# copy running-config startup-config

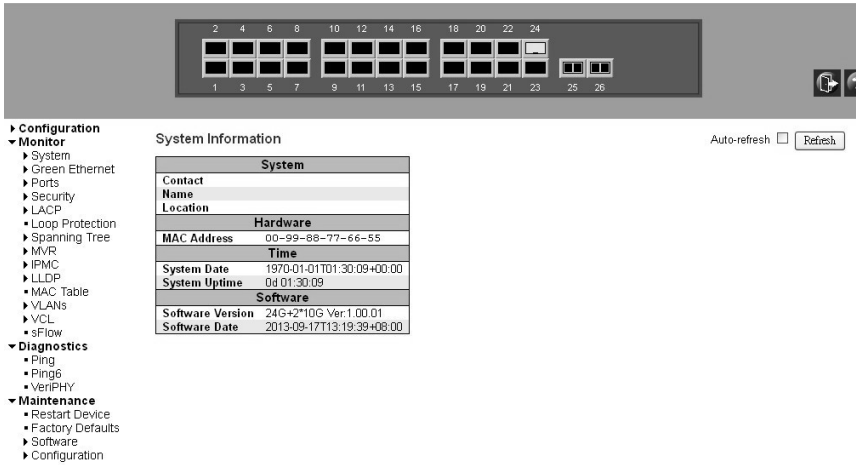
## 6.2 Web, Telnet, and SNMP Interfaces

### 6.2.1 Web Interface 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 6.1 to complete the console connection.
2 Login in with "**admin**" (password is also "**admin**" by default.)
3 Use "**show ip interface brief**" 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-vlan)#".
  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 route xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy zzz.zzz.zzz.zzz**" command to create a IP route entry. **xxx.xxx.xxx.xxx** is the the destination IP network or host address of this route. **yyy.yyy.yyy.yyy** is the destination IP network or host mask. **zzz.zzz.zzz.zzz** is the IP address of Gateway.
  4.6 Enter "**exit**" command to go back to "#" prompt.
  4.7 Enter "**show ip interface brief**" to check the IP settings.
  4.8 Enter "**copy running-config startup-config**" to save it.

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.

## 6.2.2 Telnet and SNMP Interface Connection

**<< 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. (Refer to Section 6.2.1.) Then use "telnet <IP>" command to connect to the switch. Its operation

interface is the same as console interface.

**<< 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 (Refer to Section 6.2.1.), 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”.

# 7. Function Configuration

## 7.1 Function Brief

The switch supports lots of network management functions. Here are the brief of these functions.

1. **System**
   a. Name, Contact, Location, Mac ID, Firmware version, Up time
   b. IP Configuration
   c. Time configuration
   d. Log configuration

2. **Port**
   a. Speed, duplex, status, flow control, maximum packet size

3. **DHCP**
   a. DHCP Snooping
   b. DHCP Relay

4. **Security**
   a. Security for Switch Management
      a). Switch administrator and privilege level configuration
      b). Authentication method for console, telnet, ssh, http interfaces
      c). Switch management access limitation
      d). SSH, HTTPS configuration
      e). SNMP configuration
      f). RMON configuration
   b. Security for Network Access
      a). Network connection number limit on port
      b). 802.1x network access configuration
      c). ACL configuration
      d). DHCP snooping and reply configuration
      e). IP source guard configuration
      f). ARP inspection configuration
   c. AAA
      a). RADIUS and TACACS+ servers configuration

5. **Aggregation**
   a. Static trunk configuration
   b. LACP configuration

6. **Loop protection**
   a. Loop protection configuration

7. **Spanning Tree**
   a. Spanning tree configuration

**8. IP Multicast**
   a. IP multicast profile
   b. IGMP snooping configuration
   c. MLD snooping configuration
   d. MVR

**9. LLDP**
   a. LLDP configuration

**10. Mac Table**
   a. Aging time, learning, secure settings.
   b. Static Mac ID assignment

**11. VLAN**
   a. 802.1Q VLAN configuration
   b. Private VLAN configuration
   c. Port isolation configuration
   d. Mac-based, Protocol-based, IP Subnet-based VLAN configuration
   e. Voice VLAN configuration
   f. GVRP configuration

**12. QoS**
   a. Port default QoS configuration
   b. Port ingress policing and egress shaping configuration
   c. Egress scheduling configuration
   d. Egress tag remarking
   e. DSCP QoS, translation, classification configuration
   f. Storm control configuration
   g. WRED configuration

**13. Mirroring**
   a. Port Mirroring configuration

**14. sFlow**
   a. sFlow configuration

**15. Diagnostics**
   a. Ping function
   b. VeriPHY function

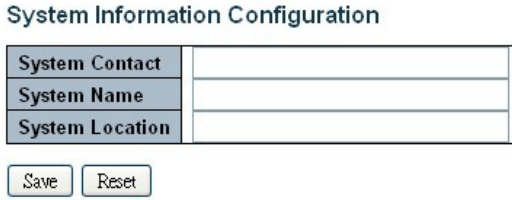
**16. Maintenance**
   a. Restart switch
   b. Restore factory default
   c. Software update
   d. Configuration upload/restore

## 7.2 System Configuration

This function covers the following items for switch setup.

**1. Name, Contact, Location, Mac ID, Firmware version, Up time**

*Configuration by Web* :
[Configuration] -> [System] -> [Information]



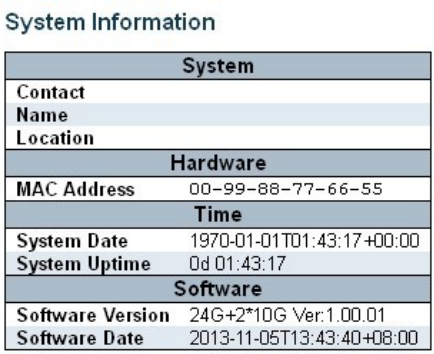

Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
System Name :
(config)# hostname <word32>
(config)# no hostname

System Contact :
(config)# snmp-server contact <line255>
(config)# no snmp-server contact

System Location :
(config)# snmp-server location <line255>
(config)# no snmp-server location

*Status by Web* :
[Monitor] -> [System] -> [Information]




Click "**?**" at this web page to get details of the settings.

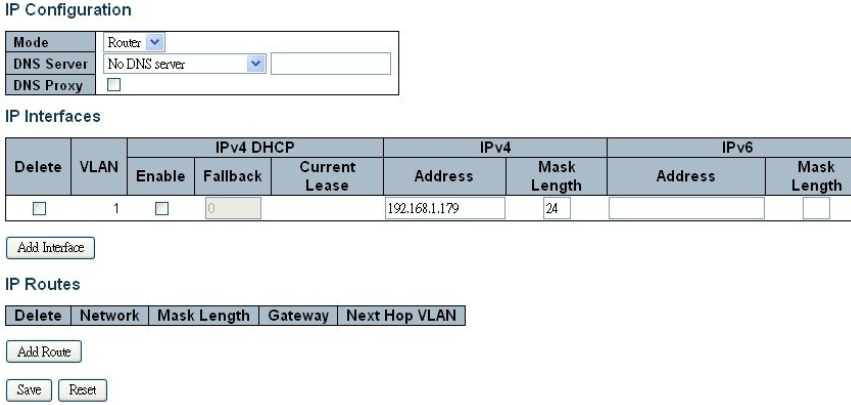
*Status by Command* :

# show version

## 2. IP configuration

This switch supports L3 routing function. It could be enabled at “Mode” setting. In Host mode, IP traffic between interfaces will not be routed. In Router mode traffic is routed between all interfaces.
Gateway of the IP configuration is set at “IP Route”.

*Configuration by Web* :
[Configuration] -> [System] -> [IP]




Click “**?**” at this web page to get details of the settings.

*Configuration by Command* :
IPv4 Address :
(config-if-vlan)# ip address { { <ipv4_addr> <ipv4_netmask> } | { dhcp [ fallback <ipv4_addr> <ipv4_netmask> [ timeout <uint> ] ] } }
For example, (config-if-vlan)# ip address 192.168.1.179 255.255.255.0
(config-if-vlan)# no ip address

IPv6 Address :
(config-if-vlan)# ipv6 address <ipv6_subnet>
For example, (config-if-vlan)# ipv6 address 1221::215:c5ff:fe03:4dc7/126
(config-if-vlan)# no ipv6 address [ <ipv6_subnet> ]

IPv4 and IPv6 Routing :
(config)# ip routing
(config)# no ip routing

DNS Proxy :
(config)# ip dns proxy
(config)# no ip dns proxy

Static Route Entry and Gateway :

(config)# ip route <destination_ip_addr> <netmask> <gateway_ip_addr>
(config)# no ip route <destination_ip_addr> <netmask> <gateway_ip_addr>

*Status by Web* :
[Monitor] -> [System] -> [IP Status]

IP Interfaces

| Interface | Type | Address | Status |
|---|---|---|---|
| OS:lo | LINK | 00-00-00-00-00-00 | <UP LOOPBACK RUNNING MULTICAST> |
| OS:lo | IPv4 | 127.0.0.1/8 | |
| OS:lo | IPv6 | fe80:1::1/64 | |
| OS:lo | IPv6 | ::1/128 | |
| VLAN1 | LINK | 00-99-88-77-66-55 | <UP BROADCAST RUNNING MULTICAST> |
| VLAN1 | IPv4 | 192.168.1.179/24 | |
| VLAN1 | IPv6 | fe80:2::299:88ff:fe77:6655/64 | |

IP Routes

| Network | Gateway | Status |
|---|---|---|
| 127.0.0.1/32 | 127.0.0.1 | <UP HOST> |
| 192.168.1.0/24 | VLAN1 | <UP HW_RT> |
| 224.0.0.0/4 | 127.0.0.1 | <UP> |
| ::1/128 | ::1 | <UP HOST> |

Neighbour cache

| IP Address | Link Address |
|---|---|
| 192.168.1.93 | VLAN1:00-0f-fe-11-89-1b |
| fe80:2::299:88ff:fe77:6655 | VLAN1:00-99-88-77-66-55 |

Click "**?**" at this web page to get details of the settings.

*Status by Command* :
Show IP Address :
# show ip interface brief
# show ipv6 interface [ vlan <vlan_list> { brief | statistics } ]

Show IP Routing Table :
# show ip route
# show ipv6 route [ interface vlan <vlan_list> ]

### 3. Time configuration

This switch can get time from NTP server, and supports Time Zone and Daylight Saving setting.

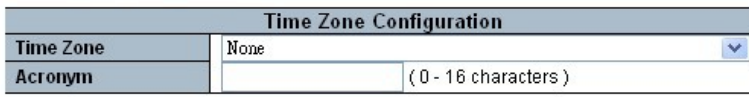
*Configuration by Web* :
[Configuration] -> [System] -> [NTP]

NTP Configuration

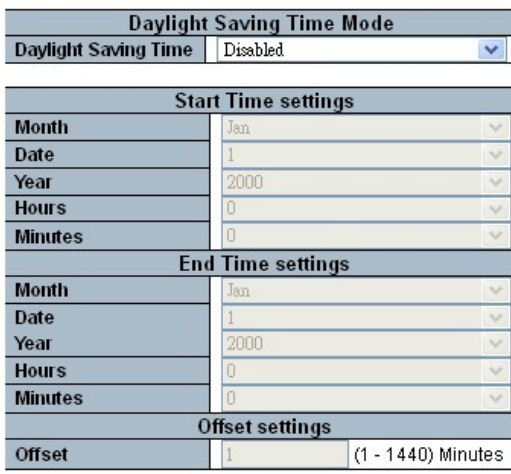

Click "**?**" at this web page to get details of the settings.

[Configuration] -> [System] -> [Time]

Time Zone Configuration




Daylight Saving Time Configuration




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
NTP :
(config)# ntp enable
(config)# ntp server <1-5> ip-address { <ipv4_ucast> | <ipv6_ucast> | <hostname> }
(config)# no ntp enable
(config)# no ntp server <1-5>

Daylight Saving Time :
(config)# clock summer-time <word16> date [ <1-12> <1-31> <2000-2097> <hhmm> <1-12> <1-31> <2000-2097> <hhmm> [ <1-1440> ] ]
(config)# clock summer-time <word16> recurring [ <1-5> <1-7> <1-12> <hhmm> <1-5> <1-7> <1-12> <hhmm> [ <1-1440> ] ]
(config)# no clock summer-time

Time Zone :
(config)# clock timezone <word16> <-23-23> [ <0-59> ]
(config)# no clock timezone

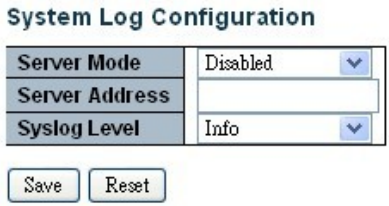
*Status by Web* :
[Configuration] -> [System] -> [NTP]
[Configuration] -> [System] -> [Time]
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show clock
# show clock detail

### 4. Log configuration

This switch can records event logs in local flash and syslog server.

*Configuration by Web* :
[Configuration] -> [System] -> [Log]




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Log Configuration :
(config)# logging host { <ipv4_ucast> | <hostname> }
(config)# logging level { info | warning | error }
(config)# logging on
(config)# no logging host
(config)# no logging on

*Status by Web* :
[Monitor] -> [System] -> [Log]

**System Log Information**

| | |
|---|---|
| Level | All |
| Clear Level | All |

The total number of entries is 4 for the given level.

Start from ID 1 with 20 entries per page.

| ID | Level | Time | Message |
|---|---|---|---|
| 1 | Info | 1970-01-01T00:00:05+00:00 | Switch just made a cold boot. |
| 2 | Info | 1970-01-01T00:00:07+00:00 | Link up on port 21 |
| 3 | Info | 1970-01-01T00:00:08+00:00 | Link down on port 21 |
| 4 | Info | 1970-01-01T00:00:10+00:00 | Link up on port 21 |

Click "**?**" at this web page to get details of the settings.

[Monitor] -> [System] -> [Detailed Log]

**Detailed System Log Information**

| | |
|---|---|
| ID | 1 |

**Message**

| | |
|---|---|
| Level | Info |
| Time | 1970-01-01T00:00:05+00:00 |
| Message | Switch just made a cold boot. |

Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show logging
# show logging <1-4294967295>
# show logging [ info ] [ warning ] [ error ]

# 7.3 Port Configuration

This function covers the following items for port setup.

## 1. Speed, Duplex, Status, Flow control, Maximum packet size

*Configuration by Web*:

[Configuration] -> [Ports]

**Port Configuration**

| Port | Link | Speed | | Flow Control | | | Maximum Frame Size | Excessive Collision Mode |
|---|---|---|---|---|---|---|---|---|
| | | Current | Configured | Current Rx | Current Tx | Configured | | |
| * | | | <> | | | ☐ | 10056 | <> |
| 1 | Down | Down | Auto | | | | 10056 | |
| 2 | Down | Down | Auto | | | | 10056 | |
| 3 | Down | Down | Auto | | | | 10056 | |
| 4 | Down | Down | Auto | | | | 10056 | |
| 5 | Down | Down | Auto | | | | 10056 | |
| 6 | Down | Down | Auto | | | | 10056 | |
| 7 | Down | Down | Auto | | | | 10056 | |
| 8 | Down | Down | Auto | | | | 10056 | |
| 9 | Down | Down | Auto | | | | 10056 | |
| 10 | Down | Down | Auto | | | | 10056 | |
| 11 | Down | Down | Auto | | | | 10056 | |
| 12 | Down | Down | Auto | | | | 10056 | |
| 13 | Down | Down | Auto | | | | 10056 | |
| 14 | Down | Down | Auto | | | | 10056 | |
| 15 | Down | Down | Auto | | | | 10056 | |
| 16 | Down | Down | Auto | | | | 10056 | |
| 17 | Down | Down | Auto | | | | 10056 | |
| 18 | Down | Down | Auto | | | | 10056 | |
| 19 | Down | Down | Auto | | | | 10056 | |
| 20 | Down | Down | Auto | | | | 10056 | |
| 21 | Down | Down | SFP_Auto_AMS | ✗ | ✗ | ☐ | 10056 | Discard |
| 22 | Down | Down | SFP_Auto_AMS | ✗ | ✗ | ☐ | 10056 | Discard |
| 23 | Down | Down | SFP_Auto_AMS | ✗ | ✗ | ☐ | 10056 | Discard |
| 24 | 100fdx | 100fdx | SFP_Auto_AMS | ✗ | ✗ | ☐ | 10056 | Discard |

Save Reset

Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :

Apply the following command for configured ports first. And the prompt will become "(config-if)# ".

For single port :
(config)# interface GigabitEthernet 1/x

For several ports :
(config)# interface GigabitEthernet 1/x,y,z

For a range of ports :
(config)# interface GigabitEthernet 1/x-y

Speed :
(config-if)# speed { 1000 | 100 | 10 | auto { [ 10 ] [ 100 ] [ 1000 ] } }
(config-if)# no speed

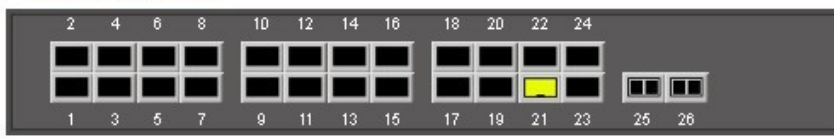
Duplex :
(config-if)# duplex { half | full | auto [ half | full ] }
(config-if)# no duplex

Flow Control :
(config-if)# flowcontrol { on | off }
(config-if)# no flowcontrol

Maximum Frame Size :
(config-if)# mtu <1518-10056>
(config-if)# no mtu

*Status by Web* :
[Configuration] -> [Ports]
[Monitor] -> [Ports] -> [State]

Port State Overview




Click "**?**" at this web page to get details of the settings.

[Monitor] -> [Ports] -> [Traffic Overview]

Port Statistics Overview

Auto-refr

| Port | Packets | | Bytes | | Errors | | Drops | | Filtered |
|---|---|---|---|---|---|---|---|---|---|
| | Received | Transmitted | Received | Transmitted | Received | Transmitted | Received | Transmitted | Received |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 13 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 14 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 15 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 17 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 18 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 19 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 20 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 21 | 19204 | 9721 | 3061121 | 6382799 | 159 | 0 | 2706 | 0 | 2706 |
| 22 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 23 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 24 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 25 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 26 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Click "**?**" at this web page to get details of the settings.

*Status by Command* :
SFP DDMI :

# show interface { GigabitEthernet } <port_list> capabilities

Link Status:
# show interface { GigabitEthernet } <port_list> status

Statistics:
# show interface { GigabitEthernet } <port_list> statistics [ { packets | bytes | errors | discards | filtered | { priority [<0~7> ] } } ] [{ up | down } ]
# clear statistics { GigabitEthernet} <port_list>

## 7.4 DHCP

This function covers the following items for DHCP functions setup.

**1. DHCP Snooping**

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.

*Configuration by Web* :
Enable/Disable, VLAN Range :
[Configuration] -> [DHCP] -> [Snooping]



Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Enable/Disable :

(config)# ip dhcp snooping
(config)# no ip dhcp snooping

Port Setting :
(config-if)# ip dhcp snooping trust
(config-if)# no ip dhcp snooping trust

*Status by Web* :
[Monitor] -> [DHCP] -> [Snooping Table]


Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# clear ip dhcp snooping statistics [ interface <port_type_list> ]
# show ip dhcp snooping [ table | interface <port_type_list> ]

**2. DHCP Relay**

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.

*Configuration by Web* :
Enable/Disable, VLAN Range :
[Configuration] -> [DHCP] -> [Relay]

DHCP Relay Configuration

| | |
|---|---|
| Relay Mode | Disabled |
| Relay Server | 0.0.0.0 |
| Relay Information Mode | Disabled |
| Relay Information Policy | Keep |

Save Reset

Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Enable/Disable :
(config)# ip dhcp relay
(config)# no ip dhcp relay

(config)# ip dhcp relay information option
(config)# no ip dhcp relay information option

(config)# ip dhcp relay information policy { drop | keep | replace }
(config)# no ip dhcp relay information policy

DHCP Relay Server :
(config)# ip helper-address <ipv4_ucast>
(config)# no ip helper-address

*Status by Web* :
[Monitor] -> [DHCP] -> [Relay Statistics]

DHCP Relay Statistics

Auto-refresh Refresh

Server Statistics

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

Client Statistics

| Transmit to Client | Transmit Error | Receive from Client | Receive Agent Option | Replace Agent Option | Keep Agent Option | Drop Agent Option |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# clear ip dhcp relay statistics
# show ip dhcp relay [ statistics ]

## 7.5 Security Configuration

This function covers the following items for security setup.

### 7.5.1 Security for Switch Management

**1. Administrator and Privilege level configuration**

About the privilege level of the user...

The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

*Configuration by Web* :

Create User :

[Configuration] -> [Security] -> [Switch] -> [Users]


Click "**?**" at this web page to get details of the settings.

Privilege Levels :

[Configuration] -> [Security] -> [Switch] -> [Privilege Levels]

**Privilege Level Configuration**

| Group Name | Privilege Levels | | | |
|---|---|---|---|---|
| | Configuration Read-only | Configuration/Execute Read/write | Status/Statistics Read-only | Status/Statistics Read/write |
| Aggregation | 5 | 10 | 5 | 10 |
| DHCP | 5 | 10 | 5 | 10 |
| Dhcp_Client | 5 | 10 | 5 | 10 |
| Diagnostics | 5 | 10 | 5 | 10 |
| IP2 | 5 | 10 | 5 | 10 |
| IPMC_Snooping | 5 | 10 | 5 | 10 |
| LACP | 5 | 10 | 5 | 10 |
| LLDP | 5 | 10 | 5 | 10 |
| Loop_Protect | 5 | 10 | 5 | 10 |
| MAC_Table | 5 | 10 | 5 | 10 |
| Maintenance | 15 | 15 | 15 | 15 |
| Mirroring | 5 | 10 | 5 | 10 |
| MVR | 5 | 10 | 5 | 10 |
| NTP | 5 | 10 | 5 | 10 |
| Ports | 5 | 10 | 1 | 10 |
| Private_VLANs | 5 | 10 | 5 | 10 |
| QoS | 5 | 10 | 5 | 10 |
| RPC | 5 | 10 | 5 | 10 |
| Security | 5 | 10 | 5 | 10 |
| sFlow | 5 | 10 | 5 | 10 |
| Spanning_Tree | 5 | 10 | 5 | 10 |

Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Create User :
(config)# username <word31> privilege <0-15> password encrypted <word4-44>
(config)# username <word31> privilege <0-15> password none
(config)# username <word31> privilege <0-15> password unencrypted <line31>
(config)# no username <word31>

Privilege Levels :
(config)# web privilege group <cword> level { [ cro <0-15> ] [ crw <0-15> ] [ sro <0-15> ] [ srw <0-15> ] }
Note 1 : <cword> : Function Name
Note 2 : cro : Configuration Read-only
crw : Configuration/Execute Read/write
sro : Status/Statistics Read-only
srw : Status/Statistics Read/write
(config)# no web privilege group [ <cword> ] level

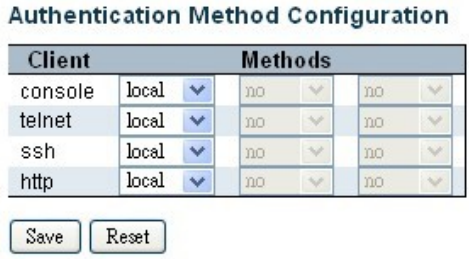
*Status by Web* :
User :
[Configuration] -> [Security] -> [Switch] -> [Users]
Click "**?**" at this web page to get details of the settings.

Privilege Levels :
[Configuration] -> [Security] -> [Switch] -> [Privilege Levels]
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show users
# show web privilege group [ <cword> ] level

**2. Authentication method for Console, Telnet, SSH, Http interfaces**
This function allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces.

*Configuration by Web* :
[Configuration] -> [Security] -> [Switch] -> [Auth Method]




Click "**?**" at this web page to get details of the settings.

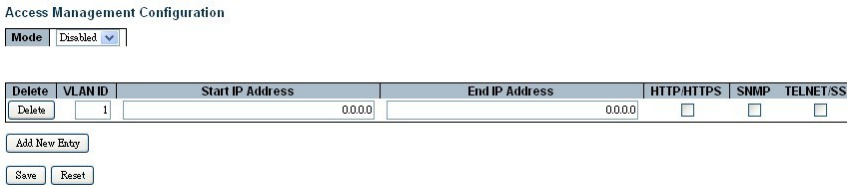
*Configuration by Command* :
(config)# aaa authentication login { console | telnet | ssh | http } { [ local | radius | tacacs ] ... }
(config)# no aaa authentication login { console | telnet | ssh | http }

*Status by Web* :
[Configuration] -> [Security] -> [Switch] -> [Auth Method]
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show aaa

**3. Switch Management Access Limit**
This function can limit the switch management source interfaces.

*Configuration by Web* :
[Configuration] -> [Security] -> [Switch] -> [Access Management]




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
(config)# access management
(config)# access management <1-16> <1-4094> <ipv4_addr> [ to <ipv4_addr> ] { [ web ] [ snmp ] [ telnet ] | all }
(config)# no access management
(config)# no access management <1~16>

*Status by Web* :
[Configuration] -> [Security] -> [Switch] -> [Access Management]
Click "**?**" at this web page to get details of the settings.

[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 |

Click "**?**" at this web page to get details of the settings.

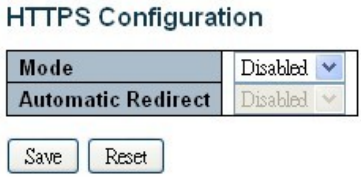
*Status by Command* :
# show access management [ statistics | <1~16> ]
# clear access management statistics

**4. SSH, HTTPS configuration**
This function is used to enabled/disable SSH and HTTPS security functions.

*Configuration by Web* :
SSH :
[Configuration] -> [Security] -> [Switch] -> [SSH]


Click "**?**" at this web page to get details of the settings.

HTTPS :
[Configuration] -> [Security] -> [Switch] -> [HTTPS]




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
SSH :
(config)# ip ssh
(config)# no ip ssh

HTTPS :
(config)# ip http secure-redirect
(config)# ip http secure-server
(config)# no ip http secure-redirect
(config)# no ip http secure-server

*Status by Web* :
SSH :
[Configuration] -> [Security] -> [Switch] -> [SSH]
Click "**?**" at this web page to get details of the settings.

HTTPS :
[Configuration] -> [Security] -> [Switch] -> [HTTPS]
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
SSH :
# show ip ssh

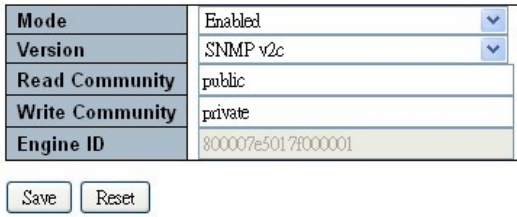
HTTPS :
# show ip http server secure status

## 5. SNMP configuration

SNMP is an acronym for Simple Network Management Protocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

*Configuration by Web* :
[Configuration] -> [Security] -> [Switch] -> [SNMP] -> [System]

SNMP System Configuration

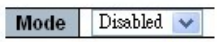



Click "**?**" at the web page to get details of the settings.

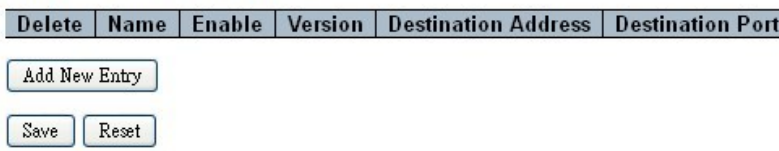
[Configuration] -> [Security] -> [Switch] -> [SNMP] -> [Trap]

Trap Configuration

Global Settings




Trap Destination Configurations




Click [Add New Entry]. The following page will appear.

**SNMP Trap Configuration**

| | |
|---|---|
| Trap Config Name | |
| Trap Mode | Disabled |
| Trap Version | SNMP v2c |
| Trap Community | Public |
| Trap Destination Address | |
| Trap Destination Port | 162 |
| Trap Inform Mode | Disabled |
| Trap Inform Timeout (seconds) | 3 |
| Trap Inform Retry Times | 5 |
| Trap Probe Security Engine ID | Enabled |
| Trap Security Engine ID | |
| Trap Security Name | None |

**SNMP Trap Event**

| | |
|---|---|
| System | * Warm Start  Cold Start |
| Interface | Link up none specific all switches<br>*Link down none specific all switches<br>LLDP none specific all switches |
| AAA | * Authentication Fail |
| Switch | * STP  RMON |

Click "**?**" at the web page to get details of the settings.

[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 |

Add New Entry  Save  Reset

Click "**?**" at the web page to get details of the settings.

[Configuration] -> [Security] -> [Switch] -> [SNMP] -> [Users]

**SNMPv3 User Configuration**

| Delete | Engine ID | User Name | Security Level | Authentication Protocol | Authentication Password | Privacy Protocol | Privacy Password |
|---|---|---|---|---|---|---|---|
| Delete | | | Auth, Priv | MD5 | | DES | |

Add New Entry  Save  Reset

Click "**?**" at the web page to get details of the settings.

[Configuration] -> [Security] -> [Switch] -> [SNMP] -> [Groups]

**SNMPv3 Group Configuration**

| Delete | Security Model | Security Name | Group Name |
|---|---|---|---|
| ☐ | v1 | public | default_ro_group |
| ☐ | v1 | private | default_rw_group |
| ☐ | v2c | public | default_ro_group |
| ☐ | v2c | private | default_rw_group |
| ☐ | usm | default_user | default_rw_group |

Add New Entry | Save | Reset

Click "**?**" at the web page to get details of the settings.

[Configuration] -> [Security] -> [Switch] -> [SNMP] -> [Views]

**SNMPv3 View Configuration**

| Delete | View Name | View Type | OID Subtree |
|---|---|---|---|
| ☐ | default_view | included | .1 |

Add New Entry | Save | Reset

Click "**?**" at the web page to get details of the settings.

[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

Click "**?**" at the web page to get details of the settings.

*Configuration by Command* :
Enable/Disable :
(config)# snmp-server
(config)# no snmp-server

Version :
(config)# snmp-server version { v1 | v2c | v3 }
(config)# no snmp-server version

Community :
(config)# snmp-server community v2c <word127> [ ro | rw ]
(config)# snmp-server community v3 <word127> [ <ipv4_addr> <ipv4_netmask> ]
(config)# no snmp-server community v2c
(config)# no snmp-server community v3 <word127>

Engine ID :
(config)# snmp-server engine-id local <word10-32>
(config)# no snmp-server engined-id local

System Information :
(config)# snmp-server host <word32>
(config)# snmp-server contact <line255>
(config)# snmp-server location <line255>
(config)# no snmp-server host <word32>
(config)# no snmp-server contact
(config)# no snmp-server location

Trap :
(config)# snmp-server trap
(config)# no snmp-server trap
(config)# snmp-server host <word32> traps [ linkup ] [ linkdown ] [ lldp ]
no snmp-server host <word32> traps

Users (v3) :
(config)# snmp-server user <word32> engine-id <word10-32> [ { md5 <word8-32> | sha <word8-40> } [ priv { des | aes } <word8-32> ] ]
(config)# no snmp-server user <word32> engine-id <word10-32>

Groups (v3) :
(config)# snmp-server security-to-group model { v1 | v2c | v3 } name <word32> group <word32>
(config)# no snmp-server security-to-group model { v1 | v2c | v3 } name <word32>

Views (v3) :
(config)# snmp-server view <word32> <word255> { include | exclude }
(config)# no snmp-server view <word32> <word255>

Access (v3) :
(config)# snmp-server access <word32> model { v1 | v2c | v3 | any } level { auth | noauth | priv } [ read <word255> ] [ write <word255> ]
(config)# no snmp-server access <word32> model { v1 | v2c | v3 | any } level { auth | noauth | priv }

*Status by Web* :
[Configuration] -> [Security] -> [Switch] -> [SNMP] -> [System]
[Configuration] -> [Security] -> [Switch] -> [SNMP] -> [Trap]
[Configuration] -> [Security] -> [Switch] -> [SNMP] -> [Communities]
[Configuration] -> [Security] -> [Switch] -> [SNMP] -> [Users]
[Configuration] -> [Security] -> [Switch] -> [SNMP] -> [Groups]
[Configuration] -> [Security] -> [Switch] -> [SNMP] -> [Views]
[Configuration] -> [Security] -> [Switch] -> [SNMP] -> [Access]
Click "**?**" at the web page to get details of the settings.

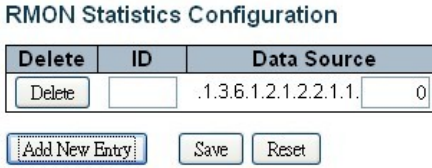
*Status by Command* :

# show snmp
# show snmp access [ <word32> { v1 | v2c | v3 | any } { auth | noauth | priv } ]
# show snmp community v3 [ <word127> ]
# show snmp host [ <word32> ] [ system ] [ switch ] [ interface ] [ aaa ]
# show snmp security-to-group [ { v1 | v2c | v3 } <word32> ]
# show snmp user [ <word32> <word10-32> ]
# show snmp view [ <word32> <word255> ]

## 6. RMON configuration

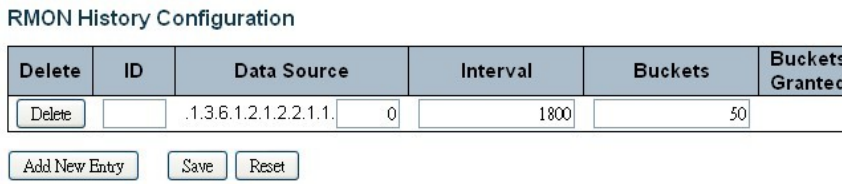
RMON (Remote Network Monitoring) provides standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of distributed local area networks (LANs) from a central site.
RMON specifically defines the information that any network monitoring system will be able to provide.
RMON can be supported by monitoring devices (known as "probes"), e.g. LAN switches includes software in each switch that can trap information as traffic flows through and record it in its MIB. A software agent can gather the information for presentation to the network administrator with a graphical user interface.

*Configuration by Web* :
[Configuration] -> [Security] -> [Switch] -> [RMON] -> [Statistics]



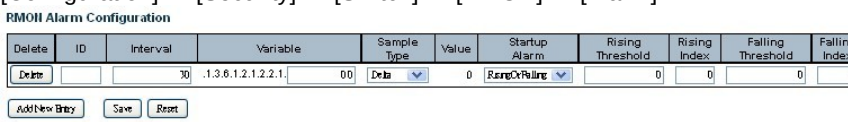

Click "**?**" at the web page to get details of the settings.

[Configuration] -> [Security] -> [Switch] -> [RMON] -> [History]



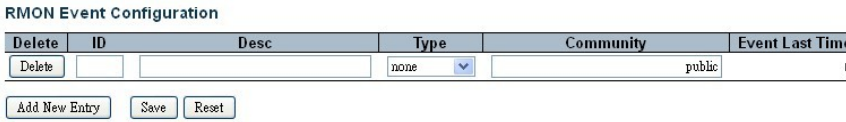

Click "**?**" at the web page to get details of the settings.

[Configuration] -> [Security] -> [Switch] -> [RMON] -> [Alarm]




Click "**?**" at the web page to get details of the settings.

[Configuration] -> [Security] -> [Switch] -> [RMON] -> [Event]




Click "**?**" at the web page to get details of the settings.

*Configuration by Command* :
Create an Alarm Entry :
(config)# rmon alarm <1-65535> <word255> <1-2147483647> { absolute | delta } rising-threshold <-2147483648-2147483647> [ <0-65535> ] falling-threshold <-2147483648-2147483647> [ <0-65535> ] { [ rising | falling | both ] }
(config)# no rmon alarm <1-65535>

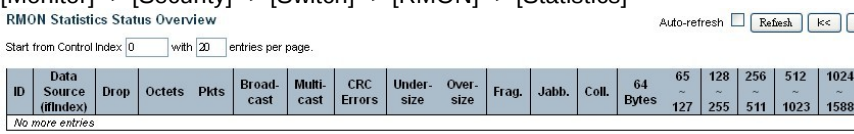
Configure Threshold for Variables :
(config)# rmon alarm <1-65535> { ifInOctets | ifInUcastPkts | ifInNUcastPkts | ifInDiscards | ifInErrors | ifInUnknownProtos | ifOutOctets | ifOutUcastPkts | ifOutNUcastPkts | ifOutDiscards | ifOutErrors } <uint> <1-2147483647> { absolute | delta } rising-threshold <-2147483648-2147483647> [ <0-65535> ] falling-threshold <-2147483648-2147483647> [ <0-65535> ] { [ rising | falling | both ] }
(config)# no rmon alarm <1-65535>

Create a History Entry :
(config)# rmon collection history <1-65535> [ buckets <1-65535> ] [ interval <1-3600> ]
(config)# no rmon collection history <1-65535>

Create a Statistics Entry :
(config)# rmon collection stats <1-65535>
(config)# no rmon collection stats <1-65535>

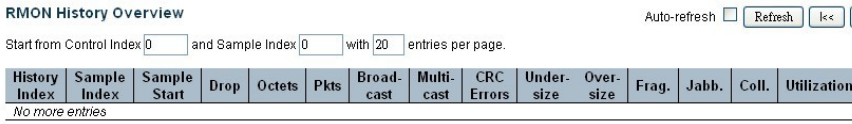
Create an Event Entry :
(config)# rmon event <1-65535> [ log ] [ trap <word127> ] { [ description <line127> ] }
(config)# no rmon event <1-65535>

*Status by Web* :
[Configuration] -> [Security] -> [Switch] -> [RMON] -> [Statistics]
[Configuration] -> [Security] -> [Switch] -> [RMON] -> [History]
[Configuration] -> [Security] -> [Switch] -> [RMON] -> [Alarm]
[Configuration] -> [Security] -> [Switch] -> [RMON] -> [Event]
[Monitor] -> [Security] -> [Switch] -> [RMON] -> [Statistics]



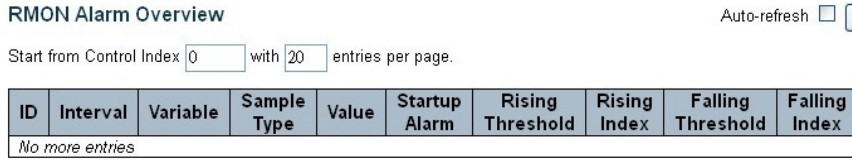
Click “**?**” at the web page to get details of the settings.

[Monitor] -> [Security] -> [Switch] -> [RMON] -> [History]



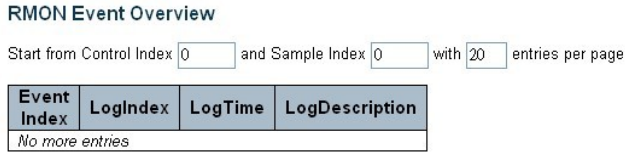

Click “**?**” at the web page to get details of the settings.

[Monitor] -> [Security] -> [Switch] -> [RMON] -> [Alarm]




Click “**?**” at the web page to get details of the settings.

[Monitor] -> [Security] -> [Switch] -> [RMON] -> [Event]




Click “**?**” at the web page to get details of the settings.

*Status by Command* :
# show rmon alarm [ <1~65535> ]
# show rmon event [ <1~65535> ]
# show rmon history [ <1~65535> ]
# show rmon statistics [ <1~65535> ]

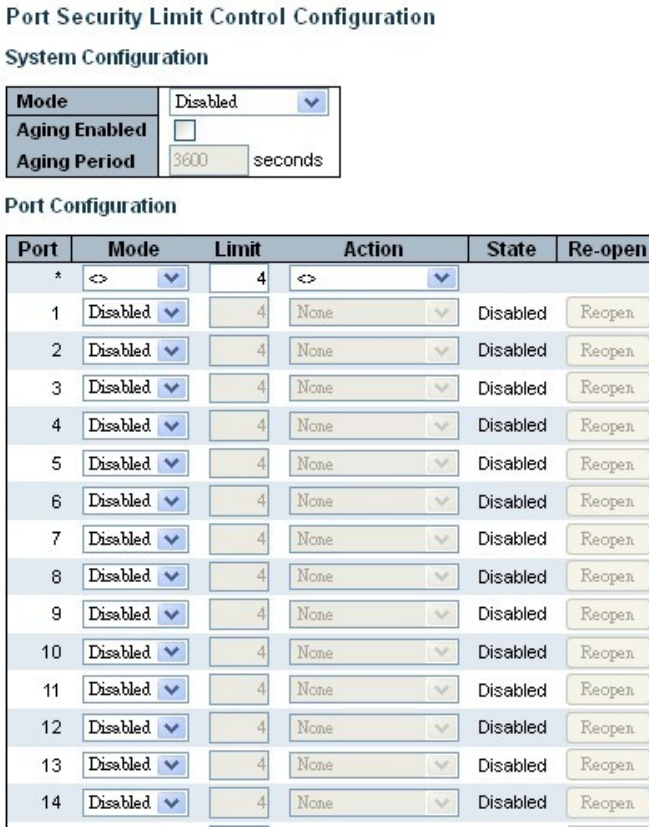
### 7.5.2 Security for Network Management

**1. Mac ID Number Limit Control on Port configuration**

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.

*Configuration by Web* :

[Configuration] -> [Security] -> [Network] -> [Limit Control]




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :

Enable/Disable :

(config)# port-security

(config)# no port-security

Aging :

(config)# port-security aging
(config)# port-security aging time <10-10000000>
(config)# no port-security aging
(config)# no port-security aging time

Enable/Disable by Port :
(config-if)# port-security
(config-if)# no port-security

Control Number and Action by Port :
(config-if)# port-security maximum [ <1-1024> ]
(config-if)# port-security violation { protect | trap | trap-shutdown | shutdown }
(config-if)# no port-security maximum
(config-if)# no port-security violation

*Status by Web* :
[Configuration] -> [Security] -> [Network] -> [Limit Control]
[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 | - | - |
| 11 | ---- | Disabled | - | - |
| 12 | ---- | Disabled | - | - |
| 13 | ---- | Disabled | - | - |
| 14 | ---- | Disabled | - | - |

Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show port-security switch [ interface <port_type_list> ]

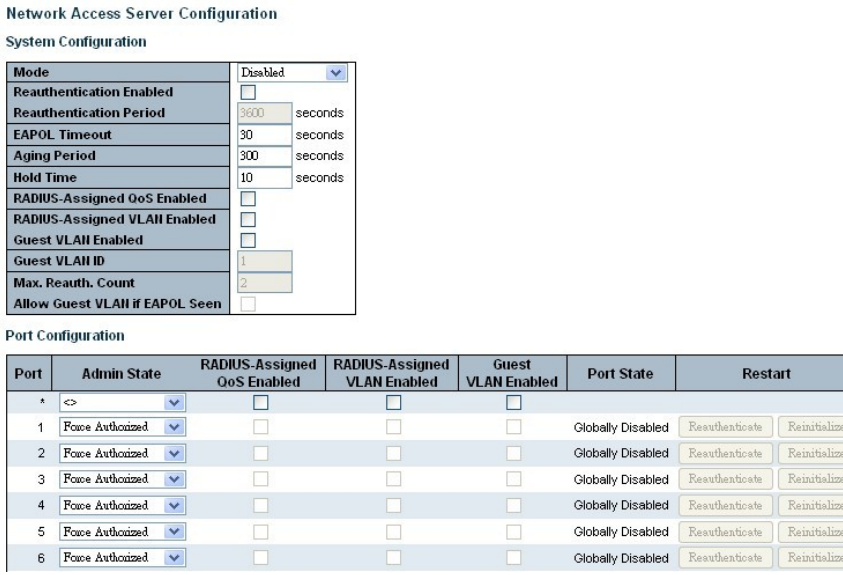
**2. 802.1x Network Access configuration**

The IEEE 802.1X standard defines a port-based access control procedure that

prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the "Configuration→Security→AAA" page. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.

MAC-based authentication allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X supplicant software installed on his system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication.

*Configuration by Web* :
[Configuration] -> [Security] -> [Network] -> [NAS]




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Enable/Disable :
(config)# dot1x system-auth-control
(config)# no dot1x system-auth-control

RADIUS-Assigned QoS / RADIUS-Assigned VLAN / Guest VLAN Enabled :
(config)# dot1x feature { [ guest-vlan ] [ radius-qos ] [ radius-vlan ] }*1
(config)# no dot1x feature { [ guest-vlan ] [ radius-qos ] [ radius-vlan ] }*1

For Guest VLAN ...
Guest VLAN ID / Max. Reauth. Count / Allow Guest VLAN if EAPOL Seen :

(config)# dot1x guest-vlan <1-4095>
(config)# dot1x max-reauth-req <1-255>
(config)# dot1x guest-vlan supplicant
(config)# no dot1x guest-vlan
(config)# no max-reauth-req
(config)# no dot1x guest-vlan supplicant

For Re-authentication ...
Reauthentication Enabled / Period / EAPOL Timeout / Aging Period / Hold Time :
(config)# dot1x re-authentication
(config)# dot1x authentication timer re-authenticate <1-3600>
(config)# dot1x timeout tx-period <1-65535>
(config)# dot1x authentication timer inactivity <10-1000000>
(config)# dot1x timeout quiet-period <10-1000000>
(config)# no dot1x re-authentication
(config)# no dot1x authentication timer re-authenticate
(config)# no dot1x timeout tx-period
(config)# no dot1x authentication timer inactivity
(config)# no dot1x timeout quiet-period

For Configuration by Port ...
Admin State :
(config-if)# dot1x port-control { force-authorized | force-unauthorized | auto | single | multi | mac-based }
(config-if)# no dot1x port-control

RADIUS-Assigned QoS / RADIUS-Assigned VLAN / Guest VLAN Enabled :
(config-if)# dot1x radius-qos
(config-if)# dot1x radius-vlan
(config-if)# dot1x guest-vlan
(config-if)# no dot1x radius-qos
(config-if)# no dot1x radius-vlan
(config-if)# no dot1x guest-vlan

Do Re-initialize / Re-authenticate :
(config-if)# dot1x initialize [ interface <port_type_list> ]
(config-if)# dot1x re-authenticate

*Status by Web* :
[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 | | | - | |
| 11 | Force Authorized | Globally Disabled | | | - | |
| 12 | Force Authorized | Globally Disabled | | | - | |
| 13 | Force Authorized | Globally Disabled | | | - | |
| 14 | Force Authorized | Globally Disabled | | | - | |
| 15 | Force Authorized | Globally Disabled | | | - | |
| 16 | Force Authorized | Globally Disabled | | | - | |
| 17 | Force Authorized | Globally Disabled | | | - | |
| 18 | Force Authorized | Globally Disabled | | | - | |
| 19 | Force Authorized | Globally Disabled | | | - | |
| 20 | Force Authorized | Globally Disabled | | | - | |
| 21 | Force Authorized | Globally Disabled | | | - | |
| 22 | Force Authorized | Globally Disabled | | | - | |
| 23 | Force Authorized | Globally Disabled | | | - | |
| 24 | Force Authorized | Globally Disabled | | | - | |
| 25 | Force Authorized | Globally Disabled | | | - | |
| 26 | Force Authorized | Globally Disabled | | | - | |

Click "**?**" at this web page to get details of the settings.

[Monitor] -> [Security] -> [Network] -> [NAS] -> [Port]

**NAS Statistics Port 1**

**Port State**

| | |
|---|---|
| **Admin State** | Force Authorized |
| **Port State** | Globally Disabled |

Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# clear dot1x statistics [ interface <port_type_list> ]
# show dot1x statistics { eapol | radius | all } [ interface <port_type_list> ]

### 3. ACL configuration

ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program. (ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID. There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.)

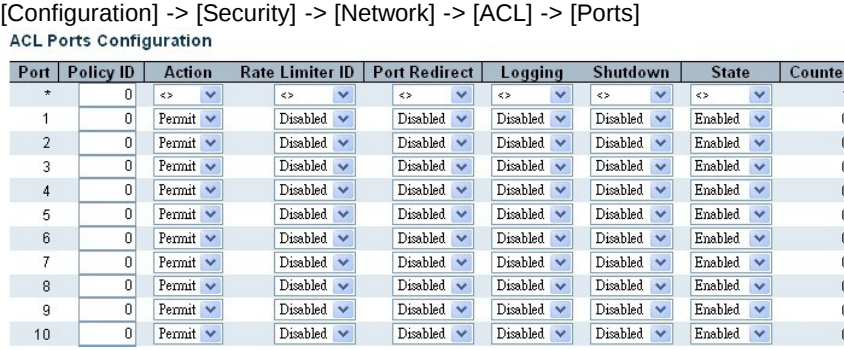
Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

There are 3 web-pages associated with the manual ACL configuration:

[ ACL | Access Control List ] : The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" web-page. There are number of parameters that can be configured with an ACE. Read the Web page help text to get further information for each of them. The maximum number of ACEs is 64.
[ ACL | Ports ] : The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List" - page. You can also set up specific traffic properties (Action / Rate Limiter / Port copy, etc) for each ingress port. They will though only apply if the frame gets past the ACE matching without getting matched. In that case a counter associated with that port is incremented. See the Web page help text for each specific port property.
[ ACL | Rate Limiters ] : Under this page you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under "Ports" and "Access Control List" web-pages you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

*Configuration by Web* :
Port Default Configuration :
[Configuration] -> [Security] -> [Network] -> [ACL] -> [Ports]


ACL Ports Configuration

| Port | Policy ID | Action | Rate Limiter ID | Port Redirect | Logging | Shutdown | State | Counter |
|---|---|---|---|---|---|---|---|---|
| * | 0 | <> | <> | <> | <> | <> | <> | * |
| 1 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 2 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 3 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 4 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 5 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 6 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 7 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 8 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 9 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 10 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |

Click "**?**" at this web page to get details of the settings.

Rate Limiter Configuration :
[Configuration] -> [Security] -> [Network] -> [ACL] -> [Rate Limiters]

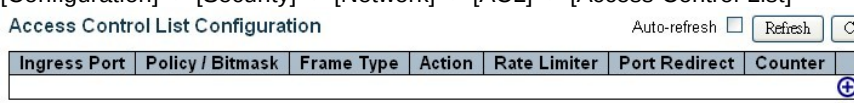
**ACL Rate Limiter Configuration**

| Rate Limiter ID | Rate (pps) |
|---|---|
| * | 1 |
| 1 | 1 |
| 2 | 1 |
| 3 | 1 |
| 4 | 1 |
| 5 | 1 |
| 6 | 1 |
| 7 | 1 |
| 8 | 1 |
| 9 | 1 |
| 10 | 1 |
| 11 | 1 |
| 12 | 1 |
| 13 | 1 |
| 14 | 1 |
| 15 | 1 |
| 16 | 1 |

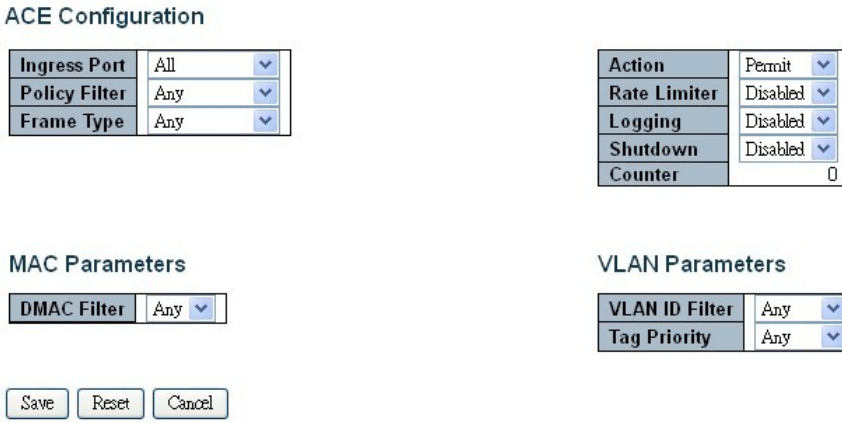
Save Reset

Click "**?**" at this web page to get details of the settings.

ACL Entry Configuration :
[Configuration] -> [Security] -> [Network] -> [ACL] -> [Access Control List]




Click "(+)", the following page will appear.




Click "**?**" at this web page to get details of the settings.

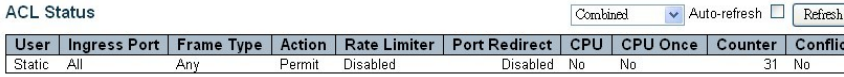
*Configuration by Command* :
Port Default Configuration :
(config-if)# access-list policy <0-255>
(config-if)# access-list action { permit | deny }
(config-if)# access-list rate-limiter <1-16>
(config-if)# access-list redirect interface { <port_type_id> | <port_type_list> }
(config-if)# access-list logging
(config-if)# access-list shutdown
(config-if)# access-list port-state
(config-if)# no access-list policy
(config-if)# no access-list rate-limiter
(config-if)# no access-list redirect
(config-if)# no access-list logging
(config-if)# no access-list shutdown
(config-if)# no access-list port-state

Rate Limiter Configuration :
(config)# access-list rate-limiter [ <1~16> ] pps <0-131071>

ACL Entry Configuration :
- Create a ACL Entry with default setting :
(config)# access-list ace [ update ] <1-256>
- Delete a ACL Entry :
(config)# no access-list ace <1~256>
- Ingress Port :
(config)# access-list ace [ update ] <1-256> ingress { interface { <port_type_id> | <port_type_list> } | any }
- Policy Filter :
(config)# access-list ace [ update ] <1-256> policy <0-255> [ policy-bitmask <0x0-0xFF> ]
- Frame Type :
(config)# access-list ace [ update ] <1-256> frametype { any | arp | etype

[ etype-value { <0x600-0x7ff,0x801-0x805,0x807-0x86dc,0x86de-0xffff> | any } ] | ipv4 | ipv4-icmp | ipv4-tcp | ipv4-udp | ipv6 | ipv6-icmp | ipv6-tcp | ipv6-udp }
- DMAC Filter :
(config)# access-list ace [ update ] <1-256> dmac-type { unicast | multicast | broadcast | any }
- VLAN ID Filter :
(config)# access-list ace [ update ] <1-256> vid { <1-4095> | any }
- Tag Priority :
(config)# access-list ace [ update ] <1-256> tag-priority { <0-7> | any }
- Action if matched :
(config)# access-list ace [ update ] <1-256> action { permit | deny }
- Rate Limiter if matched :
(config)# access-list ace [ update ] <1-256> rate-limiter { <1-16> | disable }
- Logging if matched :
(config)# access-list ace [ update ] <1-256> logging
- Shutdown if matched :
(config)# access-list ace [ update ] <1-256> shutdown
Disable shutdown :
(config)# access-list ace [ update ] <1-256> disable
- Redirect frame to specific port if matched :
(config)# access-list ace [ update ] <1-256> redirect { disable | interface { <port_type_id> | <port_type_list> } }
- Insert the current ACE before the next ACE ID :
(config)# access-list ace [ update ] <1-256> { last | <1-256> }

*Status by Web* :
[Monitor] -> [Security] -> [Network] -> [ACL Status]




| User | Ingress Port | Frame Type | Action | Rate Limiter | Port Redirect | CPU | CPU Once | Counter | Conflict |
|---|---|---|---|---|---|---|---|---|---|
| Static | All | Any | Permit | Disabled | Disabled | No | No | 31 | No |

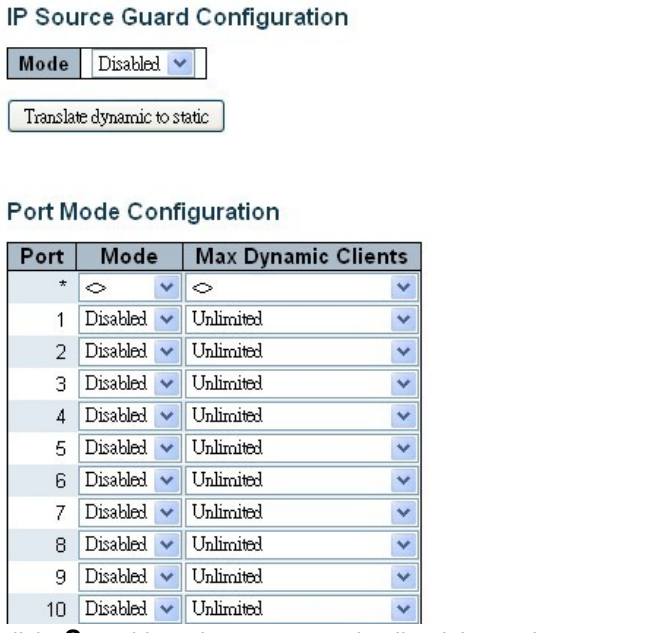
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# clear access-list ace statistics
# show access-list ace statistics [ <1~256> ] [ interface { <port_type_id> | <port_type_list> } ] [ rate-limiter ]
# show access-list ace-status [ static ] [ link-oam ] [ loop-protect ] [ dhcp ] [ ptp ] [ upnp ] [ arp-inspection ] [ mep ] [ ipmc ] [ ip-source-guard ] [ ip-mgmt ] [ conflicts ]

## 4. IP Source Guard

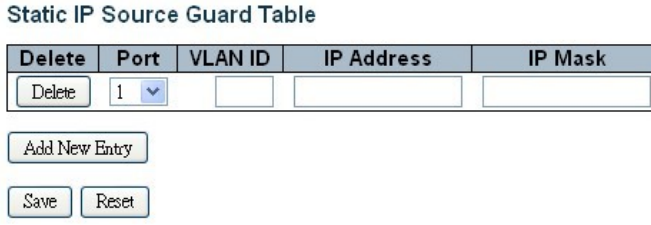
IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

*Configuration by Web* :
Enable/Disable, Dynamic Client Number :
[Configuration] -> [Security] -> [Network] -> [IP Source Guard] -> [Configuration]




Click "**?**" at this web page to get details of the settings.

Assign Static IP Source Guard Table :
[Configuration] -> [Security] -> [Network] -> [IP Source Guard] -> [Static Table]




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Enable/Disable :
(config)# ip verify source
(config)# no ip verify source

Dynamic Client Number :
(config)# ip verify source limit <0-2>
(config)# no ip verify source limit

Translate Dynamic to Static :
(config)# ip verify source translate

Assign Static Entry :
(config)# ip source binding interface <port_type_id> <vlan_id> <ipv4_ucast> <ipv4_netmask>
(config)# ip source binding interface <port_type_id> <vlan_id> <ipv4_ucast> <mac_ucast>
(config)# no ip source binding interface <port_type_id> <vlan_id> <ipv4_ucast> <ipv4_netmask>
(config)# no ip source binding interface <port_type_id> <vlan_id> <ipv4_ucast> <mac_ucast>

*Status by Web* :
[Monitor] -> [Security] -> [Network] -> [IP Source Guard]

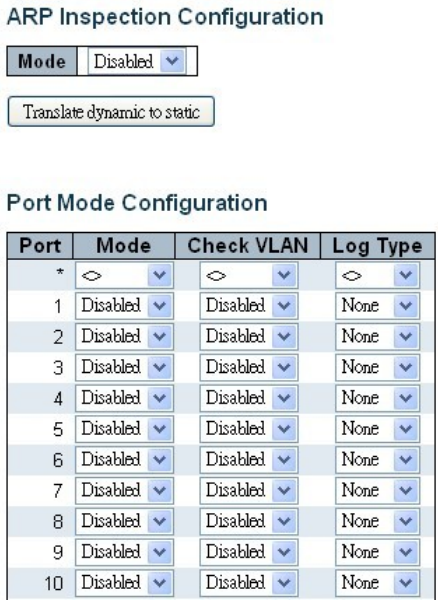

Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show ip verify source [ interface <port_type_list> ]
# show ip source binding [ dhcp-snooping | static ] [ interface <port_type_list> ]

**5. ARP Inspection**

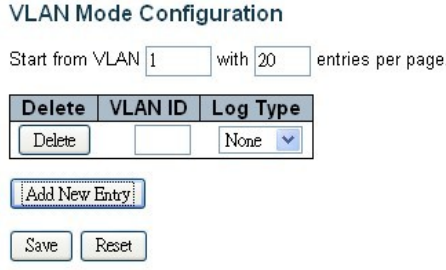
ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

*Configuration by Web* :
Enable/Disable, Configuration on Port :
[Configuration] -> [Security] -> [Network] -> [ARP Inspection] -> [Port Configuration]



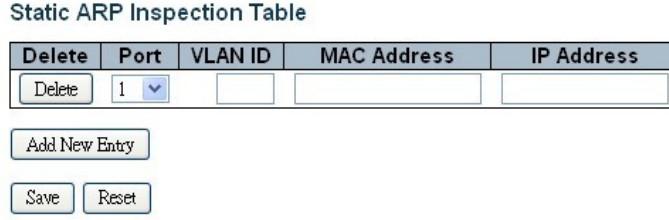

Click "**?**" at this web page to get details of the settings.

Specify ARP Inspection is enabled on which VLAN :
[Configuration] -> [Security] -> [Network] -> [ARP Inspection] -> [VLAN Configuration]



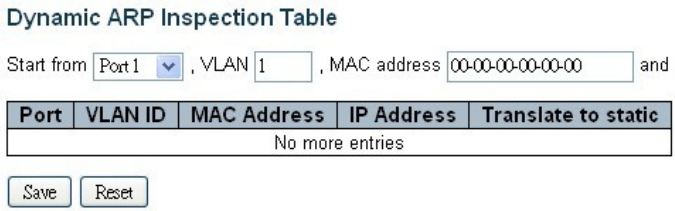

Click "**?**" at this web page to get details of the settings.

Assign Static ARP Inspection Entry :
[Configuration] -> [Security] -> [Network] -> [ARP Inspection] -> [Static Table]



Click "**?**" at this web page to get details of the settings.

Show Dynamic ARP Inspection Table :
[Configuration] -> [Security] -> [Network] -> [ARP Inspection] -> [Dynamic Table]




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Clear ARP cache :
# clear ip arp

Enable/Disable :
# ip arp inspection
# no ip arp inspection

Check VLAN :
# ip arp inspection check-vlan
# no ip arp inspection check-vlan

Create ARP Static Entry :
# ip arp inspection entry interface <port_type_id> <vlan_id> <mac_ucast> <ipv4_ucast>
# no ip arp inspection entry interface <port_type_id> <vlan_id> <mac_ucast> <ipv4_ucast>

Logging :
# ip arp inspection logging { deny | permit | all }
# no ip arp inspection logging
# ip arp inspection vlan <vlan_list> logging { deny | permit | all }
# no ip arp inspection vlan <vlan_list> logging

Specify ARP Inspection is enabled on which VLAN :
# ip arp inspection vlan <vlan_list>
# no ip arp inspection vlan <vlan_list>

# ip arp inspection trust
# no ip arp inspection trust

Translate Dynamic to Static :
# ip arp inspection translate [ interface <port_type_id> <vlan_id> <mac_ucast> <ipv4_ucast> ]

*Status by Web* :

[Monitor] -> [Security] -> [Network] -> [ARP Inspection]


Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show ip arp
# show ip arp inspection [ interface <port_type_list> | vlan <vlan_list> ]
# show ip arp inspection entry [ dhcp-snooping | static ] [ interface <port_type_list> ]

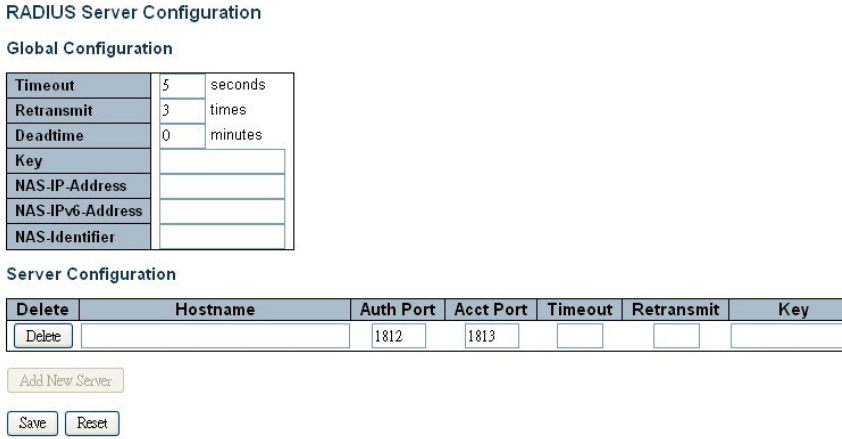
### 7.5.3 Security for AAA Server Configuration

**1. RADIUS Server configuration**

RADIUS is an acronym for Remote Authentication Dial In User Service. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service. RADIUS Server is a server that provides such services.

*Configuration by Web* :

[Configuration] -> [Security] -> [AAA] -> [RADIUS]




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :

Global Configuration :

(config)# radius-server attribute 32 <line1-255>
(config)# radius-server attribute 4 <ipv4_ucast>
(config)# radius-server attribute 95 <ipv6_ucast>
(config)# radius-server deadtime <1-1440>
(config)# radius-server key <line1-63>
(config)# radius-server retransmit <1-1000>
(config)# radius-server timeout <1-1000>
(config)# no radius-server attribute 32
(config)# no radius-server attribute 4
(config)# no radius-server attribute 95
(config)# no radius-server deadtime
(config)# no radius-server key
(config)# no radius-server retransmit
(config)# no radius-server timeout

Server Configuration :

(config)# radius-server host { <word1-255> | <ipv4_ucast> | <ipv6_ucast> } [ auth-port <0-65535> ] [ acct-port <0-65535> ] [ timeout <1-1000> ] [ retransmit

<1-1000> ] [ key <line1-63> ]
(config)# no radius-server host { <word1-255> | <ipv4_ucast> | <ipv6_ucast> } [ auth-port <0-65535> ] [ acct-port <0-65535> ]

*Status by Web* :
[Monitor] -> [Security] -> [AAA] -> [RADIUS Overview]

RADIUS Authentication Server Status Overview

| # | IP Address | Status |
|---|---|---|
| 1 | 0.0.0.0:0 | Disabled |
| 2 | 0.0.0.0:0 | Disabled |
| 3 | 0.0.0.0:0 | Disabled |
| 4 | 0.0.0.0:0 | Disabled |
| 5 | 0.0.0.0:0 | Disabled |

RADIUS Accounting Server Status Overview

| # | IP Address | Status |
|---|---|---|
| 1 | 0.0.0.0:0 | Disabled |
| 2 | 0.0.0.0:0 | Disabled |
| 3 | 0.0.0.0:0 | Disabled |
| 4 | 0.0.0.0:0 | Disabled |
| 5 | 0.0.0.0:0 | Disabled |

Click "**?**" at this web page to get details of the settings.

[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 | | | 0.0.0.0:0 |
| 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 | | | 0.0.0.0:0 |
| State | | | Disabled |
| Round-Trip Time | | | 0 ms |

Click "**?**" at this web page to get details of the settings.

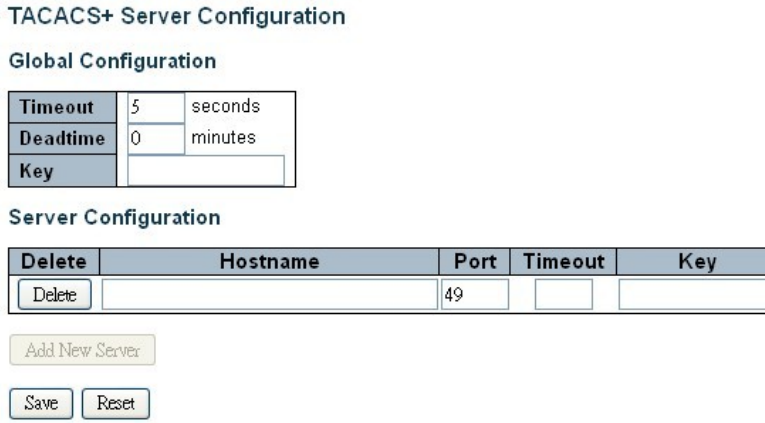
*Status by Command* :

# show radius-server [ statistics ]

## 2. TACACS+ Server configuration

TACACS+ is an acronym for Terminal Acess Controller Access Control System Plus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services. TACACS+ Server is a server that provides such services.

*Configuration by Web* :
[Configuration] -> [Security] -> [AAA] -> [TACACS+]




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Global Configuration :
(config)# tacacs-server deadtime <1-1440>
(config)# tacacs-server key <line1-63>
(config)# tacacs-server timeout <1-1000>
(config)# no tacacs-server deadtime
(config)# no tacacs-server key
(config)# no tacacs-server timeout

Server Configuration
(config)# tacacs-server host { <word1-255> | <ipv4_ucast> | <ipv6_ucast> } [ port <0-65535> ] [ timeout <1-1000> ] [ key <line1-63> ]
(config)# no tacacs-server host { <word1-255> | <ipv4_ucast> | <ipv6_ucast> } [ port <0-65535> ]

*Status by Web* :
[Configuration] -> [Security] -> [AAA] -> [TACACS+]
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show tacacs-server

## 7.6 Aggregation

Port Aggregation(Link Aggregation) uses multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

### 1. Static

*Configuration by Web* :
[Configuration] -> [Aggregation] -> [Static]

Aggregation Mode Configuration

| Hash Code Contributors | |
|---|---|
| Source MAC Address | ☐ |
| Destination MAC Address | ☐ |
| IP Address | ☐ |
| TCP/UDP Port Number | ☐ |

Aggregation Group Configuration

| | Port Members | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Group ID | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| Normal | ◉ | ◉ | ◉ | ◉ | ◉ | ◉ | ◉ | ◉ | ◉ | ◉ | ◉ | ◉ | ◉ | ◉ | ◉ | ◉ | ◉ | ◉ | ◉ | ◉ | ◉ | ◉ | ◉ | ◉ | ◉ | ◉ |
| 1 | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| 2 | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| 3 | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| 4 | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| 5 | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| 6 | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| 7 | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| 8 | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| 9 | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| 10 | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| 11 | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| 12 | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| 13 | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Traffic distribution mode :
(config)# aggregation mode { [ smac ] [ dmac ] [ ip ] [ port ] }
(config)# no aggregation mode

Add Ports to Aggregation Group :
(config-if)# aggregation group <uint>
(config-if)# no aggregation group

*Status by Web* :
[Configuration] -> [Aggregation] -> [Static]
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show aggregation [ mode ]

## 2. LACP

*Configuration by Web* :
[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 |

Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
System Priority :
(config)# lacp system-priority <1-65535>
(config)# no lacp system-priority <1-65535>

LACP Port Configuration :
(config-if)# lacp
(config-if)# lacp key { <1-65535> | auto }
(config-if)# lacp port-priority <1-65535>
(config-if)# lacp role { active | passive }
(config-if)# lacp timeout { fast | slow }
(config-if)# no lacp
(config-if)# no lacp key { <1-65535> | auto }
(config-if)# no lacp port-priority <1-65535>
(config-if)# no lacp role { active | passive }
(config-if)# no lacp timeout { fast | slow }

*Status by Web* :
[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* | | | | | |

Click "**?**" at this web page to get details of the settings.

[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 | - | - | - | - | - |

Click "**?**" at this web page to get details of the settings.

[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 |

Click "**?**" at this web page to get details of the settings.

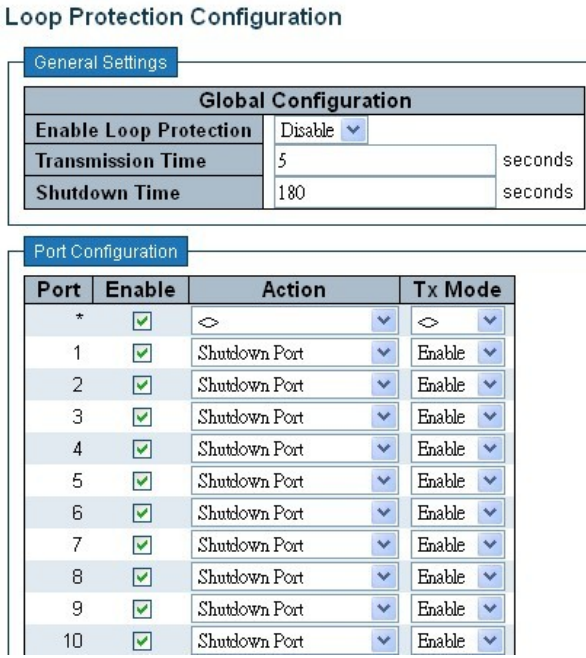
*Status by Command* :
# clear lacp statistics
# show lacp { internal | statistics | system-id | neighbour }

## 7.7 Loop Protection

This function is used to configure Loop Protection function. Loop on port will cause packet storm in switch.

If Loop Protection 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 interval.

*Configuration by Web* :
[Configuration] -> [Loop Protection]




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Global Enable/Disable :
(config)# loop-protect
(config)# no loop-protect

Global Transmission Time :
(config)# loop-protect transmit-time <1-10>
(config)# no loop-protect transmit-time

Global Shutdown Time :
(config)# loop-protect shutdown-time <0-604800>

(config)# no loop-protect shutdown-time

Port Loop Protection Enable/Disable :
(config-if)# loop-protect
(config-if)# no loop-protect

Port Action if loop detected :
(config-if)# loop-protect action { [ shutdown ] [ log ] }
(config-if)# no loop-protect action

Port Actively Generate PDUs
(config-if)# loop-protect tx-mode
(config-if)# no loop-protect tx-mode

*Status by Web* :
[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 | Down | - | - |
| 8 | Shutdown | Enabled | 0 | Down | - | - |
| 9 | Shutdown | Enabled | 0 | Down | - | - |
| 10 | Shutdown | Enabled | 0 | Down | - | - |
| 11 | Shutdown | Enabled | 0 | Down | - | - |
| 12 | Shutdown | Enabled | 0 | Down | - | - |
| 13 | Shutdown | Enabled | 0 | Down | - | - |
| 14 | Shutdown | Enabled | 0 | Down | - | - |
| 15 | Shutdown | Enabled | 0 | Down | - | - |
| 16 | Shutdown | Enabled | 0 | Down | - | - |

Click "**?**" at this web page to get details of the settings.

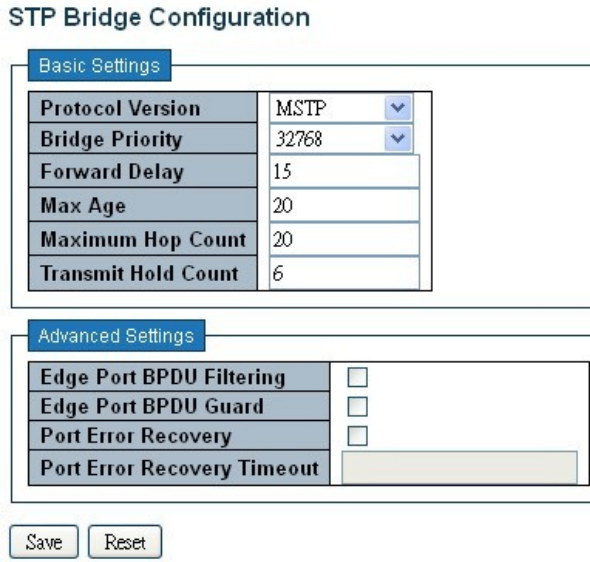
*Status by Command* :
# show loop-protect [ interface <port_type_list> ]

## 7.8 Spanning Tree

Spanning tree is a protocol to prevent network loop in network topology. If network loop happens, it will cause 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.
This switch supports MSTP/RSTP/STP functions. Configuring them for spanning tree operation is done here.

**1. STP Bridge Configuration**
Configure general spanning tree bridge operation settings here.

*Configuration by Web* :
[Configuration] -> [Spanning Tree] -> [Bridge Settings]




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Protocol Version :
(config)# spanning-tree mode { stp | rstp | mstp }
(config)# no spanning-tree mode

Forward Delay :
(config)# spanning-tree mst forward-time <4-30>
(config)# no spanning-tree mst forward-time

Max Age :
(config)# spanning-tree mst max-age <6-40> [ forward-time <4-30> ]
(config)# no spanning-tree mst max-age

Maximum Hop Count :
(config)# spanning-tree mst max-hops <6-40>
(config)# no spanning-tree mst max-hops

Transmit Hold Count :
(config)# spanning-tree transmit hold-count <1-10>
(config)# no spanning-tree transmit hold-count

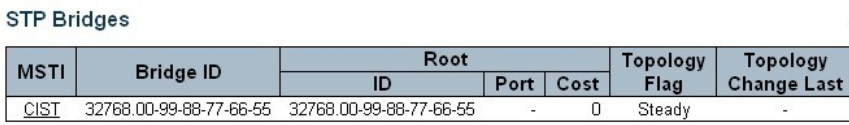
Edge Port BPDU Filtering :
(config)# spanning-tree edge bpdu-filter
(config)# no spanning-tree edge bpdu-filter

Edge Port BPDU Guard :
(config)# spanning-tree edge bpdu-guard
(config)# no spanning-tree edge bpdu-guard

Port Error Recovery Timeout :
(config)# spanning-tree recovery interval <30-86400>
(config)# no spanning-tree recovery interval

Set the STP migration check :
# clear spanning-tree detected-protocols [ interface <port_type_list> ]

*Status by Web* :
[Monitor] -> [Spanning Tree] -> [Bridge Status]


STP Bridges

| MSTI | Bridge ID | Root | | | Topology Flag | Topology Change Last |
|---|---|---|---|---|---|---|
| | | ID | Port | Cost | | |
| CIST | 32768.00-99-88-77-66-55 | 32768.00-99-88-77-66-55 | - | 0 | Steady | - |

Click "**?**" at this web page to get details of the settings.

Click the entry under "MSTI", Detailed Bridge Status will be shown.

STP Detailed Bridge Status

| STP Bridge Status | |
|---|---|
| Bridge Instance | CIST |
| Bridge ID | 32768.00-99-88-77-66-55 |
| Root ID | 32768.00-99-88-77-66-55 |
| Root Cost | 0 |
| Root Port | - |
| Regional Root | 32768.00-99-88-77-66-55 |
| 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 |
|---|---|---|---|---|---|---|---|
| *No ports or aggregations active* | | | | | | | |

Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show spanning-tree summary
# show spanning-tree active
# show spanning-tree mst

## 2. MSTI Configuration - VLAN Mapping

*Configuration by Web* :
[Configuration] -> [Spanning Tree] -> [MSTI Mapping]

MSTI Configuration

Add VLANs separated by spaces or comma.

**Unmapped VLANs are mapped to the CIST**. (The default bridge instance).

Configuration Identification

| | |
|---|---|
| Configuration Name | 00-99-88-77-66-55 |
| Configuration Revision | 0 |

MSTI Mapping

| MSTI | VLANs Mapped |
|---|---|
| MSTI1 | |
| MSTI2 | |
| MSTI3 | |
| MSTI4 | |

Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Configuration Identification :
(config)# spanning-tree mst name <word32> revision <0-65535>
(config)# no spanning-tree mst name

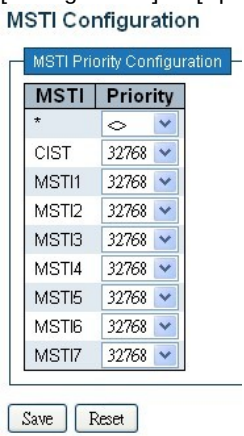
MSTI VLAN Mapping :
(config)# spanning-tree mst <0-7> vlan <vlan_list>
(config)# no spanning-tree mst <0-7> vlan

*Status by Web* :
[Configuration] -> [Spanning Tree] -> [MSTI Mapping]
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show spanning-tree mst configuration

### 3. MSTI Configuration - Priority

*Configuration by Web* :
[Configuration] -> [Spanning Tree] -> [MSTI Priorities]



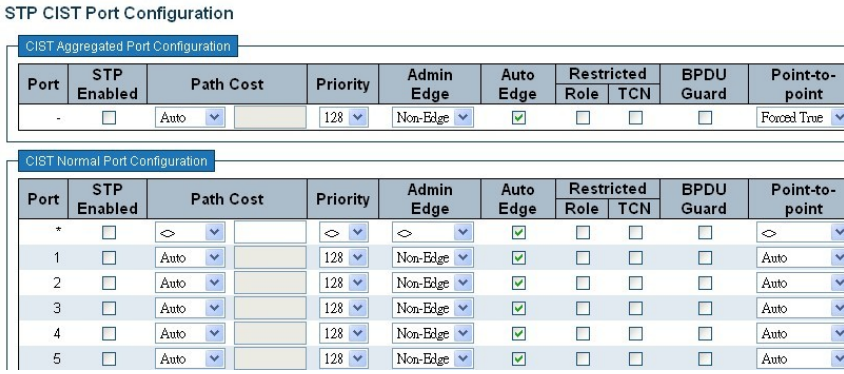

Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
MSTI Priority Configuration :
(config)# spanning-tree mst <0-7> priority <0-61440>
(config)# no spanning-tree mst <0-7> priority

*Status by Web* :
[Configuration] -> [Spanning Tree] -> [MSTI Priorities]
Click "**?**" at this web page to get details of the settings.

## 4. STP CIST Port Configuration

*Configuration by Web* :
[Configuration] -> [Spanning Tree] -> [CIST Ports]




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Enable/Disable on Port :
(config-if)# spanning-tree
(config-if)# no spanning-tree

Path Cost :
(config-if)# spanning-tree mst <0-7> cost { <1-200000000> | auto }
(config-if)# no spanning-tree mst <0-7> cost

Priority :
(config-if)# spanning-tree mst <0-7> port-priority <0-240>
(config-if)# no spanning-tree mst <0-7> port-priority

Admin Edge :
(config-if)# spanning-tree edge
(config-if)# no spanning-tree edge

Auto Edge :
(config-if)# spanning-tree auto-edge
(config-if)# no spanning-tree auto-edge

Restricted Role :
(config-if)# spanning-tree restricted-role
(config-if)# no spanning-tree restricted-role

Restricted TCN :
(config-if)# spanning-tree restricted-tcn
(config-if)# no spanning-tree restricted-tcn

BPDU Guard :

(config-if)# spanning-tree bpdu-guard
(config-if)# no spanning-tree bpdu-guard

Point-to-Point :
(config-if)# spanning-tree link-type { point-to-point | shared | auto }
(config-if)# no spanning-tree link-type

*Status by Web* :
[Monitor] -> [Spanning Tree] -> [Port Status]

STP Port Status

| Port | CIST Role | CIST State | Uptime |
|---|---|---|---|
| 1 | Non-STP | Forwarding | - |
| 2 | Non-STP | Forwarding | - |
| 3 | Non-STP | Forwarding | - |
| 4 | Non-STP | Forwarding | - |
| 5 | Non-STP | Forwarding | - |
| 6 | Non-STP | Forwarding | - |
| 7 | Non-STP | Forwarding | - |
| 8 | Non-STP | Forwarding | - |
| 9 | Non-STP | Forwarding | - |
| 10 | Non-STP | Forwarding | - |

Click "**?**" at this web page to get details of the settings.

[Monitor] -> [Spanning Tree] -> [Port Statistics]

STP Statistics

| Port | Transmitted | | | | Received | | | | Discarded | |
|---|---|---|---|---|---|---|---|---|---|---|
| | MSTP | RSTP | STP | TCN | MSTP | RSTP | STP | TCN | Unknown | Illegal |
| *No ports enabled* | | | | | | | | | | |

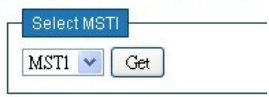
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# clear spanning-tree statistics [ interface <port_type_list> ]
# show spanning-tree interface <port_type_list>
# show spanning-tree detailed interface <port_type_list>

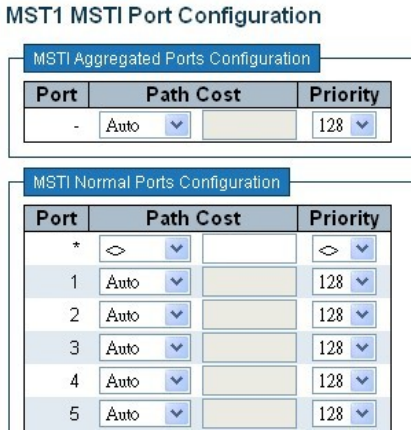
### 5. MSTI Port Configuration

*Configuration by Web* :
[Configuration] -> [Spanning Tree] -> [MSTI Ports]

MSTI Port Configuration




Select a MSTI and click [Get]. The port configuration page for the MSTI will appear.




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Path Cost :
(config-if)# spanning-tree mst <0-7> cost { <1-200000000> | auto }
(config-if)# no spanning-tree mst <0-7> cost

Port Priority :
(config-if)# spanning-tree mst <0-7> port-priority <0-240>
(config-if)# no spanning-tree mst <0-7> port-priority

*Status by Web* :
[Configuration] -> [Spanning Tree] -> [MSTI Ports]
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show spanning-tree mst <0-7> interface <port_type_list>

## 7.9 IP Multicast

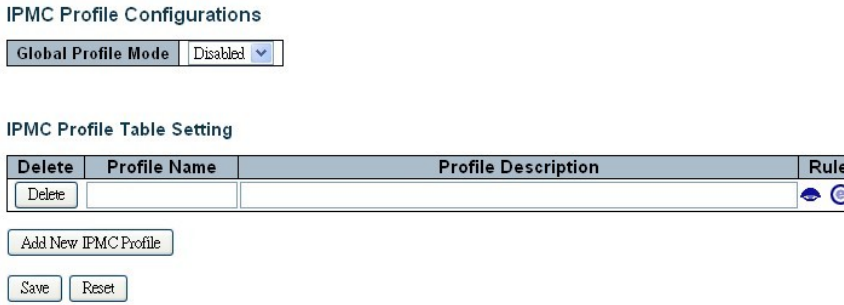
IP multicast is a method of sending Internet Protocol (IP) datagrams to a group of interested receivers in a single transmission. It is often employed for streaming media applications on the Internet and private networks.

### 7.9.1 IP Multicast Profile

**1. Profile Table**

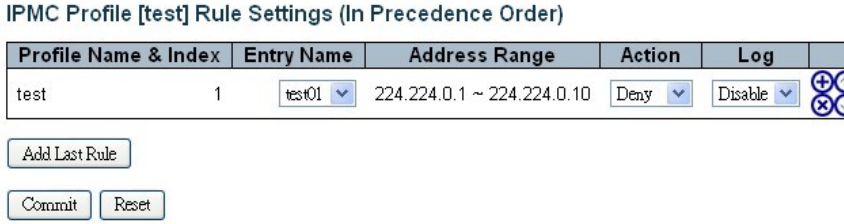
IPMC Profile is an acronym for IP MultiCast Profile. IPMC Profile is used to deploy the access control on IP multicast streams.

*Configuration by Web* :
[Configuration] -> [IPMC Profile] -> [Profile Table]




Click "**?**" at this web page to get details of the settings.

After profile name and description are set and saved, "Rule" can be configured. Clicking "(e)", the following page will appear for adding entry. (Entries are created at "[Configuration] -> [IPMC Profile] -> [Address Entry]" web page.)



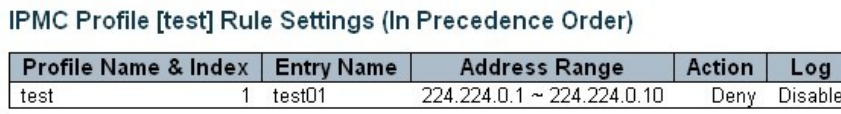

*Configuration by Command* :
Enable/Disable :
(config)# ipmc profile
(config)# no ipmc profile

Create/Delete IP Multicast Profile :
(config)# ipmc profile <word16>
And the prompt will become "(config-ipmc-profile)#".
(config)# no ipmc profile <word16>

Edit/Delete IP Multicast Profile Rule :
(config-ipmc-profile)# range <word16> { permit | deny } [ log ] [ next <word16> ]
(config-ipmc-profile)# no range <word16>
"<word16>" is the name of Address Entry.

Edit/Delete Description of Profile :
(config-ipmc-profile)# description <line64>
(config-ipmc-profile)# no description <line64>

*Status by Web* :
[Configuration] -> [IPMC Profile] -> [Profile Table]
Clicking the "eye" icon, the entry table will be shown.

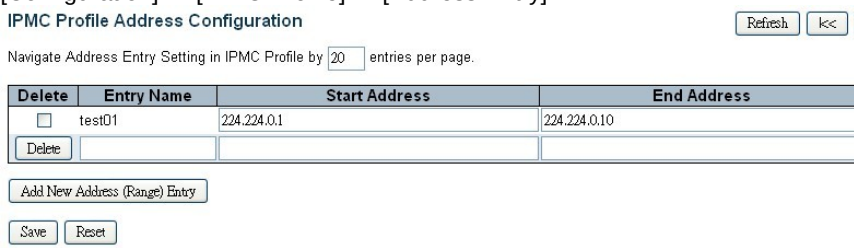

IPMC Profile [test] Rule Settings (In Precedence Order)

| Profile Name & Index | Entry Name | Address Range | Action | Log |
|---|---|---|---|---|
| test 1 | test01 | 224.224.0.1 ~ 224.224.0.10 | Deny | Disable |

*Status by Command* :
# show ipmc profile [ <word16> ] [ detail ]

## 2. Address Entry

*Configuration by Web* :
[Configuration] -> [IPMC Profile] -> [Address Entry]




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Create/Delete IP Multicast Address Entry for Profile :
(config)# ipmc range <word16> { <ipv4_mcast> [ <ipv4_mcast> ] | <ipv6_mcast> [ <ipv6_mcast> ] }
(config)# no ipmc range <word16>

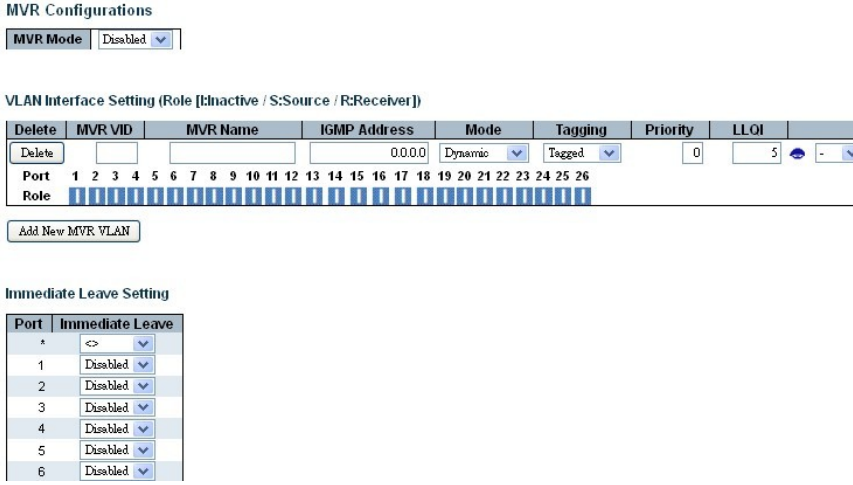
*Status by Web* :
[Configuration] -> [IPMC Profile] -> [Address Entry]
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show ipmc range [ <word16> ]

### 7.9.2 MVR

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 4 MVR VLANs with corresponding channel profile for each Multicast VLAN. The channel profile is defined by the IPMC Profile which provides the filtering conditions.

*Configuration by Web* :
[Configuration] -> [MVR]




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Enable/Disable :
(config)# mvr
(config)# no mvr

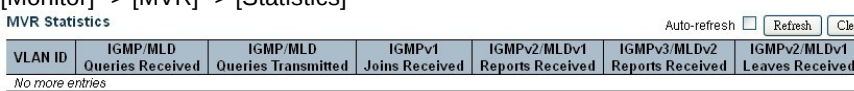
VLAN Interface Setting :
(config)# mvr vlan <vlan_list> [ name <word16> ]
(config)# mvr vlan <vlan_list> channel <word16>
(config)# mvr vlan <vlan_list> frame priority <0-7>
(config)# mvr vlan <vlan_list> frame tagged
(config)# mvr vlan <vlan_list> igmp-address <ipv4_ucast>
(config)# mvr vlan <vlan_list> last-member-query-interval <0-31744>
(config)# mvr vlan <vlan_list> mode { dynamic | compatible }
(config)# mvr name <word16> channel <word16>

(config)# mvr name <word16> frame priority <0-7>
(config)# mvr name <word16> frame tagged
(config)# mvr name <word16> igmp-address <ipv4_ucast>
(config)# mvr name <word16> last-member-query-interval <0-31744>
(config)# mvr name <word16> mode { dynamic | compatible }
(config)# no mvr vlan <vlan_list>
(config)# no mvr vlan <vlan_list> channel
(config)# no mvr vlan <vlan_list> frame priority
(config)# no mvr vlan <vlan_list> frame tagged
(config)# no mvr vlan <vlan_list> igmp-address
(config)# no mvr vlan <vlan_list> last-member-query-interval
(config)# no mvr vlan <vlan_list> mode
(config)# no mvr name <word16> channel
(config)# no mvr name <word16> frame priority
(config)# no mvr name <word16> frame tagged
(config)# no mvr name <word16> igmp-address
(config)# no mvr name <word16> last-member-query-interval
(config)# no mvr name <word16> mode

Immediate Leave Setting on Port :
Enable/Disable :
(config-if)# mvr immediate-leave
(config-if)# no mvr immediate-leave

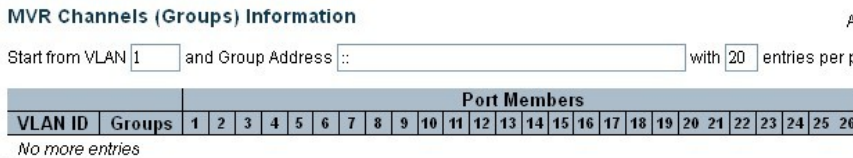
Port Role :
(config-if)# mvr vlan <vlan_list> type { source | receiver }
(config-if)# no mvr vlan <vlan_list> type
(config-if)# mvr name <word16> type { source | receiver }
(config-if)# no mvr name <word16> type

*Status by Web* :
[Monitor] -> [MVR] -> [Statistics]



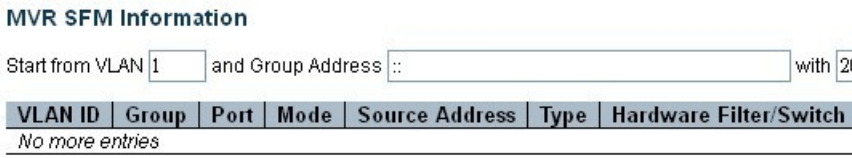

Click "**?**" at this web page to get details of the settings.

[Monitor] -> [MVR] -> [MVR Channel Groups]




Click "**?**" at this web page to get details of the settings.

[Monitor] -> [MVR] -> [MVR SFM Information]




Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show mvr [ vlan <vlan_list> | name <word16> ] [ group-database [ interface <port_type_list> ] [ sfm-information ] ] [ detail ]
# clear mvr [ vlan <vlan_list> | name <word16> ] statistics

### 7.9.3 IP Multicast

**1. IGMP Snooping**

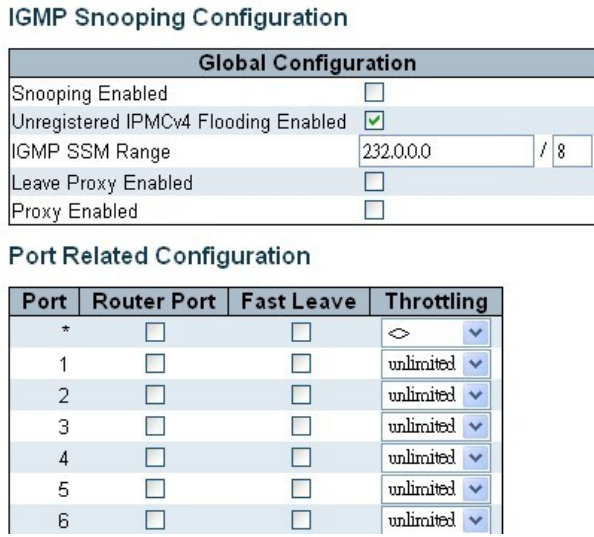
IGMP is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast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

IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.

*Configuration by Web* :

Global Basic and Port Related Configuration :

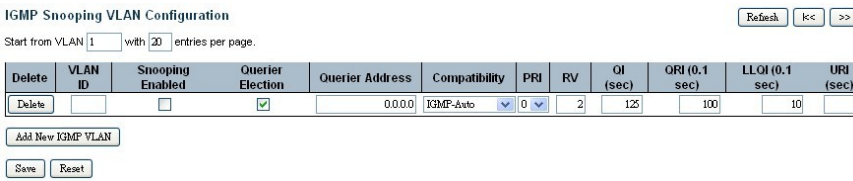
[Configuration] -> [IPMC] -> [IGMP Snooping] -> [Basic Configuration]




Click "**?**" at this web page to get details of the settings.

IGMP Snooping VLAN Configuration :

[Configuration] -> [IPMC] -> [IGMP Snooping] -> [VLAN Configuration]




Click "**?**" at this web page to get details of the settings.

IGMP Snooping Port Filtering Profile :
[Configuration] -> [IPMC] -> [IGMP Snooping] -> [Port Filtering Profile]


Click "**?**" at this web page to get details of the settings.
Note: After Profile is selected, clicking the "eye" icon will show the profile content.

*Configuration by Command* :
IGMP Snooping Basic Configuration :
- Snooping Enable/Disable :
(config)# ip igmp snooping
(config)# no ip igmp snooping

- Unregistered IPMCv4 Flooding Enable/Disable :
(config)# ip igmp unknown-flooding
(config)# no ip igmp unknown-flooding

- IGMP SSM Range :
(config)# ip igmp ssm-range <ipv4_mcast> <4-32>
(config)# no ip igmp ssm-range

- Proxy Enable/Disable :
(config)# ip igmp host-proxy
(config)# no ip igmp host-proxy

- Leave Proxy Enable/Disable :
(config)# ip igmp host-proxy leave-proxy
(config)# no ip igmp host-proxy leave-proxy

Port Related Basic Configuration :
- Router Port Enable/Disable :
(config-if)# ip igmp snooping mrouter

(config-if)# no ip igmp snooping mrouter

- Immediate-Leave Enable/Disable :
(config-if)# ip igmp snooping immediate-leave
(config-if)# no ip igmp snooping immediate-leave

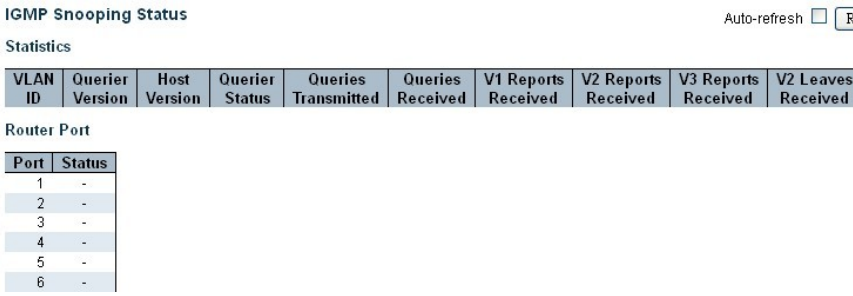
- Throttling(Max. Group Number) :
(config-if)# ip igmp snooping max-groups <1-10>
(config-if)# no ip igmp snooping max-groups

IGMP Snooping VLAN Configuration :
- Assign VLAN for IGMP Snooping :
(config)# ip igmp snooping vlan <vlan_list>
(config)# no ip igmp snooping vlan [ <vlan_list> ]

- Configure IGMP Snooping for VLAN :
(config-if-vlan)# ip igmp snooping
(config-if-vlan)# ip igmp snooping compatibility { auto | v1 | v2 | v3 }
(config-if-vlan)# ip igmp snooping last-member-query-interval <0-31744>
(config-if-vlan)# ip igmp snooping priority <0-7>
(config-if-vlan)# ip igmp snooping querier { election | address <ipv4_ucast> }
(config-if-vlan)# ip igmp snooping query-interval <1-31744>
(config-if-vlan)# ip igmp snooping query-max-response-time <0-31744>
(config-if-vlan)# ip igmp snooping robustness-variable <1-255>
(config-if-vlan)# ip igmp snooping unsolicited-report-interval <0-31744>
(config-if-vlan)# no ip igmp snooping
(config-if-vlan)# no ip igmp snooping compatibility
(config-if-vlan)# no ip igmp snooping last-member-query-interval
(config-if-vlan)# no ip igmp snooping priority
(config-if-vlan)# no ip igmp snooping querier { election | address }
(config-if-vlan)# no ip igmp snooping query-interval
(config-if-vlan)# no ip igmp snooping query-max-response-time
(config-if-vlan)# no ip igmp snooping robustness-variable
(config-if-vlan)# no ip igmp snooping unsolicited-report-interval

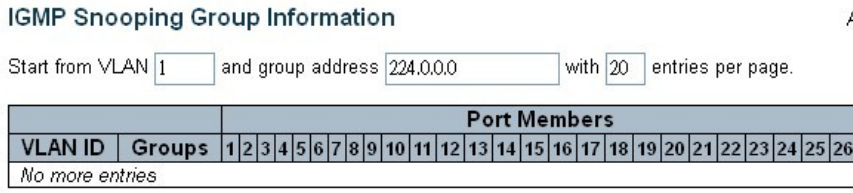
IGMP Snooping Port Filtering Profile :
(config-if)# ip igmp snooping filter <word16>
(config-if)# no ip igmp snooping filter

*Status by Web* :
[Monitor] -> [IPMC] -> [IGMP Snooping] -> [Status]



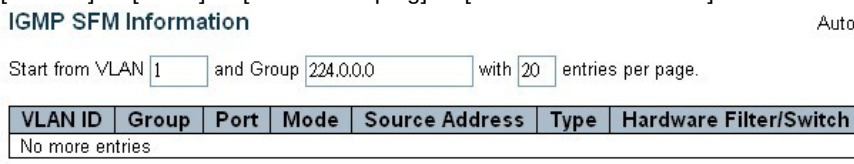

Click "**?**" at this web page to get details of the settings.

[Monitor] -> [IPMC] -> [IGMP Snooping] -> [Groups Information]




Click "**?**" at this web page to get details of the settings.

[Monitor] -> [IPMC] -> [IGMP Snooping] -> [IPv4 SFM Information]




Click "**?**" at this web page to get details of the settings.

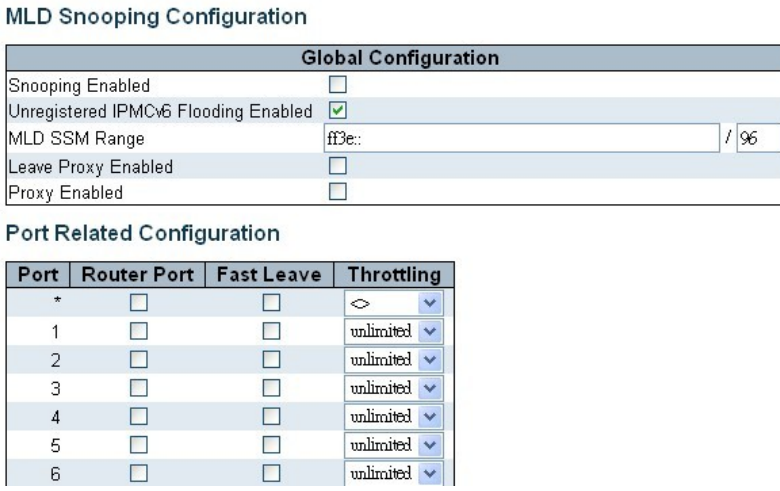
*Status by Command* :
# clear ip igmp snooping [ vlan <vlan_list> ] statistics
# show ip igmp snooping [ vlan <vlan_list> ] [ group-database [ interface <port_type_list> ] [ sfm-information ] ] [ detail ]
# show ip igmp snooping mrouter [ detail ]

## 2. MLD Snooping

MLD is an acronym for Multicast Listener Discovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.
MLD snooping allows the switch to examine MLD packets and make forwarding decisions based on their content. You can configure the switch to use MLD snooping in subnets that receive MLD queries from either MLD or the MLD snooping querier. MLD snooping constrains IPv6 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv6 multicast traffic only

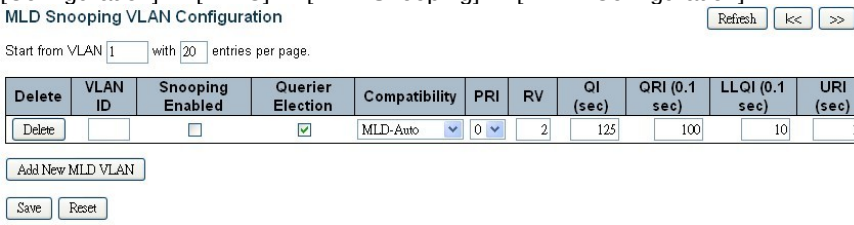
to those ports that want to receive it.

*Configuration by Web* :
Global Basic and Port Related Configuration :
[Configuration] -> [IPMC] -> [MLD Snooping] -> [Basic Configuration]




Click "**?**" at this web page to get details of the settings.

MLD Snooping VLAN Configuration :
[Configuration] -> [IPMC] -> [MLD Snooping] -> [VLAN Configuration]




Click "**?**" at this web page to get details of the settings.

MLD Snooping Port Filtering Profile :
[Configuration] -> [IPMC] -> [MLD Snooping] -> [Port Filtering Profile]

Click "**?**" at this web page to get details of the settings.
Note: After Profile is selected, clicking the "eye" icon will show the profile content.

*Configuration by Command* :
MLD Snooping Basic Configuration :
- Snooping Enable/Disable :
(config)# ipv6 mld snooping
(config)# no ipv6 mld snooping

- Unregistered IPMCv6 Flooding Enable/Disable :
(config)# ipv6 mld unknown-flooding
(config)# no ipv6 mld unknown-flooding

- MLD SSM Range :
(config)# ipv6 mld ssm-range <ipv6_mcast> <8-128>
(config)# no ipv6 mld ssm-range

- Proxy Enable/Disable :
(config)# ipv6 mld host-proxy
(config)# no ipv6 mld host-proxy

- Leave Proxy Enable/Disable :
(config)# ipv6 mld host-proxy leave-proxy
(config)# no ipv6 mld host-proxy leave-proxy

Port Related Basic Configuration :
- Router Port Enable/Disable :
(config-if)# ipv6 mld snooping mrouter
(config-if)# no ipv6 mld snooping mrouter

- Immediate-Leave Enable/Disable :
(config-if)# ipv6 mld snooping immediate-leave
(config-if)# no ipv6 mld snooping immediate-leave

- Throttling(Max. Group Number) :
(config-if)# ipv6 mld snooping max-groups <1-10>
(config-if)# no ipv6 mld snooping max-groups

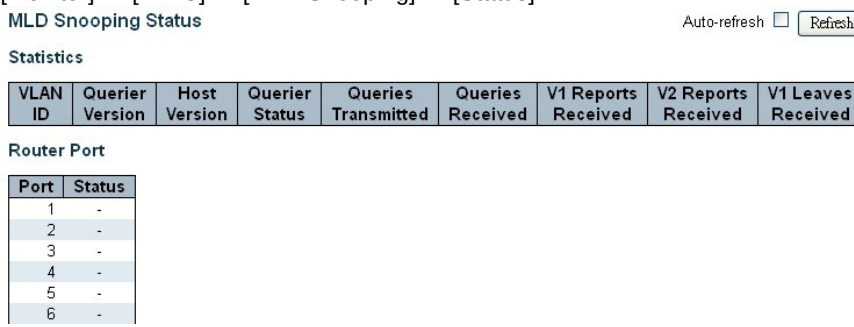
MLD Snooping VLAN Configuration :
- Assign VLAN for MLD Snooping :
(config)# ipv6 mld snooping vlan <vlan_list>
(config)# no ipv6 mld snooping vlan [ <vlan_list> ]

- Configure MLD Snooping for VLAN :
(config-if-vlan)# ipv6 mld snooping
(config-if-vlan)# ipv6 mld snooping compatibility { auto | v1 | v2 }
(config-if-vlan)# ipv6 mld snooping last-member-query-interval <0-31744>
(config-if-vlan)# ipv6 mld snooping priority <0-7>
(config-if-vlan)# ipv6 mld snooping querier election

(config-if-vlan)# ipv6 mld snooping query-interval <1-31744>
(config-if-vlan)# ipv6 mld snooping query-max-response-time <0-31744>
(config-if-vlan)# ipv6 mld snooping robustness-variable <1-255>
(config-if-vlan)# ipv6 mld snooping unsolicited-report-interval <0-31744>
(config-if-vlan)# no ipv6 mld snooping
(config-if-vlan)# no ipv6 mld snooping compatibility
(config-if-vlan)# no ipv6 mld snooping last-member-query-interval
(config-if-vlan)# no ipv6 mld snooping priority
(config-if-vlan)# no ipv6 mld snooping querier election
(config-if-vlan)# no ipv6 mld snooping query-interval
(config-if-vlan)# no ipv6 mld snooping query-max-response-time
(config-if-vlan)# no ipv6 mld snooping robustness-variable
(config-if-vlan)# no ipv6 mld snooping unsolicited-report-interval

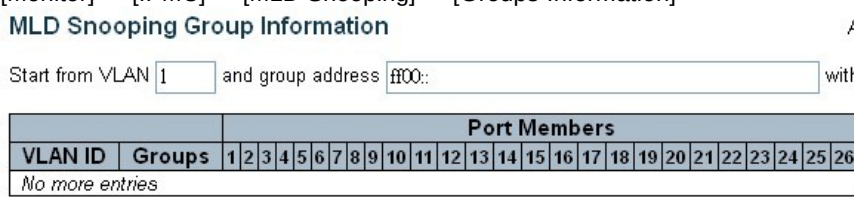
MLD Snooping Port Filtering Profile :
(config-if)# ipv6 mld snooping filter <word16>
(config-if)# no ipv6 mld snooping filter

*Status by Web* :
[Monitor] -> [IPMC] -> [MLD Snooping] -> [Status]



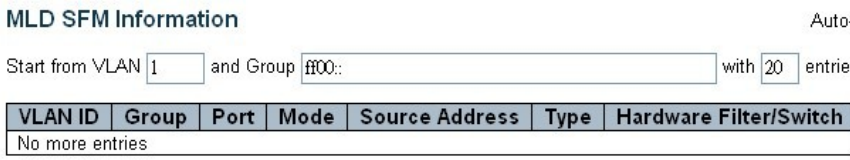

Click "**?**" at this web page to get details of the settings.

[Monitor] -> [IPMC] -> [MLD Snooping] -> [Groups Information]




Click "**?**" at this web page to get details of the settings.

[Monitor] -> [IPMC] -> [MLD Snooping] -> [IPv6 SFM Information]



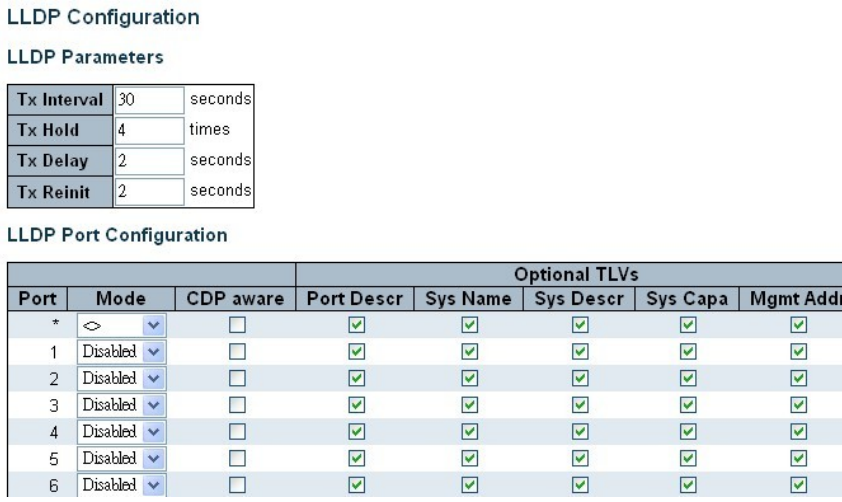

Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# clear ipv6 mld snooping [ vlan <vlan_list> ] statistics
# show ipv6 mld snooping [ vlan <vlan_list> ] [ group-database [ interface <port_type_list> ] [ sfm-information ] ] [ detail ]
# show ipv6 mld snooping mrouter [ detail ]

## 7.10 LLDP

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).

*Configuration by Web* :
[Configuration] -> [LLDP]




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
General Configuration :
- Tx Interval :
(config)# lldp timer <5-32768>
(config)# no lldp timer

- Tx Hold :
(config)# lldp holdtime <2-10>
(config)# no lldp holdtime

- Tx Delay :
(config)# lldp transmission-delay <1-8192>

(config)# no lldp transmission-delay

- Tx Reinit :
(config)# lldp reinit <1-10>
(config)# no lldp reinit

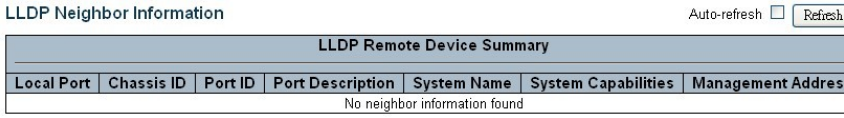
Port Configuration :
- Enable/Disabled transmision of LLDP frames :
(config-if)# lldp transmit
(config-if)# no lldp transmit

- Enable/Disable decoding of received LLDP frames :
(config-if)# lldp receive
(config-if)# no lldp receive

- Optional TLVs to transmit :
(config-if)# lldp tlv-select { management-address | port-description | system-capabilities | system-description | system-name }
(config-if)# no lldp tlv-select { management-address | port-description | system-capabilities | system-description | system-name }

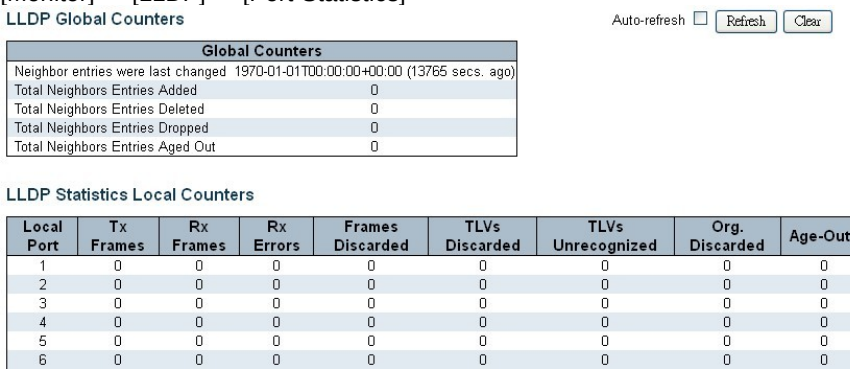
- CDP aware :
(config-if)# lldp cdp-aware
(config-if)# no lldp cdp-aware

*Status by Web* :
[Monitor] -> [LLDP] -> [Neighbors]




Click "**?**" at this web page to get details of the settings.

[Monitor] -> [LLDP] -> [Port Statistics]




Click "**?**" at this web page to get details of the settings.

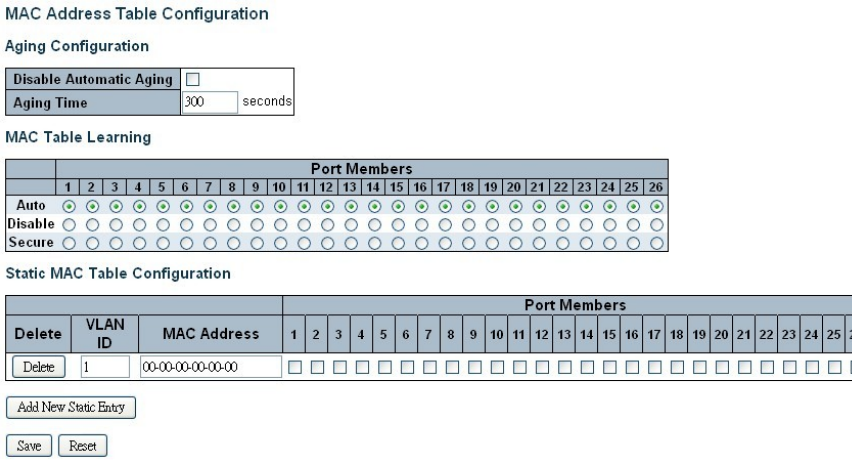
*Status by Command* :
# clear lldp statistics
# show lldp neighbors [ interface <port_type_list> ]
# show lldp statistics [ interface <port_type_list> ]

## 7.11 MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to ( based upon the DMAC address in the frame ). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.
The frames also contain a MAC address ( SMAC address ), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.

*Configuration by Web* :
[Configuration] -> [MAC Table]




Click "**?**" at this web page to get details of the settings.

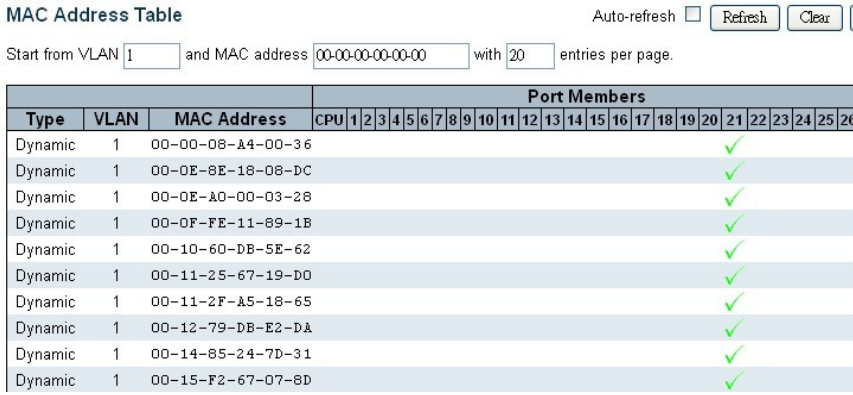
*Configuration by Command* :
Aging Configuration :
(config)# mac address-table aging-time <0,10-1000000>
(config)# no mac address-table

Static MAC Table Configuration :
(config)# mac address-table static <mac_addr> vlan <vlan_id> interface <port_type_list>
(config)# no mac address-table static <mac_addr> vlan <vlan_id> interface <port_type_list>

MAC Address Learning on Port :
(config-if)# mac address-table learning
(config-if)# no mac address-table learning

MAC Address Secure on Port :
(config-if)# mac address-table learning secure
(config-if)# no mac address-table learning secure

*Status by Web* :
[Monitor] -> [MAC Table]




Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# clear mac address-table
# show mac address-table [ conf | static | aging-time | { { learning | count } [ interface <port_type_list> ] } | { address <mac_addr> [ vlan <vlan_id> ] } | vlan <vlan_id> | interface <port_type_list> ]

## 7.12 VLAN

VLAN(Virtual LAN) is a method to restrict communication between switch ports. At layer 2, the network is partioned into multiple, distinct, mutually isolated broadcast domains.
This switch supports 802.1Q VLAN, Private VLAN, MAC-based VLAN, Protocol-based VLAN, IP Subnet-based VLAN, and Voice VLAN for different VLAN applications.

### 7.12.1 802.1Q VLAN

IEEE 802.1Q is the networking standard that supports Virtual LANs (VLANs) on an Ethernet network. The standard defines a system of VLAN tagging for Ethernet frames and the accompanying procedures to be used by bridges and switches in handling such frames.
Portions of the network which are VLAN-aware (i.e., IEEE 802.1Q conformant) can include VLAN tags. Traffic on a VLAN-unaware (i.e., IEEE 802.1D conformant) portion of the network will not contain VLAN tags. When a frame enters the VLAN-aware portion of the network, a tag is added to represent the VLAN membership of the frame's port or the port/protocol combination, depending on whether port-based or port-and-protocol-based VLAN classification is being used. Each frame must be distinguishable as being within exactly one VLAN. A frame in the VLAN-aware portion of the network that does not contain a VLAN tag is assumed to be flowing on the native (or default) VLAN.

*Configuration by Web* :
[Configuration] -> [VLANs]

Global VLAN Configuration

| | |
|---|---|
| Existing VLANs | 1 |
| Ethertype for Custom S-ports | 88A8 |

Port VLAN Configuration

| Port | Mode | Port VLAN | Port Type | Ingress Filtering | VLAN Trunking | Ingress Acceptance | Egress Tagging | Allowed VLANs | Forbidden VLANs |
|---|---|---|---|---|---|---|---|---|---|
| * | <> | 1 | <> | ☑ | ☐ | <> | <> | 1 | |
| 1 | Access | 1 | C-Port | ☑ | ☐ | Tagged and Untagged | Untag All | 1 | |
| 2 | Access | 1 | C-Port | ☑ | ☐ | Tagged and Untagged | Untag All | 1 | |
| 3 | Access | 1 | C-Port | ☑ | ☐ | Tagged and Untagged | Untag All | 1 | |
| 4 | Access | 1 | C-Port | ☑ | ☐ | Tagged and Untagged | Untag All | 1 | |
| 5 | Access | 1 | C-Port | ☑ | ☐ | Tagged and Untagged | Untag All | 1 | |
| 6 | Access | 1 | C-Port | ☑ | ☐ | Tagged and Untagged | Untag All | 1 | |
| 7 | Access | 1 | C-Port | ☑ | ☐ | Tagged and Untagged | Untag All | 1 | |
| 8 | Access | 1 | C-Port | ☑ | ☐ | Tagged and Untagged | Untag All | 1 | |
| 9 | Access | 1 | C-Port | ☑ | ☐ | Tagged and Untagged | Untag All | 1 | |
| 10 | Access | 1 | C-Port | ☑ | ☐ | Tagged and Untagged | Untag All | 1 | |

Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Add/Delete a VLAN :
(config)# vlan <vlan_list>
(config)# no vlan <vlan_list>

Ethertype for Custom S-ports :
(config)# vlan ethertype s-custom-port <0x0600-0xffff>

(config)# no vlan ethertype s-custom-port <0x0600-0xffff>

Port VLAN Configuration :
- Port Mode :
(config-if)# switchport mode { access | trunk | hybrid }
(config-if)# no switchport mode

- Port VLAN ID :
If port is in Access mode, ...
(config-if)# switchport access vlan <vlan_id>
(config-if)# no switchport access vlan
If port is in Trunk mode, ...
(config-if)# switchport trunk native vlan <vlan_id>
(config-if)# no switchport trunk native vlan <vlan_id>
If port is in Hybrid mode, ...
(config-if)# switchport hybrid native vlan { <vlan_id> | none }
(config-if)# no switchport hybrid native vlan { <vlan_id> | none }

- Port Type : (If port is in Hybrid mode.)
(config-if)# switchport hybrid port-type { unaware | c-port | s-port | s-custom-port }
(config-if)# no switchport hybrid port-type

- Ingress Filter : (If port is in Hybrid mode.)
(config-if)# switchport hybrid ingress-filtering
(config-if)# no switchport hybrid ingress-filtering

- Ingress Acceptance : (If port is in Hybrid mode.)
(config-if)# switchport hybrid acceptable-frame-type { all | tagged | untagged }
(config-if)# no switchport hybrid acceptable-frame-type

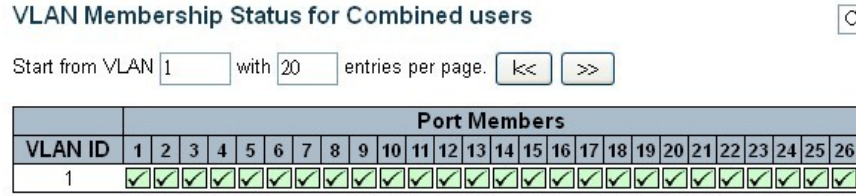
- Egress Tagging :
If port is in Trunk mode, ...
(config-if)# switchport trunk vlan tag native
(config-if)# no switchport trunk vlan tag native
If port is in Hybrid mode, ...
(config-if)# switchport hybrid egress-tag { none | all [ except-native ] }
(config-if)# no switchport hybrid egress-tag

- Allowed VLANs :
If port is in Trunk mode, ...
(config-if)# switchport trunk allowed vlan { all | none | [ add | remove | except ] <vlan_list> }
(config-if)# no switchport trunk allowed vlan
If port is in Hybrid mode, ...
(config-if)# switchport hybrid allowed vlan { all | none | [ add | remove | except ] <vlan_list> }
(config-if)# no switchport hybrid allowed vlan

- Forbidden VLANs :

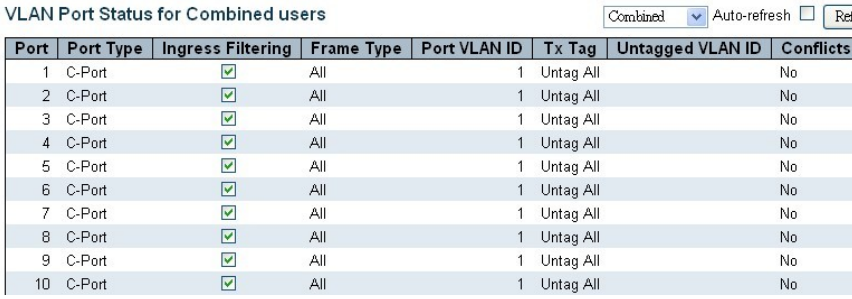
(config-if)# switchport forbidden { add | remove } { { vid <vlan_id> } | { name <word> } }
(config-if)# no switchport forbidden vlan

*Status by Web* :
[Monitor] -> [VLANs] -> [Membership]




Click "**?**" at this web page to get details of the settings.

[Monitor] -> [VLANs] -> [Ports]




| Port | Port Type | Ingress Filtering | Frame Type | Port VLAN ID | Tx Tag | Untagged VLAN ID | Conflicts |
|---|---|---|---|---|---|---|---|
| 1 | C-Port | ☑ | All | 1 | Untag All | | No |
| 2 | C-Port | ☑ | All | 1 | Untag All | | No |
| 3 | C-Port | ☑ | All | 1 | Untag All | | No |
| 4 | C-Port | ☑ | All | 1 | Untag All | | No |
| 5 | C-Port | ☑ | All | 1 | Untag All | | No |
| 6 | C-Port | ☑ | All | 1 | Untag All | | No |
| 7 | C-Port | ☑ | All | 1 | Untag All | | No |
| 8 | C-Port | ☑ | All | 1 | Untag All | | No |
| 9 | C-Port | ☑ | All | 1 | Untag All | | No |
| 10 | C-Port | ☑ | All | 1 | Untag All | | No |

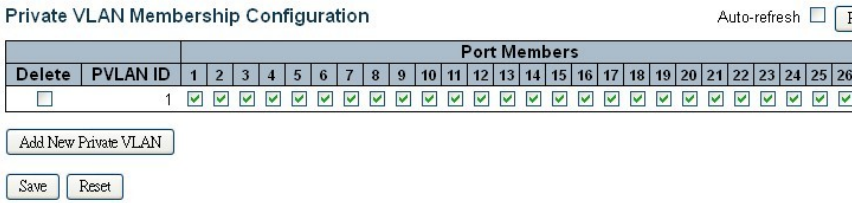
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show vlan [ id <vlan_list> | name <vword32> | brief ]

### 7.12.2 Private VLANs

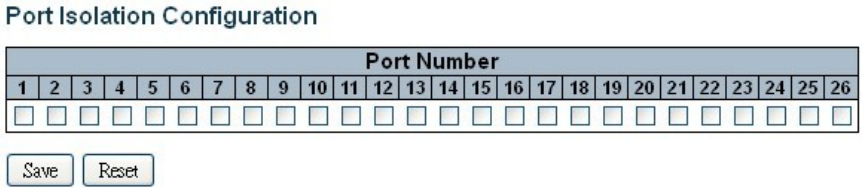
In a private VLAN, PVLANs provide layer 2 isolation between ports within the same broadcast domain. Isolated ports configured as part of PVLAN cannot communicate with each other. Member ports of a PVLAN can communicate with each other.

*Configuration by Web* :
Create/Edit Private VLAN :
[Configuration] -> [Private VLANs] -> [Membership]




Click "**?**" at this web page to get details of the settings.

Edit Port Isolation Setting :
[Configuration] -> [Private VLANs] -> [Port Isolation]




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Assign ports to Private VLAN :
(config-if)# pvlan <range_list>
(config-if)# no pvlan <range_list>

Set ports as Isolation :
(config-if)# pvlan isolation
(config-if)# no pvlan isolation

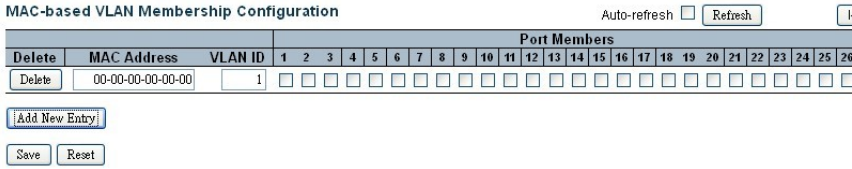
*Status by Web* :
[Configuration] -> [Private VLANs] -> [Membership]
[Configuration] -> [Private VLANs] -> [Port Isolation]
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show pvlan [ <range_list> ]

### 7.12.3 MAC-based VLAN

As a way of grouping VLAN members, MAC address-based VLAN (MAC-based VLAN) decides the VLAN for forwarding an untagged frame based on the source MAC address of the frame.

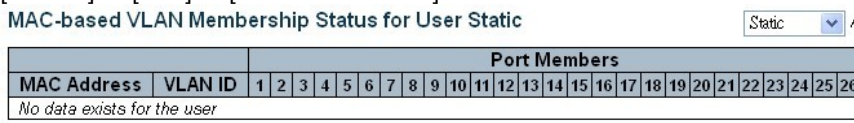
*Configuration by Web* :
[Configuration] -> [VCL] -> [MAC-based VLAN]




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Add/Remove ports to Mac-based VLAN :
(config-if)# switchport vlan mac <mac_ucast> vlan <vlan_id>
(config-if)# no switchport vlan mac <mac_ucast> vlan <vlan_id>

*Status by Web* :
[Monitor] -> [VCL] -> [MAC-based VLAN]



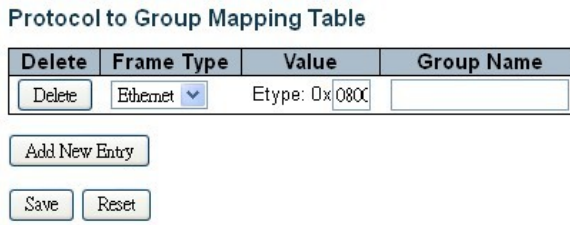

Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show vlan mac

### 7.12.4 Protocol-based VLAN

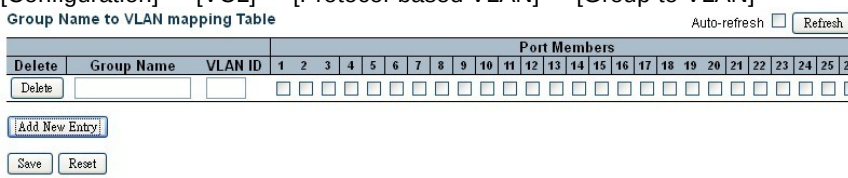
With protocol-based VLAN membership, computers are assigned to VLANs by using the protocol that is in use. For example, this method enables an Internetwork Packet Exchange (IPX) network or Internet Protocol (IP) network to have its own VLAN.

*Configuration by Web* :
Create/Delete Protocol to Group Mapping :
[Configuration] -> [VCL] -> [Protocol-based VLAN] -> [Protocol to Group]




Click "**?**" at this web page to get details of the settings.

Create/Delete Group to VLAN Mapping :
[Configuration] -> [VCL] -> [Protocol-based VLAN] -> [Group to VLAN]




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Add/Delete Protocol Group :
(config)# vlan protocol { { eth2 { <0x600-0xffff> | arp | ip | ipx | at } } | { snap { <0x0-0xffffff> | rfc_1042 | snap_8021h } <0x0-0xffff> } | { llc <0x0-0xff> <0x0-0xff> } } group <word16>
(config)# no vlan protocol { { eth2 { <0x600-0xffff> | arp | ip | ipx | at } } | { snap { <0x0-0xffffff> | rfc_1042 | snap_8021h } <0x0-0xffff> } | { llc <0x0-0xff> <0x0-0xff> } } group <word16>

Add/Remove ports to Protocol-based VLAN :
(config-if)# switchport vlan protocol group <word16> vlan <vlan_id>
(config-if)# no switchport vlan protocol group <word16> vlan <vlan_id>

*Status by Web* :
[Configuration] -> [VCL] -> [Protocol-based VLAN] -> [Protocol to Group]
[Configuration] -> [VCL] -> [Protocol-based VLAN] -> [Group to VLAN]
Click "**?**" at this web page to get details of the settings.

*Status by Command* :

# show vlan protocol [ eth2 { <0x600-0xffff> | arp | ip | ipx | at } ] [ snap { <0x0-0xffffff> | rfc_1042 | snap_8021h } <0x0-0xffff> ] [ llc <0x0-0xff> <0x0-0xff> ]

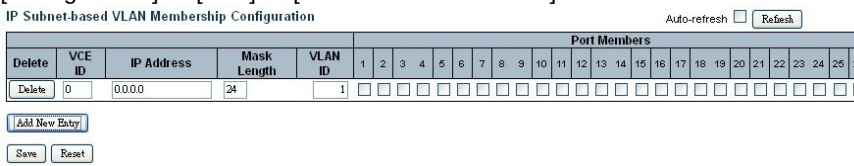
### 7.12.5 IP Subnet-based VLAN

In an IP subnet-based VLAN, all the end workstations in an IP subnet are assigned to the same VLAN. In this VLAN, users can move their workstations without reconfiguring their network addresses. IP subnet VLANs are based on Layer 3 information from packet headers. The switch makes use of the network-layer address (for example, the subnet address for TCP/IP networks) in determining VLAN membership. If a packet is untagged or priority tagged, the switch associates the packet with any matching IP subnet classification. If no IP subnet classification can be made, the packet is subjected to the normal VLAN classification rules of the switch.

This IP subnet capability does not imply a routing function or that the VLAN is routed. The IP subnet classification feature affects only the VLAN assignment of a packet. Appropriate 802.1Q VLAN configuration must exist in order for the packet to be switched.

*Configuration by Web* :

[Configuration] -> [VCL] -> [IP Subnet-based VLAN]




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :

Add/Remove ports to IP Subnet-based VLAN :

(config-if)# switchport vlan ip-subnet id <1-128> <ipv4_subnet> vlan <vlan_id>

(config-if)# no switchport vlan ip-subnet id <1~128>

*Status by Web* :

[Configuration] -> [VCL] -> [IP Subnet-based VLAN]

Click "**?**" at this web page to get details of the settings.

*Status by Command* :

# show vlan ip-subnet [ id <1-128> ]

### 7.12.6 Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

*Configuration by Web* :
Voice VLAN Configuration :
[Configuration] -> [Voice VLAN] -> [Configuration]

Voice VLAN Configuration

| | |
|---|---|
| Mode | Disabled |
| VLAN ID | 1000 |
| Aging Time | 86400 seconds |
| Traffic Class | 7 (High) |

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 |

Click "**?**" at this web page to get details of the settings.

OUI Definition :
[Configuration] -> [Voice VLAN] -> [OUI]

Voice VLAN OUI Table

| Delete | Telephony OUI | Description |
|---|---|---|
| ☐ | 00-01-e3 | Siemens AG phones |
| ☐ | 00-03-6b | Cisco phones |
| ☐ | 00-0f-e2 | H3C phones |
| ☐ | 00-60-b9 | Philips and NEC AG phones |
| ☐ | 00-d0-1e | Pingtel phones |
| ☐ | 00-e0-75 | Polycom phones |
| ☐ | 00-e0-bb | 3Com phones |

Add New Entry

Save Reset

Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Enable/Disable :
(config)# voice vlan
(config)# no voice vlan

VLAN ID :
(config)# voice vlan vid <vlan_id>
(config)# no voice vlan vid

Aging Time :
(config)# voice vlan aging-time <10-10000000>
(config)# no voice vlan aging-time

Traffic Class :
(config)# voice vlan class { <0-7> | low | normal | medium | high }
(config)# no voice vlan class

OUI Definition :
(config)# voice vlan oui <oui> [ description <line32> ]
(config)# no voice vlan oui <oui>

Port Configuration :
- Mode :
(config-if)# switchport voice vlan mode { auto | force | disable }
(config-if)# no switchport voice vlan mode

- Security :
(config-if)# switchport voice vlan security
(config-if)# no switchport voice vlan security

- Discovery Protocol :
(config-if)# switchport voice vlan discovery-protocol { oui | lldp | both }
(config-if)# no switchport voice vlan discovery-protocol

*Status by Web* :
[Configuration] -> [Voice VLAN] -> [Configuration]
[Configuration] -> [Voice VLAN] -> [OUI]
Click "**?**" at this web page to get details of the settings.

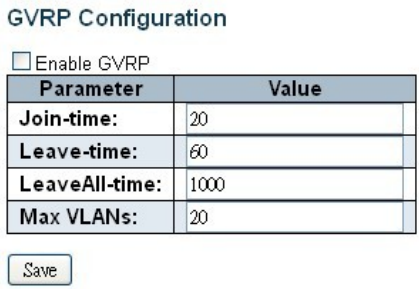
*Status by Command* :
# show voice vlan [ oui <oui> | interface <port_type_list> ]

### 7.12.7 GVRP

GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network . GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. This allows network devices to dynamically exchange VLAN configuration information with other devices.

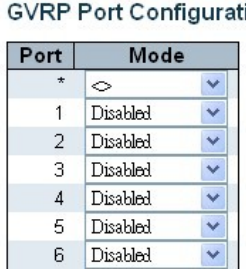
GVRP is based on GARP (Generic Attribute Registration Protocol), a protocol that defines procedures by which end stations and switches in a local area network (LAN) can register and de-register attributes, such as identifiers or addresses, with each other. Every end station and switch thus has a current record of all the other end stations and switches that can be reached. GVRP, like GARP, eliminates unnecessary network traffic by preventing attempts to transmit information to unregistered users. In addition, it is necessary to manually configure only one switch and all the other switches will be configured accordingly.

*Configuration by Web* :
General GVRP Configuration :
[Configuration] -> [GVRP] -> [Global config]




Click "**?**" at this web page to get details of the settings.

Port GVRP Configuration :
[Configuration] -> [GVRP] -> [Port config]




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :

Enable/Disable GVRP :
(config)# gvrp
(config)# no gvrp

Max. VLAN Number :
(config)# gvrp max-vlans <1-4095>
(config)# no gvrp max-vlans <1-4095>

GVRP Time Intervals :
(config)# gvrp time { [ join-time <1-20> ] [ leave-time <60-300> ] [ leave-all-time <1000-5000> ] }*1
(config)# no gvrp time { [ join-time <1-20> ] [ leave-time <60-300> ] [ leave-all-time <1000-5000> ] }*1

Enable/Disable GVRP on Port :
(config-if)# gvrp
(config-if)# no gvrp

Emit a Request for test on Port :
(config-if)# gvrp join-request vlan <vlan_list>
(config-if)# gvrp leave-request vlan <vlan_list>

*Status by Web* :
[Configuration] -> [GVRP] -> [Global config]
[Configuration] -> [GVRP] -> [Port config]
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show gvrp protocol-state interface <port_type_list> vlan <vlan_list>
# show vlan status gvrp

## 7.13 QoS

QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols. A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services. Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

Every incoming frame is classified to a QoS class, which is used throughout the device for providing queuing, scheduling and congestion control guarantees to the frame according to what was configured for that specific QoS class. There is a mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.

### 7.13.1 Port Ingress Classification

This setting is used to configure the basic QoS Ingress Classification settings for all switch ports. [DSCP Based] is used to enable/disable doing QoS by DSCP in IP header. Check it, and it is enabled.

About DSCP classification ...
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.

*Configuration by Web* :
[Configuration] -> [QoS] -> [Port Classification]

QoS Ingress Port Classification

| Port | QoS class | DP level | DSCP Based |
|---|---|---|---|
| * | <> | <> | ☐ |
| 1 | 0 | 0 | ☐ |
| 2 | 0 | 0 | ☐ |
| 3 | 0 | 0 | ☐ |
| 4 | 0 | 0 | ☐ |
| 5 | 0 | 0 | ☐ |
| 6 | 0 | 0 | ☐ |
| 7 | 0 | 0 | ☐ |
| 8 | 0 | 0 | ☐ |

Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Port Ingress QoS Class :

(config-if)# qos cos <0-7>
(config-if)# no qos cos

Port Ingress DPL :
(config-if)# qos dpl <dpl>
(config-if)# no qos dpl

Enable/Disable DSCP QoS on Port :
(config-if)# qos trust dscp
(config-if)# no qos trust dscp

*Status by Web* :
[Configuration] -> [QoS] -> [Port Classification]
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show qos interface [ <port_type_list> ]

### 7.13.2 Port Ingress Policers

This setting 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

*Configuration by Web* :
[Configuration] -> [QoS] -> [Port Policing]

QoS Ingress Port Policers

| Port | Enabled | Rate | Unit | Flow Control |
|---|---|---|---|---|
| * | ☐ | 500 | <> | ☐ |
| 1 | ☐ | 500 | kbps | |
| 2 | ☐ | 500 | kbps | |
| 3 | ☐ | 500 | kbps | |
| 4 | ☐ | 500 | kbps | |
| 5 | ☐ | 500 | kbps | |
| 6 | ☐ | 500 | kbps | |
| 7 | ☐ | 500 | kbps | |
| 8 | ☐ | 500 | kbps | |

Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Port Ingress Policer :
(config-if)# qos policer <uint> [ fps ] [ flowcontrol ]
(config-if)# no qos policer

*Status by Web* :
[Configuration] -> [QoS] -> [Port Policing]
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show qos interface [ <port_type_list> ]

### 7.13.3 Port and Queue Egress Shapers

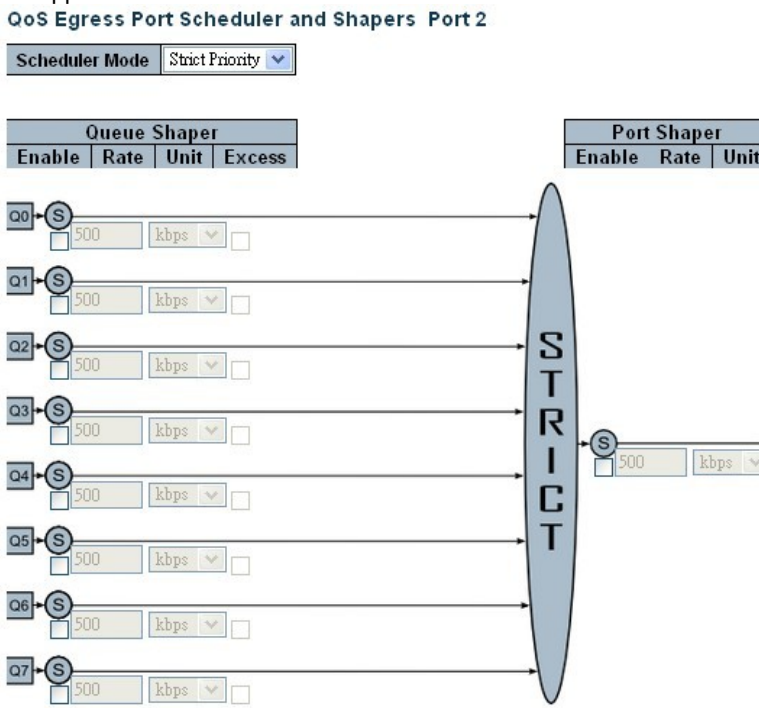
This setting will show egress shaper settings of each port and each queue.
Click Port number to configure its Egress Shaper.

*Configuration by Web* :
[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 | disabled | 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 |

Click port number, port and queue egress scheduler and shapers setting page will appear.




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
Click “**?**” at this web page to get details of the settings.

*Configuration by Command* :
Port Egress Shaper :
(config-if)# qos shaper <uint>
(config-if)# no qos shaper

Queue Egress Shaper of Port :
(config-if)# qos queue-shaper queue <0~7> <uint> [ excess ]
(config-if)# no qos queue-shaper queue <0~7>

*Status by Web* :
[Configuration] -> [QoS] -> [Port Shaping]
Click “**?**” at this web page to get details of the settings.

*Status by Command* :
# show qos interface [ <port_type_list> ]

### 7.13.4 Port Egress Schedulers

This setting will show port egress scheduler mode and weight of each queue.
Click Port number to configure its Egress Scheduler.

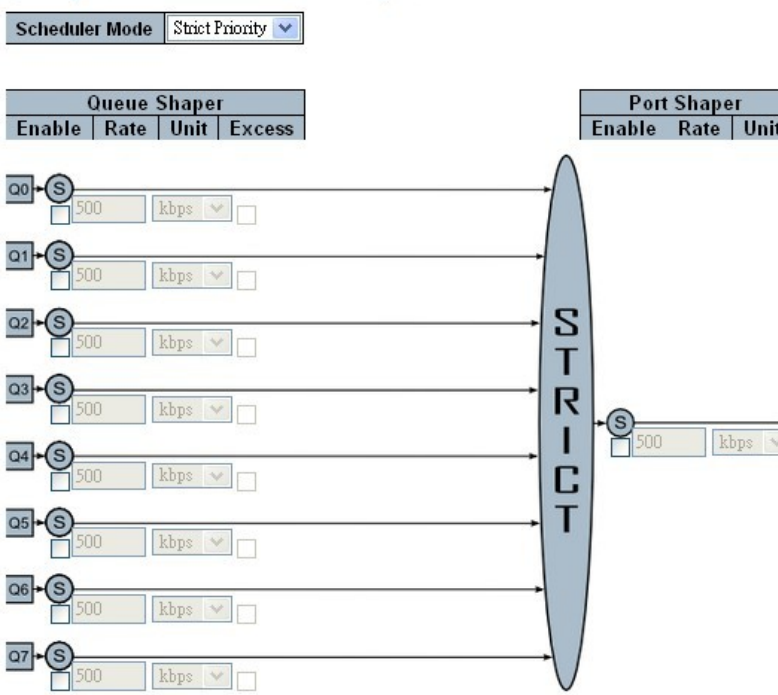
*Configuration by Web* :
[Configuration] -> [QoS] -> [Port Scheduler]

**QoS Egress Port Schedulers**

| Port | Mode | Weight | | | | | |
|---|---|---|---|---|---|---|---|
| | | Q0 | Q1 | Q2 | Q3 | Q4 | Q5 |
| 1 | Strict Priority | - | - | - | - | - | - |
| 2 | Strict Priority | - | - | - | - | - | - |
| 3 | Strict Priority | - | - | - | - | - | - |
| 4 | Strict Priority | - | - | - | - | - | - |
| 5 | Strict Priority | - | - | - | - | - | - |
| 6 | Strict Priority | - | - | - | - | - | - |
| 7 | Strict Priority | - | - | - | - | - | - |
| 8 | Strict Priority | - | - | - | - | - | - |

Click port number, port and queue egress scheduler and shapers setting page will appear.

**QoS Egress Port Scheduler and Shapers Port 2**




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
Click “**?**” at this web page to get details of the settings.

*Configuration by Command* :
Weighting of Queue for WRR :
(config-if)# qos wrr <1-100> <1-100> <1-100> <1-100> <1-100> <1-100>
(config-if)# no qos wrr

*Status by Web* :
[Configuration] -> [QoS] -> [Port Scheduler]
Click “**?**” at this web page to get details of the settings.

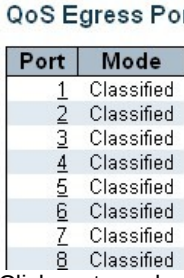
*Status by Command* :
# show qos interface [ <port_type_list> ]

### 7.13.5 Port Egress Tag Remarking

This setting 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.

*Configuration by Web* :
[Configuration] -> [QoS] -> [Port Tag Remarking]




Click port number, port egress tag remarking setting page will apear.

If in Classified mode, ...


If in Default mode, ...


If in Mapped mode, ...

QoS Egress Port Tag Remarking Port 2

| Tag Remarking Mode | Mapped |
|---|---|

DP level Configuration

| Classified DP level | DP level |
|---|---|
| 0 | 0 |
| 1 | 1 |
| 2 | 1 |
| 3 | 1 |

(QoS class, DP level) to (PCP, DEI) Mapping

| QoS class | DP level | PCP | DEI |
|---|---|---|---|
| * | * | <> | <> |
| 0 | 0 | 1 | 0 |
| 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 1 |

Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Default PCP and DEI setting :
(config-if)# qos tag-remark pcp <0-7> dei <0-1>
(config-if)# no qos tag-remark

Map PCP and DEI setting :
(config-if)# qos tag-remark mapped [ yellow <0-4> ]
(config-if)# no qos tag-remark

Internal Priority to PCP and DEI Map : (Egress)
(config-if)# qos map cos-tag cos <0~7> dpl <0~1> pcp <0-7> dei <0-1>
(config-if)# no qos map cos-tag cos <0~7> dpl <0~1>

*Status by Web* :
[Configuration] -> [QoS] -> [Port Tag Remarking]
Click port number, port egress tag remarking setting page will apear.
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show qos interface [ <port_type_list> ]

### 7.13.6 Port DSCP Configuration

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”. 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: Rewrite enabled with remapping setting in [DSCP Translation] page from the internal DSCP value.

*Configuration by Web* :
[Configuration] -> [QoS] -> [Port DSCP]

QoS Port DSCP Configuration

| Port | Ingress | | Egress |
|---|---|---|---|
| | Translate | Classify | Rewrite |
| * | ☐ | <> | <> |
| 1 | ☐ | Disable | Disable |
| 2 | ☐ | Disable | Disable |
| 3 | ☐ | Disable | Disable |
| 4 | ☐ | Disable | Disable |
| 5 | ☐ | Disable | Disable |
| 6 | ☐ | Disable | Disable |

Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Ingress DSCP Translate Enable/Disable :
(config-if)# qos dscp-translate
(config-if)# no qos dscp-translate

Ingress Classify DSCP values :
(config-if)# qos dscp-classify { zero | selected | any }
(config-if)# no qos dscp-classify

Egress DSCP Rewrite : :
(config-if)# qos dscp-remark { rewrite | remap | remap-dp }
(config-if)# no qos dscp-remark

*Status by Web* :
[Configuration] -> [QoS] -> [Port DSCP]
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show qos interface [ <port_type_list> ]

### 7.13.7 DSCP to Internal Priority Mapping (Ingress)

This setting 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 will not be applied.

*Configuration by Web* :

[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 |
| 7 | ☐ | 0 | 0 |

Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :

DSCP to Internal Priority Mapping and trust :

(config)# qos map dscp-cos { <0~63> | <dscp> } cos <0-7> dpl <dpl>

(config)# no qos map dscp-cos { <0~63> | <dscp> }

*Status by Web* :

[Configuration] -> [QoS] -> [DSCP-Based QoS]

Click "**?**" at this web page to get details of the settings.

*Status by Command* :

# show qos maps dscp-cos cos-dscp

### 7.13.8 DSCP Ingress Translation and Egress Remap

This setting is used to configure the 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, the settings are applied to Egress Rewrite in [Port DSCP] page. Please refer to the description about Egress Rewrite in [Port DSCP] page

*Configuration by Web* :

[Configuration] -> [QoS] -> [DSCP Translation]

DSCP Translation

| DSCP | Ingress | | Egress |
|---|---|---|---|
| | Translate | Classify | Remap |
| * | <> | ☐ | <> |
| 0 (BE) | 0 (BE) | ☐ | 0 (BE) |
| 1 | 1 | ☐ | 1 |
| 2 | 2 | ☐ | 2 |
| 3 | 3 | ☐ | 3 |
| 4 | 4 | ☐ | 4 |
| 5 | 5 | ☐ | 5 |
| 6 | 6 | ☐ | 6 |
| 7 | 7 | ☐ | 7 |

Click “**?**” at this web page to get details of the settings.

*Configuration by Command* :

Ingress DSCP values translation mapping :

(config)# qos map dscp-ingress-translation { <0~63> | <dscp> } to { <0-63> | <dscp> }

(config)# no qos map dscp-ingress-translation { <0~63> | <dscp> }

DSCP values selected for ingress classify :

(config)# qos map dscp-classify { <0~63> | <dscp> }

(config)# no qos map dscp-classify { <0~63> | <dscp> }

Egress DSCP values translation mapping :

(config)# qos map dscp-egress-translation { <0~63> | <dscp> } <0~1> to { <0-63> | <dscp> }

(config)# no qos map dscp-egress-translation { <0~63> | <dscp> } <0~1>

*Status by Web* :
[Configuration] -> [QoS] -> [DSCP Translation]
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
Ingress DSCP values translation mapping :
# show qos maps dscp-ingress-translation

DSCP values selected for ingress classify :
# show qos maps dscp-classify

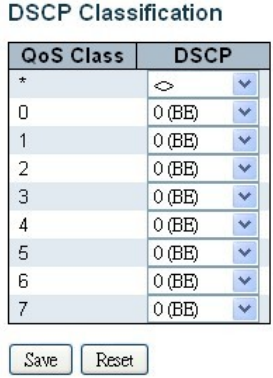
Egress DSCP values translation mapping :
# show qos maps dscp-egress-translation

### 7.13.9 Internal Priority to DSCP Mapping (Egress)

This setting is used to configure the mapping of QoS class 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

*Configuration by Web* :
[Configuration] -> [QoS] -> [DSCP Classification]




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Internal Priority to DSCP Mapping :
(config)# qos map cos-dscp <0~7> dscp { <0-63> | <dscp> }
(config)# no qos map cos-dscp <0~7>

*Status by Web* :
[Configuration] -> [QoS] -> [DSCP Classification]
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
Internal Priority to DSCP Mapping :
# show qos maps cos-dscp

### 7.13.10 QoS Control List

QCL is an acronym for QoS Control List. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects.
Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.
QCE is an acronym for QoS Control Entry. It describes QoS class associated with a particular QCE ID.

*Configuration by Web* :
[Configuration] -> [QoS] -> [QoS Control List]

QoS Control List Configuration

| QCE | Port | DMAC | SMAC | Tag Type | VID | PCP | DEI | Frame Type | Action | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | CoS | DPL | DSCP | ⊕ |

Click “(+)” to create a QoS Control Entry.

QCE Configuration

| Port Members | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |

Key Parameters

| | |
|---|---|
| Tag | Any |
| VID | Any |
| PCP | Any |
| DEI | Any |
| SMAC | Any |
| DMAC Type | Any |
| Frame Type | Any |

Action Parameters

| | |
|---|---|
| Class | 0 |
| DPL | Default |
| DSCP | Default |

Click “**?**” at this web page to get details of the settings.

*Configuration by Command* :
Create/Edit a QoS Control Entry :
- Setup matched DMAC :
(config)# qos qce <1-256> dmac { unicast | multicast | broadcast | any }
- Setup matched frame type :
(config)# qos qce <1-256> frame-type { any | { etype [ { <0x600-0x7ff,0x801-0x86dc,0x86de-0xffff> | any } ] } | { llc [ dsap { <0-0xff> | any } ] [ ssap { <0-0xff> | any } ] [ control { <0-0xff> | any } ] } | { snap [ { <0-0xffff> | any } ] }
- Setup port members :
(config)# qos qce <1-256> interface <port_type_list>
- Setup matched SMAC :
(config)# qos qce <1-256> smac { <mac_addr> | <oui> | any }
- Setup tag options :
(config)# qos qce <1-256> tag { [ type { untagged | tagged | c-tagged | s-tagged | any } ] [ vid { <vcap_vr> | any } ] [ pcp { <pcp> | any } ] [ dei { <0-1> | any } ] }*1 ]

- Setup action :
(config)# qos qce <1-256> action { [ cos { <0-7> | default } ] [ dpl { <0-1> | default } ] [ dscp { <0-63> | <dscp> | default } ]
- Place QCE before the next QCE ID
(config)# qos qce <1-256> next <uint>
- Place QCE at the end
(config)# qos qce <1-256> last

Delete a QoS Control Entry :
(config)# no qos qce <1~256>

Refresh QCE tables in hardware :
(config)# qos qce refresh

*Status by Web* :
[Configuration] -> [QoS] -> [QoS Control List]
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show qos qce [ <1-256> ]

### 7.13.11 Port Storm Control

This setting allows you to configure the storm control settings for all switch ports.
There is a storm rate control for unicast frames, broadcast frames and unknown (flooded) frames.

*Configuration by Web* :
[Configuration] -> [QoS] -> [Storm Control]

QoS Port Storm Control

| Port | Unicast Frames | | | Broadcast Frames | | | Unknown Frames | | |
|---|---|---|---|---|---|---|---|---|---|
| | Enabled | Rate | Unit | Enabled | Rate | Unit | Enabled | Rate | Unit |
| * | ☐ | 500 | <> | ☐ | 500 | <> | ☐ | 500 | <> |
| 1 | ☐ | 500 | kbps | ☐ | 500 | kbps | ☐ | 500 | kbps |
| 2 | ☐ | 500 | kbps | ☐ | 500 | kbps | ☐ | 500 | kbps |
| 3 | ☐ | 500 | kbps | ☐ | 500 | kbps | ☐ | 500 | kbps |
| 4 | ☐ | 500 | kbps | ☐ | 500 | kbps | ☐ | 500 | kbps |
| 5 | ☐ | 500 | kbps | ☐ | 500 | kbps | ☐ | 500 | kbps |
| 6 | ☐ | 500 | kbps | ☐ | 500 | kbps | ☐ | 500 | kbps |
| 7 | ☐ | 500 | kbps | ☐ | 500 | kbps | ☐ | 500 | kbps |
| 8 | ☐ | 500 | kbps | ☐ | 500 | kbps | ☐ | 500 | kbps |
| 9 | ☐ | 500 | kbps | ☐ | 500 | kbps | ☐ | 500 | kbps |
| 10 | ☐ | 500 | kbps | ☐ | 500 | kbps | ☐ | 500 | kbps |

Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Enable/Rate Setting :
(config-if)# qos storm { unicast | broadcast | unknown } <100-13200000> [ fps ]

Disable :
(config-if)# no qos storm { unicast | broadcast | unknown }

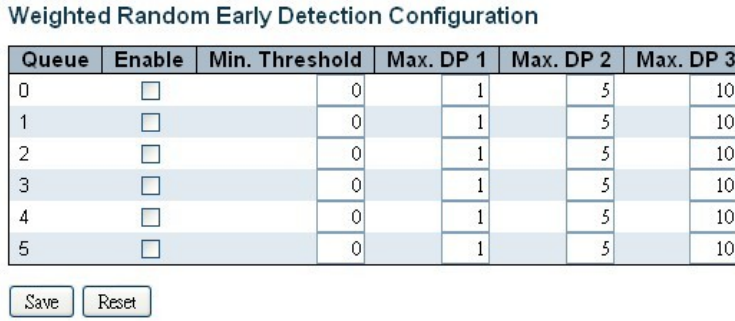
*Status by Web* :
[Configuration] -> [QoS] -> [Storm Control]
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show qos interface [ <port_type_list> ]

### 7.13.12 Weighted Random Early Detection Configuration

Weighted random early detection (WRED) is a queueing discipline for a network scheduler suited for congestion avoidance. It is an extension to random early detection (RED) where a single queue may have several different queue thresholds. Each queue threshold is associated to a particular traffic class.
For example, a queue may have lower thresholds for lower priority packet. A queue buildup will cause the lower priority packets to be dropped, hence protecting the higher priority packets in the same queue. In this way quality of service prioritization is made possible for important packets from a pool of packets using the same buffer.
It is more likely that standard traffic will be dropped instead of higher prioritized traffic.

*Configuration by Web* :
[Configuration] -> [QoS] -> [WRED]




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
(config)# qos wred queue <0~5> min_th <0-100> mdp_1 <0-100> mdp_2 <0-100> mdp_3 <0-100>
(config)# no qos wred queue <0~5>

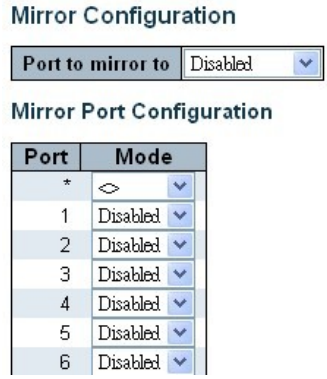
*Status by Web* :
[Configuration] -> [QoS] -> [WRED]
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show qos wred

## 7.14 Port Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)
Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

*Configuration by Web* :
[Configuration] -> [Mirroring]




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Mirroring Destination Port :
(config)# monitor destination interface <port_type_id>
(config)# no monitor destination

Mirroring Source Port :
(config)# monitor source { { interface <port_type_list> } | { cpu [ <range_list> ] } } { both | rx | tx }
(config)# no monitor source { { interface <port_type_list> } | { cpu [ <range_list> ] } }

*Status by Web* :
[Configuration] -> [Mirroring]
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# show running-config feature monitor

## 7.15 sFlow

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.
Additional information can be found at http://sflow.org.

*Configuration by Web* :
[Configuration] -> [sFlow]

**sFlow Configuration**

**Agent Configuration**

| IP Address | 127.0.0.1 |
|---|---|

**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 |

Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Agent IP Address :
(config)# sflow agent-ip { ipv4 <ipv4_addr> | ipv6 <ipv6_addr> }
(config)# no sflow agent-ip

Receiver Configuration :
- Receiver IP Address :
(config)# sflow collector-address [ receiver <range_list> ] [ <word> ]
(config)# no sflow collector-address [ receiver <range_list> ]
- Receiver UDP Port :
(config)# sflow collector-port [ receiver <range_list> ] <1-65535>
(config)# no sflow collector-port [ receiver <range_list> ]
- Timeout Interval :
(config)# sflow timeout [ receiver <range_list> ] <0-2147483647>

(config)# no sflow timeout [ receiver <range_list> ]
- Max. Datagram Size
(config)# sflow max-datagram-size [ receiver <range_list> ] <200-1468>
(config)# no sflow max-datagram-size [ receiver <range_list> ]

Configuration on Port :
- Counter Poller :
(config-if)# sflow counter-poll-interval [ sampler <range_list> ] [ <1-3600> ]
(config-if)# no sflow counter-poll-interval [ <range_list> ]
- Flow Sampler Enable/Disable :
(config-if)# sflow [ <range_list> ]
(config-if)# no sflow [ <range_list> ]
- Flow Sampler Max. Size :
(config-if)# sflow max-sampling-size [ sampler <range_list> ] [ <14-200> ]
(config-if)# no sflow max-sampling-size [ sampler <range_list> ]
- Flow Sampler Sampling Rate :
(config-if)# sflow sampling-rate [ sampler <range_list> ] [ <1-4294967295> ]

*Status by Web* :
[Monitor] -> [sFlow]

**sFlow Statistics**

**Receiver Statistics**

| | |
|---|---|
| Owner | <none> |
| IP Address/Hostname | 0.0.0.0 |
| Timeout | 0 |
| Tx Successes | 0 |
| Tx Errors | 0 |
| Flow Samples | 0 |
| Counter Samples | 0 |

**Port Statistics**

| Port | Rx Flow Samples | Tx Flow Samples | Counter Samples |
|---|---|---|---|
| 1 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 |

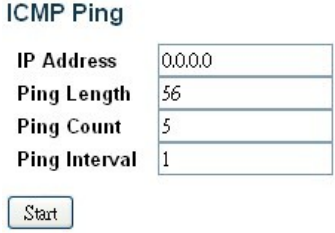
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
# clear sflow statistics { receiver [ <range_list> ] | samplers [ interface [ <range_list> ] <port_type_list> ] }
# show sflow
# show sflow statistics { receiver [ <range_list> ] | samplers [ interface [ <range_list> ] <port_type_list> ] }

## 7.16 Diagnostics

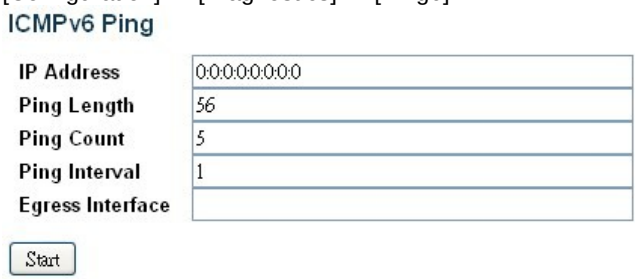
This switch supports network connection diagnostics by ping test and TX port cable connection test.

*Configuration by Web* :
Ping by IPv4 :
[Configuration] -> [Diagnostics] -> [Ping]



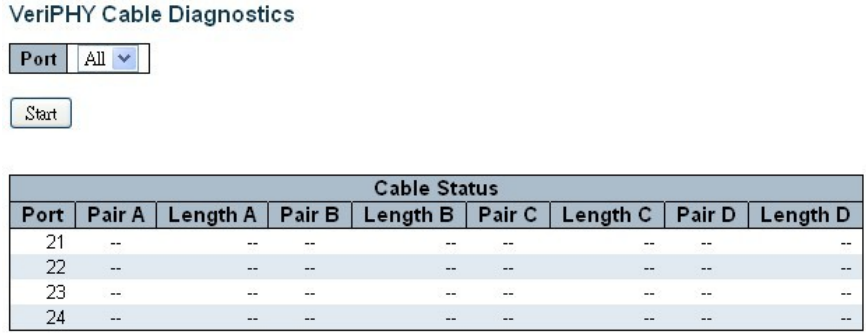

Click "**?**" at this web page to get details of the settings.

Ping by IPv6 :
[Configuration] -> [Diagnostics] -> [Ping6]




Click "**?**" at this web page to get details of the settings.

Verify Cable Connection :
[Configuration] -> [Diagnostics] -> [VeriPHY]




Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
Ping by IPv4 :
# ping ip <word1-255> [ repeat <1-60> ] [ size <2-1452> ] [ interval <0-30> ]

Ping by IPv6 :
# ping ipv6 <ipv6_addr> [ repeat <1-60> ] [ size <2-1452> ] [ interval <0-30> ] [ interface vlan <vlan_id> ]

Verify Cable Connection :
# show interface <port_type_list> veriphy

*Status by Web* :
Ping by IPv4 :
[Configuration] -> [Diagnostics] -> [Ping]
Click "**?**" at this web page to get details of the settings.

Ping by IPv6 :
[Configuration] -> [Diagnostics] -> [Ping6]
Click "**?**" at this web page to get details of the settings.

Verify Cable Connection :
[Configuration] -> [Diagnostics] -> [VeriPHY]
Click "**?**" at this web page to get details of the settings.

*Status by Command* :
Ping by IPv4 :
# ping ip <word1-255> [ repeat <1-60> ] [ size <2-1452> ] [ interval <0-30> ]

Ping by IPv6 :
# ping ipv6 <ipv6_addr> [ repeat <1-60> ] [ size <2-1452> ] [ interval <0-30> ] [ interface vlan <vlan_id> ]

Verify Cable Connection :
# show interface <port_type_list> veriphy
Note : This test supports TX ports cable connection only.

## 7.17 Maintenance

The maintenance functions for the switch include system reboot, software update/select, configuration backup/restore/factory default.

*Configuration by Web* :
System Reboot :
[Configuration] -> [Maintenance] -> [Restart Device]


Click "**?**" at this web page to get details of the settings.

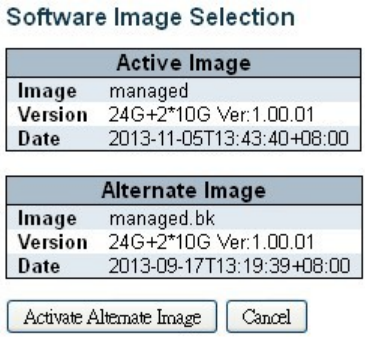
Factory Default :
[Configuration] -> [Maintenance] -> [Factory Defaults]


Click "**?**" at this web page to get details of the settings.

Software Upload :
[Configuration] -> [Maintenance] -> [Software] -> [Upload]


Click "**?**" at this web page to get details of the settings.

Software Image Select :
[Configuration] -> [Maintenance] -> [Software] -> [Image Select]

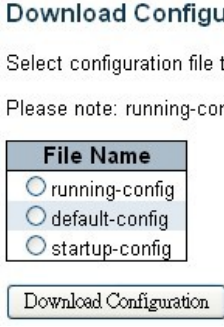



Click "**?**" at this web page to get details of the settings.

Configuration :
- Save running-config to startup-config :
[Configuration] -> [Maintenance] -> [Configuration] -> [Save startup-config]

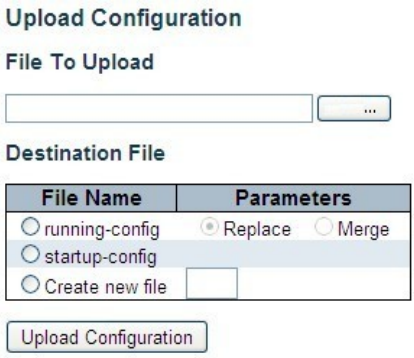

Click "**?**" at this web page to get details of the settings.

- Configuration Download :
[Configuration] -> [Maintenance] -> [Configuration] -> [Download]



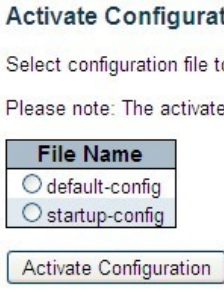

Click "?" at this web page to get details of the settings.

- Configuration Upload :
[Configuration] -> [Maintenance] -> [Configuration] -> [Upload]




Click "**?**" at this web page to get details of the settings.

- Configuration Activate :
[Configuration] -> [Maintenance] -> [Configuration] -> [Activate]




Click "**?**" at this web page to get details of the settings.

- Configuration Delete :
[Configuration] -> [Maintenance] -> [Configuration] -> [Delete]


Click "**?**" at this web page to get details of the settings.

*Configuration by Command* :
System Reboot :
# reload cold

Factory Default :
# reload defaults [ keep-ip ]

Software Upload :
# firmware upgrade <tftp://server/path-and-filename>

Software Image Select :
# firmware swap

Configuration :
- Save running-config to startup-config :
# copy running-config startup-config
- Configuration Download :
# copy { startup-config | running-config } <tftp://server/path-and-filename> [ syntax-check ]
- Configuration Upload :
# copy <tftp://server/path-and-filename> { startup-config | running-config } [ syntax-check ]
- Configuration Activate :
# copy { startup-config | default-config | <word> } running-config
- Configuration Delete :
# delete <word>

Terminal Configuration :
- Enable command line editing
# terminal editing
# no terminal editing
- Set the EXEC timeout
# terminal exec-timeout <0-1440> [ <0-3600> ]
# no terminal exec-timeout
- Description of the interactive help system
# terminal help
- Control the command history function
# terminal history size <0-32>
# no terminal history size
- Set number of lines on a screen
# terminal length <0,3-512>
# no terminal length
- Set width of the display terminal
# terminal width <0,40-512>
# no terminal width

*Status by Web* :
System Reboot :
[Configuration] -> [Maintenance] -> [Restart Device]
Click "**?**" at this web page to get details of the settings.

Factory Default :
[Configuration] -> [Maintenance] -> [Factory Defaults]
Click "**?**" at this web page to get details of the settings.

Software Upload :
[Configuration] -> [Maintenance] -> [Software] -> [Upload]

Click “**?**” at this web page to get details of the settings.

Software Image Select :
[Configuration] -> [Maintenance] -> [Software] -> [Image Select]
Click “**?**” at this web page to get details of the settings.

Configuration :
- Save running-config to startup-config :
[Configuration] -> [Maintenance] -> [Configuration] -> [Save startup-config]
Click “**?**” at this web page to get details of the settings.
- Configuration Download :
[Configuration] -> [Maintenance] -> [Configuration] -> [Download]
Click “**?**” at this web page to get details of the settings.
- Configuration Upload :
[Configuration] -> [Maintenance] -> [Configuration] -> [Upload]
Click “**?**” at this web page to get details of the settings.
- Configuration Activate :
[Configuration] -> [Maintenance] -> [Configuration] -> [Activate]
Click “**?**” at this web page to get details of the settings.
- Configuration Delete :
[Configuration] -> [Maintenance] -> [Configuration] -> [Delete]
Click “**?**” at this web page to get details of the settings.

*Status by Command* :
Show running configuration :
# show running-config [ all-defaults ]
# show running-config feature <cword> [ all-defaults ]
# show running-config interface <port_type_list> [ all-defaults ]
# show running-config interface vlan <vlan_list> [ all-defaults ]
# show running-config line { console | vty } <range_list> [ all-defaults ]
# show running-config vlan <vlan_list> [ all-defaults ]

Show Terminal Configuration :
# show terminal

# 8. Software Update and Backup

This switch supports software update and configuration backup/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 7.17 for Software Update and Configuration Backup/Restore.

2. **From console/telnet command**: Doing by TFTP protocol and done by "copy" command. Please refer to the description of "*Maintenance*" function in Section 7.17.

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

## [ 24SFP+4TX(combo) Model ]

| | |
|---|---|
| **Access Method** | Ethernet, CSMA/CD |
| **Standards Conformance** | IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE<br>IEEE 802.3z, IEEE 802.3ab (1000Base) |
| **Communication Rate** | 10/100/1000Mbps for TX, Full / Half duplex (auto-negotiation)<br>100/1000Mbps for SFP |
| **TX MDI/MDIX** | Auto-Detect |
| **Indicator Panel** | LEDs for each unit : Power, System<br>each port : Link/Act(Green:1000M, Yellow:10/100M) |
| **Number of Ports** | 24* SFP, 4* RJ45 TX ports, (24 GE Ports totally) |
| **Console** | D-Sub 9 |
| | |
| **Dimensions** | 440 x 172 x 44 mm |
| **Certification** | CE Mark, FCC Class A |
| **Temperature** | Standard Operating: 0 to 50℃ |
| **Humidity** | 10% to 90% (Non-condensing) |
| | |
| **Bridging Function** | Filtering, forwarding and learning |
| **Switching Method** | Store-and-forward |
| **Address Table** | 16K entries |
| **Filtering/Forwarding Rate** | Line speed |
| **Maximum Packet Size** | 10056 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<br>Port Auto MDI/MDI-X<br>Port frame size (jumbo frames), Maximum ingress frame size (10056 bytes)<br>Port state (administrative status)<br>Port status (link monitoring)<br>Port statistics (MIB counters) |
| **L2 Switching** | Auto MAC address learning/aging and MAC addresses (static)<br>DHCP snooping<br>ARP inspection<br>Port Mirroring |
| **L3 Switching** | DHCP option 82 relay<br>IPv4 Unicast: Static routing |
| **VLANs** | IEEE 802.1Q static VLAN(4096 entries Max.), Voice VLAN, Port isolation, Private VLAN, MAC based VLAN, Protocol based VLAN, IP subnet based VLAN |
| **Spanning Tree** | IEEE 802.1s MSTP(Multiple spanning tree)<br>IEEE 802.1w RSTP(Rapid spanning tree)<br>IEEE 802.1D STP(Spanning tree)<br>BPDU Guard & Restricted Role |
| **Link Aggregation** | Static and LACP |
| **IP Multicast** | IGMP v2 and v3 snooping<br>MLD v1 snooping<br>IGMP filtering profile<br>IPMC throttling, filtering, leave proxy<br>MVR and MVR profile |
| **QoS** | Traffic Classes (8 active priorities)<br>Port Default Priority, User Priority,<br>Input priority mapping<br>QoS Control List (QCL Mode)<br>Storm Control for UC, BC and Unknown<br>Port policers<br>Global/VCAP (ACL) policers<br>Port egress shaper<br>Queue egress shapers<br>DiffServ (RFC2474) remarking<br>Tag remarking<br>Scheduler mode |

| | |
|---|---|
| **Security** | Port-Based 802.1X, Single 802.1X, Multiple 802.1X,<br>MAC-Based Authentication<br>VLAN Assignment , QoS Assignment, Guest VLAN<br>RADIUS Accounting<br>MAC Address Limit<br>IP MAC binding, IP/MAC binding dynamic to static<br>TACACS+<br>Web & CLI Authentication<br>Authorization (15 user levels)<br>ACLs for filtering/policing/port copy<br>IP source guard |
| **Synchronization** | NTPv4 Client |
| **SFP DDMI** | Yes |
| **Management** | DHCP Client,<br>DNS client, proxy<br>HTTP Server<br>CLI - Console Port & Telnet<br>Text Configuration download or upload<br>Management access filtering<br>HTTPS<br>SSHv2<br>IPv6 Management<br>System Syslog<br>Software Upload via web<br>SNMP v1 / v2c / v3 Agent<br>RMON (Group 1, 2, 3 & 9)<br>RMON alarm and event(CLI,web)<br>SNMP multiple trap destinations<br>IEEE 802.1AB-2005 Link Layer Discovery LLDP<br>Cisco™ Discovery filtering - CDP<br>sFlow<br>Daylight Saving |

# 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