Communicate via ***Micro network***

Micronet®
Making Communication Easier

User Manual

26-PORT GIGABIT MANAGED PoE SWITCH

Model No.: SP6526P

About This Manual

Copyright

Copyright © 2017 Manufacture Technology Corp. All rights reserved.

The products and programs described in this User Guide are licensed products of Manufacture Technology, This User Guide contains proprietary information protected by copyright, and this User Guide and all accompanying hardware, software and documentation are copyrighted. No parts of this User Guide may be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine-readable from by any means by electronic or mechanical. Including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of Manufacture Technology.

.

Purpose

This GUI user guide gives specific information on how to operate and use the management functions of the SP6526P via HTTP/HTTPs web browser

Audience

The Manual is intended for use by network administrators who are responsible for operating and maintaining network equipment; consequently, it assumes a basic working knowledge of general switch functions, the Internet Protocol (IP), and Hypertext Transfer Protocol (HTTP).

CONVENTIONS

The following conventions are used throughout this manual to show information.

WARRANTY

See the Customer Support/ Warranty booklet included with the product. A copy of the specific warranty terms applicable to your Manufacture products and replacement parts can be obtained from your Manufacture Sales and Service Office authorized dealer.

Disclaimer

Manufacture Technology does not warrant that the hardware will work properly in all environments and applications, and marks no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose. Manufacture disclaims liability for any inaccuracies or omissions that may have occurred. Information in this User Guide is subject to change without notice and does not represent a commitment on the part of Manufacture. Manufacture assumes no responsibility for any inaccuracies that may be contained in this User Guide. Manufacture makes no commitment to update or keep current the information in this User Guide, and reserves the righter to make improvements to this User Guide and /or to the products described in this User Guide, at any time without notice.

Table of Contents

ABOUT THIS MANUAL .... **II**

INTRODUCTION **1**

CHAPTER 1 OPERATION OF WEB-BASED MANAGEMENT **2**

CHAPTER 2 FIRST TIME WIZARD **3**

CHAPTER 3 SYSTEM **6**

3-1 SYSTEM INFORMATION 6
3-2 IP ADDRESS 9
3-2.1 IP Settings *9*
3-2.2 Advanced IP Settings *11*
3-2.3 Status *14*
3-3 SYSTEM TIME 17
3-4 LOG 20
3-4.1 Syslog Configuration *20*
3-4.2 View Log *22*
3-5 LLDP 24
3-5.1 LLDP Configuration *24*
3-5.2 LLDP-MED Configuration *27*
3-5.3 LLDP Neighbour *34*
3-5.4 LLDP-MED Neighbour *36*
3-5.5 LLDP Statistics *40*
3-6 UPNP 42

CHAPTER 4 PORT MANAGEMENT **44**

4-1 PORT CONFIGURATION 44
4-2 PORT STATISTICS 47
4-3 SFP PORT INFO 51
4-4 ENERGY EFFICIENT ETHERNET 53
4-5 LINK AGGREGATION 54
4-5.1 Port *54*
4-5.2 Aggregator View *56*
4-5.3 Aggregation Hash Mode *58*
4-5.4 LACP System Priority *60*
4-6 LOOP PROTECTION 61
4-6.1 Configuration *61*
4-6.2 Status *63*

CHAPTER 5 POE MANAGEMENT **65**

5-1 POE CONFIGURATION 65
5-2 POE STATUS 67
5-3 POE POWER DELAY 69
5-4 POE AUTO CHECKING 70
5-5 POE SCHEDULE PROFILE 72

CHAPTER 6 VLAN MANAGEMENT **73**

6-1 VLAN CONFIGURATION 73
6-2 VLAN MEMBERSHIP 77
6-3 VLAN PORT STATUS 79
6-4 VLAN SELECTIVE QINQ CONFIGURATION 81
6-5 MAC-BASED VLAN 83
6-5.1 Configuration *83*

6-5.2 Status *85*
6-6 PROTOCOL-BASED VLAN 86
6-6.1 Protocol to Group *86*
6-6.2 Group to VLAN *88*
6-7 IP SUBNET-BASED VLAN 90
6-8 PRIVATE VLAN 92
6-9 PORT ISOLATION 94
6-10 VOICE VLAN 95
6-10.1 Configuration *95*
6-10.2 OUI *98*

CHAPTER 7 QUALITY OF SERVICE 99

7-1 GLOBAL SETTINGS 99
7-2 PORT SETTINGS 101
7-3 PORT POLICING 103
7-4 PORT SHAPER 104
7-5 STORM CONTROL 106
7-6 PORT SCHEDULER 108
7-7 COS/802.1P MAPPING 109
7-8 COS/802.1P REMARKING 110
7-9 IP PRECEDENCE MAPPING 111
7-10 IP PRECEDENCE REMARKING 112
7-11 DSCP MAPPING 113
7-12 DSCP REMARKING 114

CHAPTER 8 SPANNING TREE 115

8-1 STATE 115
8-2 REGION CONFIG 117
8-3 INSTANCE VIEW 118

CHAPTER 9 MAC ADDRESS TABLES 125

9-1 CONFIGURATION 125
9-2 INFORMATION 128

CHAPTER 10 MULTICAST 130

10-1 IGMP SNOOPING 130
10-1.1 Basic Configuration *130*
10-1.2 VLAN Configuration *133*
10-1.3 Status *136*
10-1.4 Group Information *139*
10-1.5 IGMP SFM Information *141*
10-2 MLD SNOOPING 144
10-2.1 Basic Configuration *144*
10-2.2 VLAN Configuration *147*
10-2.3 Status *149*
10-2.4 Groups Information *152*
10-2.5 MLD SFM Information *154*
10-3 MULTICAST FILTERING PROFILE 156
10-3.1 Filtering Profile Table *156*
10-3.2 Filtering Address Entry *160*

CHAPTER 11 MVR 162

11-3.1 Basic Configuration *162*
11-3.2 Status *166*
11-3.3 MVR Groups Information *168*

11-3.4 MVR SFM Information ... *170*

CHAPTER 12 DHCP ... 173

12-1 SNOOPING ... 173

12-1.1 Configuration ... *173*

12-1.2 Snooping Table ... *175*

12-1.3 Detailed Statistics ... *177*

12-2 RELAY ... 180

12-2.1 Configuration ... *180*

12-2.2 Statistics ... *182*

12-3 SERVER ... 184

CHAPTER 13 SECURITY ... 186

13-1 MANAGEMENT ... 186

13-1.1 Account ... *186*

13-1.2 Privilege Levels ... *189*

13-1.3 Auth Method ... *191*

13-1.4 Access Management ... *194*

13-2 SNMP ... 196

13-2.1 Configuration ... *196*

13-2.2 SNMPv3 ... *198*

13-2.3 Trap Event Severity ... *209*

13-3 RMON CONFIGURATION ... 211

13-3.1 Statistics ... *211*

13-3.2 History ... *216*

13-3.3 Alarm ... *221*

13-3.4 Event ... *228*

13-3 IEEE 802.1X ... 232

13-3.1 Configuration ... *232*

13-3.2 Status ... *238*

13-4 IP SOURCE GUARD ... 240

13-4.1 Configuration ... *241*

13-4.2 Static Table ... *243*

13-4.3 Dynamic Table ... *245*

13-5 ARP INSPECTION ... 247

13-5.1 Configuration ... *247*

13-5.2 VLAN Configuration ... *249*

13-5.3 Static Table ... *251*

13-5.4 Dynamic Table ... *253*

13-6 PORT SECURITY ... 255

13-6.1 Configuration ... *255*

13-6.2 Status ... *258*

13-7 RADIUS ... 260

13-7.1 Configuration ... *260*

13-7.2 Status ... *263*

13-8 TACACS+ ... 270

13-8.1 Configuration ... *270*

CHAPTER 14 ACCESS CONTROL ... 273

14-1 ACCESS CONTROL LIST ... 273

CHAPTER 15 EVENT NOTIFICATION ... 281

15-1 SNMP TRAP ... 281

CHAPTER 16 DIAGNOSTICS ... 283

16-1 PING 283
16-2 CABLE DIAGNOSTICS 285
16-3 TRACEROUTE 287
16-4 MIRROR 289

CHAPTER 17 MAINTENANCE 291

17-1 CONFIGURATION 291
17-1.1 Save startup-config 291
17-1.2 Backup 293
17-1.3 Restore 295
17-1.4 Activate config 297
17-1.5 Delete config 299
17-2 RESTART DEVICE 300
17-3 FACTORY DEFAULTS 301
17-4 FIRMWARE 302
17-4.1 Firmware Upgrade 302
17-4.2 Firmware Selection 303

CHAPTER 18 DEVICE MANAGEMENT SYSTEM 305

18-1 DMS OVERVIEW 305
18-2 DMS MODE 307
DMS Information 307
18-3 GRAPHICAL MONITORING 308
Topology View 308
Floor View 317
Map View 319
18-4 MANAGEMENT 321
Device List 321
18-5 MAINTENANCE 323
Floor Image 323

CHAPTER 19 COMMAND LINE INTERFACE 324

19-1 LOGIN 325
19-2 COMMANDS OF CLI 326
19-3 GLOBAL COMMANDS OF CLI 327

CHAPTER 20 CLEAR OF CLI 329

20-1 ACCESS-LIST 329
20-2 IP 329
20-3 LLDP 330
20-4 LOGGING 330
20-5 MAC 331
20-6 SPANNING-TREE 331
20-7 STATISTICS 331

CHAPTER 21 CONFIGURE COMMANDS OF CLI 333

21-1 TERMINAL 334

CHAPTER 22 COPY COMMANDS OF CLI 415

CHAPTER 23 DELETE COMMANDS OF CLI 416

CHAPTER 24 DIAGNOSTICS COMMANDS OF CLI 417

CHAPTER 25 DIR COMMANDS OF CLI 418

CHAPTER 26 FIND-SWITCH COMMANDS OF CLI 419

CHAPTER 27 FIRMWARE COMMANDS OF CLI 419

CHAPTER 28 MORE COMMANDS OF CLI 421

CHAPTER 29 PING COMMANDS OF CLI 423

CHAPTER 30 RELOAD COMMANDS OF CLI 424

CHAPTER 31 SHOW COMMANDS OF CLI 425

31-1 AAA 425
31-2 ACCESS 426
31-3 ACCESS-LIST 427
31-4 AGGREGATION 427
31-5 CLOCK 428
31-6 DMS 428
31-7 DOT1X 428
31-8 EVENT 429
31-9 INTERFACE 430
31-10 IP 432
31-11 IPV6 433
31-12 LLDP 434
31-13 LOGGING 435
31-14 LOOP-PROTECT 436
31-15 MAC 437
31-16 MVR 438
31-17 NTP 438
31-18 POE 439
31-19 PORT-SECURITY 440
31-20 PRIVILEGE 440
31-21 PVLAN 441
31-22 QOS 441
31-23 RADIUS-SERVER 442
31-24 RMON 443
31-25 RUNNING-CONFIG 443
31-26 SNMP 445
31-27 SPANNING-TREE 447
31-28 SYSTEM 447
31-29 TACACS-SERVER 448
31-30 TRAP 448
31-31 UPNP 449
31-32 VERSION 449
31-33 VLAN 450
31-34 VOICE 452

CHAPTER 32 SSL COMMANDS OF CLI 455

CHAPTER 33 TERMINAL COMMANDS OF CLI 456

CHAPTER 34 TRACEROUTE COMMANDS OF CLI 457

CHAPTER 35 CLI COMMAND REFERENCES 458

35-1 PRIVILEGE LEVEL 458
35-2 COMMAND MODES 458

INTRODUCTION

Overview

Micronet SP6526P is a 26-Port managed PoE switch with 24-Port 10/100/1000Mbps PoE and 2-Port Gigabit SFP supporting fiber expansion. It is compliant with IEEE802.3af/at, featuring up to 30 watts per port and 370 Watts total PoE power to fulfill most of the demanding network camera and other IT/network applications. With its PoE features such as PoE scheduling, auto-checking, configuring, and power delay, it helps you utilize PoE power more efficiently, smartly, and maximizes the power usage.

For more secured and smooth network, SP6526P is equipped with a long list of layer 2 & layer 3 management and security features such as VLAN, link aggregation, QoS, DHCP client and snooping, secure shell, secure sockets layer, IPv6, and more. With these features, you will have quick deployment, smooth and safe network; giving your infrastructure expansion with more functionality, security, and manageability for different network applications.

- Provide 370W Total PoE Power, with 24 PoE ports IEEE802.3af/at
- Support automatic Voice VLAN for quick deployment of VoIP, and IP-based surveillance system
- Support Link Aggregation (IEEE 802.3ad) to increase bandwidth by automatically aggregate several links together
- Support QoS (Port-based/IEEE 802.1p) feature to preserve network bandwidth and allow maximum control of network resources
- Support STP ,Reserve STP (RSTP) and MSTP features to ensure faster recovery from failed links and enhance overall network reliability
- Support DHCP client and snooping, port mirroring ,and rate limiting features to enhance network security.
- Allow Telnet, and IPv6 Web interface (both HTTP and HTTPS) access
- Support Device Management System to facilitate installation, configuration, and troubleshooting
- Support IEEE 802.1Q VLAN-segmented broadcast domains to reduce broadcast traffic and increase LAN security and performance
- Support 802.3az Green-Ethernet to save power usage
- Support PoE Port configuration, scheduling, auto-checking, and power delay to enhance Power performance
- Support Secure Shell (SSH) & Secure Sockets Layer (SSL/HTTPS) for secure network management

Chapter 1 Operation of Web-based Management

Initial Configuration

This chapter instructs you how to configure and manage the SP6526P through the web user interface. With this facility, you can easily access and monitor through any one port of the switch all the status of the switch, including MIBs status, each port activity, Spanning tree status, port aggregation status, multicast traffic, VLAN and priority status, even illegal access record and so on.

The default values of the SP6526P are listed in the table below:

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Username	admin
Password	admin

After the SP6526P has been finished configuration it interface, you can browse it. For instance, type **http://192.168.1.1** in the address row in a browser, it will show the following screen and ask you inputting username and password in order to login and access authentication.

The default username is **"admin"** and password is **admin**. For the first time to use, please enter the default username and password, and then click the **<Login>** button. The login process now is completed. In this login menu, you have to input the complete username and password respectively, the SP6526P will not give you a shortcut to username automatically. This looks inconvenient, but safer.

In the SP6526P, allowed two or more users using administrator's identity to manage this switch, which administrator to do the last setting, it will be an available configuration to effect the system.

NOTE:

When you login the Switch WEB page to manage. You must first type the Username of the admin. Password was blank, so when you type after the end Username, please press enter. Management page to enter WEB.

When you login SP6526P series switch Web UI management, you can use both ipv4 ipv6 login to manage

To optimize the display effect, we recommend you use Microsoft IE 6.0 above, Netscape V7.1 above or Firefox V1.00 above and have the resolution 1024x768. The switch supported neutral web browser interface

NOTE:
AS SP6526P the function enable dhcp, so If you do not have DHCP server to provide ip addresses to the switch, the Switch **default ip 192.168.1.1**

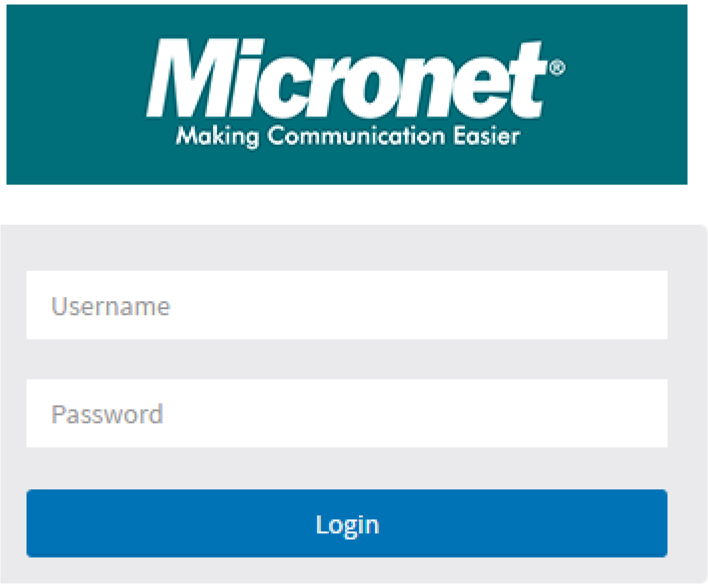


Figure 1: The login page

Chapter 2 First Time Wizard

The first time you use this device you can configure some basic settings, such as password, IP address, date & time, system information.

According to the following procedure:

Step1: Change default password

Configure new password and enter it again.

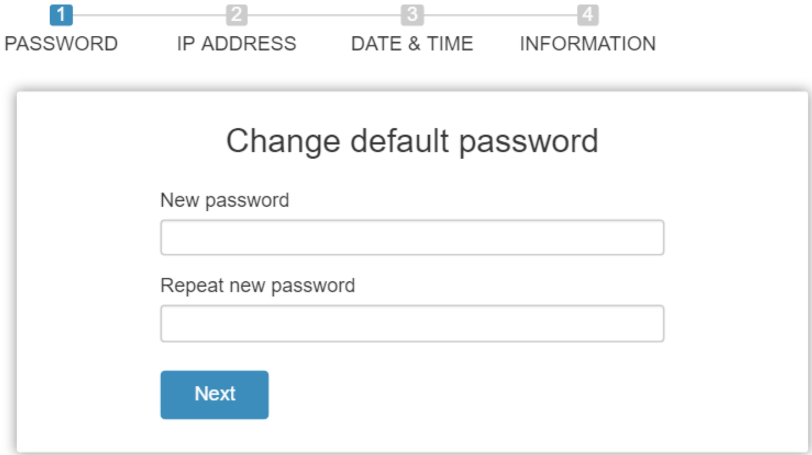
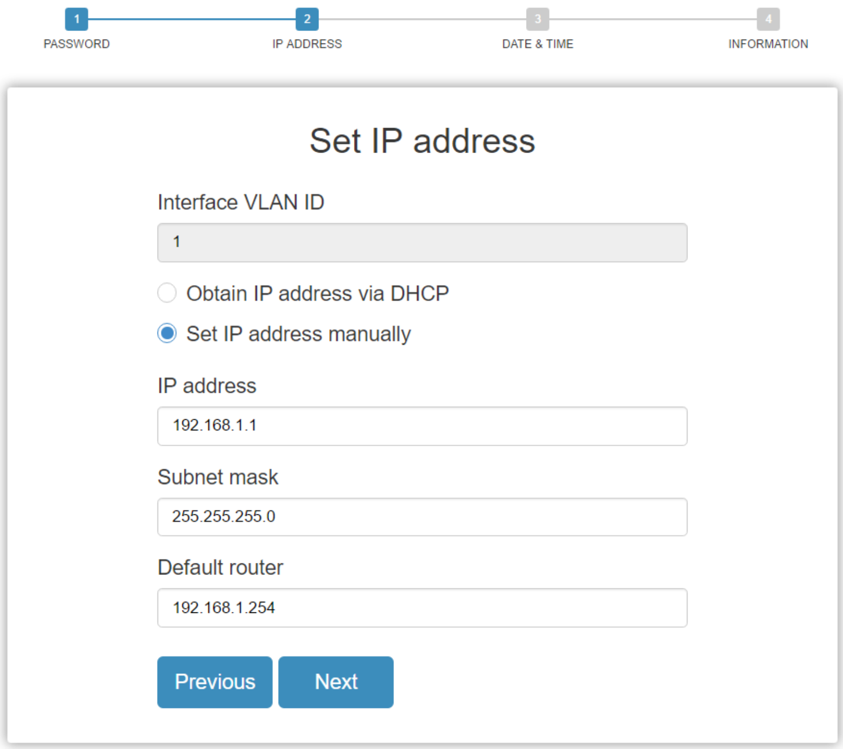


Figure 2: Change default password

Step2: Set IP address

Select “obtain IP address via DHCP” or “Set IP address manually” to set IP address.



Set IP address

Interface VLAN ID: 1

○ Obtain IP address via DHCP

● Set IP address manually

IP address: 192.168.1.1

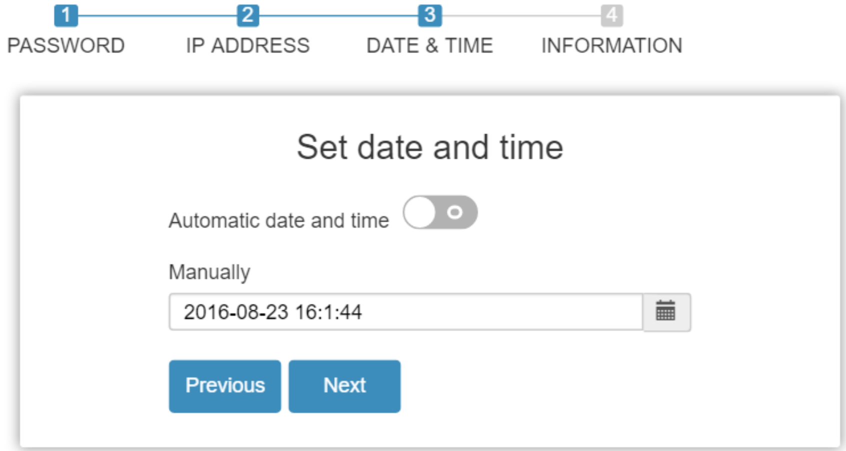
Subnet mask: 255.255.255.0

Default router: 192.168.1.254

Figure 2: Set IP address

Step3: Set date and time

Enable “Automatic data and time” or select manually to set date and time.



Set date and time

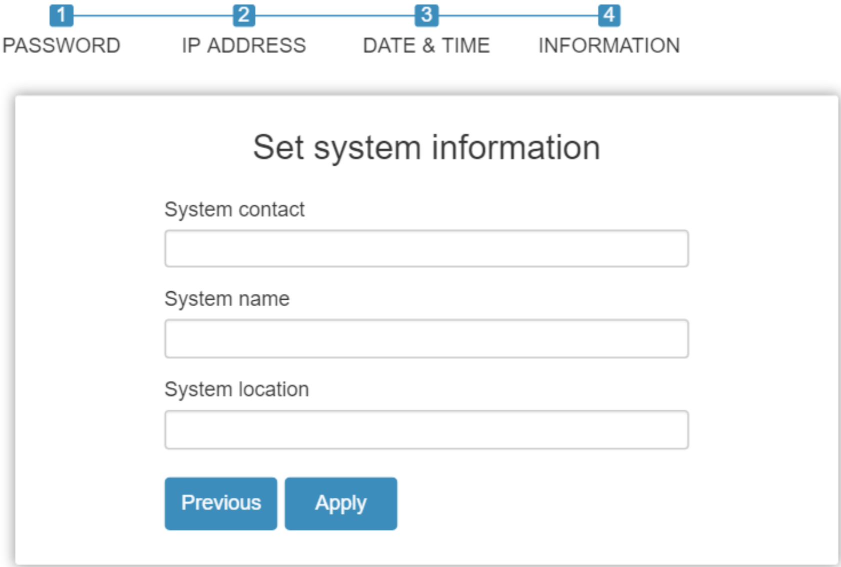
Automatic date and time: ○

Manually: 2016-08-23 16:1:44

Figure 2: Set date and time

Step4: Set system information

You can set some system information to this device, such as “System contact”, “System name”, “System location”.



Set system information

System contact

System name

System location

Figure 2: Set system information

Chapter 3 System

This chapter describes the entire basic configuration tasks which includes the System Information and any management of the Switch (e.g. Time, Account, IP, Syslog and NTP.)

3-1 System Information

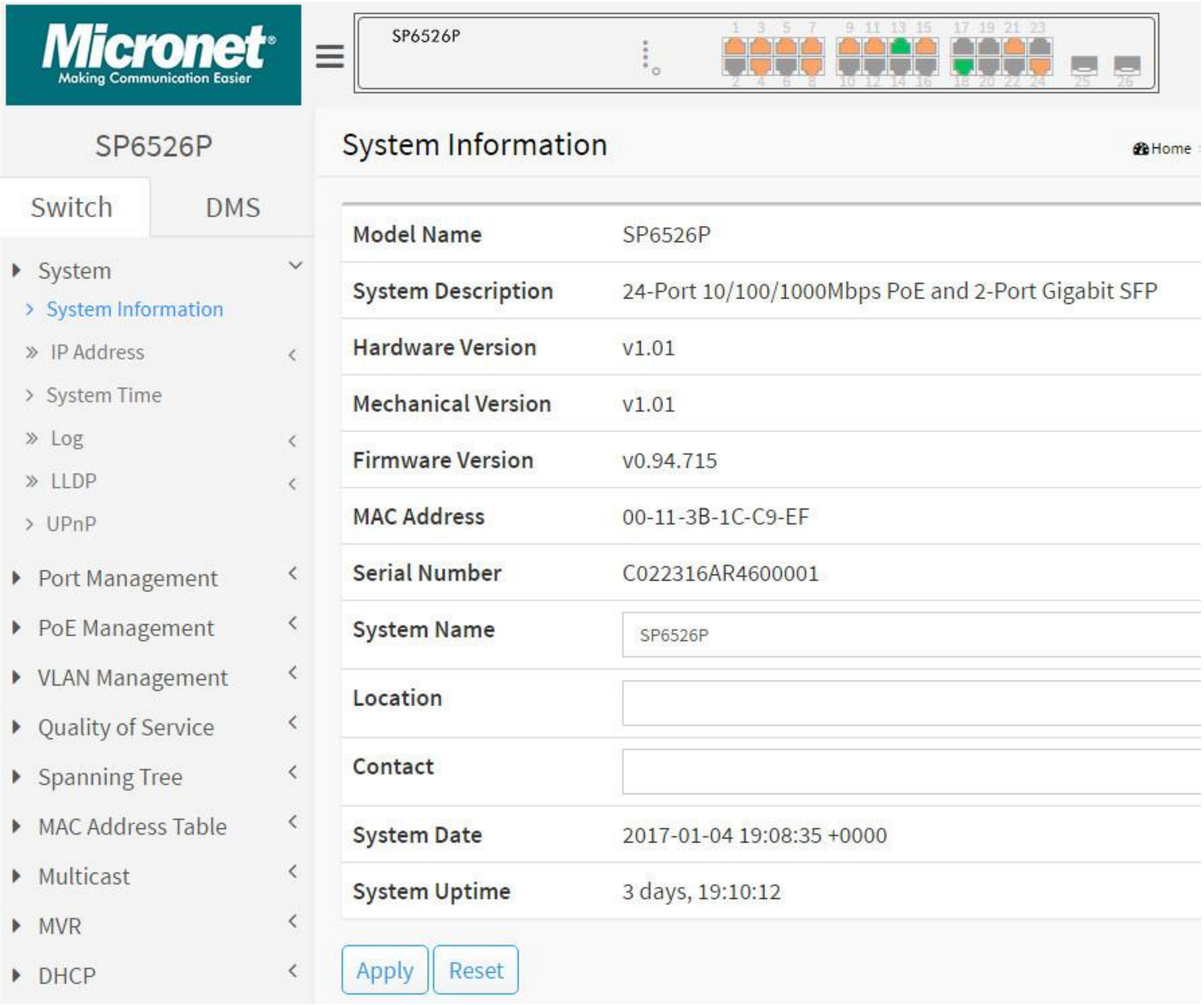
You can identify the system by configuring system name, location and the contact of the switch.

The switch system's contact information is provided here.

Web interface

To configure System Information in the web interface:

1. Click System and System Information.
2. Write System Name, Location, Contact information in this page.
3. Click Apply



System Information

Model Name	SP6526P
System Description	24-Port 10/100/1000Mbps PoE and 2-Port Gigabit SFP
Hardware Version	v1.01
Mechanical Version	v1.01
Firmware Version	v0.94.715
MAC Address	00-11-3B-1C-C9-EF
Serial Number	C022316AR4600001
System Name	SP6526P
Location	
Contact	
System Date	2017-01-04 19:08:35 +0000
System Uptime	3 days, 19:10:12

Figure 3-1: System Information

Parameter description:

- **Model Name**

  Displays the factory defined model name for identification purpose.

- **System Description**

  Displays the system description.

- **Hardware-Mechanical Version**

  The hardware and mechanical version of this switch.

- **Firmware Version**

  The software version of this switch.

- **MAC Address**

  The MAC Address of this switch.

- **Series Number**

  The serial number of this switch.

- **System name :**

  An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Z, a-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 128.

- **Location :**

  The physical location of this node(e.g., telephone closet, 3rd floor). The allowed string length is 0 to 128, and the allowed content is the ASCII characters from 32 to 1.

- **Contact :**

  The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 128, and the allowed content is the ASCII characters from 32 to 126.

- **System Date**

  The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any.

- **System Uptime**

  The period of time the device has been operational.

3-2 IP Address

3-2.1 IP Settings

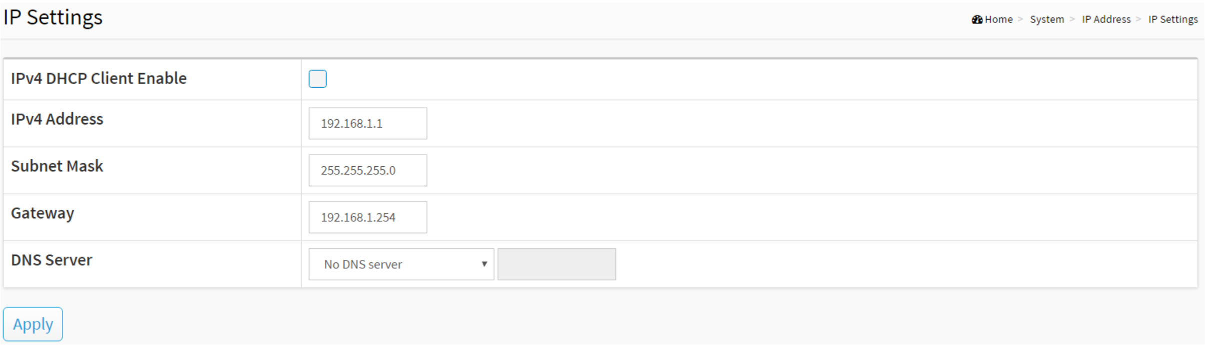
The IPv4 address for the switch could be obtained via DHCP Server for VLAN 1. To manually configure an address, you need to change the switch's default settings to values that are compatible with your network. You may also need to establish a default gateway between the switch and management stations that exist on another network segment.

Configure the IP basic settings

Web Interface

To configure an IP Settings in the web interface:

1. Click System, IP Address and IP Settings.
2. Enable or Disable the IPv4 DHCP Client.
3. Specify the IPv4 Address, Subnet Mask, Gateway.
4. Select DNS Server.
5. Click Apply



IP Settings

Home > System > IP Address > IP Settings

IPv4 DHCP Client Enable	□
IPv4 Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
DNS Server	No DNS server ▾

Apply

Figure 3-2.1: The IP settings

Parameter description:

- **IPv4 DHCP Client Enable :**

  Enable the DHCP client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCP protocol. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.

- **IPv4 Address :**

  The IPv4 address of the interface in dotted decimal notation.
  If DHCP is enabled, this field is not used. The field may also be left blank if IPv4 operation on the interface is not desired.

- **Subnet Mask :**

  User IP subnet mask of the entry.

- **Gateway :**

  The IP address of the IP gateway. Valid format is dotted decimal notationor a valid IPv6 notation. Gateway and Network must be of the same type.

- **DNS Server :**

  This setting controls the DNS name resolution done by the switch. The following modes are supported:

  - No DNS server
    No DNS server will be used.
  - Configured
    Explicitly provide the IP address of the DNS Server in dotted decimal notation.
  - From this DHCP interface
    Specify from which DHCP-enabled interface a provided DNS server should be preferred.
  - From any DHCP interfaces
    The first DNS server offered from a DHCP lease to a DHCP-enabled interface will be used.

Buttons

- **Apply :**

  Click to save changes.

3-2.2 Advanced IP Settings

Configure the switch-managed IP information on this page

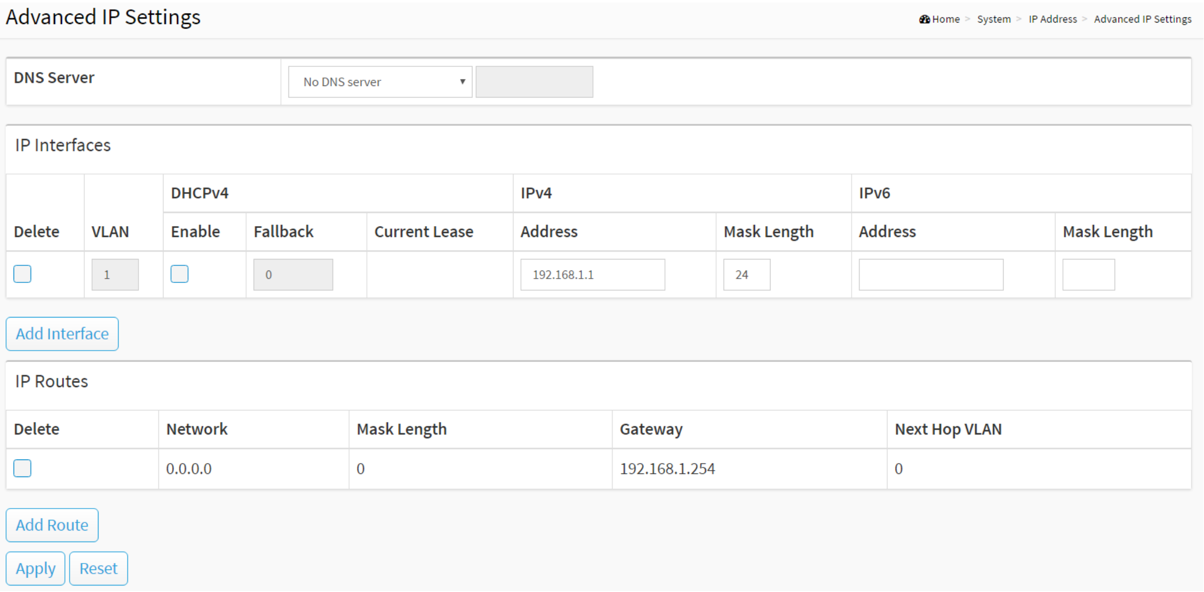
Configure IP basic settings, control IP interfaces and IP routes.

The maximum number of interfaces supported is 8 and the maximum number of routes is 8.

Web Interface

To configure an Advanced IP Settings in the web interface:

1. Click System, IP Address and Advanced IP Settings.
2. Click Add Interface then you can create new Interface on the switch.
3. Click Add Route then you can create new Route on the switch
4. Click Apply



Advanced IP Settings

Home > System > IP Address > Advanced IP Settings

DNS Server	No DNS server ▾	

IP Interfaces

		DHCPv4			IPv4		IPv6	
Delete	VLAN	Enable	Fallback	Current Lease	Address	Mask Length	Address	Mask Length
□	1	□	0		192.168.1.1	24		

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
□	0.0.0.0	0	192.168.1.254	0

Figure 3-2.2: The advanced IP settings

Parameter description:

IP Configuration

- **DNS Server :**

  This setting controls the DNS name resolution done by the switch. The following modes are supported:

  - No DNS server
    No DNS server will be used.
  - Configured
    Explicitly provide the IP address of the DNS Server in dotted decimal notation.
  - From this DHCP interface
    Specify from which DHCP-enabled interface a provided DNS server should be preferred.
  - From any DHCP interfaces

The first DNS server offered from a DHCP lease to a DHCP-enabled interface will be used.

IP Interfaces

- **Delete :**

  Select this option to delete an existing IP interface.

- **VLAN :**

  The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating an new interface.

- **IPv4 DHCP Enabled :**

  Enable the DHCP client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCP protocol. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.

- **IPv4 DHCP Fallback Timeout :**

  The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds.

- **IPv4 DHCP Current Lease :**

  For DHCP interfaces with an active lease, this column show the current interface address, as provided by the DHCP server.

- **IPv4 Address :**

  The IPv4 address of the interface in dotted decimal notation.
  If DHCP is enabled, this field is not used. The field may also be left blank if IPv4 operation on the interface is not desired.

- **IPv4 Mask :**

  The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for a IPv4 address.
  If DHCP is enabled, this field is not used. The field may also be left blank if IPv4 operation on the interface is not desired.

- **IPv6 Address :**

  The IPv6 address of the interface. A IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::215:c5ff:fe03:4dc7. The symbol :: is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, ::192.1.2.34.
  The field may be left blank if IPv6 operation on the interface is not desired.

- **IPv6 Mask :**

  The IPv6 network mask, in number of bits (prefix length). Valid values are between 1 and 128 bits for a IPv6 address.
  The field may be left blank if IPv6 operation on the interface is not desired.

IP Routes

- **Delete :**

  Select this option to delete an existing IP route.

- **Network :**

  The destination IP network or host address of this route. Valid format is dotted decimal notation or a valid IPv6 notation. A default route can use the value 0.0.0.0 or IPv6 :: notation.

- **Mask Length :**

  The destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bits respectively 128 for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything).

- **Gateway :**

  The IP address of the IP gateway. Valid format is dotted decimal notation or a valid IPv6 notation. Gateway and Network must be of the same type.

- **Next Hop VLAN (Only for IPv6) :**

  The VLAN ID (VID) of the specific IPv6 interface associated with the gateway.
  The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid.
  If the IPv6 gateway address is link-local, it must specify the next hop VLAN for the gateway.
  If the IPv6 gateway address is not link-local, system ignores the next hop VLAN for the gateway.

Buttons

- **Add Interface :**

  Click to add a new IP interface. A maximum of 8 interfaces is supported.

- **Add Route :**

  Click to add a new IP route. A maximum of 8 routes is supported.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

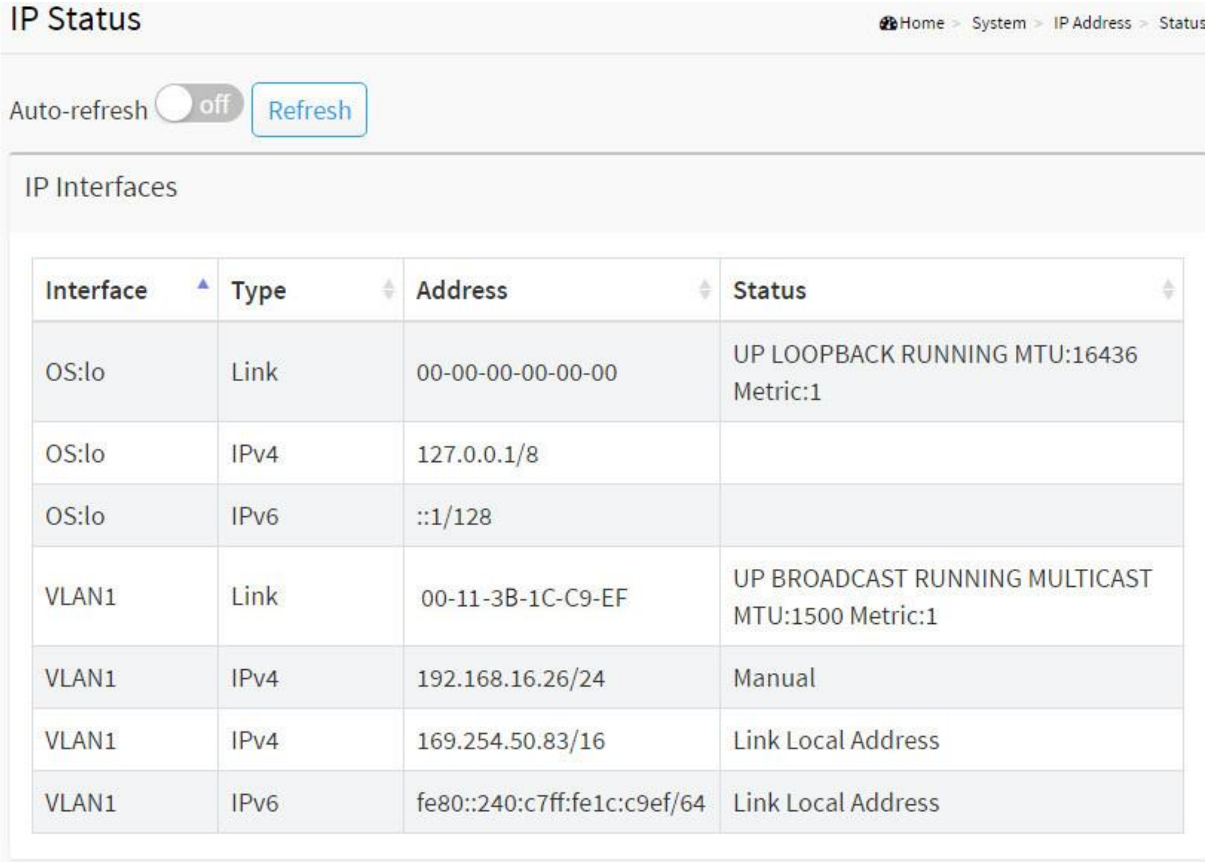
3-2.3 Status

This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IP routes and the neighbour cache (ARP cache) status.

Web Interface

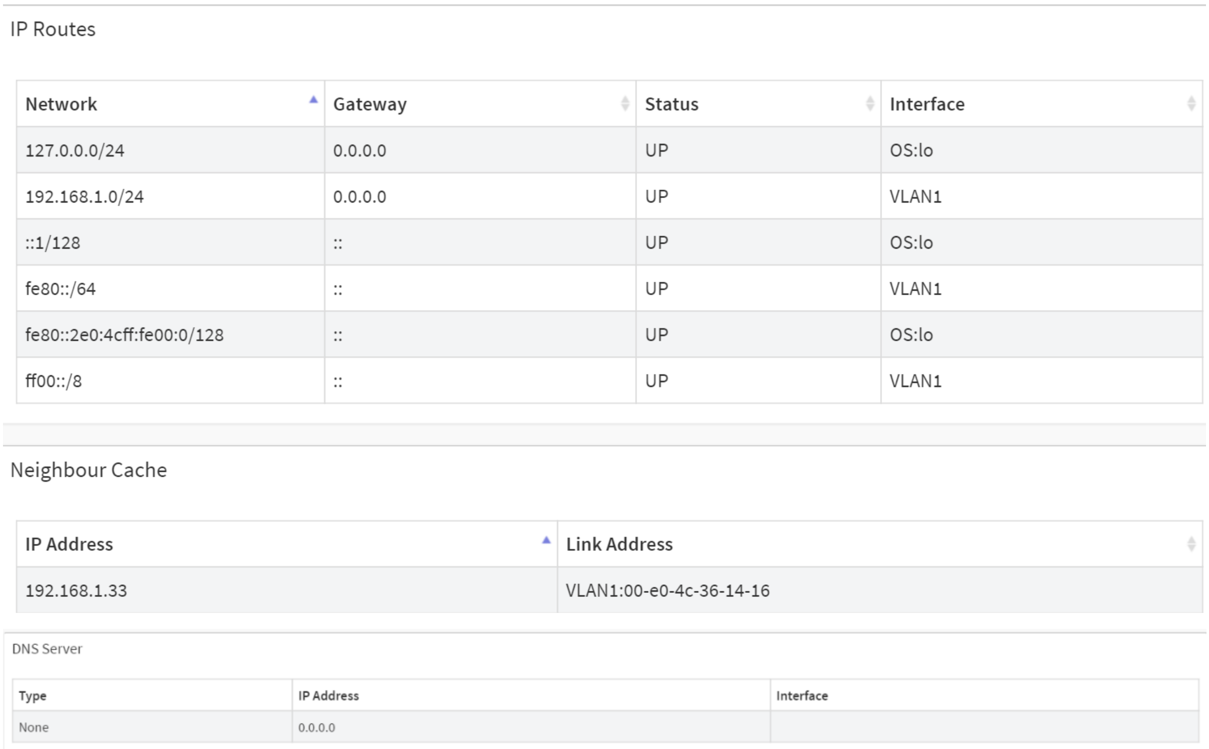
To display the log configuration in the web interface:

1. Click System, IP Address and Status.
2. Display the IP Configuration information.



IP Interfaces

Interface	Type	Address	Status
OS:lo	Link	00-00-00-00-00-00	UP LOOPBACK RUNNING MTU:16436 Metric:1
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	::1/128	
VLAN1	Link	00-11-3B-1C-C9-EF	UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
VLAN1	IPv4	192.168.16.26/24	Manual
VLAN1	IPv4	169.254.50.83/16	Link Local Address
VLAN1	IPv6	fe80::240:c7ff:fe1c:c9ef/64	Link Local Address



IP Routes

Network	Gateway	Status	Interface
127.0.0.0/24	0.0.0.0	UP	OS:lo
192.168.1.0/24	0.0.0.0	UP	VLAN1
::1/128	::	UP	OS:lo
fe80::/64	::	UP	VLAN1
fe80::2e0:4cff:fe00:0/128	::	UP	OS:lo
ff00::/8	::	UP	VLAN1

Neighbour Cache

IP Address	Link Address
192.168.1.33	VLAN1:00-e0-4c-36-14-16

DNS Server

Type	IP Address	Interface
None	0.0.0.0	

Figure 3-2.3: The IP Status

Parameter description:

IP Interfaces

- **Interface :**

  Show the name of the interface.

- **Type :**

  Show the address type of the entry. This may be LINK or IPv4.

- **Address :**

  Show the current address of the interface (of the given type).

- **Status :**

  Show the status flags of the interface (and/or address).

IP Routes

- **Network :**

  Show the destination IP network or host address of this route.

- **Gateway :**

  Show the gateway address of this route.

- **Status :**

  Show the status flags of the route.

- **Interface:**

  Show the name of the interface.

Neighbor cache

- **IP Address :**

  Show the IP address of the entry.

- **Link Address :**

  Show the Link (MAC) address for which a binding to the IP address given exist.

DNS Server

- **Type :**

  Show the address type of the entry. This may be LINK or IPv4.

- **IP Address :**

  Show the current address of the interface (of the given type).

- **Interface :**

  Show the name of the interface.

Buttons

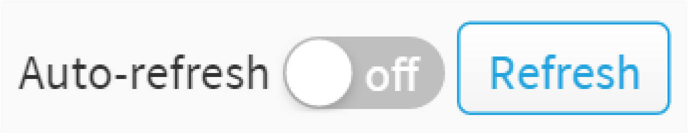


Figure 3-2.3: The IP Status buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

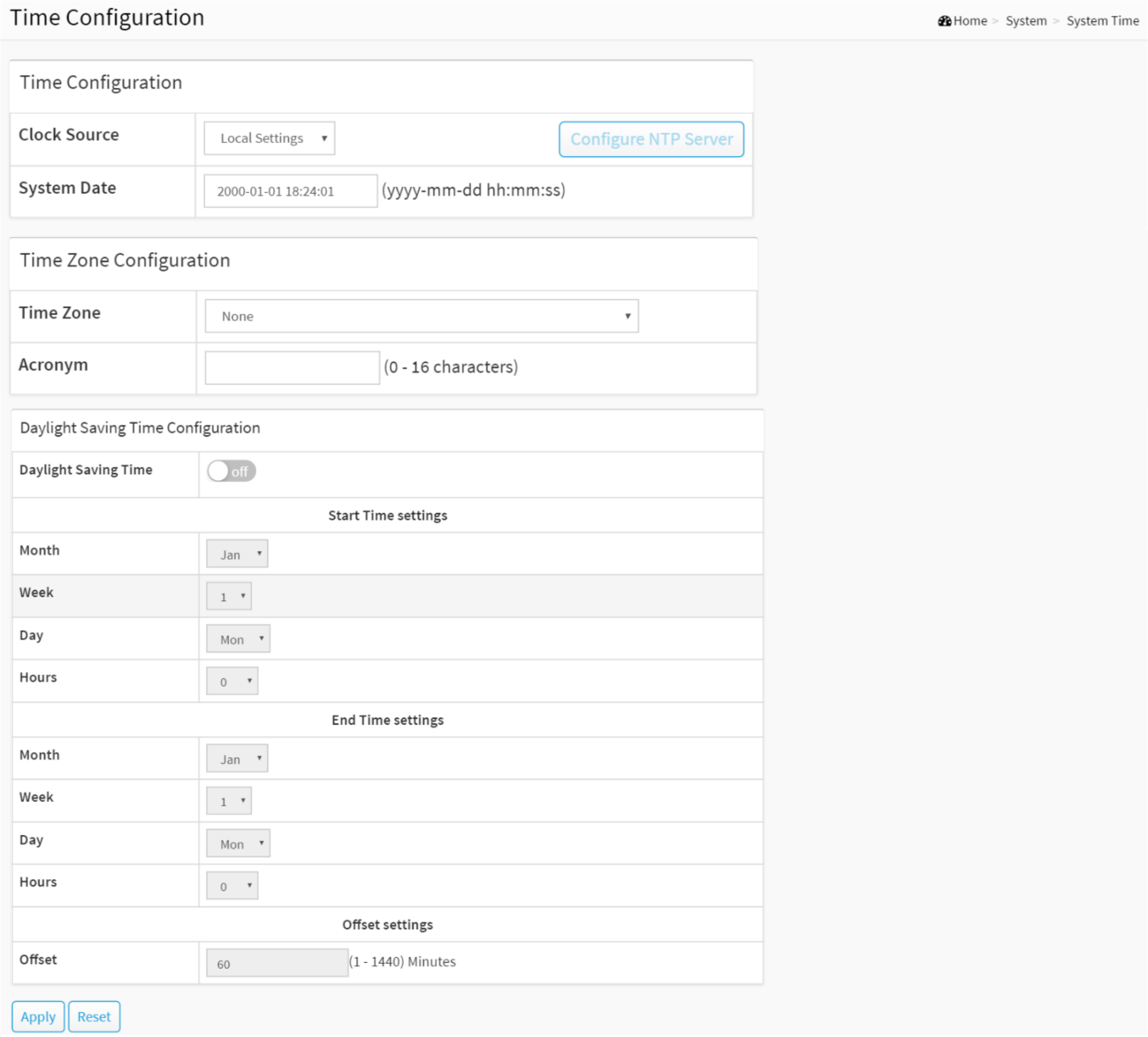
3-3 System Time

The switch provides manual and automatic ways to set the system time via NTP. Manual setting is simple and you just input “Year”, “Month”, “Day”, “Hour” and “Minute” within the valid value range indicated in each item.

Web Interface

To configure Time in the web interface:

1. Click System and System Time
2. Specify the Time parameter.
3. Click Apply.



Time Configuration

Home > System > System Time

Time Configuration

Clock Source	Local Settings ▾ Configure NTP Server
System Date	2000-01-01 18:24:01 (yyyy-mm-dd hh:mm:ss)

Time Zone Configuration

Time Zone	None ▾
Acronym	(0 - 16 characters)

Daylight Saving Time Configuration

Daylight Saving Time	off
Start Time settings	
Month	Jan ▾
Week	1 ▾
Day	Mon ▾
Hours	0 ▾
End Time settings	
Month	Jan ▾
Week	1 ▾
Day	Mon ▾
Hours	0 ▾
Offset settings	
Offset	60 (1 - 1440) Minutes

Figure 3-3: The time configuration

Parameter description:

Time Configuration

- **Clock Source :**

  There are two modes for configuring how the Clock Source from. Select "Local Settings" : Clock Source from Local Time. Select "NTP Server" : Clock Source from NTP Server.

- **System Date :**

  Show the current time of the system. The year of system date limits between 2000 and 2037.

Time Zone Configuration

- **Time Zone :**

  Lists various Time Zones worldwide. Select appropriate Time Zone from the drop down and click Apply to set.

- **Acronym :**

  User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range: Up to 16 characters)

Daylight Saving Time Configuration

- **Daylight Saving Time :**

  This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select 'Disable' to disable the Daylight Saving Time configuration. Select 'Recurring' and configure the Daylight Saving Time duration to repeat the configuration every year. Select 'Non-Recurring' and configure the Daylight Saving Time duration for single time configuration. (Default: Disabled).

Recurring Configuration

- **Start time settings :**

  Week - Select the starting week number.

  Day - Select the starting day.

  Month - Select the starting month.

  Hours - Select the starting hour.

- **End time settings :**

  Week - Select the ending week number.

  Day - Select the ending day.

  Month - Select the ending month.

  Hours - Select the ending hour.

- **Offset settings :**

  Offset - Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440)

NOTE: The under "Start Time Settings" and "End Time Settings" was displayed what you set on the "Start Time Settings" and "End Time Settings" field information.

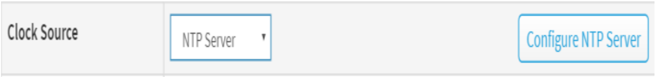
Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

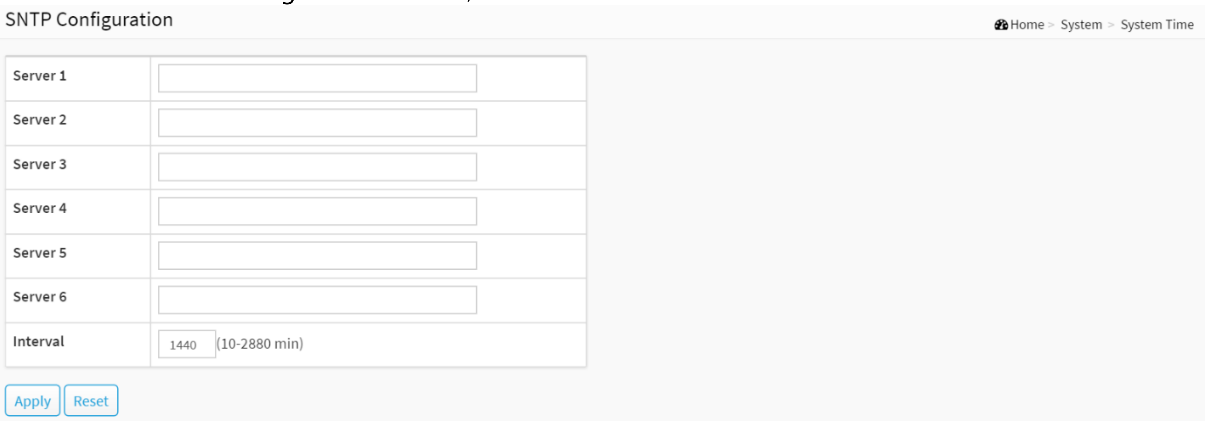


Clock Source: NTP Server

Figure 3-3: The Configure NTP Server button

- **Configure NTP Server :**

  Click to configure NTP server, When Clock Source select from NTP Server.



SNTP Configuration

Server 1	
Server 2	
Server 3	
Server 4	
Server 5	
Server 6	
Interval	1440 (10-2880 min)

Figure 3-3: The SNTP configuration

NTP is Network Time Protocol and is used to sync the network time based Greenwich Mean Time (GMT). If use the NTP mode and select a built-in NTP time server or manually specify an user-defined NTP server as well as Time Zone, the switch will sync the time in a short after pressing <Apply> button. Though it synchronizes the time automatically, NTP does not update the time periodically without user's processing.

Time Zone is an offset time of GMT. You have to select the time zone first and then perform time sync via NTP because the switch will combine this time zone offset and updated NTP time to come out the local time, otherwise, you will not able to get the correct time. The switch supports configurable time zone from –12 to +13 step 1 hour.

Default Time zone: +8 Hrs.

Parameter description :

- **Server 1 to 6:**

  Provide the NTP IPv4 or IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

- **Interval**

  You can specify the time interval in seconds after which a time check and, in case of deviation, a resynchronization of the internal device clock against the specified timeserver via Network Time Protocol(NTP) should be performed.

Buttons

These buttons are displayed on the SNTP page:

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

3-4 Log

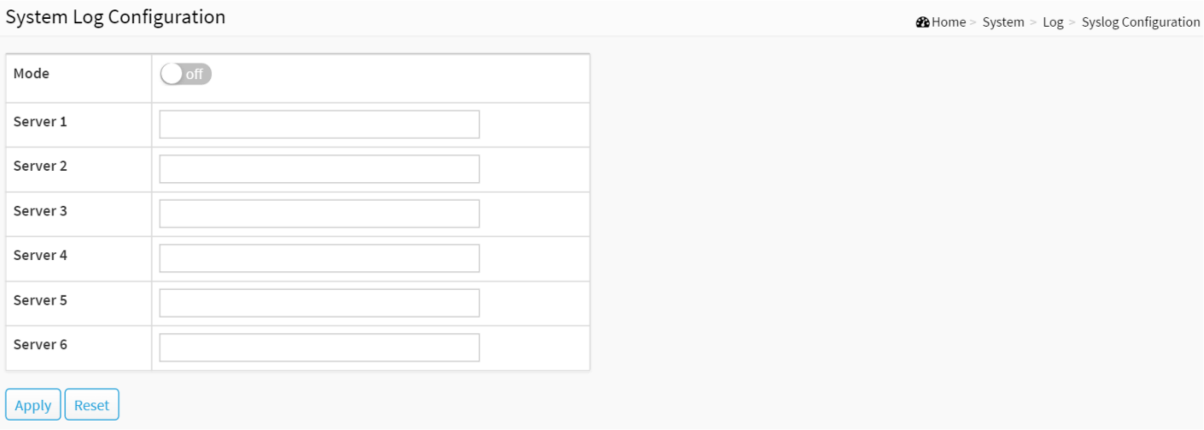
3-4.1 Syslog Configuration

The Syslog Configuration is a standard for logging program messages . It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It can be used as well a generalized informational, analysis and debugging messages. It is supported by a wide variety of devices and receivers across multiple platforms.

Web Interface

To configure Syslog Configuration in the web interface:

1. Click System, Log and Syslog Configuration.
2. Specify the syslog parameters include IP Address of Syslog server and Port number.
3. Evoke the Syslog to enable it.
4. Click Apply.



System Log Configuration

Mode	off
Server 1	
Server 2	
Server 3	
Server 4	
Server 5	
Server 6	

Figure 3-4.1: The System Log configuration

Parameter description:

- **Mode :**

  Indicate the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are:

  On: Enable server mode operation.

  Off: Disable server mode operation.

- **Server 1 to 6 :**

  Indicates the IPv4 hosts address of syslog server. If the switch provide DNS feature, it also can be a host name.

Buttons

- **Apply :**

Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

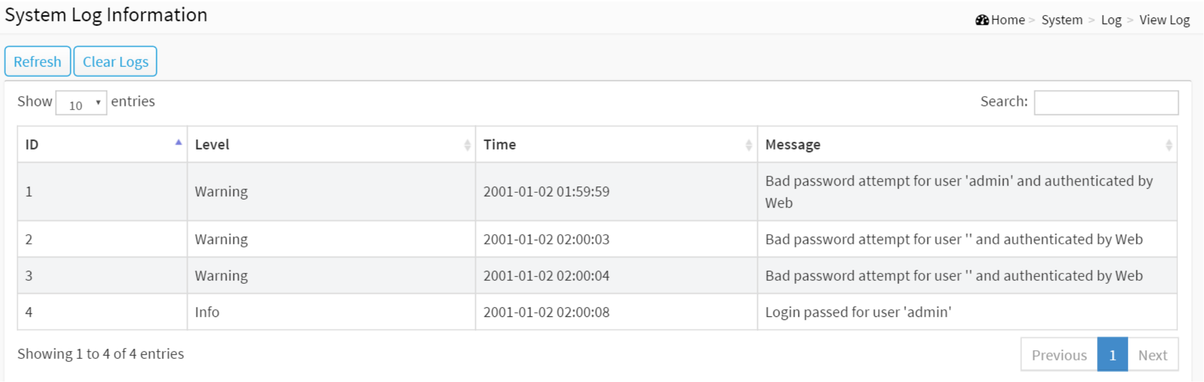
3-4.2 View Log

This section describes that display the system log information of the switch

Web Interface

To display the log Information in the web interface:

1. Click System, Log and View Log.
2. Display the log information.



ID	Level	Time	Message
1	Warning	2001-01-02 01:59:59	Bad password attempt for user 'admin' and authenticated by Web
2	Warning	2001-01-02 02:00:03	Bad password attempt for user '' and authenticated by Web
3	Warning	2001-01-02 02:00:04	Bad password attempt for user '' and authenticated by Web
4	Info	2001-01-02 02:00:08	Login passed for user 'admin'

Showing 1 to 4 of 4 entries

Figure 3-4.2: The System Log Information

Parameter description:

- **ID :**

  ID (>= 1) of the system log entry.

- **Level :**

  level of the system log entry. The following level types are supported:

  Debug : debug level message.

  Info : informational message.

  Notice : normal, but significant, condition.

  Warning : warning condition.

  Error : error condition.

  Crit : critical condition.

  Alert : action must be taken immediately.

  Emerg : system is unusable.

- **Time :**

  It will display the log record by device time. The time of the system log entry.

- **Message :**

  It will display the log detail message. The message of the system log entry.

- **Search :**

  You can search for the information that you want to see.

- **Show entries :**

You can choose how many items you want to show.

Buttons

- **Refresh :**

  Updates the system log entries, starting from the current entry ID.

- **Clear Logs :**

  Clear all the system log entries.

- **Next :**

  Updates the system log entries, turn to the next page.

- **Previous :**

  Updates the system log entries, turn to the previous page.

3-5 LLDP

The switch supports the LLDP. For current information on your switch model, The Link Layer Discovery Protocol (LLDP) provides a standards-based method for enabling switches to advertise themselves to adjacent devices and to learn about adjacent LLDP devices. The Link Layer Discovery Protocol (LLDP) is a vendor-neutral Link Layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 local area network, principally wired Ethernet. The protocol is formally referred to by the IEEE as Station and Media Access Control Connectivity Discovery specified in standards document IEEE 802.1AB.

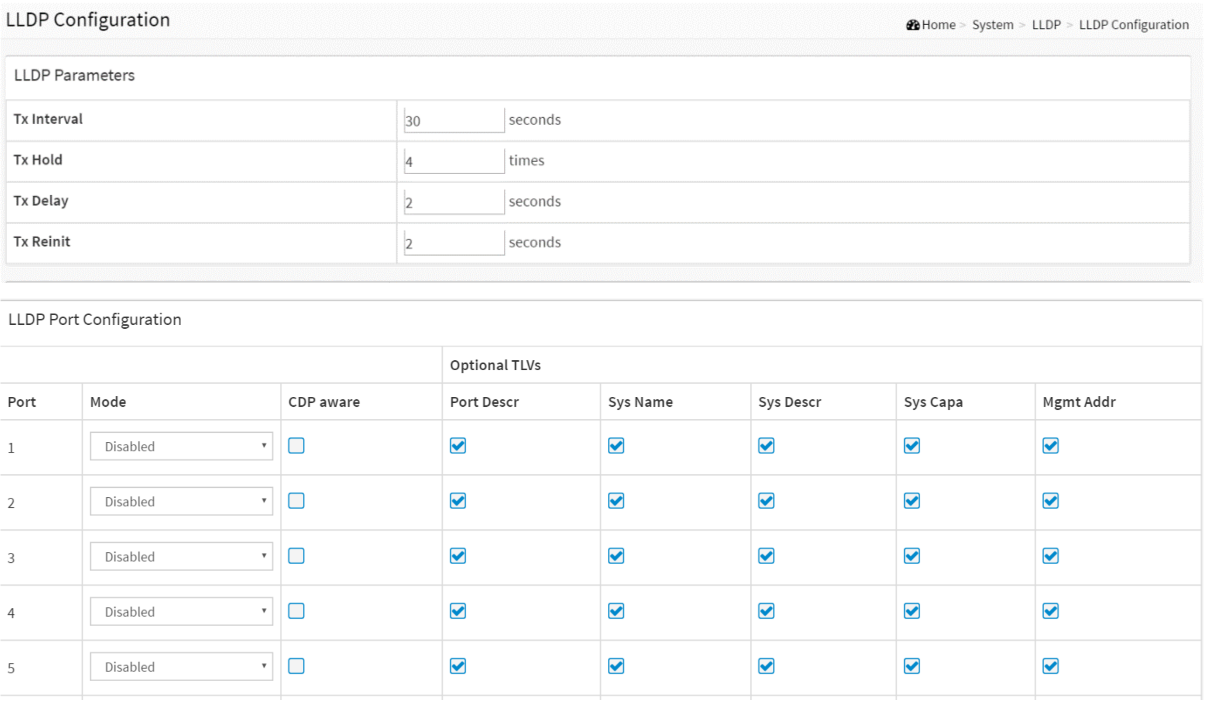
3-5.1 LLDP Configuration

You can per port to do the LLDP configuration and the detail parameters, the settings will take effect immediately. This page allows the user to inspect and configure the current LLDP port settings.

Web Interface

To configure LLDP:

1. Click System, LLDP and LLDP configuration.
2. Modify LLDP timing parameters
3. Set the required mode for transmitting or receiving LLDP messages
4. Specify the information to include in the TLV field of advertised messages
5. Click Apply



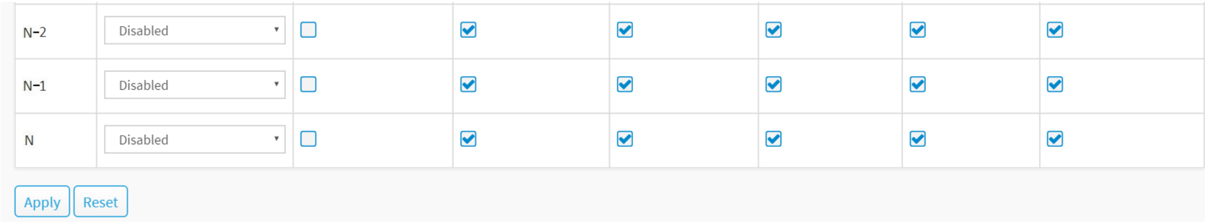
LLDP Configuration

LLDP Parameters

Tx Interval	30 seconds
Tx Hold	4 times
Tx Delay	2 seconds
Tx Reinit	2 seconds

LLDP Port Configuration

			Optional TLVs				
Port	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
1	Disabled	□	☑	☑	☑	☑	☑
2	Disabled	□	☑	☑	☑	☑	☑
3	Disabled	□	☑	☑	☑	☑	☑
4	Disabled	□	☑	☑	☑	☑	☑
5	Disabled	□	☑	☑	☑	☑	☑



N-2	Disabled	□	☑	☑	☑	☑	☑
N-1	Disabled	□	☑	☑	☑	☑	☑
N	Disabled	□	☑	☑	☑	☑	☑

Figure 3-5.1: The LLDP Configuration

Parameter description:

LLDP Parameters

- **Tx Interval :**

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

- **Tx Hold :**

  Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2 - 10 times.

- **Tx Delay :**

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

- **Tx Reinit :**

  When a port is disabled, LLDP is disabled or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

LLDP Port Configuration

The LLDP port settings relate to the currently selected, as reflected by the page header.

- **Port :**

  The switch port number of the logical LLDP port.

- **Mode :**

  Select LLDP mode.

  Rx only The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.

  Tx only The switch will drop LLDP information received from neighbors, but will send out LLDP information.

  Disabled The switch will not send out LLDP information, and will drop LLDP information received from neighbors.

  Enabled the switch will send out LLDP information, and will analyze LLDP information received from neighbors.

- **CDP Aware :**

Select CDP awareness.

The CDP operation is restricted to decode incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the port is enabled.

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

CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.

CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors' table.

CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.

CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.

Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors' table.

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

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

- **Port Descr :**

  Optional TLV: When checked the "port description" is included in LLDP information transmitted.

- **Sys Name :**

  Optional TLV: When checked the "system name" is included in LLDP information transmitted.

- **Sys Descr :**

  Optional TLV: When checked the "system description" is included in LLDP information transmitted.

- **Sys Capa :**

  Optional TLV: When checked the "system capability" is included in LLDP information transmitted.

- **Mgmt Addr :**

  Optional TLV: When checked the "management address" is included in LLDP information transmitted.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

3-5.2 LLDP-MED Configuration

Media Endpoint Discovery is an enhancement of LLDP, known as LLDP-MED that provides the following facilities:

Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and Differentiated services (Diffserv) settings) enabling plug and play networking.

Device location discovery to allow creation of location databases and, in the case of Voice over Internet Protocol (VoIP), Enhanced 911 services.

Extended and automated power management of Power over Ethernet (PoE) end points.

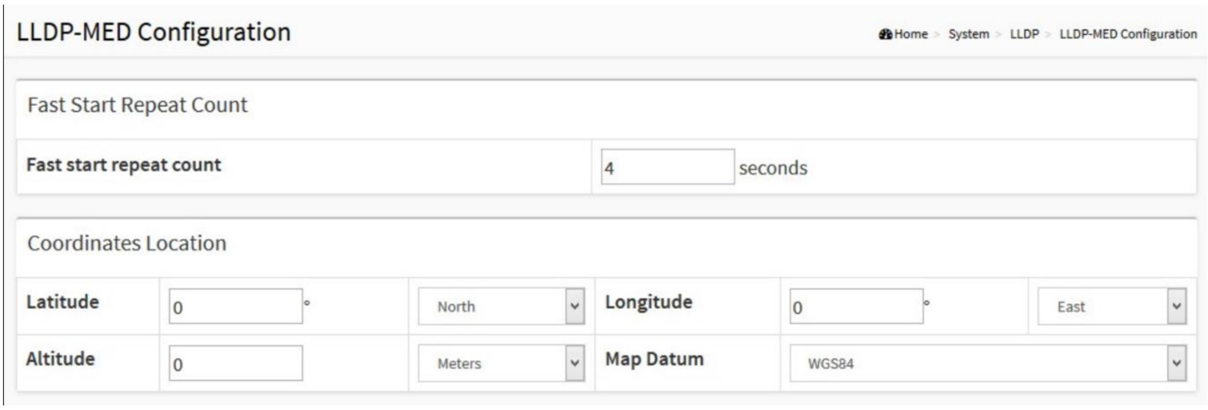
Inventory management, allowing network administrators to track their network devices, and determine their characteristics (manufacturer, software and hardware versions, and serial or asset number).

This page allows you to configure the LLDP-MED. This function applies to VoIP devices which support LLDP-MED.

Web Interface

To configure LLDP-MED:

1. Click System, LLDP and LLDP-MED Configuration
2. Modify Fast start repeat count parameter, default is 4
3. Modify Coordinates Location parameters
4. Fill Civic Address Location parameters
5. Add new policy
6. Click Apply, will show following Policy Port Configuration
7. Select Policy ID for each port
8. Click Apply

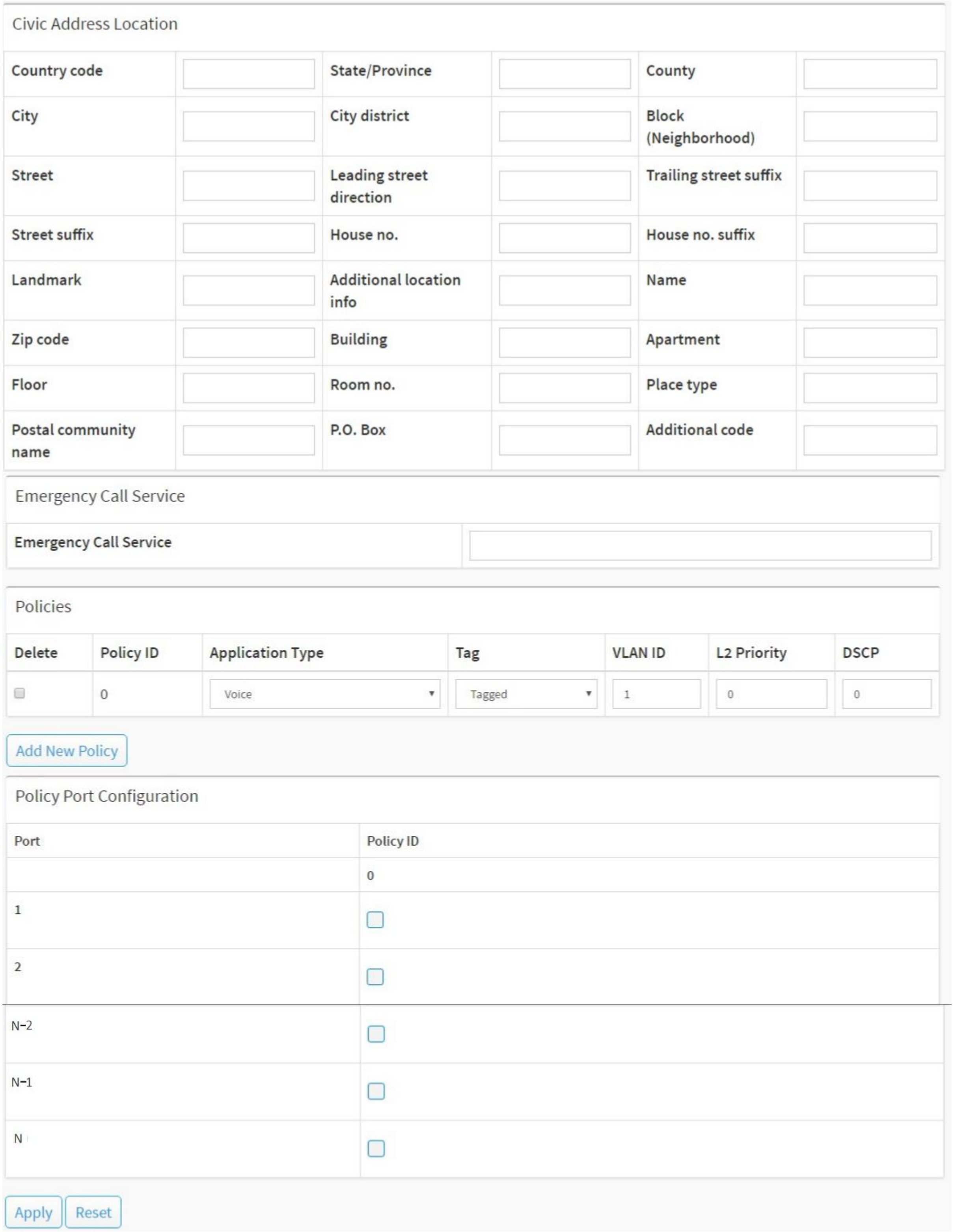


Fast Start Repeat Count

Fast start repeat count	4 seconds

Coordinates Location

Latitude	0 °	North	**Longitude**	0 °	East
Altitude	0	Meters	**Map Datum**	WGS84	



Civic Address Location

Country code		State/Province		County	
City		City district		Block (Neighborhood)	
Street		Leading street direction		Trailing street suffix	
Street suffix		House no.		House no. suffix	
Landmark		Additional location info		Name	
Zip code		Building		Apartment	
Floor		Room no.		Place type	
Postal community name		P.O. Box		Additional code	

Emergency Call Service

Emergency Call Service	

Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
□	0	Voice ▾	Tagged ▾	1	0	0

Policy Port Configuration

Port	Policy ID
	0
1	□
2	□
N-2	□
N-1	□
N	□

Figure 3-5.2: The LLDP-MED Configuration

Parameter description :

Fast start repeat count

Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.

With this in mind LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbour has been detected in order share LLDP-MED information as fast as possible to new neighbours.

Because there is a risk of an LLDP frame being lost during transmission between neighbours, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbours receiving the LLDP frame. With Fast start repeat count it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received.

It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links.

Coordinates Location

- **Latitude :**

  Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits.

  It is possible to specify the direction to either North of the equator or South of the equator.

- **Longitude :**

  Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 5 digits.

  It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.

- **Altitude :**

  Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits.

  It is possible to select between two altitude types (floors or meters).

  Meters: Representing meters of Altitude defined by the vertical datum specified.

  Floors: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.

- **Map Datum :**

  The Map Datum is used for the coordinates given in these options:

  WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, and Prime Meridian Name: Greenwich.

  NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; the associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).

  NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; the associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Civic Address Location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).

- **Country code :**

  The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.

- **State :**

  National subdivisions (state, canton, region, province, prefecture).

- **County :**

  County, parish, gun (Japan), district.

- **City :**

  City, township, shi (Japan) - Example: Copenhagen.

- **City district :**

  City division, borough, city district, ward, chou (Japan).

- **Block (Neighbourhood) :**

  Neighbourhood, block.

- **Street :**

  Street - Example: Poppelvej.

- **Leading street direction :**

  Leading street direction - Example: N.

- **Trailing street suffix :**

  Trailing street suffix - Example: SW.

- **Street suffix :**

  Street suffix - Example: Ave, Platz.

- **House no. :**

  House number - Example: 21.

- **House no. suffix :**

  House number suffix - Example: A, 1/2.

- **Landmark :**

  Landmark or vanity address - Example: Columbia University.

- **Additional location info :**

  Additional location info - Example: South Wing.

- **Name :**

  Name (residence and office occupant) - Example: Flemming Jahn.

- **Zip code :**

  Postal/zip code - Example: 2791.

- **Building :**

  Building (structure) - Example: Low Library.

- **Apartment :**

  Unit (Apartment, suite) - Example: Apt 42.

- **Floor :**

  Floor - Example: 4.

- **Room no. :**

  Room number - Example: 450F.

- **Place type :**

  Place type - Example: Office.

- **Postal community name :**

  Postal community name - Example: Leonia.

- **P.O. Box :**

  Post office box (P.O. BOX) - Example: 12345.

- **Additional code :**

  Additional code - Example: 1320300003.

- **Emergency Call Service:**

  Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

- **Emergency Call Service :**

  Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Policies

Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.

Policies are only intended for use with applications that have specific 'real-time' network policy requirements, such as interactive voice and/or video services.

The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)

2. Layer 2 priority value (IEEE 802.1D-2004)

3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

1. Voice

2. Guest Voice

3. Softphone Voice

4. Video Conferencing

5. Streaming Video

6. Control / Signalling (conditionally support a separate network policy for the media types above)

A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

It should be noted that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

- **Delete :**

  Check to delete the policy. It will be deleted during the next save.

- **Policy ID :**

  ID for the policy. This is auto generated and shall be used when selecting the polices that shall be mapped to the specific ports.

- **Application Type :**

  Intended use of the application types:

  1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.

  2. Voice Signalling (conditional) - for use in network topologies that require a different policy for the voice signalling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy.

  3. Guest Voice - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.

  4. Guest Voice Signalling (conditional) - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy.

  5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance.

  6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.

  7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.

  8. Video Signalling (conditional) - for use in network topologies that require a separate policy for the video signalling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.

- **Tag :**

  Tag indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN.

Untagged indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance.

Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.

- **VLAN ID :**

  VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003.

- **L2 Priority :**

  L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.

- **DSCP :**

  DSCP value to be used to provide Diffserv node behaviour for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

- **Port Policies Configuration :**

  Every port may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or port configuration.

- **Port :**

  The port number to which the configuration applies.

- **Policy Id :**

  The set of policies that shall apply to a given port. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

Buttons

- **Adding a new policy :**

  Click to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click "Apply".

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

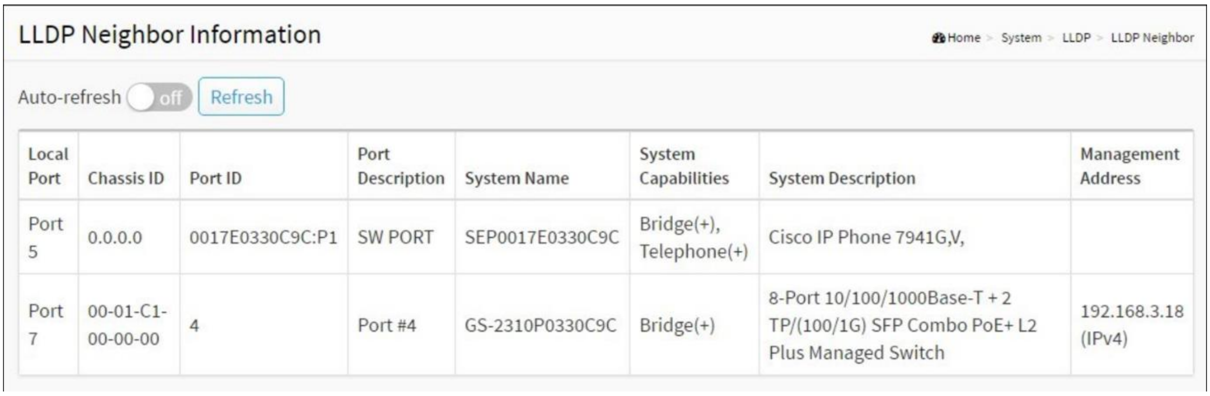
3-5.3 LLDP Neighbour

This page provides a status overview for all LLDP neighbours. The displayed table contains a row for each port on which an LLDP neighbour is detected. The columns hold the following information:

Web Interface

To show LLDP neighbours:

1. Click System, LLDP and LLDP Neighbour.
2. Click Refresh for manual update web screen
3. Click Auto-refresh for auto-update web screen



LLDP Neighbor Information

Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	System Description	Management Address
Port 5	0.0.0.0	0017E0330C9C:P1	SW PORT	SEP0017E0330C9C	Bridge(+), Telephone(+)	Cisco IP Phone 7941G,V,	
Port 7	00-01-C1-00-00-00	4	Port #4	GS-2310P0330C9C	Bridge(+)	8-Port 10/100/1000Base-T + 2 TP/(100/1G) SFP Combo PoE+ L2 Plus Managed Switch	192.168.3.18 (IPv4)

Figure 3-5.3: The LLDP Neighbour information

NOTE: If there is no device that supports LLDP in your network then the table will show "No LLDP neighbour information found".

Parameter description:

- **Local Port :**

  The port on which the LLDP frame was received.

- **Chassis ID :**

  The Chassis ID is the identification of the neighbour's LLDP frames.

- **Port ID :**

  The Remote Port ID is the identification of the neighbour port.

- **Port Description :**

  Port Description is the port description advertised by the neighbour unit.

- **System Name :**

  System Name is the name advertised by the neighbour unit.

- **System Capabilities :**

  System Capabilities describes the neighbour unit's capabilities. The possible capabilities are:

  1. Other

  2. Repeater

3. Bridge

4. WLAN Access Point

5. Router

6. Telephone

7. DOCSIS cable device

8. Station only

9. Reserved

When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

- **System Description**

  Displays the system description.

- **Management Address :**

  Management Address is the neighbour unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbour's IP address.

Buttons

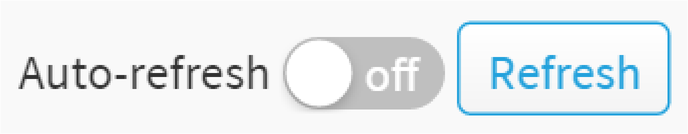


Figure 3-5.3: The LLDP Neighbor buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

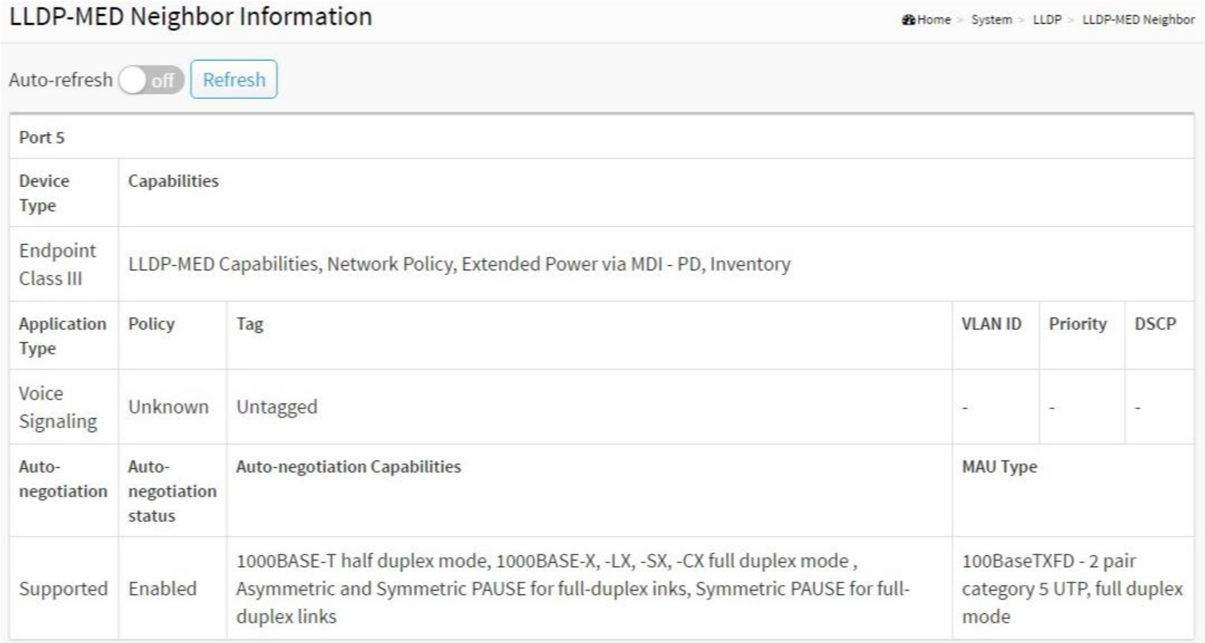
3-5.4 LLDP-MED Neighbour

This page provides a status overview of all LLDP-MED neighbours. The displayed table contains a row for each port on which an LLDP neighbour is detected. This function applies to VoIP devices which support LLDP-MED. The columns hold the following information:

Web Interface

To show LLDP-MED neighbor:

1. Click System, LLDP and LLDP-MED Neighbour.
2. Click Refresh for manual update web screen
3. Click Auto-refresh for auto-update web screen


LLDP-MED Neighbor Information
Home > System > LLDP > LLDP-MED Neighbor
Auto-refresh off
Refresh

Port 5					
Device Type	Capabilities				
Endpoint Class III	LLDP-MED Capabilities, Network Policy, Extended Power via MDI - PD, Inventory				
Application Type	Policy	Tag	VLAN ID	Priority	DSCP
Voice Signaling	Unknown	Untagged	-	-	-
Auto-negotiation	Auto-negotiation status	Auto-negotiation Capabilities	MAU Type		
Supported	Enabled	1000BASE-T half duplex mode, 1000BASE-X, -LX, -SX, -CX full duplex mode , Asymmetric and Symmetric PAUSE for full-duplex inks, Symmetric PAUSE for full-duplex links	100BaseTXFD - 2 pair category 5 UTP, full duplex mode		

Figure 3-5.4: The LLDP-MED Neighbour information

NOTE: If there is no device that supports LLDP-MED in your network then the table will show “No LLDP-MED neighbour information found”.

Parameter description

- **Port :**

  The port on which the LLDP frame was received.

- **Device Type :**

  LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices.

  ■ **LLDP-MED Network Connectivity Device Definition**

  LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

  1. LAN Switch/Router

2. IEEE 802.1 Bridge

3. IEEE 802.3 Repeater (included for historical reasons)

4. IEEE 802.11 Wireless Access Point

5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.

- **LLDP-MED Endpoint Device Definition :**

LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework.

Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following.

Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

- **LLDP-MED Generic Endpoint (Class I) :**

The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057.

Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

- **LLDP-MED Media Endpoint (Class II) :**

The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar.

Discovery services defined in this class include media-type-specific network layer policy discovery.

- **LLDP-MED Communication Endpoint (Class III) :**

The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.

Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management.

- **LLDP-MED Capabilities :**

LLDP-MED Capabilities describes the neighborhood unit's LLDP-MED capabilities. The possible capabilities are:

1. LLDP-MED capabilities

2. Network Policy

3. Location Identification

4. Extended Power via MDI - PSE

5. Extended Power via MDI - PD

6. Inventory

7. Reserved

- **Application Type :**

Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below.

1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.

2. Voice Signalling - for use in network topologies that require a different policy for the voice signalling than for the voice media.

3. Guest Voice - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.

4. Guest Voice Signalling - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media.

5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops.

6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.

7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.

8. Video Signalling - for use in network topologies that require a separate policy for the video signalling than for the video media.

- **Policy :**

Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown

Unknown: The network policy for the specified application type is currently unknown.

Defined: The network policy is defined.

- **TAG :**

TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged.

Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.

Tagged: The device is using the IEEE 802.1Q tagged frame format.

- **VLAN ID :**

VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.

- **Priority :**

  Priority is the Layer 2 priority to be used for the specified application type.One of the eight priority levels (0 through 7).

- **DSCP :**

  DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).

- **Auto-negotiation**

  Auto-negotiation identifies if MAC/PHY auto-negotiation is supported by the link partner.

- **Auto-negotiation status**

  Auto-negotiation status identifies if auto-negotiation is currently enabled at the link partner. If **Auto-negotiation** is supported and **Auto-negotiation status** is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.

- **Auto-negotiation Capabilities**

  Auto-negotiation Capabilities shows the link partners MAC/PHY capabilities.

Buttons

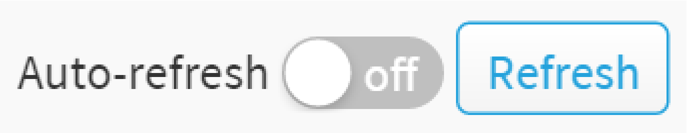


Figure 3-5.4: The LLDP Neighbor buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

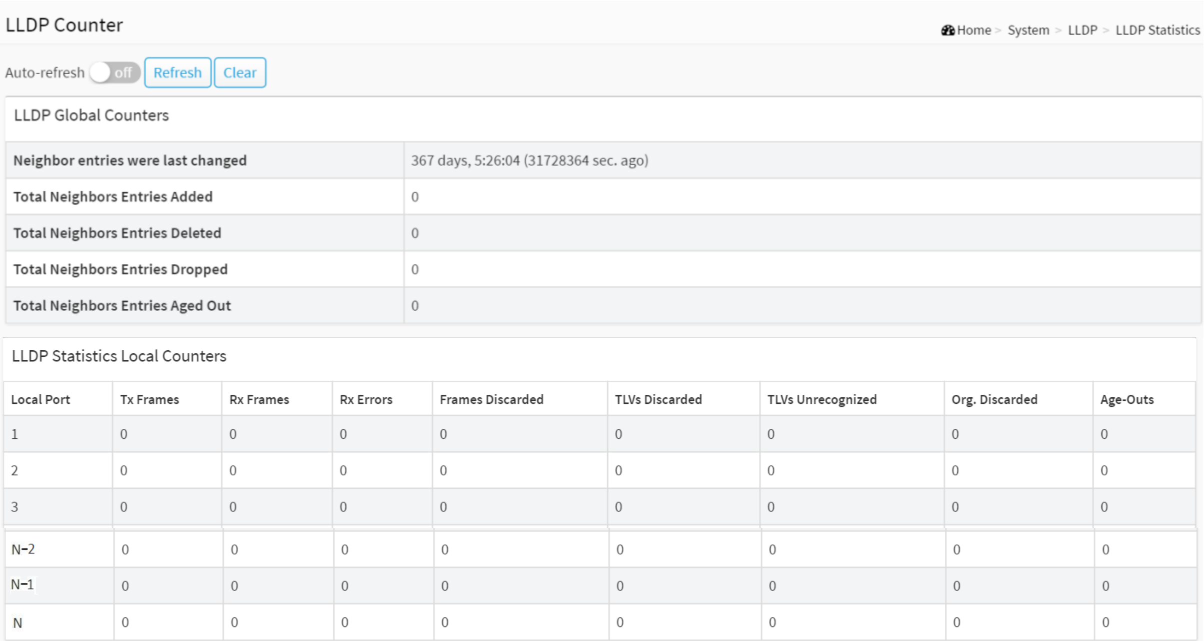
3-5.5 LLDP Statistics

Two types of counters are shown. Global counters are counters that refer to the whole switch, while local counters refer to per port counters for the currently selected switch.

Web Interface

To show LLDP Statistics:

1. Click System ,LLDP and LLDP Statistics.
2. Click Refresh for manual update web screen.
3. Click Auto-refresh for auto-update web screen.
4. Click Clear to clear all counters.



LLDP Global Counters

Neighbor entries were last changed	367 days, 5:26:04 (31728364 sec. ago)
Total Neighbors Entries Added	0
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
N-2	0	0	0	0	0	0	0	0
N-1	0	0	0	0	0	0	0	0
N	0	0	0	0	0	0	0	0

Figure 3-5.5: The LLDP Statistics information

Parameter description:

Global Counters

- **Neighbour entries were last changed at :**

  It also shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.

- **Total Neighbours Entries Added :**

  Shows the number of new entries added since switch reboot.

- **Total Neighbours Entries Deleted :**

  Shows the number of new entries deleted since switch reboot.

- **Total Neighbours Entries Dropped :**

  Shows the number of LLDP frames dropped due to the entry table being full.

- **Total Neighbours Entries Aged Out :**

Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

The displayed table contains a row for each port. The columns hold the following information:

- **Local Port :**

  The port on which LLDP frames are received or transmitted.

- **Tx Frames :**

  The number of LLDP frames transmitted on the port.

- **Rx Frames :**

  The number of LLDP frames received on the port.

- **Rx Errors :**

  The number of received LLDP frames containing some kind of error.

- **Frames Discarded :**

  If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbours" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out.

- **TLVs Discarded :**

  Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.

- **TLVs Unrecognized :**

  The number of well-formed TLVs, but with an unknown type value.

- **Org. Discarded :**

  The number of organizationally received TLVs.

- **Age-Outs :**

  Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.

Buttons

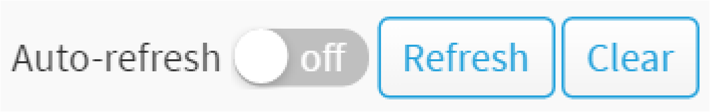


Figure 3-5.5: The LLDP Statistics information buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Clears the counters for the selected port.

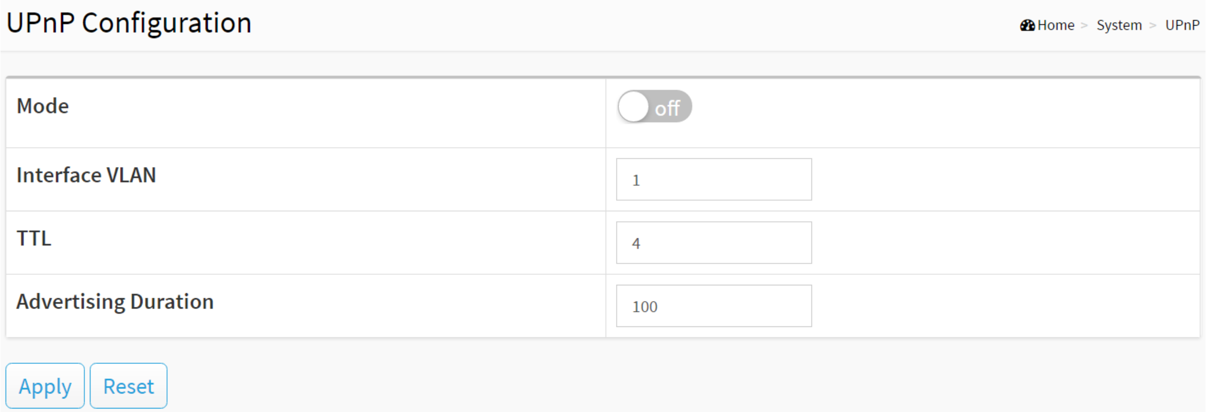
3-6 UPnP

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

Web Interface

To configure the UPnP Configuration in the web interface:

1. Click System and UPnP
2. Scroll to select the mode to enable or disable
3. Specify the parameters in each blank field.
4. Click the Apply to save the setting
5. If you want to cancel the setting then you need to click the Reset button.
6. It will revert to previously saved values



UPnP Configuration

Home > System > UPnP

Mode	off
Interface VLAN	1
TTL	4
Advertising Duration	100

Figure 3-6: The UPnP Configuration

Parameter description:

These parameters are displayed on the UPnP Configuration page:

- **Mode :**

  Indicates the UPnP operation mode. Possible modes are:

  Enabled: Enable UPnP mode operation.

  Disabled: Disable UPnP mode operation.

  When the mode is enabled, two ACEs are added automatically to trap UPNP related packets to CPU. The ACEs are automatically removed when the mode is disabled.

- **Interface VLAN :**

  Configure the interface VLAN that is used by UPnP. Allowed VLAN are in the range 1 through 4095, default being 1.

- **TTL :**

  The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range 1 to 255.

- **Advertising Duration :**

  The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range 100 to 86400.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

Chapter 4 Port Management

The section describes to configure the Port detail parameters of the switch. Others you could use the Port configure to enable or disable the Port of the switch. Monitor the ports content or status in the function.

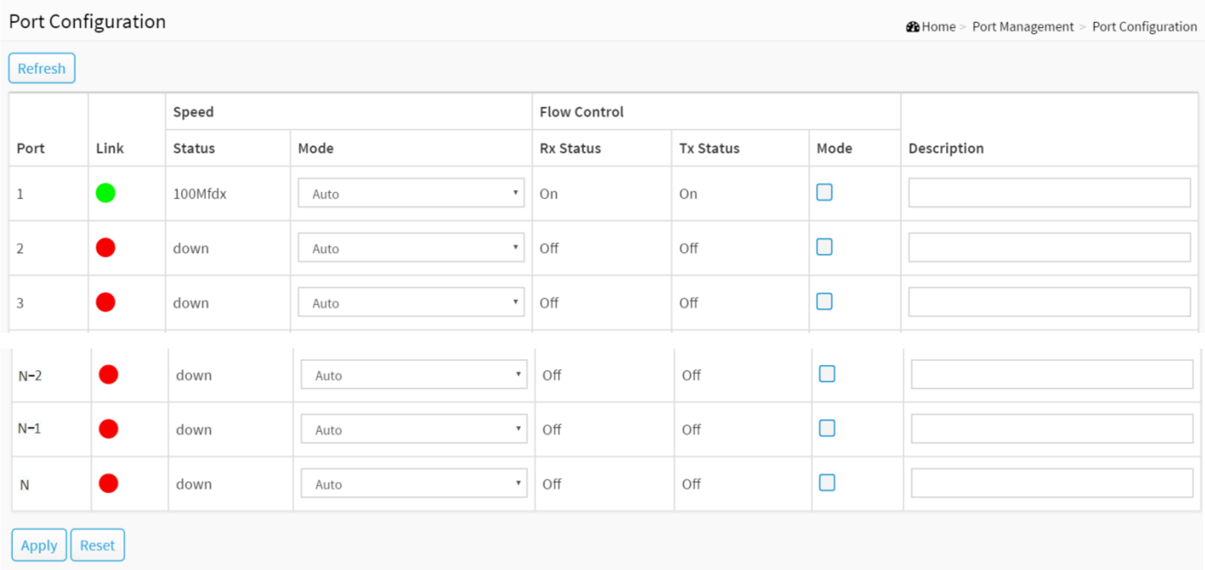
4-1 Port Configuration

This page displays current port configurations. Ports can also be configured here.

Web Interface

To configure a Current Port Configuration in the web interface:

1. Click Port Management and Port Configuration.
2. Specify the Speed Configured, Flow Control.
3. Specify the detail Port alias or description an alphanumeric string describing the full name and version identification for the system's hardware type, software version, and networking application.
4. Click Apply.



Port Configuration

		Speed		Flow Control			
Port	Link	Status	Mode	Rx Status	Tx Status	Mode	Description
1	🟢	100Mfdx	Auto	On	On	□	
2	🔴	down	Auto	Off	Off	□	
3	🔴	down	Auto	Off	Off	□	
N-2	🔴	down	Auto	Off	Off	□	
N-1	🔴	down	Auto	Off	Off	□	
N	🔴	down	Auto	Off	Off	□	

Figure 4-1: The Port Configuration

Parameter description:

- **Port :**

  This is the logical port number for this row.

- **Link :**

  The current link state is displayed graphically. Green indicates the link is up and red that it is down.

- **Current Link Speed :**

  Provides the current link speed of the port.

- **Configured Link Speed :**

  Selects any available link speed for the given switch port. Only speeds supported by the specific port is shown. Possible speeds are:

  Disabled - Disables the switch port operation.

  Auto - Port auto negotiate speed with the link partner and selects the highest speed that is compatible with the link partner.

  10Mbps HDX - Forces the cu port in 10Mbps half-duplex mode.

  10Mbps FDX - Forces the cu port in 10Mbps full duplex mode.

  100Mbps HDX - Forces the cu port in 100Mbps half-duplex mode.

  100Mbps FDX - Forces the cu port in 100Mbps full duplex mode.

  1Gbps FDX - Forces the port in 1Gbps full duplex

  2.5Gbps FDX - Forces the Serdes port in 2.5Gbps full duplex mode.

  SFP_Auto_AMS - Automatically determines the speed of the SFP. Note: There is no standardized way to do SFP auto detect, so here it is done by reading the SFP rom. Due to the missing standardized way of doing SFP auto detect some SFPs might not be detectable. The port is set in AMS mode. Cu port is set in Auto mode.

  100-FX - SFP port in 100-FX speed. Cu port disabled.

  100-FX_AMS - Port in AMS mode. SFP port in 100-FX speed. Cu port in Auto mode.

  1000-X - SFP port in 1000-X speed. Cu port disabled.

  1000-X_AMS - Port in AMS mode. SFP port in 1000-X speed. Cu port in Auto mode. Ports in AMS mode with 1000-X speed has Cu port preferred. Ports in AMS mode with 100-FX speed has fiber port preferred.

- **Flow Control :**

  When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation.

  Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.

- **Description :**

  Enter up to 63 characters to be descriptive name for identifies this port.

Buttons

- **Refresh :**

  You can click them for refresh the Port link Status by manual

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

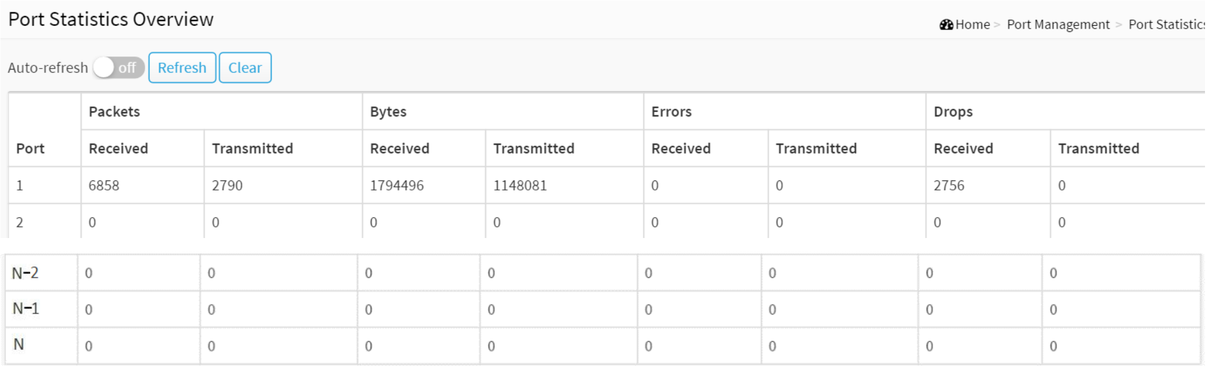
4-2 Port Statistics

The section describes to the Port statistics information and provides overview of general traffic statistics for all switch ports.

Web Interface

To Display the Port Statistics Overview in the web interface:

1. Click Port Management and Port Statistics.
2. If you want to auto-refresh then you need to evoke the "Auto-refresh".
3. Click " Refresh" to refresh the port statistics or clear all information when you click " Clear".
4. If you want to see the detail of port statistic then you need to click that port



Port Statistics Overview

	Packets		Bytes		Errors		Drops	
Port	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted
1	6858	2790	1794496	1148081	0	0	2756	0
2	0	0	0	0	0	0	0	0
N-2	0	0	0	0	0	0	0	0
N-1	0	0	0	0	0	0	0	0
N	0	0	0	0	0	0	0	0

Figure 4-2: The Port Statistics Overview

Parameter description:

- **Port :**

  The logical port for the settings contained in the same row.

- **Packets :**

  The number of received and transmitted packets per port.

- **Bytes :**

  The number of received and transmitted bytes per port.

- **Errors :**

  The number of frames received in error and the number of incomplete transmissions per port.

- **Drops :**

  The number of frames discarded due to ingress or egress congestion.

Buttons

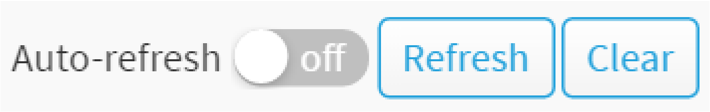


Figure 4-2: The Port Statistics Overview buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

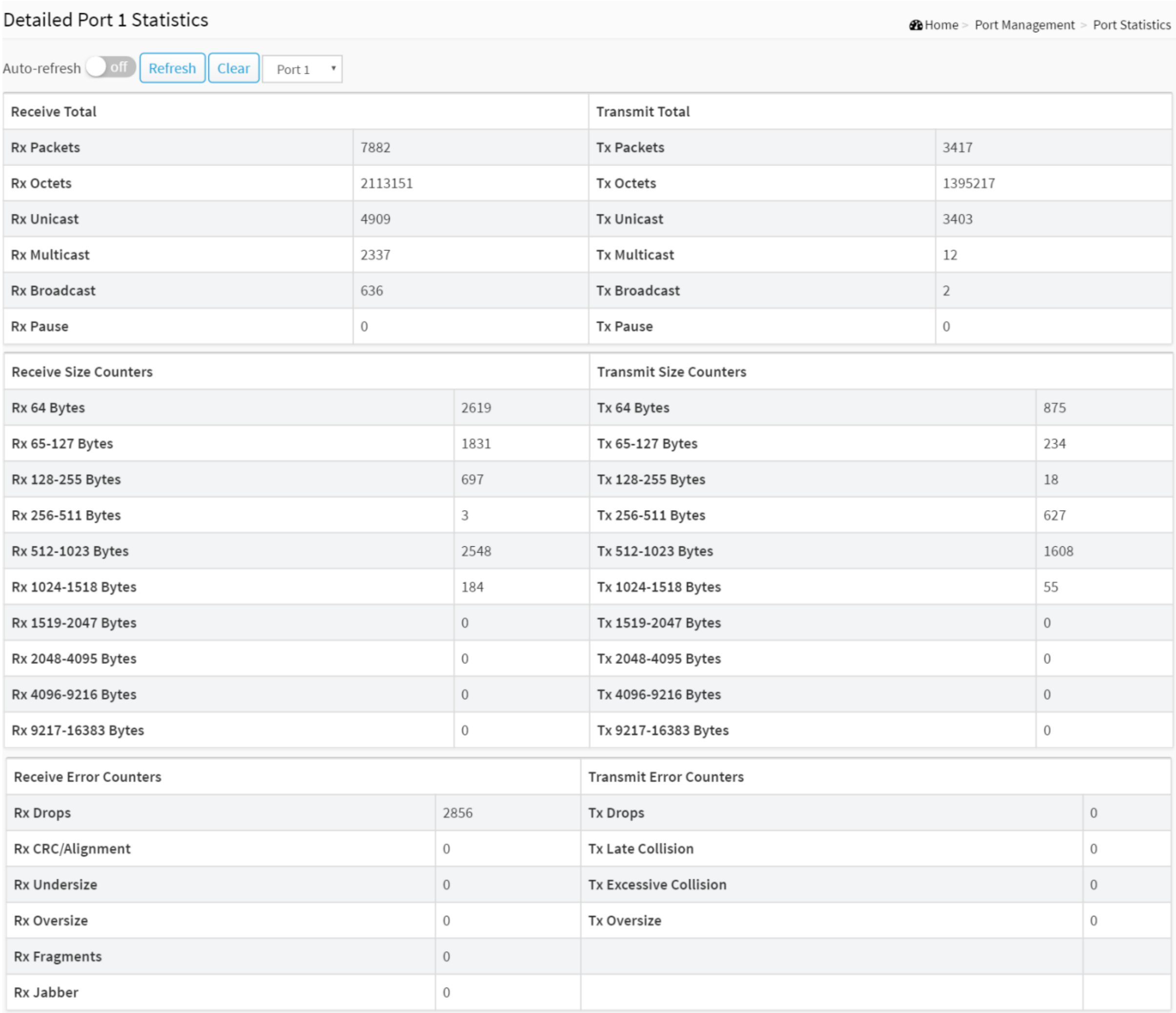
- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Clears the counters for all ports.

If you want to see the detail of port statistic then you need to click that port. The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.


Detailed Port 1 Statistics
Home > Port Management > Port Statistics
Auto-refresh off
Refresh
Clear
Port 1

Receive Total		Transmit Total	
Rx Packets	7882	Tx Packets	3417
Rx Octets	2113151	Tx Octets	1395217
Rx Unicast	4909	Tx Unicast	3403
Rx Multicast	2337	Tx Multicast	12
Rx Broadcast	636	Tx Broadcast	2
Rx Pause	0	Tx Pause	0

Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	2619	Tx 64 Bytes	875
Rx 65-127 Bytes	1831	Tx 65-127 Bytes	234
Rx 128-255 Bytes	697	Tx 128-255 Bytes	18
Rx 256-511 Bytes	3	Tx 256-511 Bytes	627
Rx 512-1023 Bytes	2548	Tx 512-1023 Bytes	1608
Rx 1024-1518 Bytes	184	Tx 1024-1518 Bytes	55
Rx 1519-2047 Bytes	0	Tx 1519-2047 Bytes	0
Rx 2048-4095 Bytes	0	Tx 2048-4095 Bytes	0
Rx 4096-9216 Bytes	0	Tx 4096-9216 Bytes	0
Rx 9217-16383 Bytes	0	Tx 9217-16383 Bytes	0

Receive Error Counters		Transmit Error Counters	
Rx Drops	2856	Tx Drops	0
Rx CRC/Alignment	0	Tx Late Collision	0
Rx Undersize	0	Tx Excessive Collision	0
Rx Oversize	0	Tx Oversize	0
Rx Fragments	0		
Rx Jabber	0		

Figure 4-2: The Detailed Port Statistics

Parameter description:

- **Upper left scroll bar:**

  To scroll which port to display the Port statistics with “Port-1”, “Port-2”, ...

Receive Total and Transmit Total

- **Rx and Tx Packets :**

  The number of received and transmitted (good and bad) packets.

- **Rx and Tx Octets :**

  The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.

- **Rx and Tx Unicast :**

  The number of received and transmitted (good and bad) unicast packets.

- **Rx and Tx Multicast :**

  The number of received and transmitted (good and bad) multicast packets.

- **Rx and Tx Broadcast :**

  The number of received and transmitted (good and bad) broadcast packets.

- **Rx and Tx Pause :**

  A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

Receive and Transmit Size Counters

The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive Error Counters

- **Rx Drops :**

  The number of frames dropped due to lack of receive buffers or egress congestion.

- **Rx CRC/Alignment :**

  The number of frames received with CRC or alignment errors.

- **Rx Undersize :**

  The number of short 1 frames received with valid CRC.

- **Rx Oversize :**

  The number of long 2 frames received with valid CRC.

- **Rx Fragments :**

  The number of short 1 frames received with invalid CRC.

- **Rx Jabber :**

  The number of long 2 frames received with invalid CRC. .

Transmit Error Counters

- **Tx Drops :**

  The number of frames dropped due to output buffer congestion.

- **Tx Late/Exc. Coll. :**

  The number of frames dropped due to excessive or late collisions.

- **Tx Oversize :**

  The number of frames dropped due to frame oversize.

Buttons

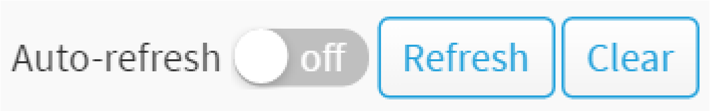


Figure 4-2: The Detailed Port Statistics buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Clears the counters for the selected port.

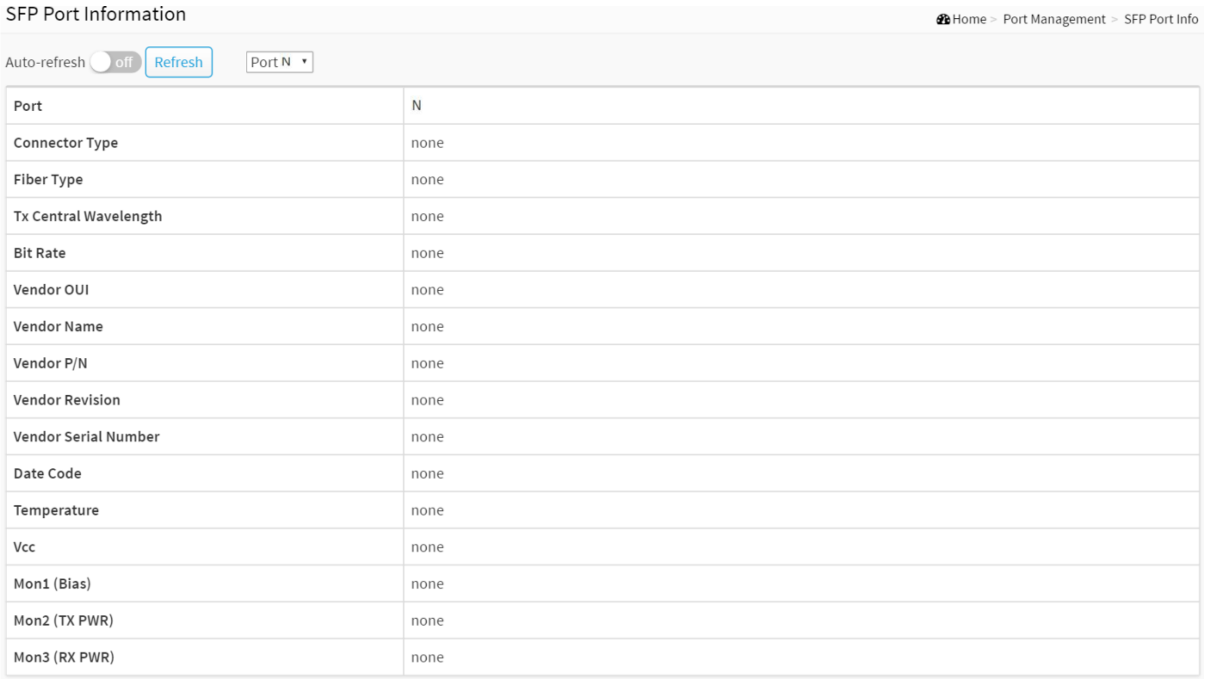
4-3 SFP Port Info

The section describes that switch could display the SFP module detail information which you connect it to the switch. The information includes: Connector type, Fiber type, wavelength, bit rate and Vendor OUI etc.

Web Interface

To Display the SFP information in the web interface:

1. Click Port Management and SFP Port Info.
2. To display the SFP Information.



Port	N
Connector Type	none
Fiber Type	none
Tx Central Wavelength	none
Bit Rate	none
Vendor OUI	none
Vendor Name	none
Vendor P/N	none
Vendor Revision	none
Vendor Serial Number	none
Date Code	none
Temperature	none
Vcc	none
Mon1 (Bias)	none
Mon2 (TX PWR)	none
Mon3 (RX PWR)	none

Figure 4-3: The SFP Port Information

Parameter description:

- **Upper left scroll bar:**

  To scroll which port to display the Port statistics.

- **Connector Type:**

  Display the connector type, for instance, UTP, SC, ST, LC and so on.

- **Fiber Type:**

  Display the fiber mode, for instance, Multi-Mode, Single-Mode.

- **Tx Central Wavelength:**

  Display the fiber optical transmitting central wavelength, for instance, 850nm, 1310nm, 1550nm and so on.

- **Bit Rate:**

  Displays the nominal bit rate of the transceiver.

- **Vendor OUI:**

Display the Manufacturer's OUI code which is assigned by IEEE.

- **Vendor Name:**

  Display the company name of the module manufacturer.

- **Vendor P/N:**

  Display the product name of the naming by module manufacturer.

- **Vendor Rev (Revision):**

  Display the module revision.

- **Vendor SN (Serial Number):**

  Show the serial number assigned by the manufacturer.

- **Date Code:**

  Show the date this SFP module was made.

- **Temperature:**

  Show the current temperature of SFP module.

- **Vcc:**

  Show the working DC voltage of SFP module.

- **Mon1(Bias) mA:**

  Show the Bias current of SFP module.

- **Mon2(TX PWR):**

  Show the transmit power of SFP module.

- **Mon3(RX PWR):**

  Show the receiver power of SFP module.

Buttons

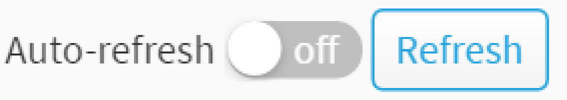


Figure 4-3: The SFP Port Information buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page.

4-4 Energy Efficient Ethernet

EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

This page allows the user to inspect and configure the current EEE port settings.

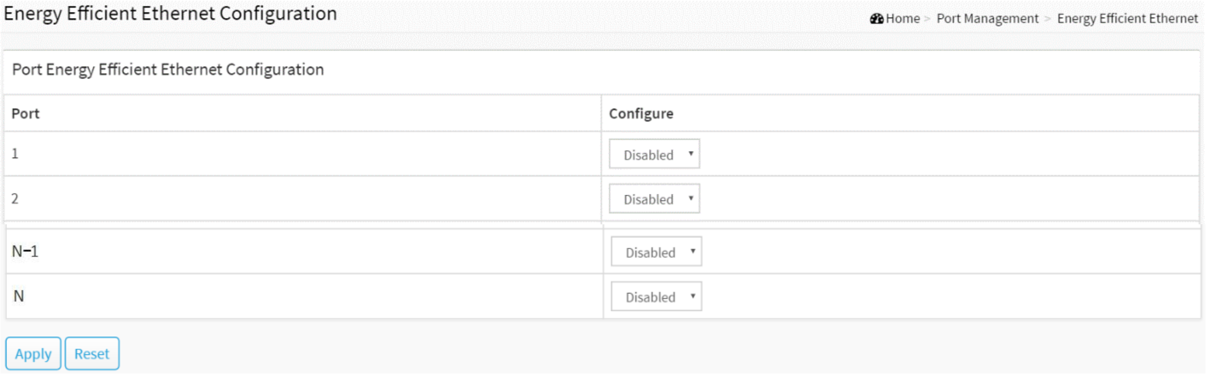
EEE is a power saving option that reduces the power usage when there is very low traffic utilization (or no traffic).

EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted all circuits are powered up. The time it takes to power up the circuits is named wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange information about the devices wakeup time using the LLDP protocol.

Web Interface

To configure an Energy Efficient Ethernet in the web interface:

1. Click Port Management and Energy Efficient Ethernet..
2. Select enable or disable Energy Efficient Ethernet by the port.
3. Click the apply to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



Energy Efficient Ethernet Configuration

Home > Port Management > Energy Efficient Ethernet

Port Energy Efficient Ethernet Configuration

Port	Configure
1	Disabled
2	Disabled
N-1	Disabled
N	Disabled

Figure 4-4: The Energy Efficient Ethernet Configuration

Parameter description:

- **Port :**

  The switch port number of the logical EEE port.

- **Configure :**

  Controls whether EEE is enabled for this switch port.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

4-5 Link Aggregation

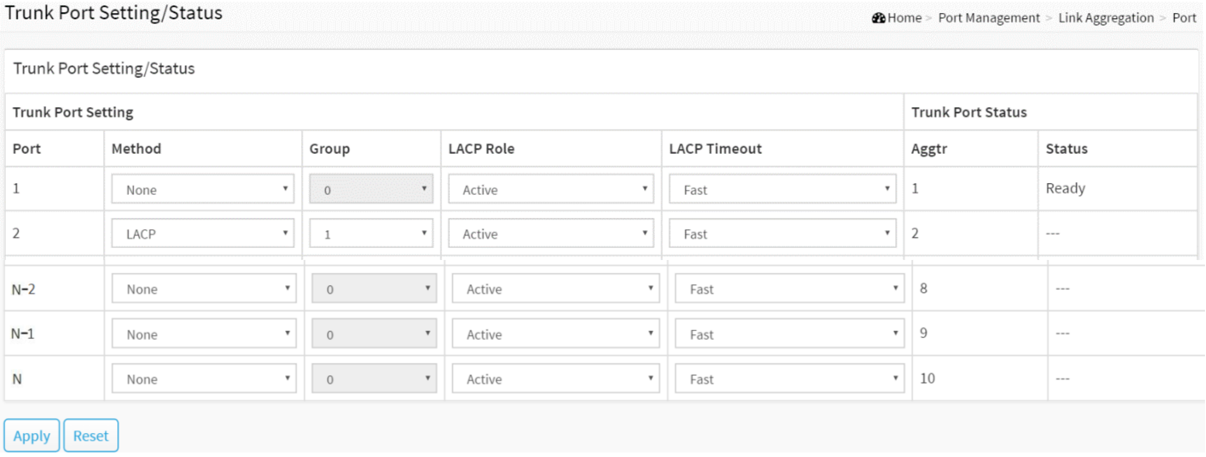
4-5.1 Port

This section describes that Port setting/status is used to configure the trunk property of each and every port in the switch system.

Web Interface

To configure the trunk property of each and every port in the web interface:

1. Click Port Management, Link Aggregation and port.
2. Specify the Method, Group, LACP Role and LACP Timeout.
3. Click the apply to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



Trunk Port Setting/Status

Home > Port Management > Link Aggregation > Port

Trunk Port Setting/Status

Trunk Port Setting					Trunk Port Status	
Port	Method	Group	LACP Role	LACP Timeout	Aggtr	Status
1	None	0	Active	Fast	1	Ready
2	LACP	1	Active	Fast	2	---
N-2	None	0	Active	Fast	8	---
N-1	None	0	Active	Fast	9	---
N	None	0	Active	Fast	10	---

Figure 4-5.1: The trunk port setting/status

Parameter description :

- **Port :**

  The logical port for the settings contained in the same row.

- **Method :**

  This determines the method a port uses to aggregate with other ports.

  - None :

    A port does not want to aggregate with any other port should choose this default setting.

  - LACP :

    A port use LACP as its trunk method to get aggregated with other ports also using LACP.

  - Static :

    A port use Static Trunk as its trunk method to get aggregated with other ports also using Static Trunk.

- **Group :**

Ports choosing the same trunking method other than "None" must be assigned a unique Group number in order to declare that they wish to aggregate with each other.

- **LACP Role:**

  This field is only referenced when a port's trunking method is LACP.

  - ◆ Active :

    An Active LACP port begins to send LACPDU to its link partner right after the LACP protocol entity started to take control of this port.

  - ◆ Passive :

    A Passive LACP port will not actively send LACPDU out before it receives an LACPDU from its link partner.

- **LACP Timeout :**

  The Timeout controls the period between BPDU transmissions.

  - ◆ Fast :

    It will transmit LACP packets each second,

  - ◆ Slow :

    It will wait for 30 seconds before sending a LACP packet.

- **Aggtr :**

  Aggtr is an abbreviation of "aggregator". Every port is also an aggregator, and its own aggregator ID is the same as its own Port No. We can regard an aggregator as a representative of a trunking group. Ports with same Group ID and using same trunking method will have the opportunity to aggregate to a particular aggregator port. This aggregator port is usually the port with the smallest Port No. within the trunking group.

- **Status :**

  This field represents the trunking status of a port which uses a trunking method other than "None". It also represents the management link status of a port which uses the "None" trunking method. "---" means "not ready"

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

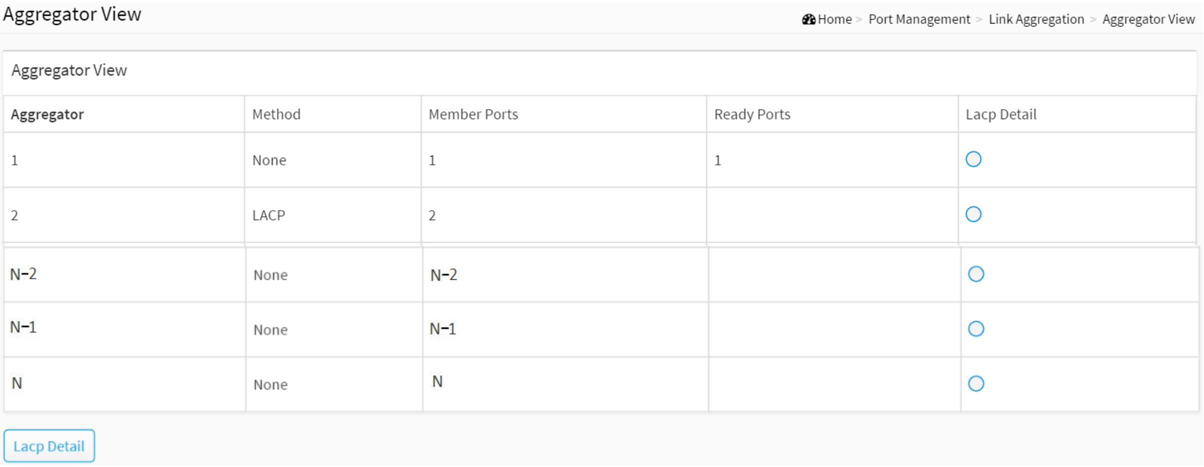
4-5.2 Aggregator View

To display the current port trunking information from the aggregator point of view.

Web Interface

To see the LACP detail in the web interface:

1. Click Port Management, Link Aggregation and Aggregator View.
2. Click the LACP Detail.



Aggregator View

Home > Port Management > Link Aggregation > Aggregator View

Aggregator View

Aggregator	Method	Member Ports	Ready Ports	Lacp Detail
1	None	1	1	○
2	LACP	2		○
N-2	None	N-2		○
N-1	None	N-1		○
N	None	N		○

Figure 4-5.2: The Aggregator View

Parameter description:

- **Aggregator :**

  It shows the aggregator ID of every port. In fact, every port is also an aggregator, and its own aggregator ID is the same as its own Port No..

- **Method :**

  Show the method a port uses to aggregate with other ports.

- **Member Ports :**

  Show all member ports of an aggregator (port).

- **Ready Ports :**

  Show only the ready member ports within an aggregator (port).

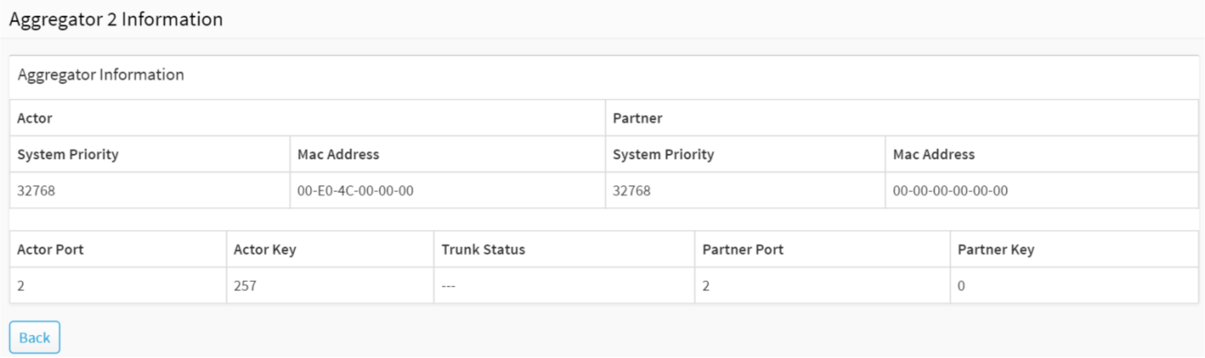
- **Lacp Detail :**

  You can select the port that you want to see the LACP Detail.

Buttons

- **Lacp Detail :**

  Click this button then you will see the aggregator information, Details will be described in the below.



Aggregator 2 Information

Aggregator Information

Actor		Partner	
System Priority	Mac Address	System Priority	Mac Address
32768	00-E0-4C-00-00-00	32768	00-00-00-00-00-00

Actor Port	Actor Key	Trunk Status	Partner Port	Partner Key
2	257	---	2	0

Figure 4-5.2: The Lacp Detail

Parameter description:

Actor

- **System Priority :**

  Show the System Priority part of the aggregation Actor. (1-65535)

- **Mac Address :**

  The system ID of the aggregation Actor.

- **Actor Port :**

  The actor's port number connected to this port.

- **Actor Key :**

  The Key that the actor has assigned to this aggregation ID.

Partner

- **System Priority :**

  Show the System Priority part of the aggregation partner. (1-65535)

- **Mac Address :**

  The system ID of the aggregation partner.

- **Partner Port :**

  The partner's port number connected to this port.

- **Partner Key :**

  The Key that the partner has assigned to this aggregation ID.

- **Trunk Status :**

  This field represents the trunking status of a port which uses a trunking method other than "None". It also represents the management link status of a port which uses the "None" trunking method. "---" means "not ready"

Button

- **Back :**

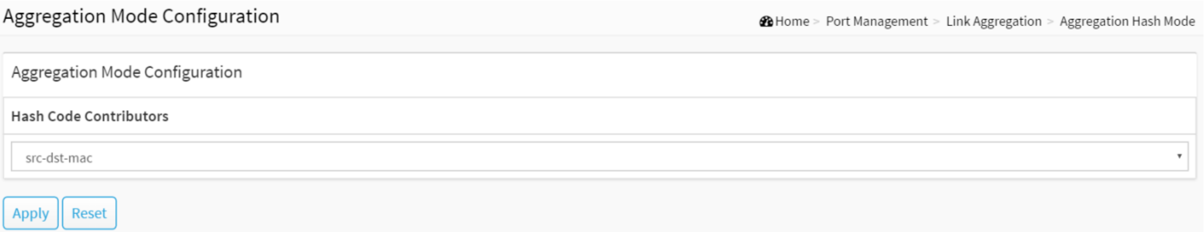
  Click to undo any changes made locally and return to the Users.

4-5.3 Aggregation Hash Mode

Web Interface

To configure the Aggregation hash mode in the web interface:

1. Click Port Management, Link Aggregation and Aggregator Hash Mode.
2. Click Hash Code Contributors to select the mode.
3. Click the apply to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



Aggregation Mode Configuration

Home > Port Management > Link Aggregation > Aggregation Hash Mode

Aggregation Mode Configuration

Hash Code Contributors: src-dst-mac

Figure 4-5.3: Aggregation Hash Mode

Parameter description:

Hash Code Contributors

- **src-mac :**

  Source MAC Address

  The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.

- **dst-mac :**

  Destination MAC Address

  The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled.

- **ip :**

  IP Address

  The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.

- **src-dst-mac :**

  Source MAC Address + Destination MAC Address.

- **src-ip :**

  Source IP Address.

- **dst-ip :**

  Destination IP Address.

- **src-dst-ip :**

  Source IP Address + Destination IP Address.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

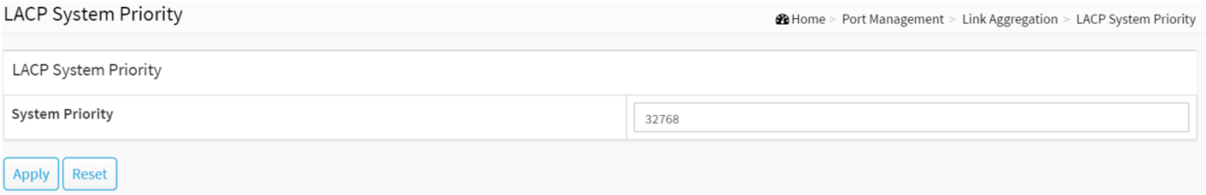
4-5.4 LACP System Priority

It is used to set the priority part of the LACP system ID. LACP will only aggregate together the ports whose peer link partners are all on a single system. Each system supports LACP will be assigned a globally unique System Identifier for this purpose. A system ID is a 64-bit field comprising a 48-bit MAC Address and 16-bit priority value. The System Priority can be set by the user. Its range is from 1 to 65535. Default: 32768

Web Interface

To configure the LACP System Priority in the web interface:

1. Click Port Management, Link Aggregation and LACP System Priority.
2. Specify the LACP System Priority.
3. Click the apply to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



LACP System Priority

Home > Port Management > Link Aggregation > LACP System Priority

LACP System Priority

System Priority	32768

Figure 4-5.4: The Lacp System Priority

Parameter description:

- **System Priority:**

  1-65535.

  Show the System Priority part of a system ID.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

4-6 Loop Protection

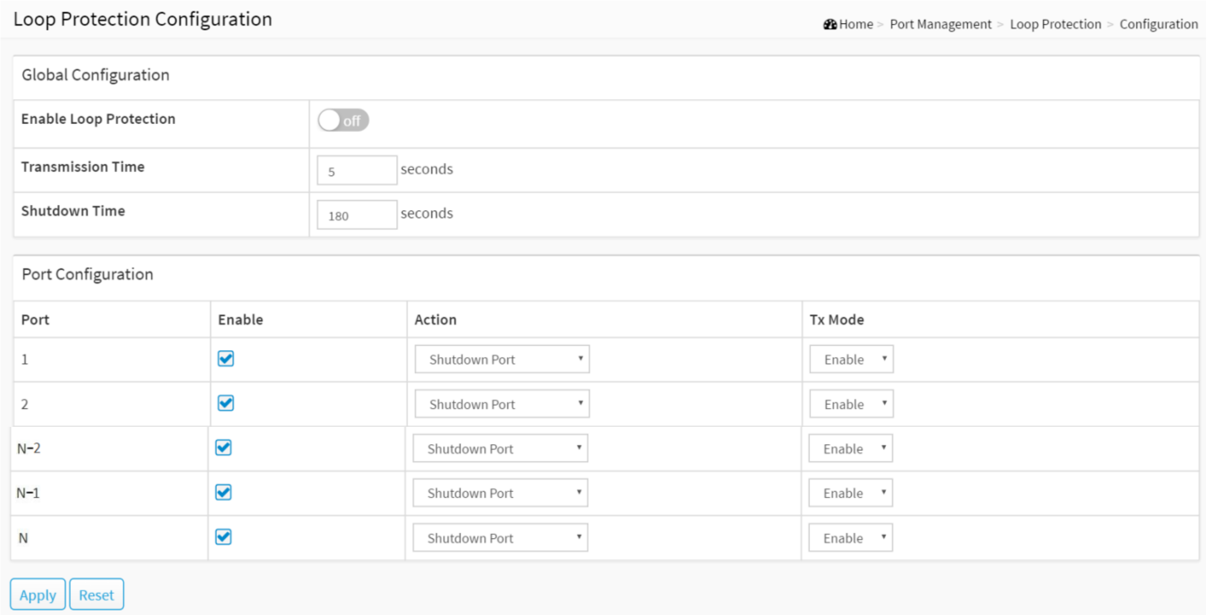
4-6.1 Configuration

The loop Protection is used to detect the presence of traffic. When switch receives packet's (looping detection frame) MAC address the same as oneself from port, show Loop Protection happens. The port will be locked when it received the looping Protection frames. If you want to resume the locked port, please find out the looping path and take off the looping path, then select the resume the locked port and click on "Resume" to turn on the locked ports.

Web Interface

To configure the Loop Protection parameters in the web interface:

1. Click Port Management, Loop Protection and Configuration.
2. Evoke to select enable or disable the port loop Protection
3. Click the apply to save the setting
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values



Loop Protection Configuration

Home > Port Management > Loop Protection > Configuration

Global Configuration

Enable Loop Protection	off
Transmission Time	5 seconds
Shutdown Time	180 seconds

Port Configuration

Port	Enable	Action	Tx Mode
1	☑	Shutdown Port	Enable
2	☑	Shutdown Port	Enable
N-2	☑	Shutdown Port	Enable
N-1	☑	Shutdown Port	Enable
N	☑	Shutdown Port	Enable

Figure 4-6.1: The Loop Protection Configuration

Parameter description :

Global Configuration

- **Enable Loop Protection :**

  Controls whether loop protections is enabled (as a whole).

- **Transmission Time :**

  The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds.

- **Shutdown Time :**

The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 10 to 604800 seconds (7 days).

Port Configuration

- **Port :**

  The switch port number of the port.

- **Enable :**

  Controls whether loop protection is enabled on this switch port

- **Action:**

  Configures the action performed when a loop is detected on a port. Valid values are Shutdown Port, Shutdown Port and Log or Log Only.

- **Tx Mode :**

  Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

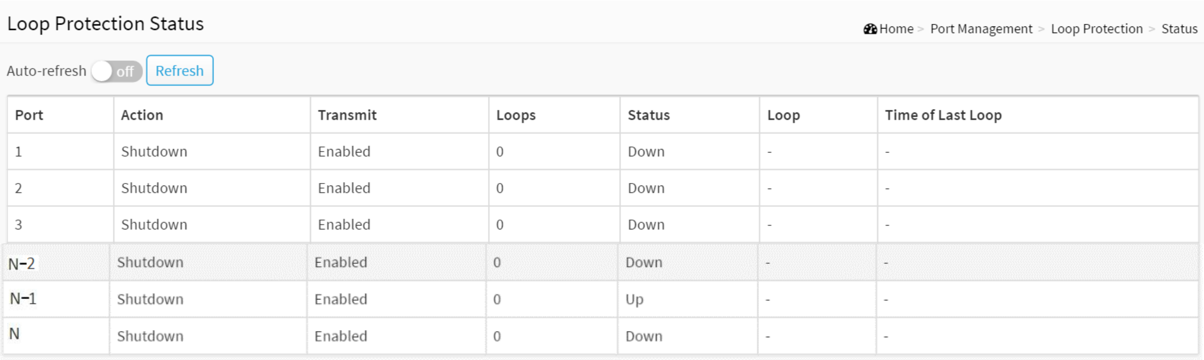
4-6.2 Status

This section displays the loop protection port status the ports of the currently selected switch.

Web Interface

To display the Loop Protection status in the web interface:

1. Click Port Management, Loop Protection and Status.
2. If you want to auto-refresh the information then you need to evoke the "Auto refresh".
3. Click "Refresh" to refresh the Loop Protection Status.


Loop Protection Status

Home > Port Management > Loop Protection > Status

Auto-refresh off Refresh

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	-	-
N-2	Shutdown	Enabled	0	Down	-	-
N-1	Shutdown	Enabled	0	Up	-	-
N	Shutdown	Enabled	0	Down	-	-

Figure 4-6.2: Loop Protection Status

Parameter description:

- **Port**

  The switch port number of the logical port.

- **Action**

  The currently configured port action.

- **Transmit**

  The currently configured port transmit mode.

- **Loops**

  The number of loops detected on this port.

- **Status**

  The current loop protection status of the port.

- **Loop**

  Whether a loop is currently detected on the port.

- **Time of Last Loop**

  The time of the last loop event detected.

Buttons

Figure 4-6.2: Loop Protection Status buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

Chapter 5 PoE Management

PoE is an acronym for Power over Ethernet. Power over Ethernet is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

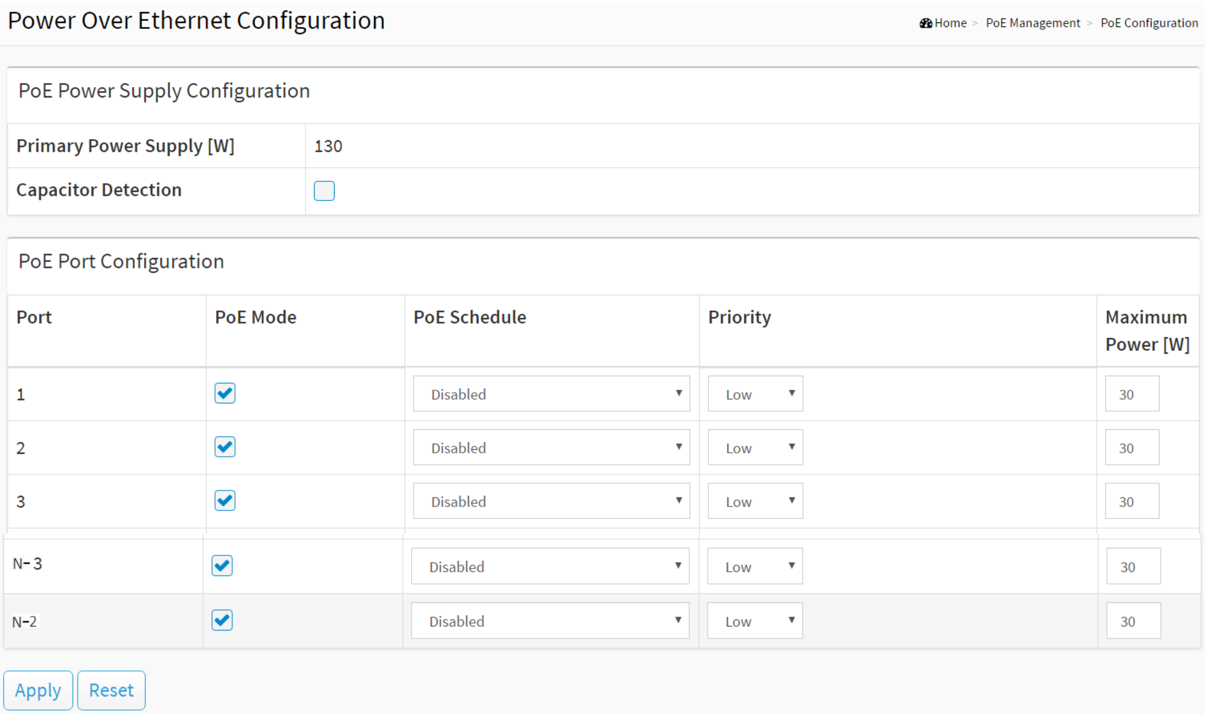
5-1 PoE Configuration

This page allows the user to inspect and configure the current PoE port settings and show all PoE Supply W.

Web Interface

To configure Power over Ethernet in the web interface:

1. Click PoE Management and PoE Configuration.
2. Specify the PoE or PoE+ Mode, PoE Schedule, Priority and Maximum Power(W).
3. Click Apply to save the configuration.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



Power Over Ethernet Configuration

PoE Power Supply Configuration

Primary Power Supply [W]	130
Capacitor Detection	☐

PoE Port Configuration

Port	PoE Mode	PoE Schedule	Priority	Maximum Power [W]
1	☑	Disabled	Low	30
2	☑	Disabled	Low	30
3	☑	Disabled	Low	30
N-3	☑	Disabled	Low	30
N-2	☑	Disabled	Low	30

Figure 5-1: PoE Configuration

Parameter description:

PoE Power Supply Configuration

- **Primary Power Supply [W] :**

  To display watts for the primary power supply.

- **Capacitor Detection :**

  Click to enable or disable the capacitor configuration.

PoE Port Configuration

- **Port :**

  This is the logical port number for this row.

- **PoE Mode :**

  The PoE Mode represents the PoE operating mode for the port. Enable or Disable PoE.

- **PoE Schedule :**

  Disable or Select the PoE Schedule profile.

- **Priority :**

  The Priority represents the ports priority. There are three levels of power priority named Low, High and Critical.

  The priority is used in the case where the remote devices requires more power than the power supply can deliver. In this case the port with the lowest priority will be turn off starting from the port with the highest port number.

- **Maximum Power [W] :**

  The Maximum Power value contains a numerical value that indicates the maximum power in watts that can be delivered to a remote device.

  The maximum allowed value is 30 W.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

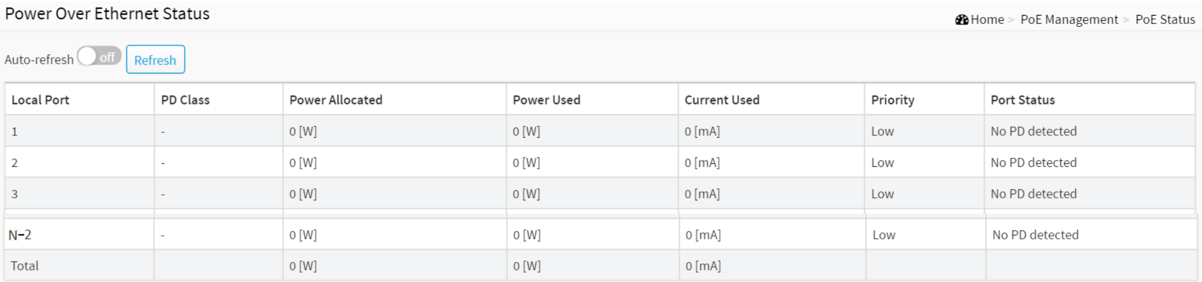
5-2 PoE Status

This page allows the user to inspect the current status for all PoE ports.

Web Interface

To Display PoE Status in the web interface:

1. Click PoE Management and PoE Status
2. Scroll “Auto-refresh” to on/off.
3. Click “Refresh” to refresh the port detailed statistics.



Power Over Ethernet Status

Local Port	PD Class	Power Allocated	Power Used	Current Used	Priority	Port Status
1	-	0 [W]	0 [W]	0 [mA]	Low	No PD detected
2	-	0 [W]	0 [W]	0 [mA]	Low	No PD detected
3	-	0 [W]	0 [W]	0 [mA]	Low	No PD detected
N-2	-	0 [W]	0 [W]	0 [mA]	Low	No PD detected
Total		0 [W]	0 [W]	0 [mA]		

Figure 5-2: The PoE Status

Parameter description:

- **Local Port :**

  This is the logical port number for this row.

- **PD Class :**

  Each PD is classified according to a class that defines the maximum power the PD will use. The PD Class shows the PDs class.

  Five Classes are defined:

  Class 0: Max. power 15.4 W

  Class 1: Max. power 4.0 W

  Class 2: Max. power 7.0 W

  Class 3: Max. power 15.4 W

  Class 4: Max. power 30.0 W

- **Power Allocated :**

  The Power Allocated shows the amount of power the switch has allocated for the PD.

- **Power Used :**

  The Power Used shows how much power the PD currently is using.

- **Current Used :**

  The Power Used shows how much current the PD currently is using.

- **Priority :**

  The Priority shows the port's priority configured by the user.

- **Port Status :**

The Port Status shows the port's status. The status can be one of the following values:

PoE not available - No PoE chip found - PoE not supported for the port.

PoE turned OFF - PoE disabled : PoE is disabled by user.

PoE turned OFF - Power budget exceeded - The total requested or used power by the PDs exceeds the maximum power the Power Supply can deliver, and port(s) with the lowest priority is/are powered down.

No PD detected - No PD detected for the port.

PoE turned OFF - PD overload - The PD has requested or used more power than the port can deliver, and is powered down.

PoE turned OFF - PD is off.

Invalid PD - PD detected, but is not working correctly.

Buttons

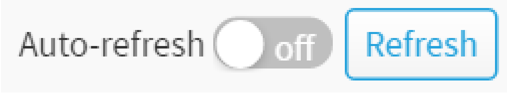


Figure 5-2: The PoE Status buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

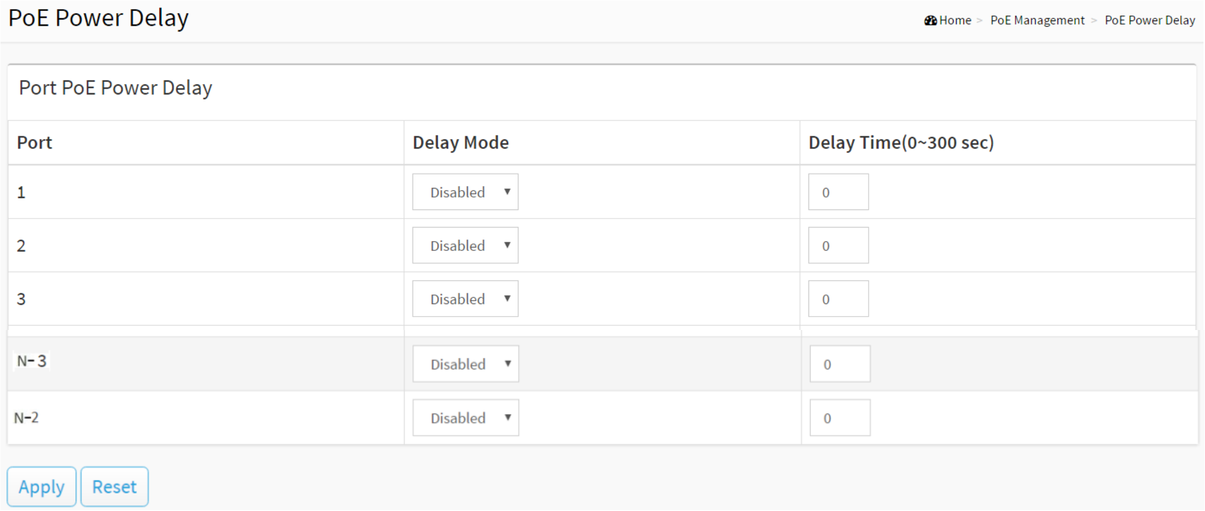
5-3 PoE Power Delay

This page allows the user to setting the delay time of power providing after device rebooted.

Web Interface

To Display Power over Ethernet Status in the web interface:

1. Click PoE Management and PoE Power delay.
2. Enable the port to the power device.
3. Specify the power providing delay time when reboot.
4. Click Apply to apply the change.



PoE Power Delay

Port PoE Power Delay

Port	Delay Mode	Delay Time(0~300 sec)
1	Disabled ▾	0
2	Disabled ▾	0
3	Disabled ▾	0
N-3	Disabled ▾	0
N-2	Disabled ▾	0

Figure 5-3: The PoE Power Delay

Parameter description:

- **Port :**

  This is the logical port number for this row.

- **Delay Mode :**

  Turn on / off the power delay function.

  Enabled: Enable POE Power Delay.

  Disabled: Disable POE Power Delay.

- **Delay Time(0~300sec) :**

  When rebooting, the PoE port will start to provide power to the PD when it out of delay time. Default: 0, range: 0-300 sec.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

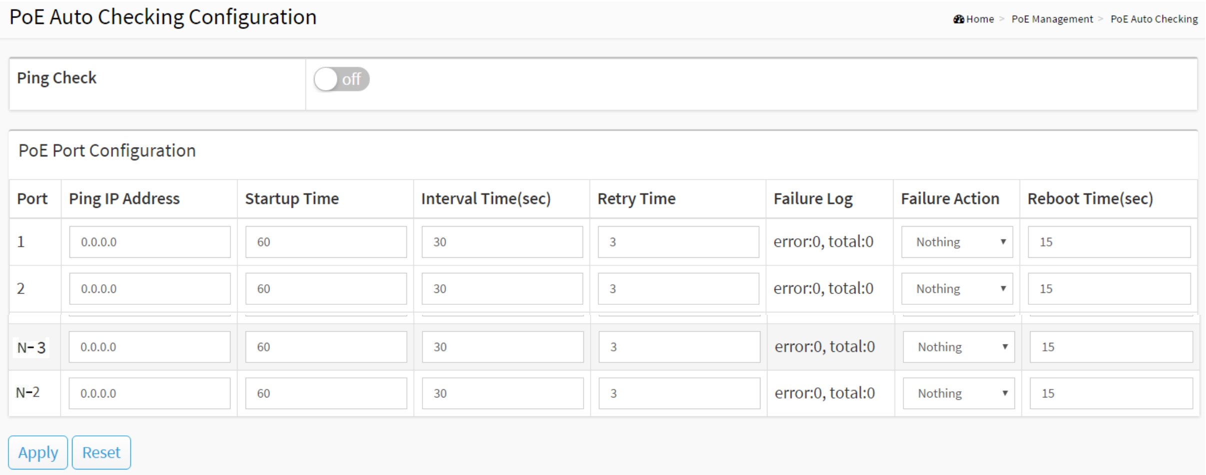
5-4 PoE Auto Checking

This page allows the user to specify the auto detection parameters to check the linking status between PoE ports and PDs. When it detected the fail connect, will reboot remote PD automatically.

Web Interface

To configue Power over Ethernet Auto Checking in the web interface:

1. Click PoE Management and PoE Auto checking.
2. Enable the Ping Check function.
3. Specify the PD’s IP address, checking startup time, interval time, retry time, failure action and reboot time.
4. Click Apply to apply the change.



PoE Auto Checking Configuration

Ping Check: off

PoE Port Configuration

Port	Ping IP Address	Startup Time	Interval Time(sec)	Retry Time	Failure Log	Failure Action	Reboot Time(sec)
1	0.0.0.0	60	30	3	error:0, total:0	Nothing	15
2	0.0.0.0	60	30	3	error:0, total:0	Nothing	15
N- 3	0.0.0.0	60	30	3	error:0, total:0	Nothing	15
N-2	0.0.0.0	60	30	3	error:0, total:0	Nothing	15

Figure 5-4: The PoE Auto Checking

Parameter description:

- **Ping Check :**

  Enable Ping Check function can detects the connection between PoE port and power device. Disable will turn off the detection.

- **Port :**

  This is the logical port number for this row.

- **Ping IP Address :**

  The PD's IP Address the system should ping.

- **Startup Time :**

  After startup time, device will enable auto checking. Default: 30, range: 30-60 sec.

- **Interval Time(sec) :**

  Device will send checking message to PD each interval time. Default: 30, range: 10-120 sec.

- **Retry Time :**

  When PoE port can't ping the PD, it will retry to send detection again. When the third time, it will trigger failure action. Default: 3, range: 1-5.

- **Failure Log :**

  Failure loggings counter.

- **Failure Action :**

  The action when the third fail detection.

  Nothing : Keep Ping the remote PD but does nothing further.

  Reboot : Cut off the power of the PoE port, make PD rebooted.

- **Reboot time(sec) :**

  When PD has been rebooted, the PoE port restored power after the specified time. Default: 15, range: 3-120 sec.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

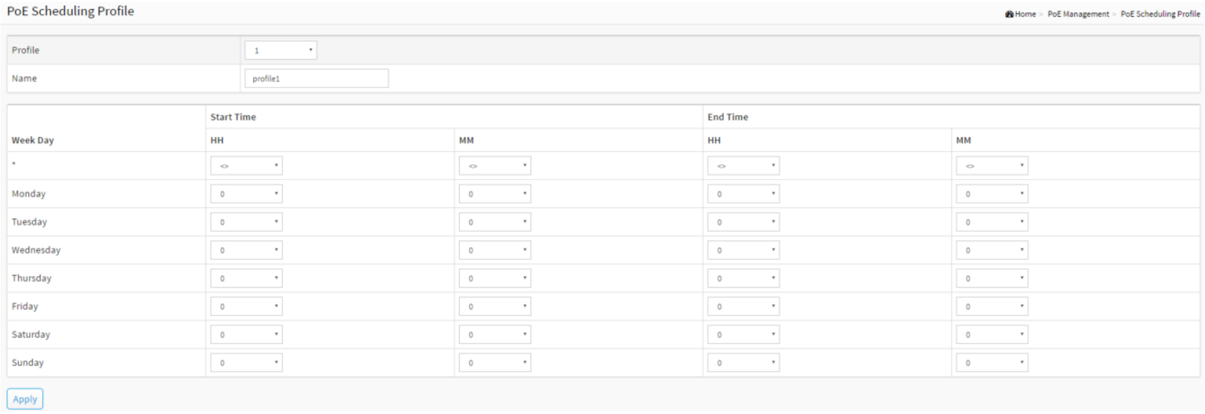
5-5 PoE Schedule Profile

This page allows user to define the profile for PoE scheduling.

Web Interface

To configure PoE Schedule Profile in the web interface:

1. Click PoE Management and PoE Scheduling Profile.
2. Select profile number and specify the profile name.
3. Select Week Day and Specify Start Time, End Time.
4. Click Apply to apply the change.



PoE Scheduling Profile

Profile	1
Name	profile1

	Start Time		End Time	
Week Day	HH	MM	HH	MM
*	<>	<>	<>	<>
Monday	0	0	0	0
Tuesday	0	0	0	0
Wednesday	0	0	0	0
Thursday	0	0	0	0
Friday	0	0	0	0
Saturday	0	0	0	0
Sunday	0	0	0	0

Figure 5-5: The PoE Schedule Profile

Parameter description:

- **Profile :**

  The index of profile. There are 16 profiles in the configuration.

- **Name :**

  The name of profile. The default name is "Profile #". User can define the name for identifying the profile.

- **Week Day :**

  The day to schedule PoE.

- **Start Time :**

  The time to start PoE. The time 00:00 means the first second of this day.

- **End Time :**

  The time to stop PoE. The time 00:00 means the last second of this day.

Buttons

- **Apply :**

  Click to save changes.

Chapter 6 VLAN Management

6-1 VLAN Configuration

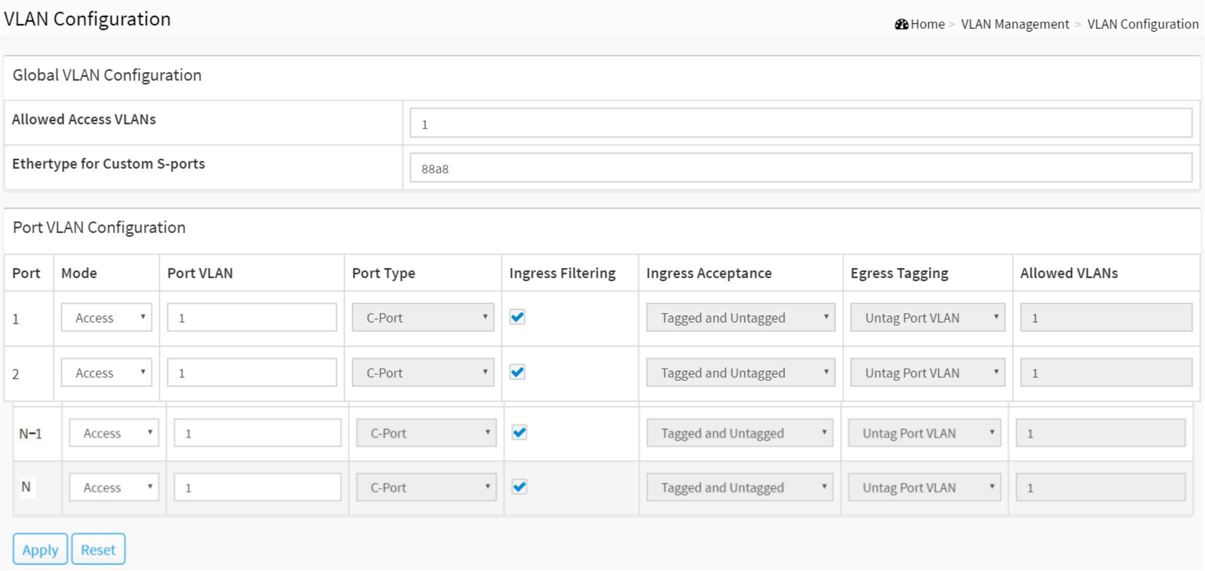
To assign a specific VLAN for management purpose. The management VLAN is used to establish an IP connection to the switch from a workstation connected to a port in the VLAN. This connection supports a VSM, SNMP, and Telnet session. By default, the active management VLAN is VLAN 1, but you can designate any VLAN as the management VLAN using the Management VLAN window. Only one management VLAN can be active at a time.

When you specify a new management VLAN, your HTTP connection to the old management VLAN is lost. For this reason, you should have a connection between your management station and a port in the new management VLAN or connect to the new management VLAN through a multi-VLAN route

Web Interface

To configure VLAN membership configuration in the web interface:

1. Click VLAN Management and VLAN Configuration.
2. Specify Existing VLANs, Ether type for Custom S-ports.
3. Click Apply.



VLAN Configuration

Global VLAN Configuration

Allowed Access VLANs	1
Ethertype for Custom S-ports	88a8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs
1	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1
2	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1
N-1	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1
N	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1

Figure 6-1: The VLAN Configuration

Parameter description:

Global VLAN Configuration

- **Allowed Access VLANs :**

  This field shows the VLANs that are created on the switch.

By default, only VLAN 1 exists. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound.

The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.

- **Ethertype for Custom S-ports :**

  This field specifies the ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.

Port VLAN Configuration

- **Port :**

  This is the logical port number of this row.

- **Mode :**

  The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below.
  Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question.
  Grayed out fields show the value that the port will get when the mode is applied.

  Access:
  Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics:
  • Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1,
  • accepts untagged frames and C-tagged frames,
  • discards all frames that are not classified to the Access VLAN,
  • on egress all frames are transmitted untagged.

  Trunk:
  Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics:
  • By default, a trunk port is member of all existing VLANs. This may be limited by the use of Allowed VLANs,
  • unless VLAN Trunking is enabled on the port, frames classified to a VLAN that the port is not a member of will be discarded,
  • by default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress,
  • egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress,
  • VLAN trunking may be enabled.

  Hybrid:
  Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:
  • Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware,
  • ingress filtering can be controlled,
  • ingress acceptance of frames and configuration of egress tagging can be configured independently.

- **Port VLAN :**

  Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4095,

default being 1.
On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0).
On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN.
The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.

- **Port Type :**

  Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required.

  Unaware:
  On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress.

  C-Port:
  On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag.

  S-Port:
  On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag.

  S-Custom-Port:
  On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag.

- **Ingress Filtering :**

  Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled.
  If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded.
  If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.

- **VLAN Trunking :**

  Trunk and Hybrid ports allow for enabling VLAN trunking.
  When VLAN trunking is enabled, frames classified to unknown VLANs are accepted on the port whether ingress filtering is enabled or not.
  This is useful in scenarios where a cloud of intermediary switches must bridge VLANs that haven't been created. By configuring the ports that connect the cloud of switches as trunking ports, they can seemlessly carry those VLANs from one end to the other.

- **Ingress Acceptance :**

  Hybrid ports allow for changing the type of frames that are accepted on ingress.

  Tagged and untagged

both tagged and untagged frames are accepted.

Tagged Only
Only tagged frames are accepted on ingress. Untagged frames are discarded.

Untagged Only
Only untagged frames are accepted on ingress. Tagged frames are discarded.

- **Egress Tagging :**

  Ports in Trunk and Hybrid mode may control the tagging of frames on egress.

  Untag Port VLAN
  Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.

  Tag All
  All frames, whether classified to the Port VLAN or not, are transmitted with a tag.

  Untag All
  All frames, whether classified to the Port VLAN or not, are transmitted without a tag.
  This option is only available for ports in Hybrid mode.

- **Allowed VLANs :**

  Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN.
  The field's syntax is identical to the syntax used in the Existing VLANs field. By default, a port may become member of all possible VLANs, and is therefore set to 1-4095.
  The field may be left empty, which means that the port will not be member of any of the existing VLANs, but if it is configured for VLAN Trunking it will still be able to carry all unknown VLANs.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

6-2 VLAN Membership

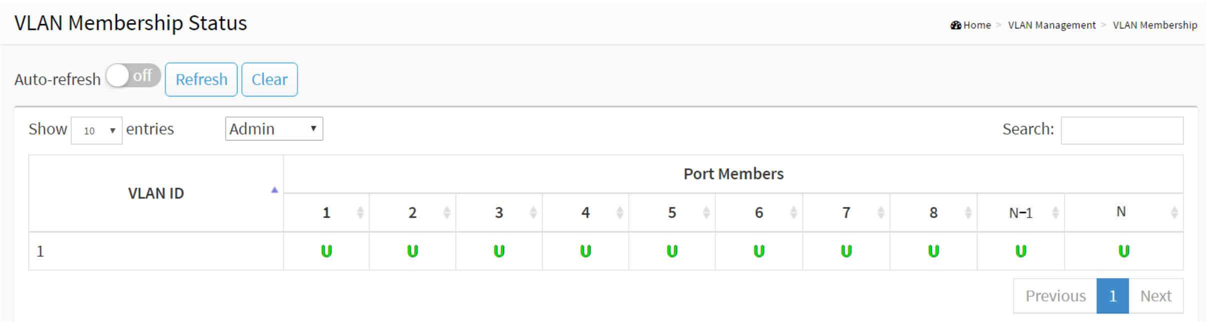
This page provides an overview of membership status of VLAN users.

The ports belong to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure VLAN membership configuration in the web interface:

1. Click VLAN Management and VLAN membership.
2. Scroll the bar to choice which VLANs would like to show up.
3. Click Refresh to update the state.



VLAN Membership Status

Auto-refresh off

Show 10 entries Admin

Search:

VLAN ID	Port Members									
	1	2	3	4	5	6	7	8	N-1	N
1	U	U	U	U	U	U	U	U	U	U

Figure 6-2: The VLAN Membership

Parameter description:

- **VLAN USER :**

Various internal software modules may use VLAN services to configure VLAN memberships on the fly.
The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.
The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.

VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configurations such as PVID and UVID. Currently we support the following VLAN user types:

NAS : NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

GVRP : Adjacent VLAN-aware devices can exchange VLAN information with each other by using Generic VLAN Registration Protocol (GVRP). GVRP is based on the Generic Attribute Registration Protocol (GARP) and propagates VLAN information throughout a bridged network.

MVR : MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.

Voice VLAN : Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones.

MSTP : The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

DMS: Shows DMS VLAN membership status.

VCL : Shows MAC-based VLAN entries configured by various MAC-based VLAN users.

- **VLAN ID :**

  VLAN ID for which the Port members are displayed.

- **Port Members :**

  A row of check boxes for each port is displayed for each VLAN ID.

  If a port is included in a VLAN, an image U and T will be displayed. Shows egress filtering frame status whether tagged or untagged. Frames classified to the Port VLAN are transmitted tagged(T) or untagged(U).

- **VLAN Membership :**

  The VLAN Membership Status Page shall show the current VLAN port members for all VLANs configured by a selected VLAN User (selection shall be allowed by a Combo Box). When combined Users are selected, it shall show this information for all the VLAN Users, and this is by default. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.

- **Show entries :**

  You can choose how many items you want to show up.

- Admin ▾ **:**

  You can choose the Vlan User.

- **Search :**

  You can search for the information that you want to see.

Buttons

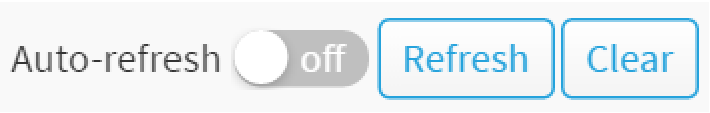


Figure 6-2: The VLAN Membership buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Click to clear the page.

- **Next :**

  Updates the system log entries, turn to the next page.

- **Previous :**

  Updates the system log entries, turn to the previous page.

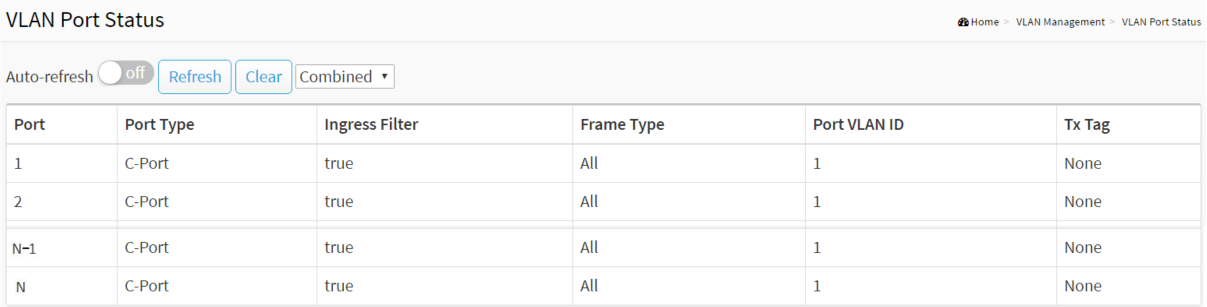
6-3 VLAN Port Status

The function Port Status gathers the information of all VLAN status and reports it by the order of Combined, Admin, NAS, GVRP, MVR, Voice VLAN, MSTP, DMS, VCL.

Web Interface

To Display VLAN Port Status in the web interface:

1. Click VLAN Management and VLAN Port Status.
2. Specify the Combined, Admin, NAS, GVRP, MVR, Voice VLAN, MSTP, DMS, VCL.
3. Display Port Status information.



Port	Port Type	Ingress Filter	Frame Type	Port VLAN ID	Tx Tag
1	C-Port	true	All	1	None
2	C-Port	true	All	1	None
N-1	C-Port	true	All	1	None
N	C-Port	true	All	1	None

Figure 6-3: The VLAN Port Status

Parameter description:

- **VLAN USER**

  VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configuration such as PVID, UVID. Currently we support following VLAN User types:

  NAS : NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

  GVRP : Adjacent VLAN-aware devices can exchange VLAN information with each other by using Generic VLAN Registration Protocol (GVRP). GVRP is based on the Generic Attribute Registration Protocol (GARP) and propagates VLAN information throughout a bridged network.

  MVR : MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.

  Voice VLAN : Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones.

  MSTP : The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

  DMS: Shows DMS VLAN membership status.

  VCL : shows MAC-based VLAN entries configured by various MAC-based VLAN users.

- **Port :**

  The logical port for the settings contained in the same row.

- **Port Type :**

  Shows the Port Type. Port type can be any of Unaware, C-port, S-port, Custom S-port.

  If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed. C-port is Customer Port. S-port is Service port. Custom S-port is S-port with Custom TPID.

- **Ingress Filtering :**

  Shows the ingress filtering on a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN, the frame is discarded.

- **Frame Type :**

  Shows whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.

- **Port VLAN ID :**

  Shows the Port VLAN ID (PVID) that a given user wants the port to have.

  The field is empty if not overridden by the selected user.

- **Tx Tag :**

  Shows egress filtering frame status whether tagged or untagged.

- Admin **:**

  You can choose the Vlan User.

Buttons

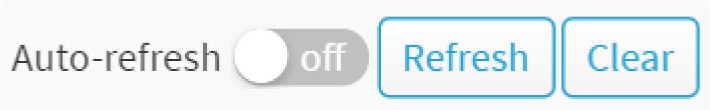


Figure 6-3: The VLAN Port Status buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Click to clear the page.

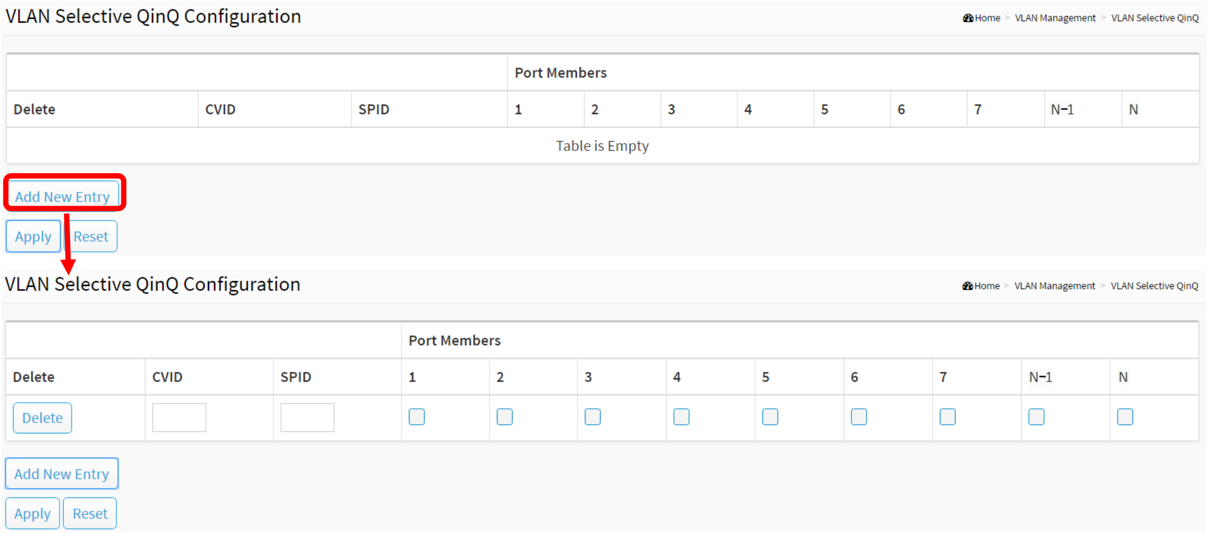
6-4 VLAN Selective QinQ Configuration

A Q-in-Q VLAN tunnel enables a service provider to segregate the traffic of different customers in their infrastructure, while still giving the customer a full range of VLANs for their internal use by adding a second 802.1Q tag to an already tagged frame.

Web Interface

To configure VLAN selective QinQ in the web interface:

1. Click VLAN Management and VLAN Selective QinQ Configuration.
2. Click "Add New Entry".
3. Specify CVID, SPID, Port Members.
4. Click Apply.



VLAN Selective QinQ Configuration

Home > VLAN Management > VLAN Selective QinQ

			Port Members								
Delete	CVID	SPID	1	2	3	4	5	6	7	N-1	N
Table is Empty											

VLAN Selective QinQ Configuration

Home > VLAN Management > VLAN Selective QinQ

			Port Members								
Delete	CVID	SPID	1	2	3	4	5	6	7	N-1	N
Delete			□	□	□	□	□	□	□	□	□

Figure 6-4: The VLAN Selective QinQ Configuration

Parameter description:

- **CVID :**

  1-4095, The customer VLAN ID List to which the tagged packets will be added.

- **SPID :**

  1-4095, This configures the VLAN to join the Service Providers VLAN as a tagged member

- **Port Members :**

  Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Buttons

- **Delete :**

  To delete a QinQ configuration entry, check this box. The entry will be deleted during the next Save.

- **Add New Entry :**

  Click to add a new QinQ configuration.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

6-5 MAC-based VLAN

6-5.1 Configuration

MAC address-based VLAN decides the VLAN for forwarding an untagged frame based on the source MAC address of the frame.

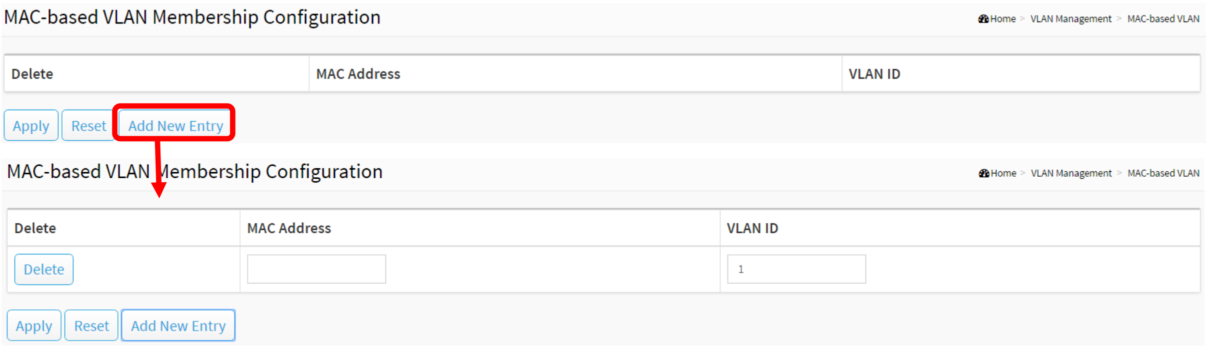
A most common way of grouping VLAN members is by port, hence the name port-based VLAN. Typically, the device adds the same VLAN tag to untagged packets that are received through the same port. Later on, these packets can be forwarded in the same VLAN. Port-based VLAN is easy to configure, and applies to networks where the locations of terminal devices are relatively fixed. As mobile office and wireless network access gain more popularity, the ports that terminal devices use to access the networks are very often non-fixed. A device may access a network through Port A this time, but through Port B the next time. If Port A and Port B belong to different VLANs, the device will be assigned to a different VLAN the next time it accesses the network. As a result, it will not be able to use the resources in the old VLAN. On the other hand, if Port A and Port B belong to the same VLAN, after terminal devices access the network through Port B, they will have access to the same resources as those accessing the network through Port A do, which brings security issues. To provide user access and ensure data security in the meantime, the MAC-based VLAN technology is developed.

MAC-based VLANs group VLAN members by MAC address. With MAC-based VLAN configured, the device adds a VLAN tag to an untagged frame according to its source MAC address. MAC-based VLANs are mostly used in conjunction with security technologies such as 802.1X to provide secure, flexible network access for terminal devices.

Web Interface

To configure MAC address-based VLAN configuration in the web interface:

1. Click VLAN Management, MAC-based VLAN and Configuration.
2. Click "Add New Entry".
3. Specify the MAC address and VLAN ID.
4. Click Apply.



MAC-based VLAN Membership Configuration

Delete	MAC Address	VLAN ID

MAC-based VLAN Membership Configuration

Delete	MAC Address	VLAN ID
Delete		1

Home > VLAN Management > MAC-based VLAN
Apply
Reset
Add New Entry
Home > VLAN Management > MAC-based VLAN
Apply
Reset
Add New Entry

Figure 6-5.1: The MAC-based VLAN Configuration

Parameter description:

- **MAC Address :**

  Indicates the MAC address.

- **VLAN ID :**

  Indicates the VLAN ID.

Buttons

- **Adding New Entry :**

  Click to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 through 4095.

  The MAC-based VLAN entry is enabled on the selected stack switch unit when you click on "Save". A MAC-based VLAN without any port members on any stack unit will be deleted when you click "Save".

  The button can be used to undo the addition of new MAC-based VLANs.

- **Delete :**

  To delete a MAC-based VLAN entry, check this box and press save. The entry will be deleted on the selected switch in the stack.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

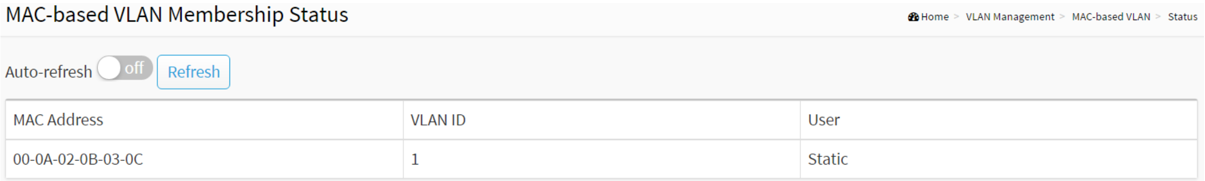
6-5.2 Status

Show the MAC-based VLAN status.

Web Interface

To Display MAC address-based VLAN configuration in the web interface:

1. Click VLAN Management, MAC-based VLAN and Status.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh” to refresh the MAC-based VLAN Membership Status.


MAC-based VLAN Membership Status
Home > VLAN Management > MAC-based VLAN > Status
Auto-refresh
off
Refresh

MAC Address	VLAN ID	User
00-0A-02-0B-03-0C	1	Static

Figure 6-5.2: The MAC-based VLAN Configuration

Parameter description:

- **MAC Address :**

  Indicates the MAC address.

- **VLAN ID :**

  Indicates the VLAN ID.

- **User:**

  Indicates the user.

Buttons

Figure 6-5.2: The MAC-based VLAN Configuration buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

6-6 Protocol-based VLAN

This section describe Protocol -based VLAN, The Switch support Protocol include Ethernet LLC SNAP Protocol,

LLC

The Logical Link Control (LLC) data communication protocol layer is the upper sub-layer of the Data Link Layer (which is itself layer 2, just above the Physical Layer) in the seven-layer OSI reference model. It provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX, Decent and Appletalk) to coexist within a multipoint network and to be transported over the same network media, and can also provide flow control and automatic repeat request (ARQ) error management mechanisms.

SNAP

The Subnetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier spaces. It is used with IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11 and other IEEE 802 physical network layers, as well as with non-IEEE 802 physical network layers such as FDDI that use 802.2 LLC.

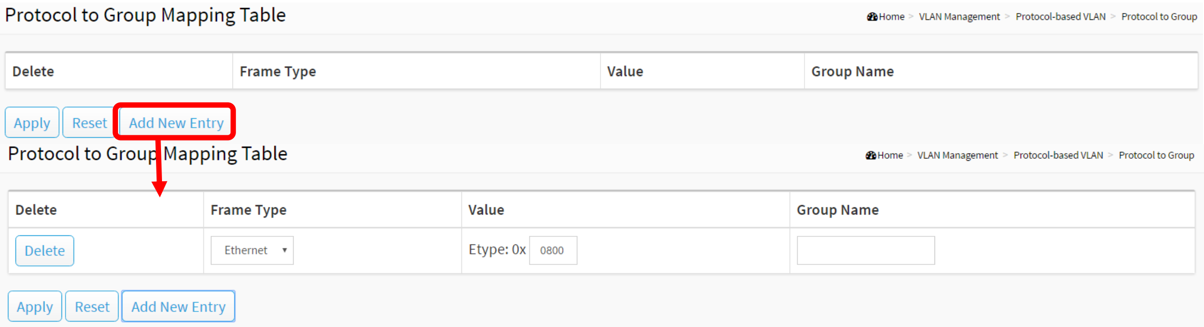
6-6.1 Protocol to Group

This page allows you to add new protocols to Group Name (unique for each Group) mapping entries as well as allow you to see and delete already mapped entries for the selected stack switch unit switch.

Web Interface

To configure Protocol -based VLAN configuration in the web interface:

1. Click VLAN Management, Protocol-based VLAN and Protocol to Group.
2. Click “Add New Entry”.
3. Specify the Ethernet LLC SNAP Protocol, Value and Group Name.
4. Click Apply.



Protocol to Group Mapping Table

Delete	Frame Type	Value	Group Name

Protocol to Group Mapping Table

Delete	Frame Type	Value	Group Name
Delete	Ethernet	Etype: 0x 0800	

Home > VLAN Management > Protocol-based VLAN > Protocol to Group
Apply
Reset
Add New Entry
Home > VLAN Management > Protocol-based VLAN > Protocol to Group
Apply
Reset
Add New Entry

Figure 6-6.1: The Protocol to Group Mapping Table

Parameter description:

- **Frame Type :**

  Frame Type can have one of the following values:

1. **Ethernet**
2. **LLC**
3. **SNAP**

NOTE: On changing the Frame type field, valid value of the following text field will vary depending on the new frame type you selected.

- **Value :**

  Valid value that can be entered in this text field depends on the option selected from the the preceding Frame Type selection menu.

  Below is the criteria for three different Frame Types:

  1. **For Ethernet:** Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff
  2. **For LLC:** Valid value in this case is comprised of two different sub-values.
     a. DSAP: 1-byte long string (0x00-0xff)
     b. SSAP: 1-byte long string (0x00-0xff)
  3. **For SNAP:** Valid value in this case also is comprised of two different sub-values.
     a.OUI: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff.
     b. PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.
     In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.

- **Group Name :**

  A valid Group Name is a unique 16-character long string.

NOTE: Special character and underscore (_) are not allowed.

Buttons

- **Delete :**

  To delete a Protocol to Group Name map entry, check this box. The entry will be deleted on the switch during the next Save.

- **Adding New Entry :**

  Click to add a new entry in mapping table. An empty row is added to the table; Frame Type, Value and the Group Name can be configured as needed.

  The button can be used to undo the addition of new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

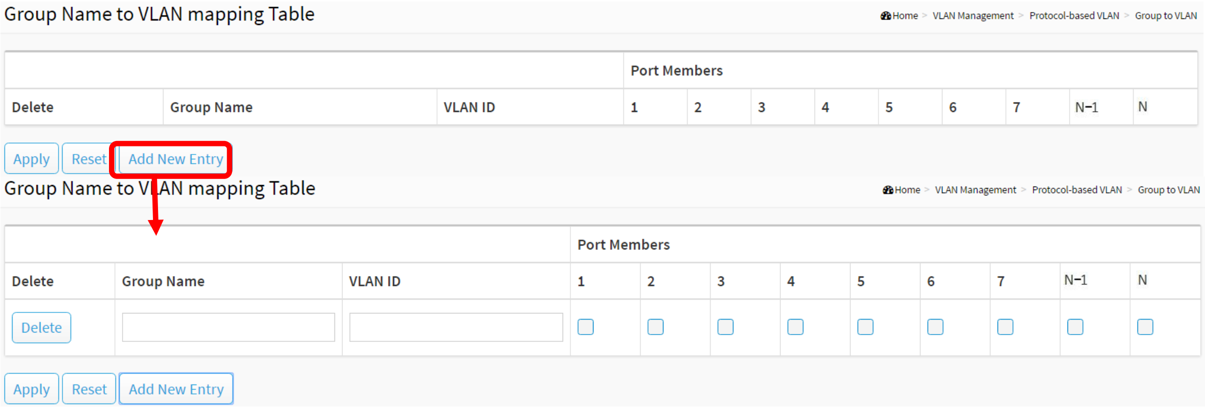
6-6.2 Group to VLAN

This section allows you to map an already configured Group Name to a VLAN for the selected stack switch unit switch.

Web Interface

To configure Group Name to VLAN mapping table configured in the web interface:

1. Click VLAN Management, Protocol-based VLAN and Group to Group.
2. Click "Add New Entry".
3. Specify the Group Name and VLAN ID.
4. Click Apply.



Group Name to VLAN mapping Table

Home > VLAN Management > Protocol-based VLAN > Group to VLAN

			Port Members								
Delete	Group Name	VLAN ID	1	2	3	4	5	6	7	N−1	N

Group Name to VLAN mapping Table

Home > VLAN Management > Protocol-based VLAN > Group to VLAN

			Port Members								
Delete	Group Name	VLAN ID	1	2	3	4	5	6	7	N−1	N
Delete			□	□	□	□	□	□	□	□	□

Figure 6-6.2: The Group Name of VLAN Mapping Table

Parameter description:

- **Group Name :**

  A valid Group Name is a string of almost 16 characters.

- **VLAN ID :**

  Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095.

- **Port Members :**

  A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Buttons

- **Delete :**

  To delete a Group Name to VLAN map entry, check this box. The entry will be deleted on the switch during the next Save

- **Adding New Entry :**

  Click to add a new entry in mapping table. An empty row is added to the table, the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The button can be used to undo the addition of new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

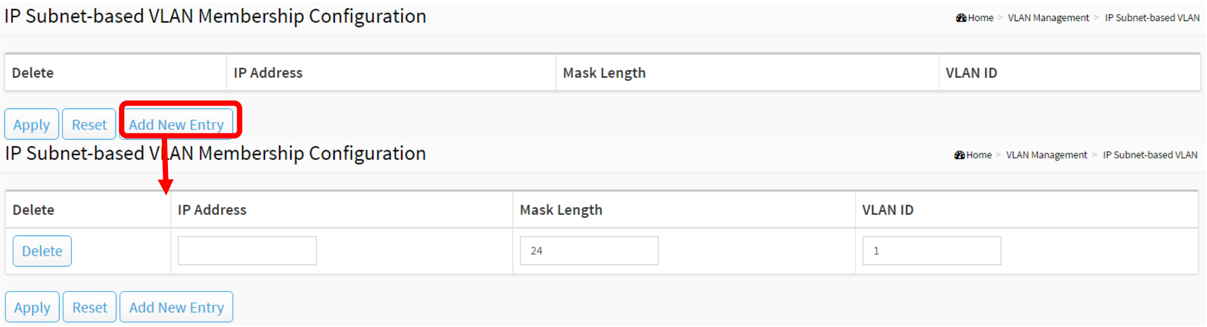
6-7 IP Subnet-based VLAN

The IP subnet-based VLAN entries can be configured here. This page allows for adding, updating and deleting IP subnet-based VLAN entries and assigning the entries to different ports. This page shows only static entries.

Web Interface

To configure IP subnet-based VLAN Membership to configured in the web interface:

1. Click VLAN Management and IP Subnet-based VLAN.
2. Click "Add New Entry".
3. Specify IP Address, Mask Length, VLAN ID.
4. Click Apply.



IP Subnet-based VLAN Membership Configuration

Home > VLAN Management > IP Subnet-based VLAN

Delete	IP Address	Mask Length	VLAN ID

Apply Reset Add New Entry

IP Subnet-based VLAN Membership Configuration

Home > VLAN Management > IP Subnet-based VLAN

Delete	IP Address	Mask Length	VLAN ID
Delete		24	1

Apply Reset Add New Entry

Figure 6-7: IP Subnet-based VLAN Membership Configuration

Parameter description:

- **IP Address :**

  Indicates the IP address.

- **Mask Length :**

  Indicates the network mask length.

- **VLAN ID :**

  Indicates the VLAN ID. VLAN ID can be changed for the existing entries.

Buttons

- **Delete :**

  To delete a IP subnet-based VLAN entry, check this box and press save. The entry will be deleted on the selected switch in the stack.

- **Adding New Entry :**

  Click "Add New Entry" to add a new IP subnet-based VLAN entry. An empty row is added to the table, and the IP subnet-based VLAN entry can be configured as needed. Any IP address/mask can be configured for the IP subnet-based VLAN entry. Legal values for a VLAN ID are 1 through 4095.

  The IP subnet-based VLAN entry is enabled on the selected stack switch unit when you click on "Save". The "Delete" button can be used to undo the addition of new IP subnet-based VLANs. The maximum possible IP subnet-based VLAN entries are limited to 128.

- **Apply :**

Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

6-8 Private VLAN

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

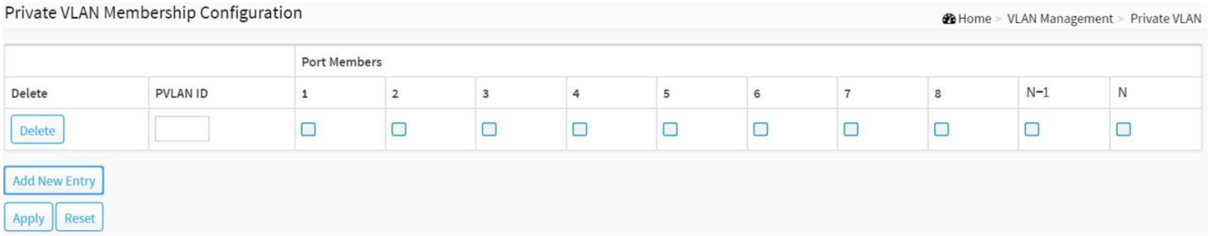
A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

VLAN Priority : Voice VLAN > MAC based VLAN > Protocol based VLAN > Tag based VLAN

Web Interface

To configure Port Isolation configuration in the web interface:

1. Click VLAN Management and Private VLAN.
2. Configure the Private VLAN membership configurations for the switch.
3. Click Apply.



Private VLAN Membership Configuration

Home > VLAN Management > Private VLAN

		Port Members									
Delete	PVLAN ID	1	2	3	4	5	6	7	8	N-1	N
Delete		□	□	□	□	□	□	□	□	□	□

Figure 6-8: The Private VLAN Configuration

Parameter description:

- **Delete :**

  To delete a private VLAN entry, check this box. The entry will be deleted during the next apply.

- **Private VLAN ID :**

  Indicates the ID of this particular private VLAN.

- **Port Members :**

  A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

- **Adding New Private VLAN :**

  Click to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry, or click "Cancel" to return to the editing and make a correction.

  The Private VLAN is enabled when you click "Apply".

The button can be used to undo the addition of new Private VLANs.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

6-9 Port Isolation

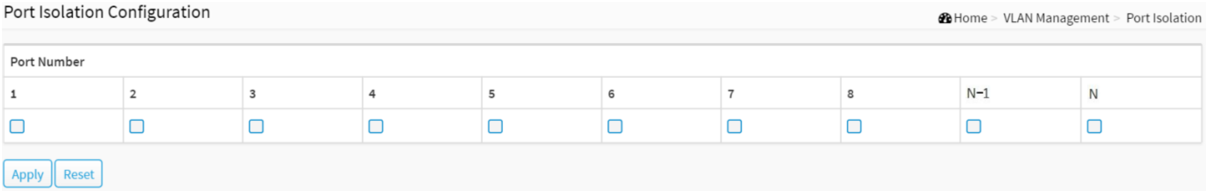
Port Isolation provides for an apparatus and method to isolate ports on layer 2 switches on the same VLAN to restrict traffic flow. The apparatus comprises a switch having said plurality of ports, each port configured as a protected port or a non-protected port. An address table memory stores an address table having a destination address and port number pair. A forwarding map generator generates a forwarding map which is responsive to a destination address of a data packet. The method for isolating ports on a layer 2 switch comprises configuring each of the ports on the layer 2 switch as a protected port or a non-protected port. A destination address on a data packet is matched with a physical address on said layer 2 switch and a forwarding map is generated for the data packet based upon the destination address on the data packet. The data packet is then sent to the plurality of ports pursuant to the forwarding map generated based upon whether the ingress port was configured as a protected or non-protected port.

This page is used for enabling or disabling port isolation on ports in a Private VLAN.A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.

Web Interface

To configure Port Isolation configuration in the web interface:

1. Click VLAN Management and Port Isolation.
2. Evoke which port want to enable Port Isolation
3. Click Apply.



Port Isolation Configuration

Port Number									
1	2	3	4	5	6	7	8	N-1	N
□	□	□	□	□	□	□	□	□	□

Figure 6-9: The Port Isolation Configuration

Parameter description:

- **Port Numbers :**

  A check box is provided for each port of a private VLAN. When checked, port isolation is enabled on that port. When unchecked, port isolation is disabled on that port. By default, port isolation is disabled on all ports.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

6-10 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.

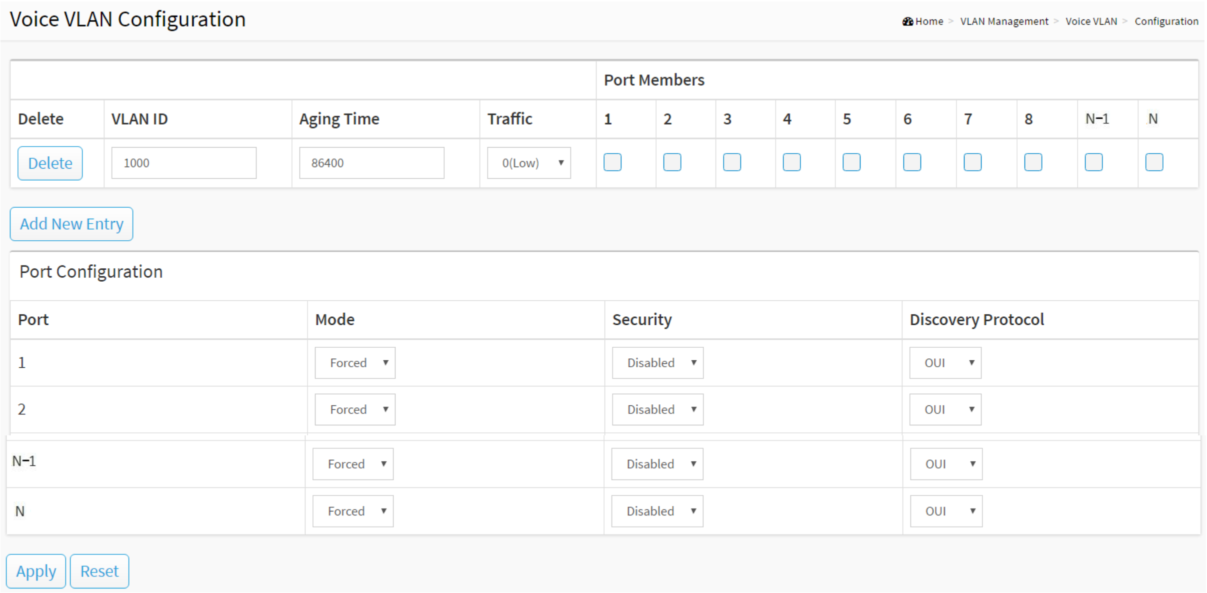
6-10.1 Configuration

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI.

Web Interface

To configure Voice VLAN in the web interface:

1. Click VLAN Management, Voice VLAN and Configuration.
2. Click "Add New Entry".
3. Select Port Members in the Voice VLAN Configuration.
4. Specify VLAN ID, Aging Time, Traffic.
5. Specify (Mode, Security, Discovery Protocol) in the Port Configuration.
6. Click Apply.



Voice VLAN Configuration

				Port Members									
Delete	VLAN ID	Aging Time	Traffic	1	2	3	4	5	6	7	8	N-1	N
Delete	1000	86400	0(Low)	□	□	□	□	□	□	□	□	□	□

Add New Entry

Port Configuration

Port	Mode	Security	Discovery Protocol
1	Forced	Disabled	OUI
2	Forced	Disabled	OUI
N-1	Forced	Disabled	OUI
N	Forced	Disabled	OUI

Apply Reset

Figure 6-10.1: The Voice VLAN Configuration

Parameter description:

- **Port Members :**

Indicates the Voice VLAN port mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering.

Select which port that you want to enable the Voice VLAN mode operation.

- **VLAN ID :**

  Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID etc. The allowed range is 1 to 4095.

- **Aging Time :**

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

- **Traffic :**

  Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.

Port Configuration

- **Port :**

  The switch port number of the Voice VLAN port.

- **Mode :**

  Indicates the Voice VLAN port mode.

  When the port mode isn't equal disabled, we must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering.

  Possible port modes are:

  Auto: Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically.

  Forced: Force join to Voice VLAN.

- **Security :**

  Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are:

  Enabled: Enable Voice VLAN security mode operation.

  Disabled: Disable Voice VLAN security mode operation.

- **Discovery Protocol :**

  Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process. Possible discovery protocols are:

  OUI: Detect telephony device by OUI address.

  LLDP: Detect telephony device by LLDP.

  Both: Both OUI and LLDP.

Buttons

- **Add New entry :**

  Click to add a new entry in Voice VLAN configuration.

- **Apply :**

  Click to save changes.

- **Reset :**

Click to undo any changes made locally and revert to previously saved values.

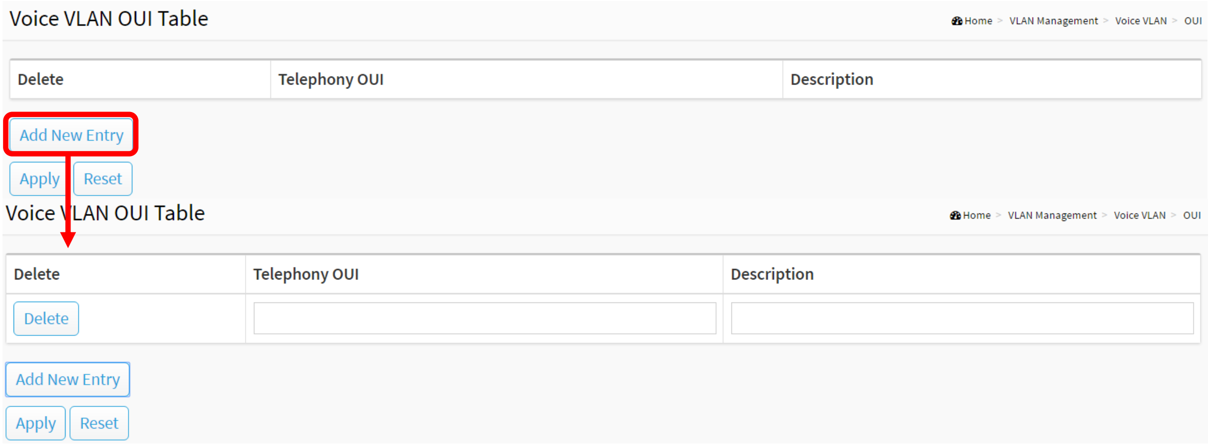
6-10.2 OUI

The section describes to Configure VOICE VLAN OUI table. The maximum entry number is 16. Modifying the OUI table will restart auto detection of OUI process.

Web Interface

To configure Voice VLAN OUI Table in the web interface:

1. Click VLAN Management, Voice VLAN and OUI
2. Select "Add new entry", "delete" in the Voice VLAN OUI table.
3. Specify Telephony OUI, Description.
4. Click Apply.



Voice VLAN OUI Table

Delete	Telephony OUI	Description

Voice VLAN OUI Table

Delete	Telephony OUI	Description
Delete		

Home > VLAN Management > Voice VLAN > OUI
Add New Entry
Apply
Reset
Home > VLAN Management > Voice VLAN > OUI
Add New Entry
Apply
Reset

Figure 6-10.2: The Voice VLAN OUI Table

Parameter description:

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **Telephony OUI :**

  A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).

- **Description :**

  The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.

- **Add New entry :**

  Click to add a new entry in Voice VLAN OUI table. An empty row is added to the table, the Telephony OUI, Description.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

Chapter 7 Quality of Service

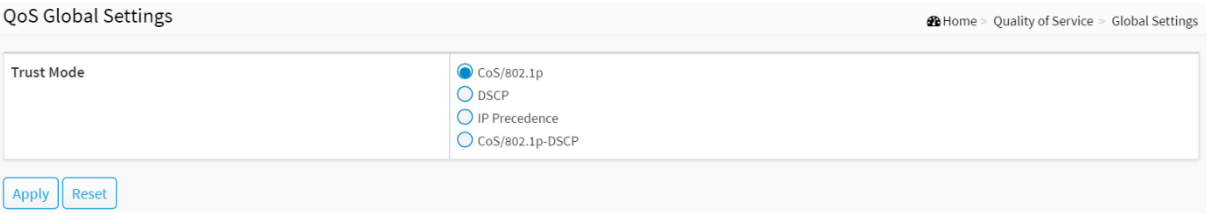
7-1 Global Settings

Use the Global Settings page to set the trust behavior for QoS basic mode. This configuration is active when the switch is in QoS basic mode. Packets entering a QoS domain are classified at the edge of the QoS domain.

Web Interface

To configure the Global Settings in the web interface:

1. Click Quality of Service and Global Settings.
2. Select the trust mode when the switch is in QoS basic mode. If a packet CoS level and DSCP tag are mapped to separate queues, the trust mode determines the queue to which the packet is assigned.
3. Click Apply to save the configuration.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



QoS Global Settings

Home > Quality of Service > Global Settings

Trust Mode	● CoS/802.1p ○ DSCP ○ IP Precedence ○ CoS/802.1p-DSCP

Figure 7-1: The QoS Global Settings

Parameter description:

Trust Mode

- **CoS/802.1p :**

  Traffic is mapped to queues based on the VPT field in the VLAN tag, or based on the per-port default CoS/802.1p value (if there is no VLAN tag on the incoming packet), the actual mapping of the VPT to queue can be configured on the CoS/802.1p to Queue page.

- **DSCP :**

  All IP traffic is mapped to queues based on the DSCP field in the IP header. The actual mapping of the DSCP to queue can be configured on the DSCP to Queue page. If traffic is not IP traffic, it is mapped to the best effort queue.

- **IP Precedence :**

  Traffic is mapped to queues based on the IP precedence. The actual mapping of the IP precedence to queue can be configured on the IP Precedence to Queue page.

- **CoS/802.1p-DSCP :**

  Uses the trust CoS mode for non-IP traffic and trust DSCP mode for IP traffic.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

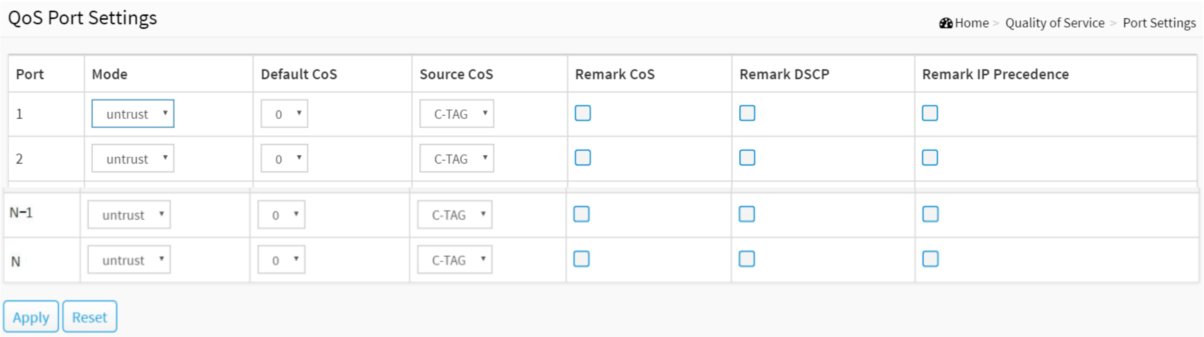
  Click to undo any changes made locally and revert to previously saved values.

7-2 Port Settings

Web Interface

To configure the QoS Port Setting in the web interface:

1. Click Quality of Service and Port Settings.
2. Select Mode, Default CoS, Source CoS, Remark CoS to each port.
3. Click which port need to enable the Remark Cos, Remark DSCP, Remark IP Precedence
4. Click Apply to save the configuration.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



QoS Port Settings

Port	Mode	Default CoS	Source CoS	Remark CoS	Remark DSCP	Remark IP Precedence
1	untrust	0	C-TAG	□	□	□
2	untrust	0	C-TAG	□	□	□
N-1	untrust	0	C-TAG	□	□	□
N	untrust	0	C-TAG	□	□	□

Figure 7-2: The QoS Port Settings

Parameter description:

- **Port :**

  The logical port for the settings contained in the same row.

- **Mode :**

  - **Untrust :**

    All ingress traffic on the port is mapped to the best effort queue and no classification/prioritization takes place.

  - **Trust :**

    Port prioritize ingress traffic is based on the system wide configured trusted mode, which is either CoS/802.1p trusted mode, IP Precedence trusted mode or DSCP trusted mode.

- **Default CoS :**

  Select the default CoS value to be assigned for incoming untagged packets. The range is 0 to 7.

- **Source CoS :**

  The CoS value is determined based on C-Tag or S-Tag for incoming tagged packets

- **Remark CoS :**

  Click the checkbox to remark the CoS/802.1p priority for egress traffic on this port.

- **Remark DSCP :**

  Click the checkbox to remark the DSCP value for egress traffic on this port.

- **Remark IP Precedence**

  Click the checkbox to remark the IP precedence for egress traffic on this port.

Note: The CoS/802.1p priority and IP Precedence, or the CoS/802.1p priority and DSCP value can be remarked simultaneously for egress traffic on a port, but the DSCP value and IP Precedence cannot be remarked simultaneously.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

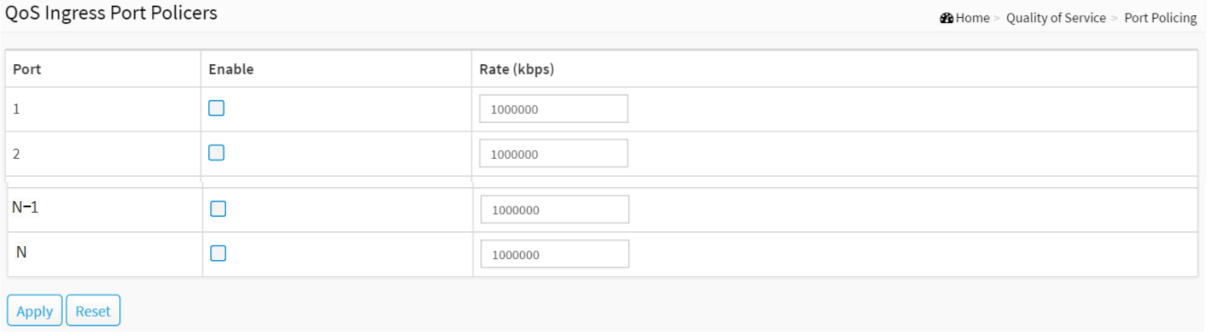
7-3 Port Policing

This section provides an overview of QoS Ingress Port Policers for all switch ports The Port Policing is useful in constraining traffic flows and marking frames above specific rates. Policing is primarily useful for data flows and voice or video flows because voice and video usually maintains a steady rate of traffic

Web Interface

To configure the QoS Port Policers in the web interface:

1. Click Quality of Service and Port Policing.
2. Click which port need to enable the QoS Ingress Port Policers, and configue the Rate limit condition.
3. Click Apply to save the configuration.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



QoS Ingress Port Policers

Home > Quality of Service > Port Policing

Port	Enable	Rate (kbps)
1	□	1000000
2	□	1000000
N-1	□	1000000
N	□	1000000

Figure 7-3: The QoS Ingress Port Policers Configuration

Parameter description:

- **Port :**

  The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.

- **Enabled :**

  To evoke which Port you need to enable the QoS Ingress Port Policers function.

- **Rate :**

  To set the Rate limit value for this port, the default is 1000000.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

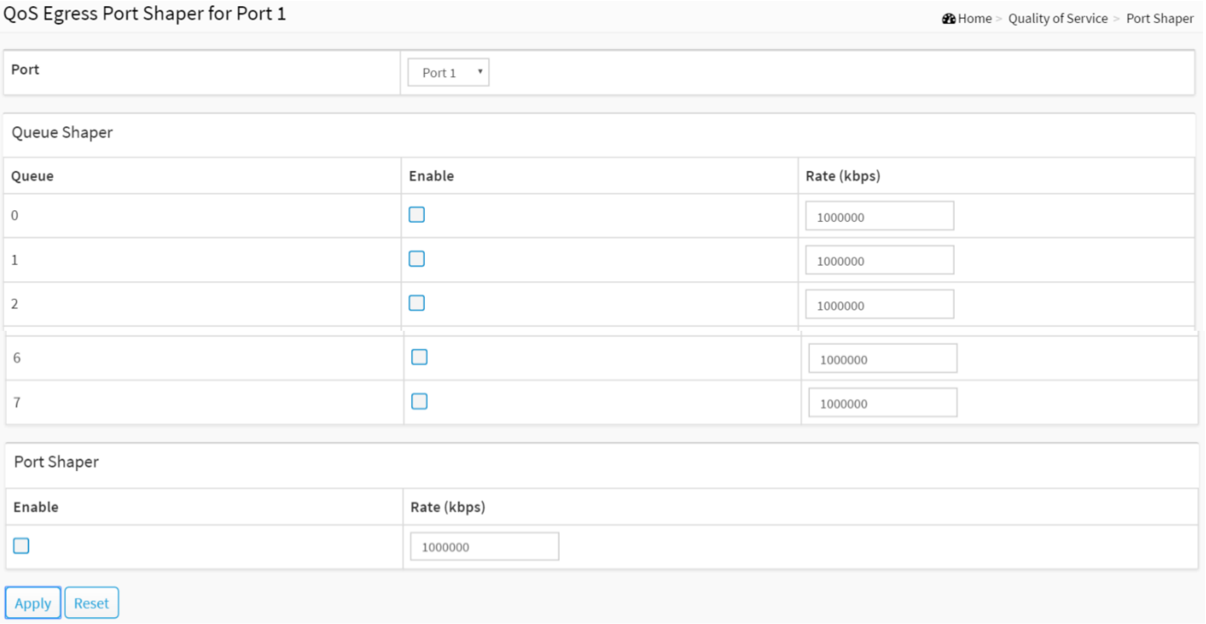
7-4 Port Shaper

This section provides an overview of QoS Egress Port Shapers for all switch ports. Others the user could get all detail information of the ports belong to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure the QoS Port Shapers in the web interface:

1. Click Quality of Service and Port Shaper.
2. Select which port need to configure QoS Egress Port Shaper.
3. Click which port need to enable, and configure the Rate limit condition.
4. Click Apply to save the configuration.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



QoS Egress Port Shaper for Port 1

Port	Port 1

Queue Shaper

Queue	Enable	Rate (kbps)
0	□	1000000
1	□	1000000
2	□	1000000
6	□	1000000
7	□	1000000

Port Shaper

Enable	Rate (kbps)
□	1000000

Figure 7-4: The QoS Egress Port Shaper

Parameter description:

- **Port :**

  The logical port for the settings contained in the same row. Click on the port number in order to configure the shapers.

Queue Shaper

- **Queue :**

  The queue number of the queue shaper on this switch port.

- **Enable :**

  Controls whether the queue shaper is enabled for this queue on this switch port.

- **Rate(kbps) :**

Controls the rate for the queue shaper. The default value is 1000000.

Port Shaper

- **Enable :**

  Controls whether the port shaper is enabled for this switch port.

- **Rate(kbps) :**

  Controls the rate for the port shaper. The default value is 1000000.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

7-5 Storm Control

The section allows user to configure the Storm control for the switch. There is a destination lookup failure storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table. The configuration indicates the permitted packet rate for unicast, multicast or broadcast traffic across the switch

Web Interface

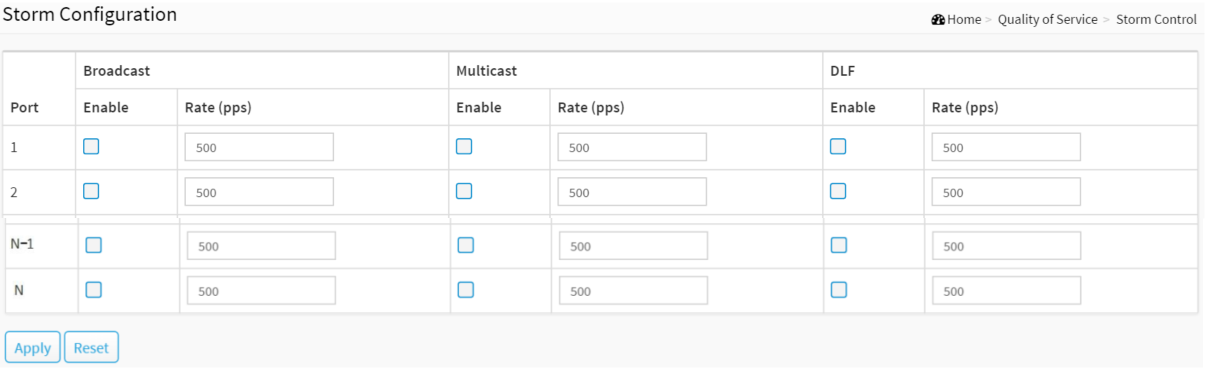
To configure the Storm Control Configuration parameters in the web interface:

1. Click Quality of Service and Storm Control.

2. Click which port need to enable, and configure the Rate limit condition.

4. Click the Apply to save the setting

5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values



Storm Configuration

	Broadcast		Multicast		DLF	
Port	Enable	Rate (pps)	Enable	Rate (pps)	Enable	Rate (pps)
1	□	500	□	500	□	500
2	□	500	□	500	□	500
N-1	□	500	□	500	□	500
N	□	500	□	500	□	500

Figure 7-5: The Storm Control Configuration

Parameter description:

- **Port :**

  The logical port for the settings contained in the same row. Click on the port number in order to configure the storm control.

- **Frame Type :**

  The settings in a particular row apply to the frame type listed here: Broadcast, Multicast or DLF(destination lookup failure).

- **Enable :**

  Enable or disable the storm control status for the given frame type.

- **Rate :**

  The rate unit is packets per second (pps). Valid values are: 0 ~ 262143 (pps).

  The 1 kpps is actually 1002.1 pps.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

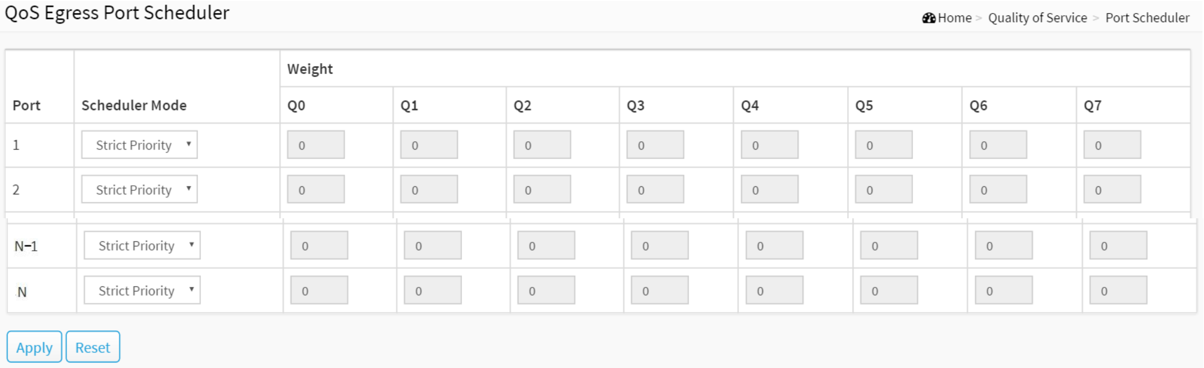
7-6 Port Scheduler

This section provides an overview of QoS Egress Port Scheduler for all switch ports. and the ports belong to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure the QoS Port Schedulers in the web interface:

1. Click Quality of Service and Port Scheduler.
2. Select Scheduler Mode for each port.
3. If you select WRR or WFQ, you can configure weight.
4. Click the Apply to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



QoS Egress Port Scheduler

Port	Scheduler Mode	Weight							
		Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
1	Strict Priority ▾	0	0	0	0	0	0	0	0
2	Strict Priority ▾	0	0	0	0	0	0	0	0
N-1	Strict Priority ▾	0	0	0	0	0	0	0	0
N	Strict Priority ▾	0	0	0	0	0	0	0	0

Figure 7-6: The QoS Egress Port Schedules

Parameter description:

- **Port :**

  The logical port for the settings contained in the same row.

- **Scheduler Mode :**

  Controls whether the scheduler mode is "Strict Priority", "WRR" or "WFQ" on this switch port.

- **Weight :**

  Controls the weight for this queue. The default value is "0". This value is restricted to 0-127. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

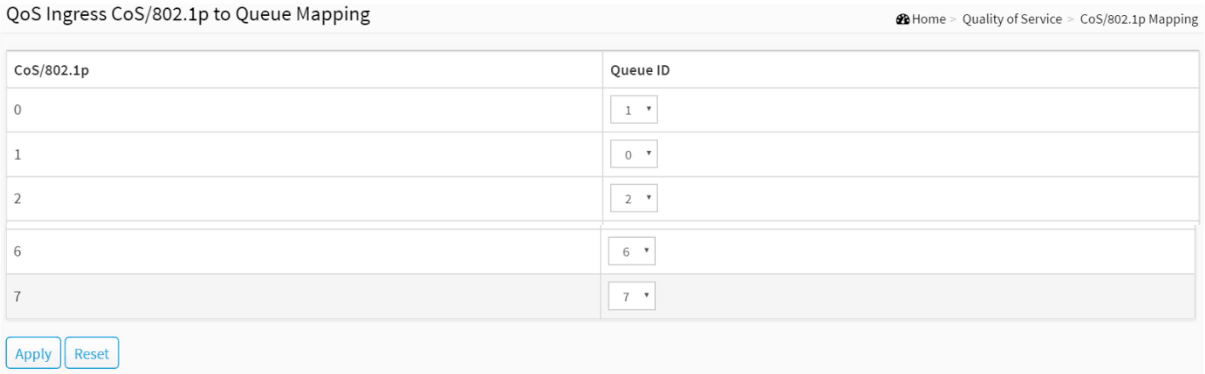
7-7 CoS/802.1p Mapping

Use the CoS/802.1p to Queue page to map 802.1p priorities to egress queues. The CoS/802.1p to Queue table determines the egress queues of the incoming packets based on the 802.1p priority in their VLAN tags. For incoming untagged packets, the 802.1p priority will be the default CoS/802.1p priority assigned to the ingress ports.

Web Interface

To configure the Cos/802.1p Mapping in the web interface:

1. Click Quality of Service and Cos/802.1p Mapping.
2. Select Queue ID.
3. Click the Apply to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



QoS Ingress CoS/802.1p to Queue Mapping

CoS/802.1p	Queue ID
0	1
1	0
2	2
6	6
7	7

Figure 7-7: The QoS Ingress CoS/802.1p to Queue Mapping

Parameter description:

- **CoS/802.1p :**

  Displays the 802.1p priority tag values to be assigned to an egress queue, where 0 is the lowest and 7 is the highest priority.

- **Queue ID :**

  Select the egress queue to which the 802.1p priority is mapped. Eight egress queues are supported, where Queue 7 is the highest priority egress queue and Queue 0 is the lowest priority egress queue.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

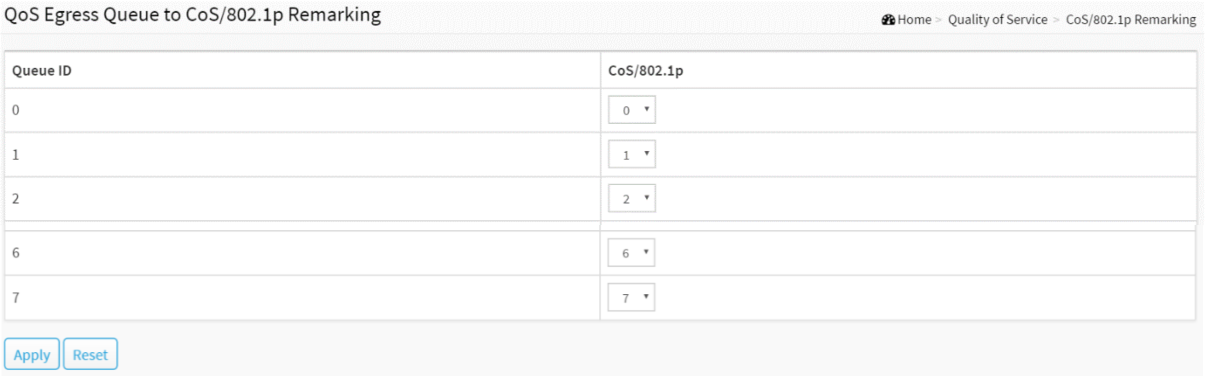
7-8 CoS/802.1p Remarking

Use the Queues to CoS/802.1p page to remark the CoS/802.1p priority for egress traffic from each queue.

Web Interface

To configure the Cos/802.1p Remarking in the web interface:

1. Click Quality of Service and Cos/802.1p Remarking.
2. Select CoS/802.1p.
3. Click the Apply to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



QoS Egress Queue to CoS/802.1p Remarking

Queue ID	CoS/802.1p
0	0
1	1
2	2
6	6
7	7

Figure 7-8: The QoS Egress Queue to CoS/802.1p Remarking

Parameter description:

- **Queue ID :**

  Displays the Queue ID, where Queue 7 is the highest priority egress queue and Queue 0 is the lowest priority egress queue.

- **CoS/802.1p :**

  For each output queue, select the CoS/802.1p priority to which egress traffic from the queue is remarked.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

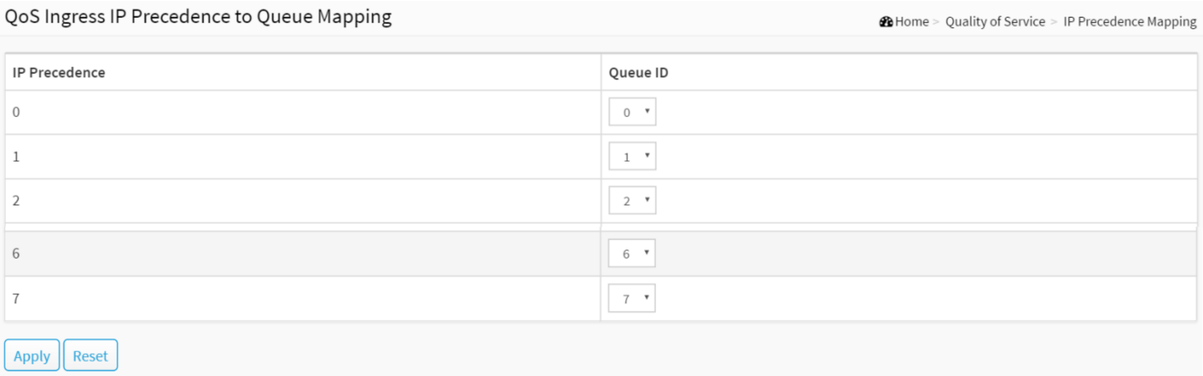
7-9 IP Precedence Mapping

To map IP precedence to egress queue.

Web Interface

To configure the IP Precedence Mapping in the web interface:

1. Click Quality of Service and IP Precedence Mapping.
2. Select Queue ID.
3. Click the Apply to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



QoS Ingress IP Precedence to Queue Mapping

IP Precedence	Queue ID
0	0
1	1
2	2
6	6
7	7

Figure 7-9: The QoS Ingress IP Precedence to Queue Mapping

Parameter description:

- **IP Precedence :**

  Displays the IP Precedence priority tag values to be assigned to an egress queue, where 0 is the lowest and 7 is the highest priority.

- **Queue ID :**

  Select the egress queue to which the IP precedence priority is mapped. Eight egress queues are supported, where Queue 7 is the highest priority egress queue and Queue 0 is the lowest priority egress queue.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

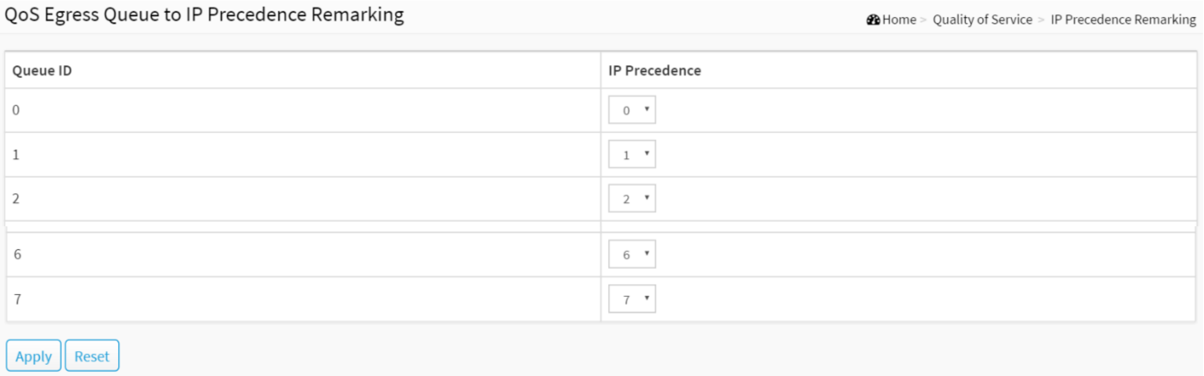
7-10 IP Precedence Remarking

To map egress queue to IP precedence.

Web Interface

To configure the IP Precedence Remarking in the web interface:

1. Click Quality of Service and IP Precedence Remarking.
2. Select IP Precedence.
3. Click the Apply to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



QoS Egress Queue to IP Precedence Remarking

Queue ID	IP Precedence
0	0
1	1
2	2
6	6
7	7

Figure 7-10: The QoS Egress Queue to IP Precedence Remarking

Parameter description:

- **Queue ID :**

  Displays the Queue ID, where Queue 7 is the highest priority egress queue and Queue 0 is the lowest priority egress queue.

- **IP Precedence :**

  For each output queue, select the IP Precedence priority to which egress traffic from the queue is remarked.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

7-11 DSCP Mapping

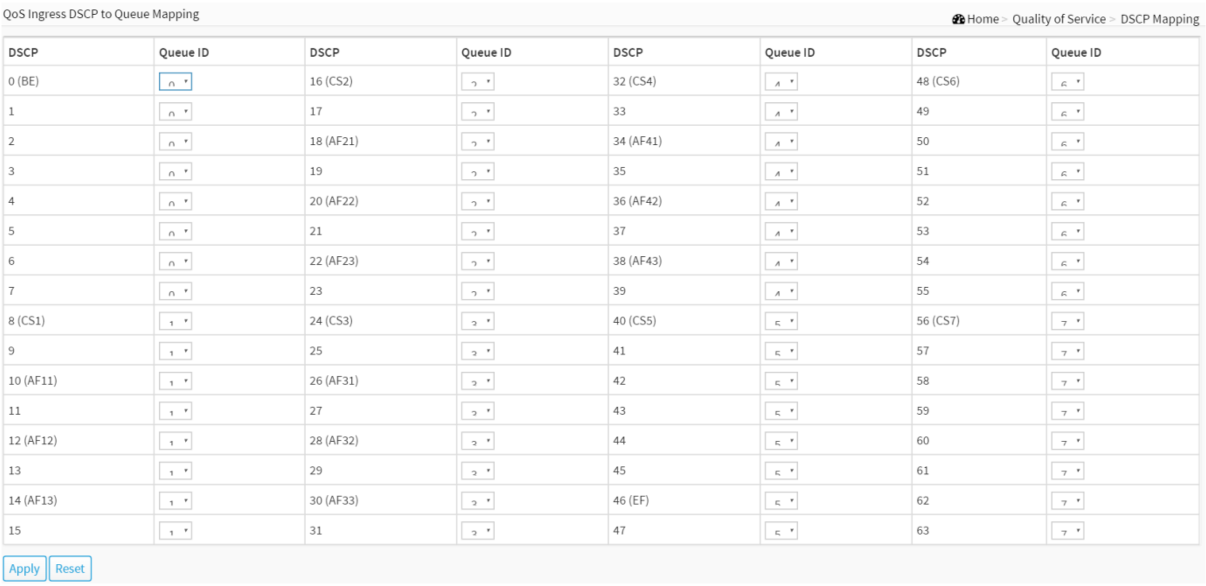
Use the DSCP to Queue page to map IP DSCP to egress queues. The DSCP to Queue table determines the egress queues of the incoming IP packets based on their DSCP values. The original VLAN Priority Tag (VPT) of the packet is unchanged.

It is possible to achieve the desired QoS in a network by simply changing the DSCP to Queue mapping, the queue schedule method, and bandwidth allocation.

Web Interface

To configure the DSCP Mapping in the web interface:

1. Click Quality of Service and DSCP Mapping.
2. Select Queue ID.
3. Click the Apply to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



QoS Ingress DSCP to Queue Mapping

DSCP	Queue ID	DSCP	Queue ID	DSCP	Queue ID	DSCP	Queue ID
0 (BE)	0	16 (CS2)	2	32 (CS4)	4	48 (CS6)	6
1	0	17	2	33	4	49	6
2	0	18 (AF21)	2	34 (AF41)	4	50	6
3	0	19	2	35	4	51	6
4	0	20 (AF22)	2	36 (AF42)	4	52	6
5	0	21	2	37	4	53	6
6	0	22 (AF23)	2	38 (AF43)	4	54	6
7	0	23	2	39	4	55	6
8 (CS1)	1	24 (CS3)	3	40 (CS5)	5	56 (CS7)	7
9	1	25	3	41	5	57	7
10 (AF11)	1	26 (AF31)	3	42	5	58	7
11	1	27	3	43	5	59	7
12 (AF12)	1	28 (AF32)	3	44	5	60	7
13	1	29	3	45	5	61	7
14 (AF13)	1	30 (AF33)	3	46 (EF)	5	62	7
15	1	31	3	47	5	63	7

Figure 7-11: The QoS Ingress DSCP to Queue Mapping

Parameter description:

- **DSCP :**

  Displays the DSCP value in the incoming packet and its associated class.

- **Queue ID :**

  Select the traffic forwarding queue from the Output Queue drop-down menu to which the DSCP value is mapped.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

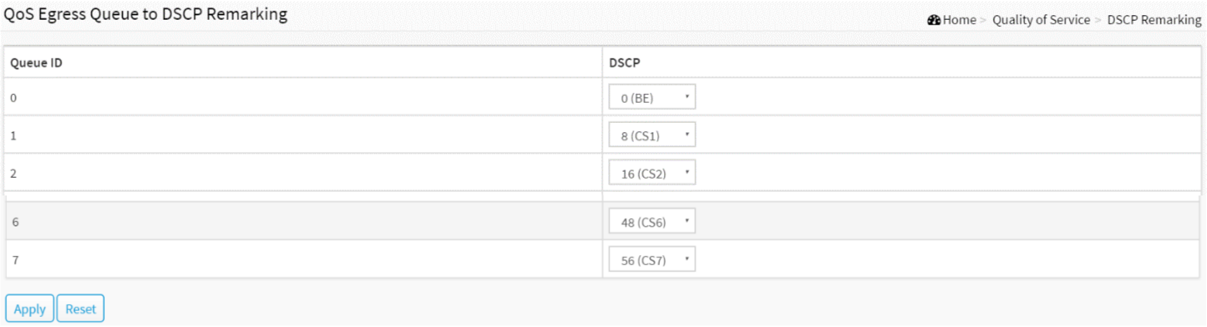
7-12 DSCP Remarking

Use the Queues to DSCP page to remark DSCP value for egress traffic from each queue.

Web Interface

To configure the DSCP Remarking in the web interface:

1. Click Quality of Service and DSCP Remarking.
2. Select DSCP.
3. Click the apply to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.


QoS Egress Queue to DSCP Remarking

Queue ID	DSCP
0	0 (BE)
1	8 (CS1)
2	16 (CS2)
6	48 (CS6)
7	56 (CS7)

Figure 7-12: The QoS Egress Queue to DSCP Remarking

Parameter description:

- **Queue ID :**

  Displays the Queue ID, where Queue 7 is the highest priority egress queue and Queue 0 is the lowest priority egress queue.

- **DSCP :**

  For each output queue, select the DSCP priority to which egress traffic from the queue is remarked.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

Chapter 8 Spanning tree

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

STP - STP uses a distributed algorithm to select a bridging device (STP- compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

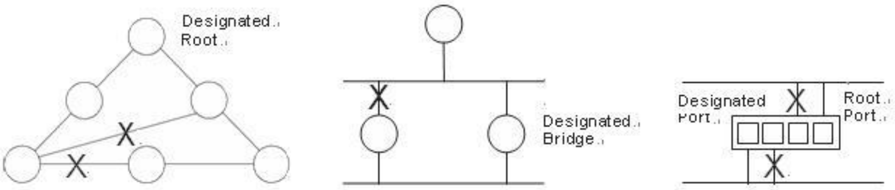


Figure 8: The Spanning Tree Protocol

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

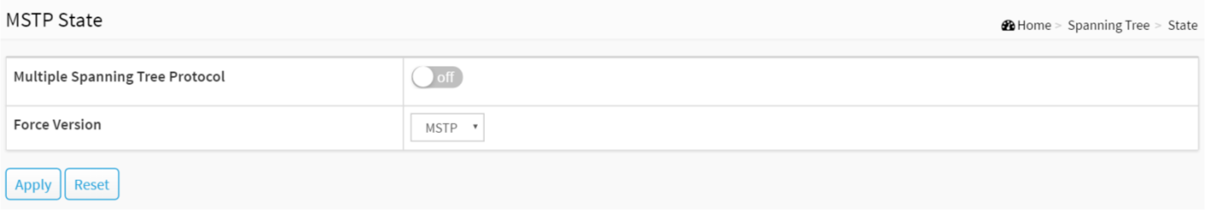
8-1 State

The section describes that you can select enable spanning tree protocol or not, and you can select what protocol version you want.

Web Interface

To configure the Spanning Tree Protocol version in the web interface:

1. Click Spanning Tree and state.
2. Evoke to enable or disable the Spanning Tree Protocol.
3. Select the Spanning Tree Protocol version.
4. Click the apply to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.


MSTP State

Multiple Spanning Tree Protocol	off
Force Version	MSTP

Figure 8-1: The Spanning Tree state

Parameter description:

- **Multiple Spanning Tree Protocol :**

  You can select enable spanning tree protocol or not.

- **Force Version :**

  The STP protocol version setting. Valid values are STP, RSTP and MSTP.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

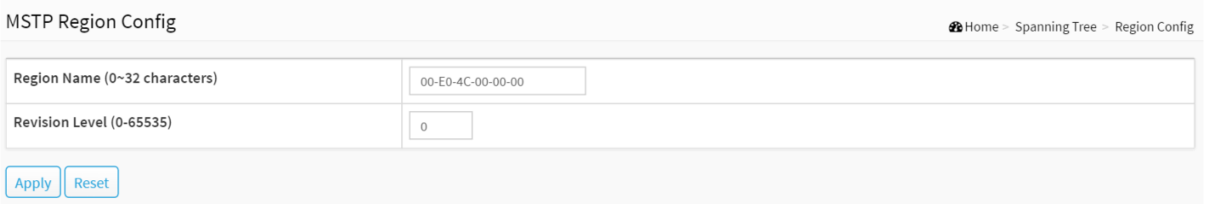
8-2 Region Config

The section describes to configure the basic identification of a MSTP bridge. Bridges participating in a common MST region must have the same Region Name and Revision Level.

Web Interface

To configure the Region Config in the web interface:

1. Click Spanning Tree and Region Config.
2. Specify the Region Name and Revision Level.
3. Click the Apply to save the setting.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.


MSTP Region Config

Region Name (0~32 characters)	00-E0-4C-00-00-00
Revision Level (0-65535)	0

Figure 8-2: The Region Configuration

Parameter description:

- **Configuration Name :**

  The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.

- **Configuration Revision :**

  The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

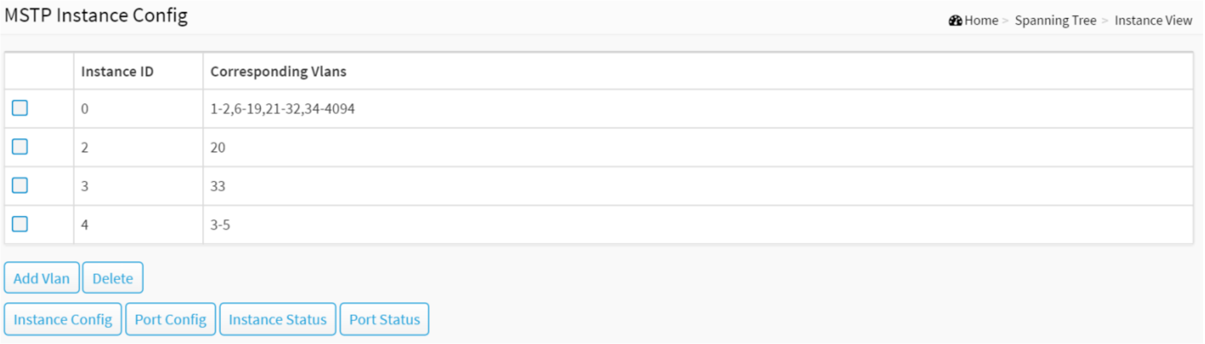
8-3 Instance View

The section providing an MST instance table which include information(vlan membership of a MSTI) of all spanning instances provisioned in the particular MST region which the bridge belongs to. Through this table, additional MSTP configuration data can be applied and MSTP status can be retrieved.

Web Interface

To configure the MSTP Instance in the web interface:

1. Click Spanning Tree and Instance.
2. Click to add vlan.
3. Specify the Instance and Port.
4. Click Instance Status and Port Status to see the detail.
5. If you want to cancel the setting then you need to click Delete.



MSTP Instance Config

	Instance ID	Corresponding Vlans
□	0	1-2,6-19,21-32,34-4094
□	2	20
□	3	33
□	4	3-5

Figure 8-3: MSTP Instance Config

Parameter description:

- **Instance ID :**

  Every spanning tree instance need to have a unique instance ID within 0~4094. Instance 0 (CIST) always exists and can not be deleted. Additional spanning instances (MSTIs) can be added or deleted. At least one vlan must be provisioned for an MSTI to declare the need for the MSTI to be existent.

- **Corresponding Vlans :**

  1-4094.

  Multiple vlans can belong to an MSTI. All vlans that are not provisioned through this will be automatically assigned to Instance 0(CIST).

Buttons

- **Add Vlan :**

  To add an MSTI and provide its vlan members or modify vlan members for a specific MSTI, you can add up to 63 so that a total of 64.

- **Delete :**

  To delete an MSTI.

- **Instance Config :**

  To provision spanning tree performance parameters per instance.

- **Port Config :**

  To provision spanning tree performance parameters per instance per port.

- **Instance Status :**

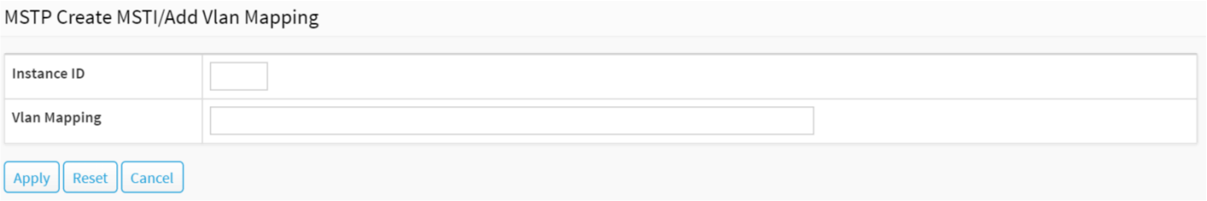
  To show the status report of a particular spanning tree instance.

- **Port Status :**

  To show the status report of all ports regarding a specific spanning tree instance.

Please refer to the following introduction:

■ **Add Vlan :**



MSTP Create MSTI/Add Vlan Mapping

Instance ID	
Vlan Mapping	

Figure 8-3: Add Vlan

Parameter description:

- **Instance ID :**

  The Range is 1-4094

- **Vlan Mapping :**

  The list of VLANs mapped to the MSTI. The VLANs can be given as a single (xx, xx being between 1 and 4094) VLAN, or a range (xx-yy), each of which must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.) Example: 2,5,20-40.

Buttons

- **Apply :**

  Click to save changes.

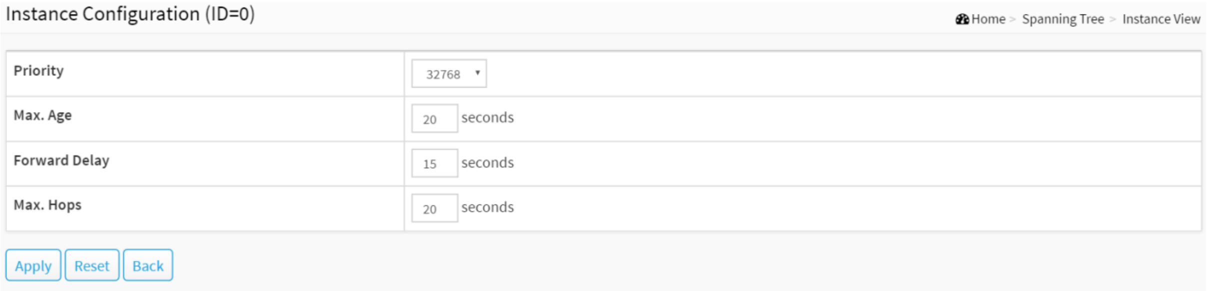
- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

- **Cancel :**

  Click to undo any changes made locally and return to the Users.

- **Instance Config to Instance 0 :**



Instance Configuration (ID=0)

Home > Spanning Tree > Instance View

Priority	32768
Max. Age	20 seconds
Forward Delay	15 seconds
Max. Hops	20 seconds

Figure 8-3: Instance Config to Instance 0

Parameter description:

- **Priority :**

  The priority parameter used in the CIST(Common and Internal Spanning Tree) connection.

  0 / 4096 / 8192 / 12288 / 16384 / 20480 / 24576 / 28672 / 32768 / 36864 / 40960 / 45056 / 49152 / 53248 / 57344 / 61440

- **MAX. Age :**

  6-40sec. The same definition as in the RSTP protocol.

- **Forward Delay :**

  4-30sec. The same definition as in the RSTP protocol.

- **MAX. Hops :**

  6-40sec. It's a new parameter for the multiple spanning tree protocol. It is used in the internal spanning tree instances. "CIST Remaining Hops" or "MSTI Remaining Hops" in the Spanning tree protocol message would decreased by one when the message is propagated to the neighboring bridge. If the Remaining Hops in a message is zero, the message (BPDU) would be regarded as invalid. Max Hops is used to specify the initial value of the Remaining Hops for Regional Root Bridge (Either CIST Regional Root or MSTI Regional Root)

Buttons

- **Apply :**

  Click to save changes.

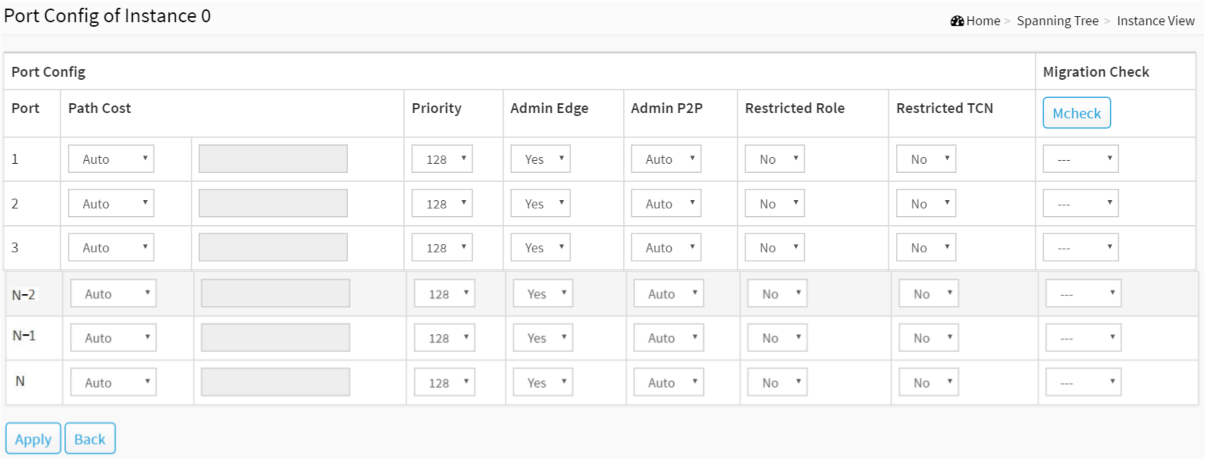
- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

- **Back :**

  Click to undo any changes made locally and return to the Users.

■ Port Config to Instance 0 :



Port Config of Instance 0

Port Config								Migration Check
Port	Path Cost		Priority	Admin Edge	Admin P2P	Restricted Role	Restricted TCN	Mcheck
1	Auto		128	Yes	Auto	No	No	---
2	Auto		128	Yes	Auto	No	No	---
3	Auto		128	Yes	Auto	No	No	---
N-2	Auto		128	Yes	Auto	No	No	---
N-1	Auto		128	Yes	Auto	No	No	---
N	Auto		128	Yes	Auto	No	No	---

Figure 8-3: Port Config to Instance 0

Parameter description:

- **Port :**

  The logical port for the settings contained in the same row.

- **Path Cost :**

  1 – 200,000,000

  The same definition as in the RSTP specification. But in MSTP, this parameter can be respectively applied to ports of CIST and ports of any MSTI.

- **Priority :**

  0 / 16 / 32 / 48 / 64 / 80 / 96 / 112 / 128 / 144 / 160 / 176 / 192 / 208 / 224 / 240

  The same definition as in the RSTP specification. But in MSTP, this parameter can be respectively applied to ports of CIST and ports of any MSTI.

- **Admin Edge :**

  Yes / No

  The same definition as in the RSTP specification for the CIST ports.

- **Admin P2P :**

  Auto / True / False

  The same definition as in the RSTP specification for the CIST ports.

- **Restricted Role :**

  Yes / No

  If "Yes" causes the Port not to be selected as Root Port for the CIST or any MSTI, even it has the best spanning tree priority vector. Such a Port will be selected as an Alternate Port after the Root Port has been selected. This parameter is "No" by default. If set, it can cause lack of spanning tree connectivity. It is set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator.

- **Restricted TCN :**

  Yes / No

  If "Yes" causes the Port not to propagate received topology change notifications and topology changes to other Ports. This parameter is “No” by default. If set it can cause temporary loss of connectivity after changes in a spanning trees active topology as a result of persistent incorrectly learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator. Or the status of MAC operation for the attached LANs transitions frequently.

- **Mcheck :**

  The same definition as in the RSTP specification for the CIST ports.

Buttons

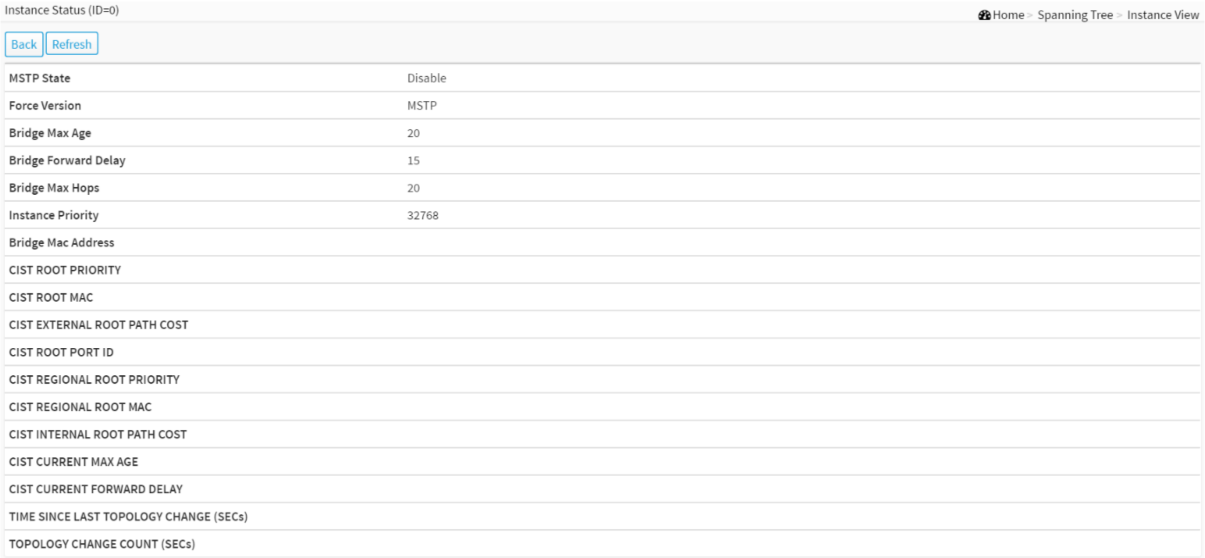
- **Apply :**

  Click to save changes.

- **Back :**

  Click to undo any changes made locally and return to the Users.

■ Instance Status to Instance 0 :



MSTP State	Disable
Force Version	MSTP
Bridge Max Age	20
Bridge Forward Delay	15
Bridge Max Hops	20
Instance Priority	32768
Bridge Mac Address	
CIST ROOT PRIORITY	
CIST ROOT MAC	
CIST EXTERNAL ROOT PATH COST	
CIST ROOT PORT ID	
CIST REGIONAL ROOT PRIORITY	
CIST REGIONAL ROOT MAC	
CIST INTERNAL ROOT PATH COST	
CIST CURRENT MAX AGE	
CIST CURRENT FORWARD DELAY	
TIME SINCE LAST TOPOLOGY CHANGE (SECs)	
TOPOLOGY CHANGE COUNT (SECs)	

Figure 8-3: Instance Status to Instance 0

Parameter description:

- **MSTP State :**

  MSTP protocol is Enable or Disable.

- **Force Version :**

  It shows the current spanning tree protocol version configured.

- **Bridge Max Age :**

  It shows the Max Age setting of the bridge itself.

- **Bridge Forward Delay :**

  It shows the Forward Delay setting of the bridge itself.

- **Bridge Max Hops :**

  It shows the Max Hops setting of the bridge itself.

- **Instance Priority :**

Spanning tree priority value for a specific tree instance(CIST or MSTI)

- **Bridge Mac Address :**

  The Mac Address of the bridge itself.

- **CIST ROOT PRIORITY :**

  Spanning tree priority value of the CIST root bridge

- **CIST ROOT MAC :**

  Mac Address of the CIST root bridge

- **CIST EXTERNAL ROOT PATH COST :**

  Root path cost value from the point of view of the bridge's MST region.

- **CIST ROOT PORT ID :**

  The port ID of the bridge's root port. In MSTP, peer port of a root port may reside in different MST region or in the same MST region. The first case indicates that the root port's owner is the CIST regional root bridge.

- **CIST REGIONAL ROOT PRIORITY :**

  Spanning tree priority value of the CIST regional root bridge. Note that CIST Regional Root bridge is different from CIST Root bridge. One exception is that when a bridge belonging to an MST region happens to be the root bridge of the CST(Common Spanning Tree). An MST Region in the CST can be regarded as a common RSTP bridge. The IST(Internal Spanning Tree) and MSTIs are transparent to bridges outside this region.

- **CIST REGIONAL ROOT MAC :**

  Mac Address of the CIST regional root bridge.

- **CIST INTERNAL ROOT PATH COST :**

  Root path cost value from the point of view of the bridges inside the IST.

- **CIST CURRENT MAX AGE :**

  Max Age of the CIST Root bridge.

- **CIST CURRENT FORWARD DELAY :**

  Forward Delay of the CIST Root bridge.

- **TIME SINCE LAST TOPOLOGY CHANGE(SECs) :**

  Time Since Last Topology Change is the elapsed time in unit of seconds for a bunch of "Topology Change and(or) Topology Change Notification receiving" to occur. When new series of Topology Changes occur again, this counter will be reset to 0.

- **TOPOLOGY CHANGE COUNT(SECs) :**

  The per spanning tree instance Topology Change Count expresses the time spent in unit of seconds since the beginning of the Spanning Tree Topology Change to the end of the STP convergence. Once there is no topology change occurring and no more topology change notification received, the Topology Change count will be reset to 0.

Buttons

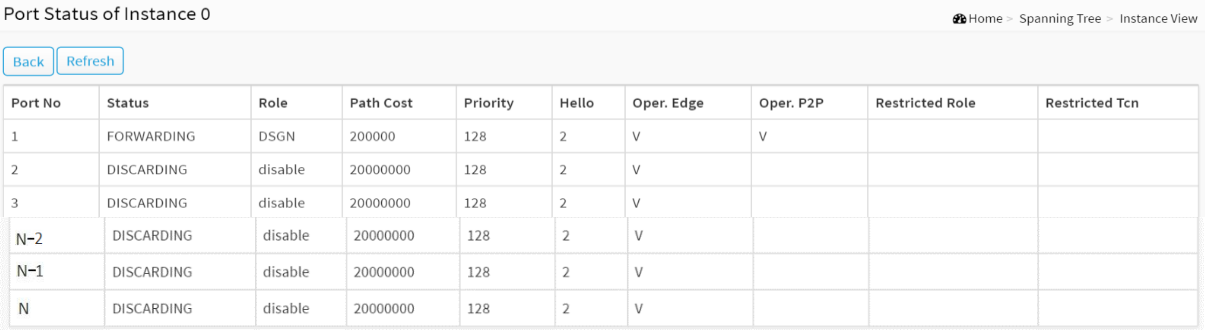
- **Back :**

  Click to undo any changes made locally and return to the Users.

- **Refresh :**

  Click to refresh the page.

- **Port Status to Instance 0 :**



Port Status of Instance 0

Port No	Status	Role	Path Cost	Priority	Hello	Oper. Edge	Oper. P2P	Restricted Role	Restricted Tcn
1	FORWARDING	DSGN	200000	128	2	V	V		
2	DISCARDING	disable	20000000	128	2	V			
3	DISCARDING	disable	20000000	128	2	V			
N-2	DISCARDING	disable	20000000	128	2	V			
N-1	DISCARDING	disable	20000000	128	2	V			
N	DISCARDING	disable	20000000	128	2	V			

Figure 8-3: Port Status to Instance 0

Parameter description:

- **Port No:**

  The port number to which the configuration applies.

- **Status:**

  The forwarding status. Same definition as of the RSTP specification Possible values are "FORWARDING" , "LEARNING" , "DISCARDING"

- **Role:**

  The role that a port plays in the spanning tree topology. Possible values are "disable"(disable port) , "alternate"(alternate port) , "backup"(backup port) , "ROOT"(root port) , "DSGN"(designated port) , "MSTR"(master port). The last 3 are possible port roles for a port to transit to FORWARDING state

- **Path Cost:**

  Display currently resolved port path cost value for each port in a particular spanning tree instance.

- **Priority:**

  Display port priority value for each port in a particular spanning tree instance.

- **Hello:**

  Per port Hello Time display. It takes the following form:

  Current Hello Time/Hello Time Setting

- **Oper. Edge:**

  Whether or not a port is an Edge Port in reality.

- **Oper. P2P:**

  Whether or not a port is a Point-to-Point Port in reality.

- **Restricted Role:**

  Same as mentioned in "Port Config"

- **Restricted Tcn:**

Same as mentioned in "Port Config"

Buttons

- **Back :**

  Click to undo any changes made locally and return to the Users.

- **Refresh :**

  Click to refresh the page.

Chapter 9 MAC Address Tables

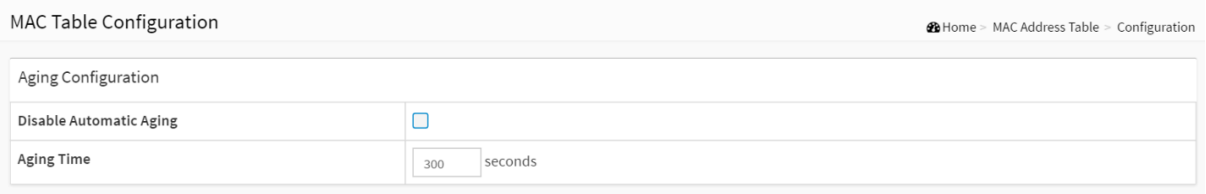
9-1 Configuration

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

Web Interface

To configure MAC Address Table in the web interface:

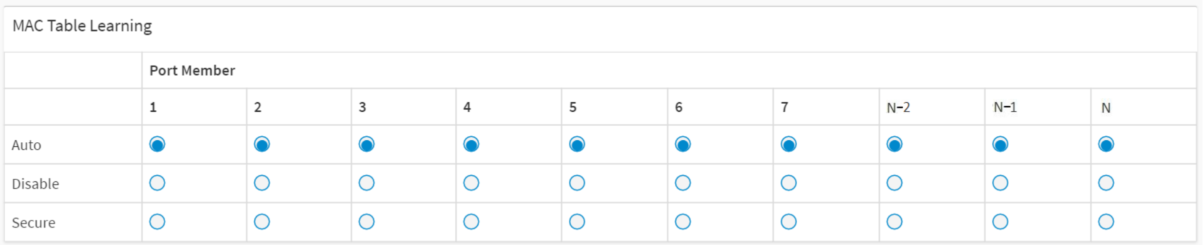
1. Click MAC Address Tables and Configuration.
2. Specify the Disable Automatic Aging and Aging Time.
3. Specify the Port Members (Auto, Disable, Secure).
4. Add new Static entry, Specify the VLAN IP and Mac address, Port Members, Block.
5. Click Apply.



MAC Table Configuration

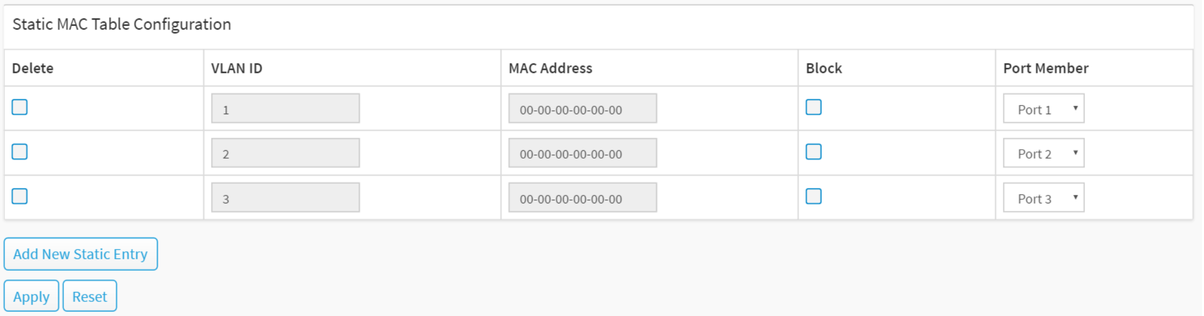
Aging Configuration

Disable Automatic Aging	□
Aging Time	300 seconds



MAC Table Learning

	Port Member									
	1	2	3	4	5	6	7	N-2	N-1	N
Auto	●	●	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○



Static MAC Table Configuration

Delete	VLAN ID	MAC Address	Block	Port Member
□	1	00-00-00-00-00-00	□	Port 1
□	2	00-00-00-00-00-00	□	Port 2
□	3	00-00-00-00-00-00	□	Port 3

Figure 9-1: The MAC Address Table Configuration

Parameter description:

Aging Configuration :

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

Configure aging time by entering a value here in seconds; for example, Age time seconds.

The allowed range is 10 to 1000000 seconds.

Disable the automatic aging of dynamic entries by checking ☑ Disable automatic aging.

MAC Table Learning

If the learning mode for a given port is greyed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X. Each port can do learning based upon the following settings:

- **Auto :**

  Learning is done automatically as soon as a frame with unknown SMAC is received.

- **Disable :**

  No learning is done.

- **Secure :**

  Only static MAC entries are learned, all other frames are dropped.

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

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 128 entries. The maximum of 128 entries is for the whole stack, and not per switch.

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **VLAN ID :**

  The VLAN ID of the entry.

- **MAC Address :**

The MAC address of the entry.

- **Block :**

  Click it, if you want block this mac address.

- **Port Members :**

  Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Buttons

- **Adding a New Static Entry :**

  Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Apply".

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

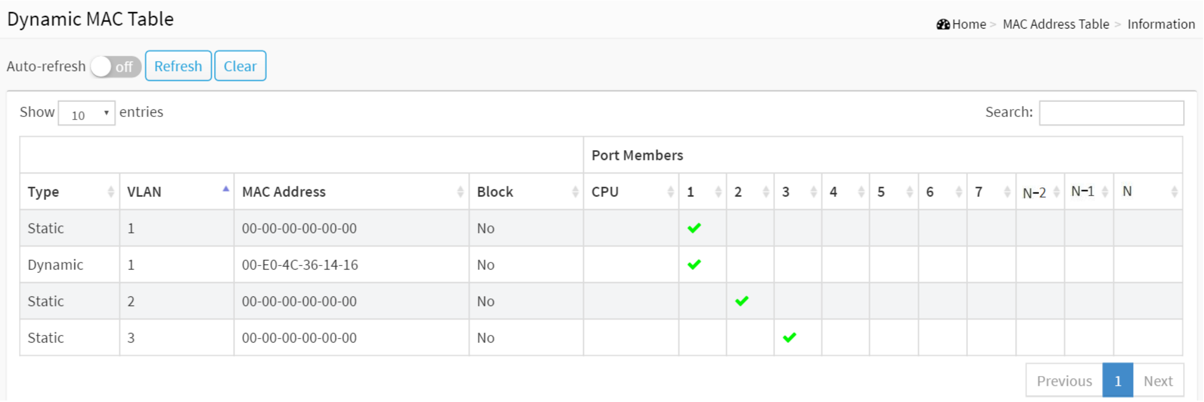
9-2 Information

Entries in the MAC Table are shown on this page. The MAC Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

Web Interface

To Display MAC Address Table in the web interface:

1. Click MAC Address Table and Information.
2. Display MAC Address Table.



Dynamic MAC Table

Home > MAC Address Table > Information

Auto-refresh off Refresh Clear

Show 10 entries Search:

				Port Members										
Type	VLAN	MAC Address	Block	CPU	1	2	3	4	5	6	7	N-2	N-1	N
Static	1	00-00-00-00-00-00	No		✓									
Dynamic	1	00-E0-4C-36-14-16	No		✓									
Static	2	00-00-00-00-00-00	No			✓								
Static	3	00-00-00-00-00-00	No				✓							

Previous 1 Next

Figure 9-2: The MAC Address Table Information

Parameter description:

Navigating the MAC Table

Each page shows up to 999 entries from the MAC table, default being 10, selected through the "entries per page" input field. When first visited, the web page will show the first 10 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

- **Type :**

  Indicates whether the entry is a static or a dynamic entry, 802.1x, DMS.

- **VLAN :**

  The VLAN ID of the entry.

- **MAC address :**

  The MAC address of the entry.

- **Block :**

  Whether the mac address is blocked or not.

- **Port Members :**

  The ports that are members of the entry.

Buttons

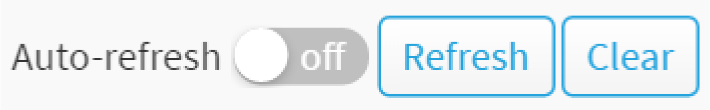


Figure 9-2: The MAC Address Table Information buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Click to clear the page.

- **Next :**

  Updates the mac address entries, turn to the next page.

- **Previous :**

  Updates the mac address entries, turn to the previous page.

NOTE:
00-11-3B-73-01-29 : your switch MAC address (for IPv4)
33-33-00-00-00-01 : Destination MAC (for IPv6 Router Advertisement)
(reference IPv6 RA.JPG)
33-33-00-00-00-02 : Destination MAC (for IPv6 Router Solicitation)
(reference IPv6 RS.JPG)
33-33-FF-73-01-29 : Destination MAC (for IPv6 Neighbor Solicitation)
(reference IPv6 DAD.JPG)
33-33-FF-A8-01-01: your switch MAC address (for IPv6 global IP)
FF-FF-FF-FF-FF-FF: for Broadcast.

Chapter 10 Multicast

10-1 IGMP Snooping

The function, is used to establish the multicast groups to forward the multicast packet to the member ports, and, in nature, avoids wasting the bandwidth while IP multicast packets are running over the network. This is because a switch that does not support IGMP or IGMP Snooping cannot tell the multicast packet from the broadcast packet, so it can only treat them all as the broadcast packet. Without IGMP Snooping, the multicast packet forwarding function is plain and nothing is different from broadcast packet.

A switch supported IGMP Snooping with the functions of query, report and leave, a type of packet exchanged between IP Multicast Router/Switch and IP Multicast Host, can update the information of the Multicast table when a member (port) joins or leaves an IP Multicast Destination Address. With this function, once a switch receives an IP multicast packet, it will forward the packet to the members who joined in a specified IP multicast group before.

The packets will be discarded by the IGMP Snooping if the user transmits multicast packets to the multicast group that had not been built up in advance. IGMP mode enables the switch to issue IGMP function that you enable IGMP proxy or snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

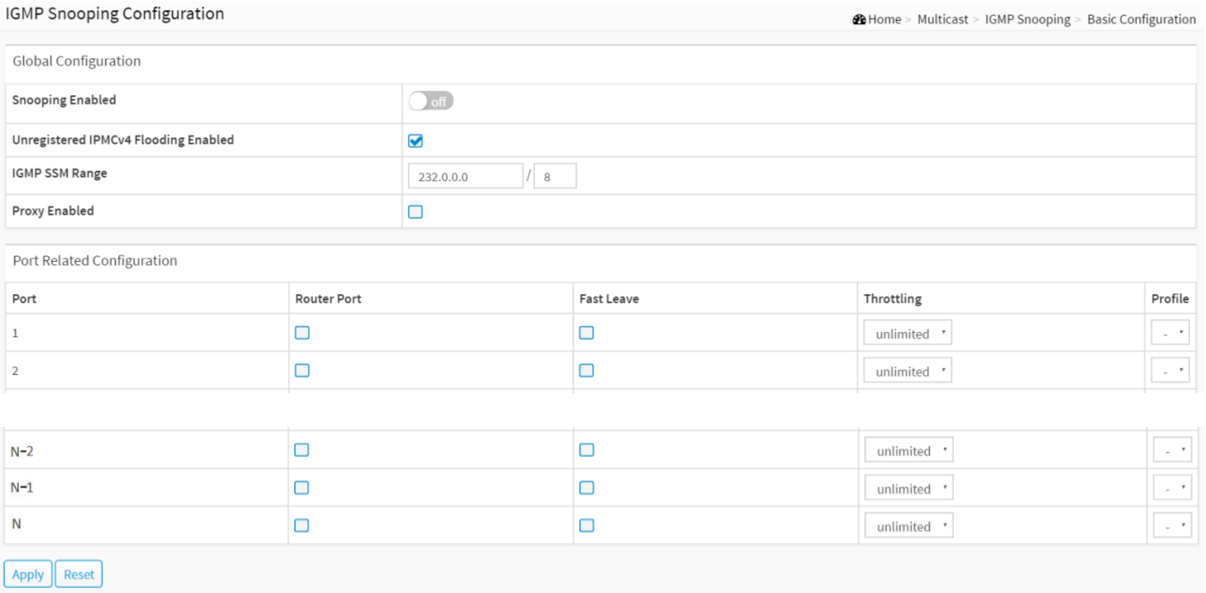
10-1.1 Basic Configuration

The section describes how to set the basic IGMP snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP

Web Interface

To configure the IGMP Snooping parameters in the web interface:

1. Click Multicast, IGMP Snooping and Basic Configuration.
2. Evoke to select enable or disable which Global configuration
3. Evoke which port wants to become a Router Port or enable/ disable the Fast Leave function..
4. Scroll to set the Throtting and Profile.
5. Click the Apply to save the setting
6. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values



IGMP Snooping Configuration

Home > Multicast > IGMP Snooping > Basic Configuration

Global Configuration	
Snooping Enabled	off
Unregistered IPMCv4 Flooding Enabled	☑
IGMP SSM Range	232.0.0.0 / 8
Proxy Enabled	□

Port Related Configuration

Port	Router Port	Fast Leave	Throttling	Profile
1	□	□	unlimited	-
2	□	□	unlimited	-
N-2	□	□	unlimited	-
N-1	□	□	unlimited	-
N	□	□	unlimited	-

Figure 10-1.1: The IGMP Snooping Configuration

Parameter description:

Global Configuration

- **Snooping Enabled :**

  Enable the Global IGMP Snooping.

- **Unregistered IPMCv4 Flooding enabled :**

  Enable unregistered IPMCv4 traffic flooding. Unregistered IPMCv4 traffic is so-called unknown multicast.

  After selected, the unregistered multicast stream will be forwarded like normal packets. Once you un-selected it, such stream will be discarded

- **IGMP SSM Range :**

  SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. Format: (IP address/ sub mask)

- **Proxy Enabled :**

  Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Port Related Configuration

- **Port :**

  It shows the physical Port index of switch.

- **Router Port :**

  Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

  If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

- **Fast Leave :**

  Enable the fast leave on the port.

- **Throttling :**

  Enable to limit the number of multicast groups to which a switch port can belong.

- **Profile:**

  You can select profile when you edit in Multicast Filtering Profile.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

10-1.2 VLAN Configuration

The section describes the VLAN configuration setting process integrated with IGMP Snooping function. For Each setting page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the button will update the displayed table starting from that or the next closest VLAN Table match.

Web Interface

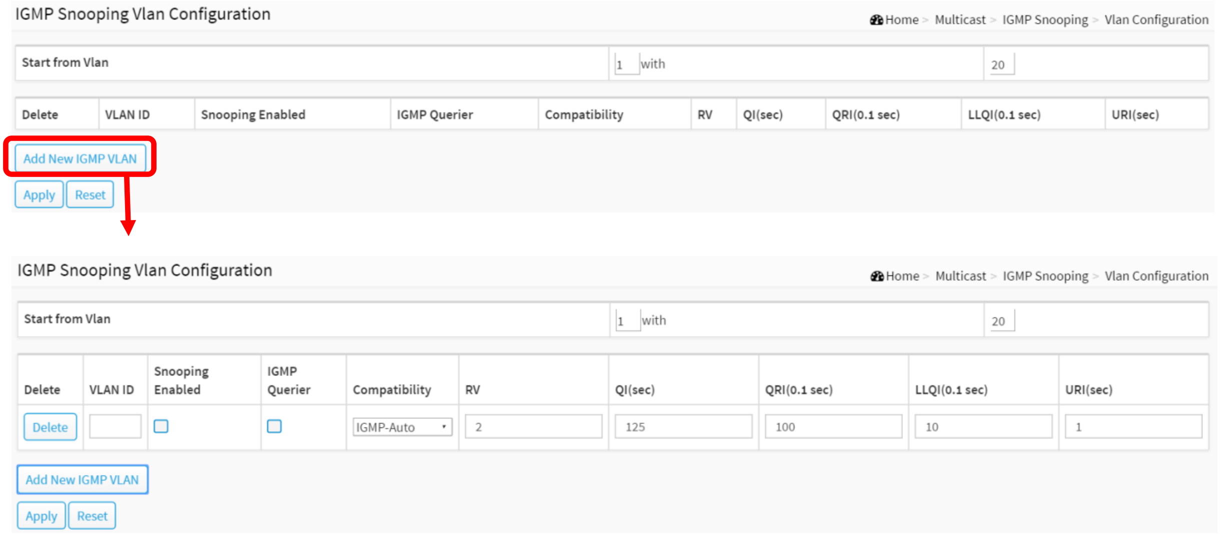
To configure the IGMP Snooping VLAN Configuration in the web interface:

1. Click Multicast, IGMP Snooping and VLAN Configuration.

2. Click to add new IGMP VLAN.

3. Click the Apply to save the setting

4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values


IGMP Snooping Vlan Configuration
Home > Multicast > IGMP Snooping > Vlan Configuration
Add New IGMP VLAN
Apply
Reset
IGMP Snooping Vlan Configuration
Home > Multicast > IGMP Snooping > Vlan Configuration
Add New IGMP VLAN
Apply
Reset

Start from Vlan	1 with	20

Delete	VLAN ID	Snooping Enabled	IGMP Querier	Compatibility	RV	QI(sec)	QRI(0.1 sec)	LLQI(0.1 sec)	URI(sec)

Start from Vlan	1 with	20

Delete	VLAN ID	Snooping Enabled	IGMP Querier	Compatibility	RV	QI(sec)	QRI(0.1 sec)	LLQI(0.1 sec)	URI(sec)
Delete		□	□	IGMP-Auto	2	125	100	10	1

Figure 10-1.2: The IGMP Snooping VLAN Configuration

Parameter description:

- **Start from Vlan :**

  You can click them Refreshes the displayed table starting from the "VLAN" input fields.

- **Delete :**

  Check to delete the entry. The designated entry will be deleted during the next save.

- **VLAN ID :**

  It displays the VLAN ID of the entry.

- **Snooping Enabled :**

  Enable the per-VLAN IGMP Snooping. Only up to 32 VLANs can be selected. .

- **IGMP Querier :**

  Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

- **Compatibility :**

  Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto.

- **Rv :**

  Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255; default robustness variable value is 2.

- **QI(sec) :**

  Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds; default query interval is 125 seconds.

- **QRI(0.1 sec) :**

  Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds; default query response interval is 100 in tenths of seconds (10 seconds).

- **LLQI (0.1 sec) :**

  Last Member Query Interval. The Last Member Query Time is the time value represented by the

Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds; default last member query interval is 10 in tenths of seconds (1 second).

- **URI(sec) :**

  Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second. .

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

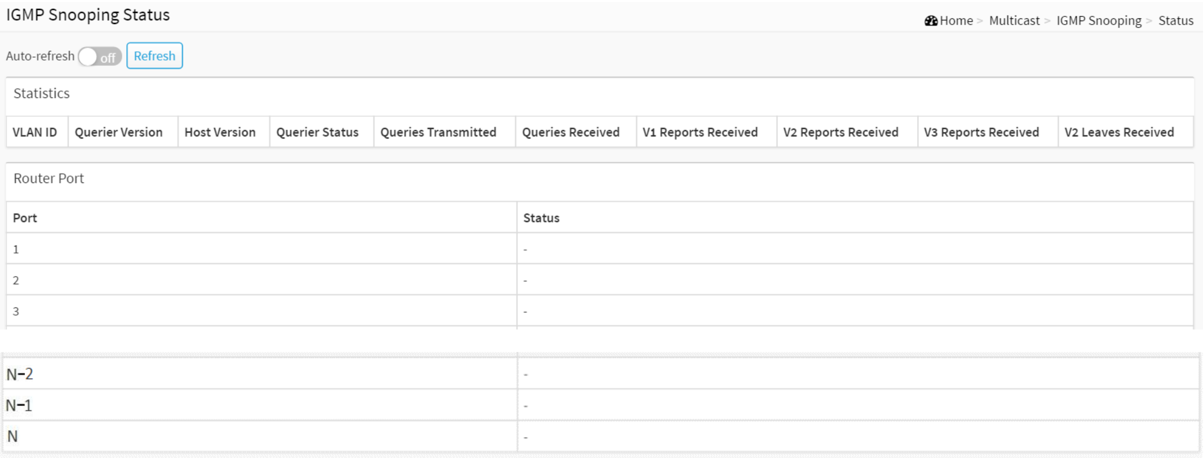
10-1.3 Status

After you complete the IGMP Snooping configuration, then you could to let the switch display the IGMP Snooping Status. The Section provides you to let switch to display the IGMP Snooping detail status.

Web Interface

To display the IGMP Snooping status in the web interface:

1. Click Multicast, IGMP Snooping and Status.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the IGMP Snooping Status.



IGMP Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received

Router Port

Port	Status
1	-
2	-
3	-
N-2	-
N-1	-
N	-

Figure 10-1.3: The IGMP Snooping Status

Parameter description:

Statistic

- **VLAN ID :**

  The VLAN ID of the entry.

- **Querier Version :**

Working Querier Version currently.

- **Host Version :**

  Working Host Version currently.

- **Querier Status :**

  Shows the Querier status is "ACTIVE" or "IDLE".

  "DISABLE" denotes the specific interface is administratively disabled.

- **Queries Transmitted :**

  The number of Transmitted Queries.

- **Queries Received :**

  The number of Received Queries.

- **V1 Reports Received :**

  The number of Received V1 Reports.

- **V2 Reports Received :**

  The number of Received V2 Reports.

- **V3 Reports Received :**

  The number of Received V3 Reports.

- **V2 Leaves Received :**

  The number of Received V2 Leaves.

Router Port

Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. Static denotes the specific port is configured to be a router port. Dynamic denotes the specific port is learnt to be a router port. Both denote the specific port is configured or learnt to be a router port.

- **Port**

  Switch port number.

- **Status**

  Indicate whether specific port is a router port or not.

Buttons

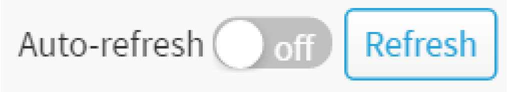


Figure 10-1.3: The IGMP Snooping Status buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

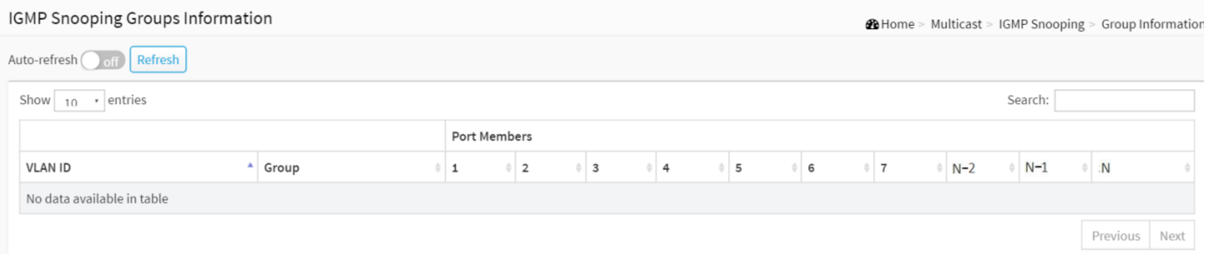
10-1.4 Group Information

After you complete to set the IGMP Snooping function then you could let the switch to display the IGMP Snooping Group Information. Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group. This will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

Web Interface

To display the IGMP Snooping Group Information in the web interface:

1. Click Multicast, IGMP Snooping and Group Information.
2. Specify how many entries to show in one page.
3. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
4. Click “Refresh” to refresh an entry of the IGMP Snooping Groups Information.
5. Click Previous/next to change page.



IGMP Snooping Groups Information

		Port Members									
VLAN ID	Group	1	2	3	4	5	6	7	N-2	N-1	N
No data available in table											

Figure 10-1.4: The IGMP Snooping Groups Information

Parameter description:

Navigating the IGMP Group Table

Each page shows up to many entries from the IGMP Group table, default being 10, selected through the "entries per page" input field. When first visited, the web page will show the first 10 entries from the beginning of the IGMP Group Table.

The "Search" input fields allow the user to select the starting point in the IGMP Group Table. It will update the displayed table starting from that or the closest next IGMP Group Table match.

This will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table.

- **Search :**

  You can search for the information that you want to see.

- **Show entries :**

  You can choose how many items you want to show up.

- **VLAN ID :**

  VLAN ID of the group.

- **Groups :**

  Group address of the group displayed.

- **Port Members :**

  Ports under this group.

Buttons

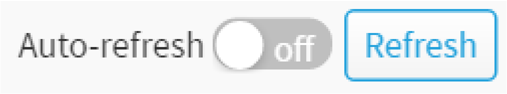


Figure 10-1.4: The IGMP Snooping Groups Information buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

- **Next :**

  Updates the group information entries, turn to the next page.

- **Previous :**

  Updates the group information entries, turn to the previous page.

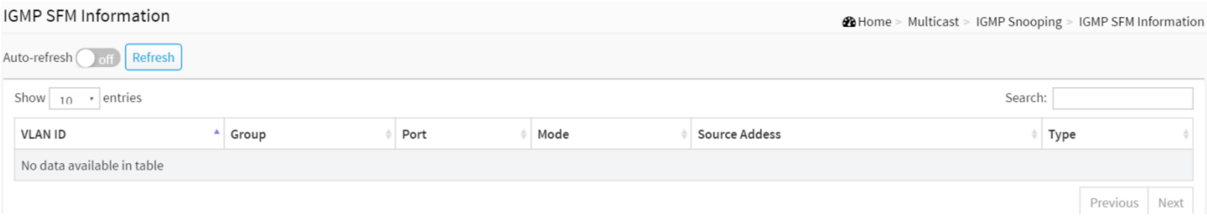
10-1.5 IGMP SFM Information

Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Web Interface

To display the IGMP SFM Information in the web interface:

1. Click Multicast, IGMP Snooping and IGMP SFM Information
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh” to refresh an entry of the IGMP Snooping Groups Information.
4. Click Previous/next to change page.



VLAN ID	Group	Port	Mode	Source Addess	Type
No data available in table					

Figure 10-1.5: The IGMP SFM Information

Parameter description:

Navigating the IGMP SFM Information Table

Each page shows up to many entries from the IGMP SFM Information table, default being 10, selected through the "entries per page" input field. When first visited, the web page will show the first 10 entries from the beginning of the IGMP SFM Information Table.

The "Search" input fields allow the user to select the starting point in the IGMP SFM Information Table. It will update the displayed table starting from that or the closest next IGMP SFM Information Table match.

This will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table.

- **Search :**

  You can search for the information that you want to see.

- **Show entries :**

  You can choose how many items you want to show up.

- **VLAN ID :**

  VLAN ID of the group.

- **Group :**

  Group address of the group displayed.

- **Port :**

  Switch port number.

- **Mode :**

  Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

- **Source Address :**

  IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

- **Type :**

  Indicates the Type. It can be either Allow or Deny.

Buttons

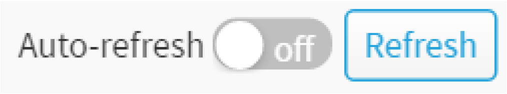


Figure 10-1.5: The IGMP Snooping Groups Information buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

- **Next :**

Updates the group information entries, turn to the next page.

- **Previous :**

  Updates the group information entries, turn to the previous page.

10-2 MLD Snooping

Curiously enough, a network node that acts as a source of IPv6 multicast traffic is only an indirect participant in MLD snooping—it just provides multicast traffic, and MLD doesn't interact with it. (Note, however, that in an application like desktop conferencing a network node may act as both a source and an MLD host; but MLD interacts with that node only in its role as an MLD host.)

A source node creates multicast traffic by sending packets to a multicast address. In IPv6, addresses with the first eight bits set (that is, "FF" as the first two characters of the address) are multicast addresses, and any node that listens to such an address will receive the traffic sent to that address. Application software running on the source and destination systems cooperates to determine what multicast address to use. (Note that this is a function of the application software, not of MLD.)

When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts

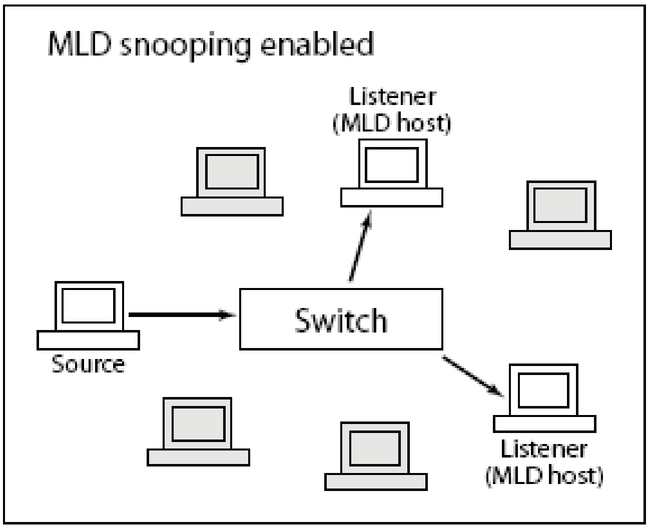


Figure 10-2: The MLD snooping enable

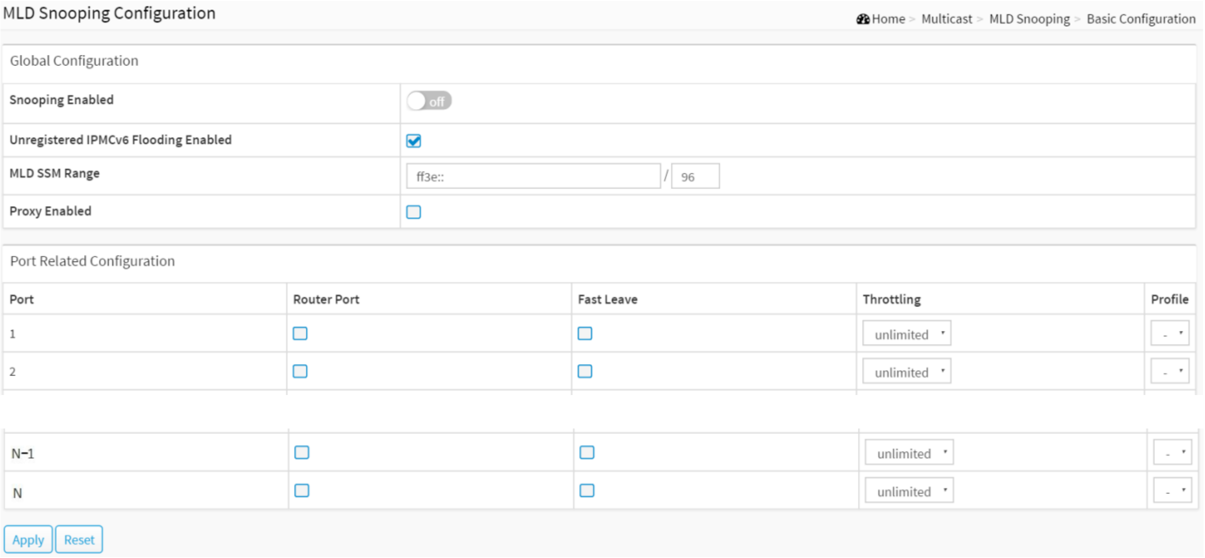
10-2.1 Basic Configuration

The section will let you understand how to configure the MLD Snooping basic configuration and the parameters.

Web Interface

To configure the MLD Snooping Configuration in the web interface:

1. Click Multicast, MLD Snooping and Basic Configuration.
2. Evoke to enable or disable the Global configuration parameters.
3. Evoke the port to join Router port and Fast Leave.
4. Scroll to select the Throtting mode with unlimited or 1 to 10
5. Click the save to save the setting
6. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values



MLD Snooping Configuration

Home > Multicast > MLD Snooping > Basic Configuration

Global Configuration

Snooping Enabled	off
Unregistered IPMCv6 Flooding Enabled	☑
MLD SSM Range	ff3e:: / 96
Proxy Enabled	□

Port Related Configuration

Port	Router Port	Fast Leave	Throttling	Profile
1	□	□	unlimited	-
2	□	□	unlimited	-
N-1	□	□	unlimited	-
N	□	□	unlimited	-

Figure 10-2.1: The MLD Snooping Basic Configuration

Parameter description :

Global Configuration

- **Snooping Enabled :**

  Enable the Global MLD Snooping.

- **Unregistered IPMCv6 Flooding enabled :**

  Enable unregistered IPMCv6 traffic flooding.

The flooding control takes effect only when MLD Snooping is enabled.

When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.

- **MLD SSM Range :**

  SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address (Using IPv6 Address) range.

- **Proxy Enabled :**

  Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Port Related Configuration

- **Router Port :**

  Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

- **Fast Leave :**

  To evoke to enable the fast leave on the port.

- **Throttling :**

  Enable to limit the number of multicast groups to which a switch port can belong.

- **Profile :**

  You can select profile when you edit in Multicast Filtering Profile.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

10-2.2 VLAN Configuration

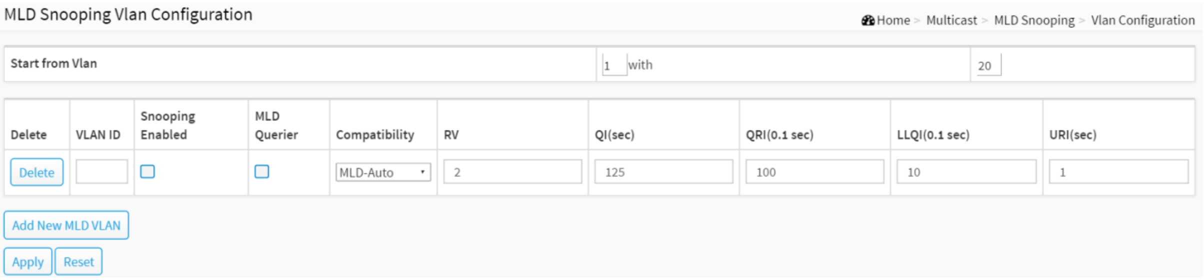
When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts

The will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

Web Interface

To configure the MLD Snooping VLAN Configuration in the web interface:

1. Click Multicast, MLD Snooping and VLAN Configuration.
2. Click Add New MLD VLAN.
3. Specify the VLAN ID with entries per page.



MLD Snooping Vlan Configuration

Start from Vlan	1 with	20

Delete	VLAN ID	Snooping Enabled	MLD Querier	Compatibility	RV	QI(sec)	QRI(0.1 sec)	LLQI(0.1 sec)	URI(sec)
Delete		□	□	MLD-Auto	2	125	100	10	1

Figure 10-2.2: The MLD Snooping VLAN Configuration

Parameter description:

- **Delete :**

  Check to delete the entry. The designated entry will be deleted during the next save.

- **VLAN ID :**

  It displays the VLAN ID of the entry.

- **Snooping Enabled :**

  Enable the per-VLAN IGMP Snooping. Only up to 32 VLANs can be selected. .

- **MLD Querier:**

  Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

- **Compatibility :**

  Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2 , default compatibility value is IGMP-Auto.

- **RV :**

  Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255; default robustness variable value is 2.

- **QI(sec) :**

  Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds; default query interval is 125 seconds.

- **QRI(0.1sec) :**

  Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds; default query response interval is 100 in tenths of seconds (10 seconds).

- **LLQI (LMQI for IGMP) :**

  Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds; default last member query interval is 10 in tenths of seconds (1 second).

- **URI(sec) :**

  Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second. .

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

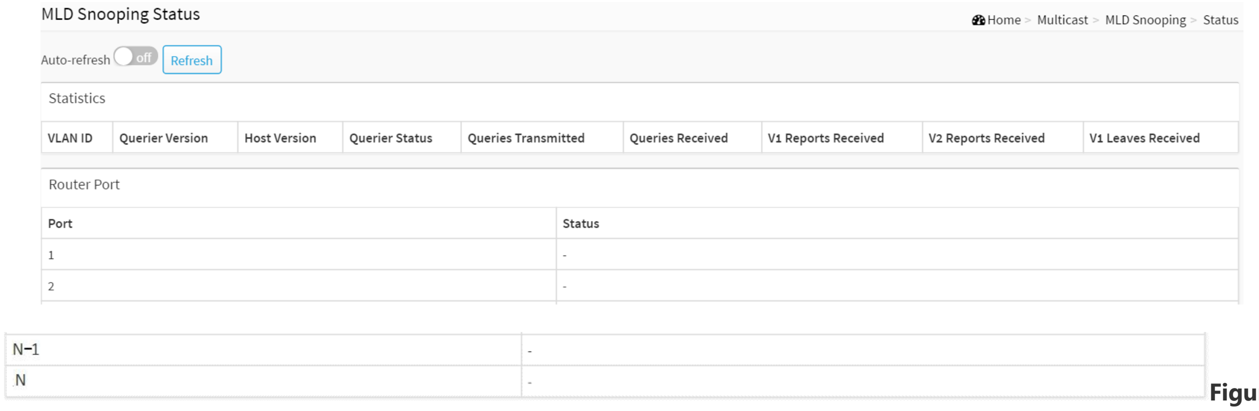
10-2.3 Status

The section describes when you complete the MLD Snooping and how to display the MLD Snooping Status and detail information. It will help you to find out the detail information of MLD Snooping status.

Web Interface

To display the MLD Snooping Status in the web interface:

1. Click Multicast, MLD Snooping and Status.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh"
3. Click "Refresh" to refresh an entry of the MLD Snooping Status Information.



MLD Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received

Router Port

Port	Status
1	-
2	-
N-1	-
N	-

Figure 10-2.3: The MLD Snooping Status

Parameter description:

- **VLAN ID :**

  The VLAN ID of the entry.

- **Querier Version :**

  Working Querier Version currently.

- **Host Version :**

  Working Host Version currently.

- **Querier Status :**

  Show the Querier status is "ACTIVE" or "IDLE".

  "DISABLE" denotes the specific interface is administratively disabled.

- **Queries Transmitted :**

  The number of Transmitted Queries.

- **Queries Received :**

  The number of Received Queries.

- **V1 Reports Received :**

  The number of Received V1 Reports.

- **V2 Reports Received :**

  The number of Received V2 Reports.

- **V1 Leaves Received :**

  The number of Received V1 Leaves.

- **Router Port**

  Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier.
  Static denotes the specific port is configured to be a router port.
  Dynamic denotes the specific port is learnt to be a router port.
  Both denote the specific port is configured or learnt to be a router port.

- **Port**

  Switch port number.

- **Status**

  Indicate whether specific port is a router port or not.

Buttons

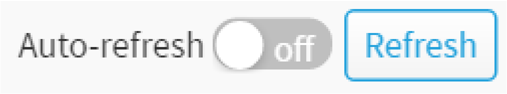


Figure 10-2.3: The MLD Snooping Status buttons

- **Auto-refresh :**

Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

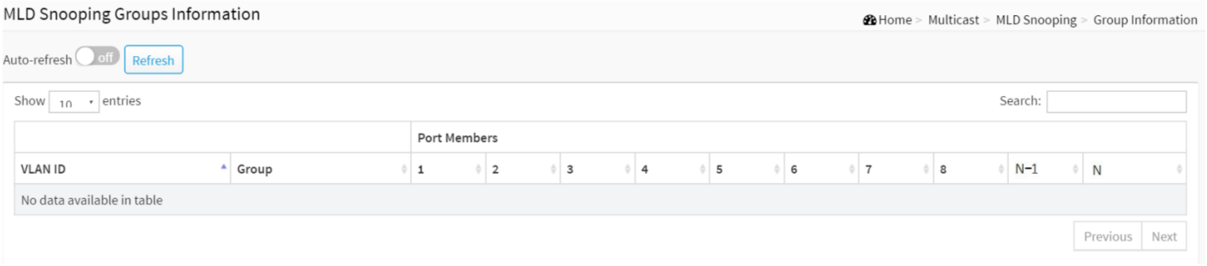
10-2.4 Groups Information

The section describes user could get the MLD Snooping Groups Information. The "Search" input fields allow the user to select the starting point in the MLD Group Table

Web Interface

To display the MLD Snooping Group information in the web interface:

1. Click Multicast, MLD Snooping and Group Information.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”
3. Click “Refresh” to refresh an entry of the MLD Snooping Group Information.



MLD Snooping Groups Information

		Port Members									
VLAN ID	Group	1	2	3	4	5	6	7	8	N-1	N
No data available in table											

Figure 10-2.4: The MLD Snooping Groups Information

Parameter description:

Navigating the MLD Group Table

Each page shows up to many entries from the MLD Group table, default being 10, selected through the "entries per page" input field. When first visited, the web page will show the first 10 entries from the beginning of the MLD Group Table.

The "Search " input fields allow the user to select the starting point in the MLD Group Table. It will update the displayed table starting from that or the closest next MLD Group Table match. This will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

- **VLAN ID :**

VLAN ID of the group.

- **Groups :**

  Group address of the group displayed.

- **Port Members :**

  Ports under this group.

- **Show entries :**

  You can choose how many items you want to show up.

Buttons

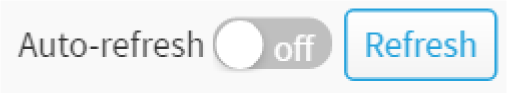


Figure 10-2.4: The MLD Snooping Groups Information buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

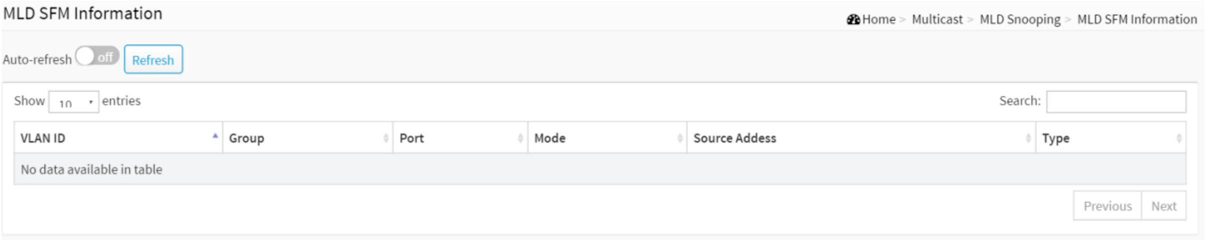
10-2.5 MLD SFM Information

Entries in the MLD SFM Information Table are shown on this page. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Web Interface

To display the MLD SFM Information in the web interface:

1. Click Multicast, MLD Snooping and MLD SFM Information.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. Click “Refresh” to refresh an entry of the MLD SFM Information.



MLD SFM Information

VLAN ID	Group	Port	Mode	Source Addess	Type
No data available in table					

Figure 10-2.5: The MLD SFM Information

Parameter description:

Navigating the MLD SFM Information Table

Each page shows up to many entries from the MLD SFM Information table, default being 10, selected through the "entries per page" input field. When first visited, the web page will show the first 10 entries from the beginning of the MLD SFM Information Table.

The "Search " input fields allow the user to select the starting point in the MLD SFM Information Table. It will update the displayed table starting from that or the closest next MLD SFM Information Table match.

This will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

- **VLAN ID :**

  VLAN ID of the group.

- **Group :**

  IP Multicast Group address.

- **Port :**

  Switch port number.

- **Mode :**

  Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

- **Source Address :**

  IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

- **Type :**

  Indicates the Type. It can be either Allow or Deny.

- **Show entries :**

  You can choose how many items you want to show off.

Buttons

Figure 10-2.5: The MLD SFM Information buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

10-3 Multicast Filtering Profile

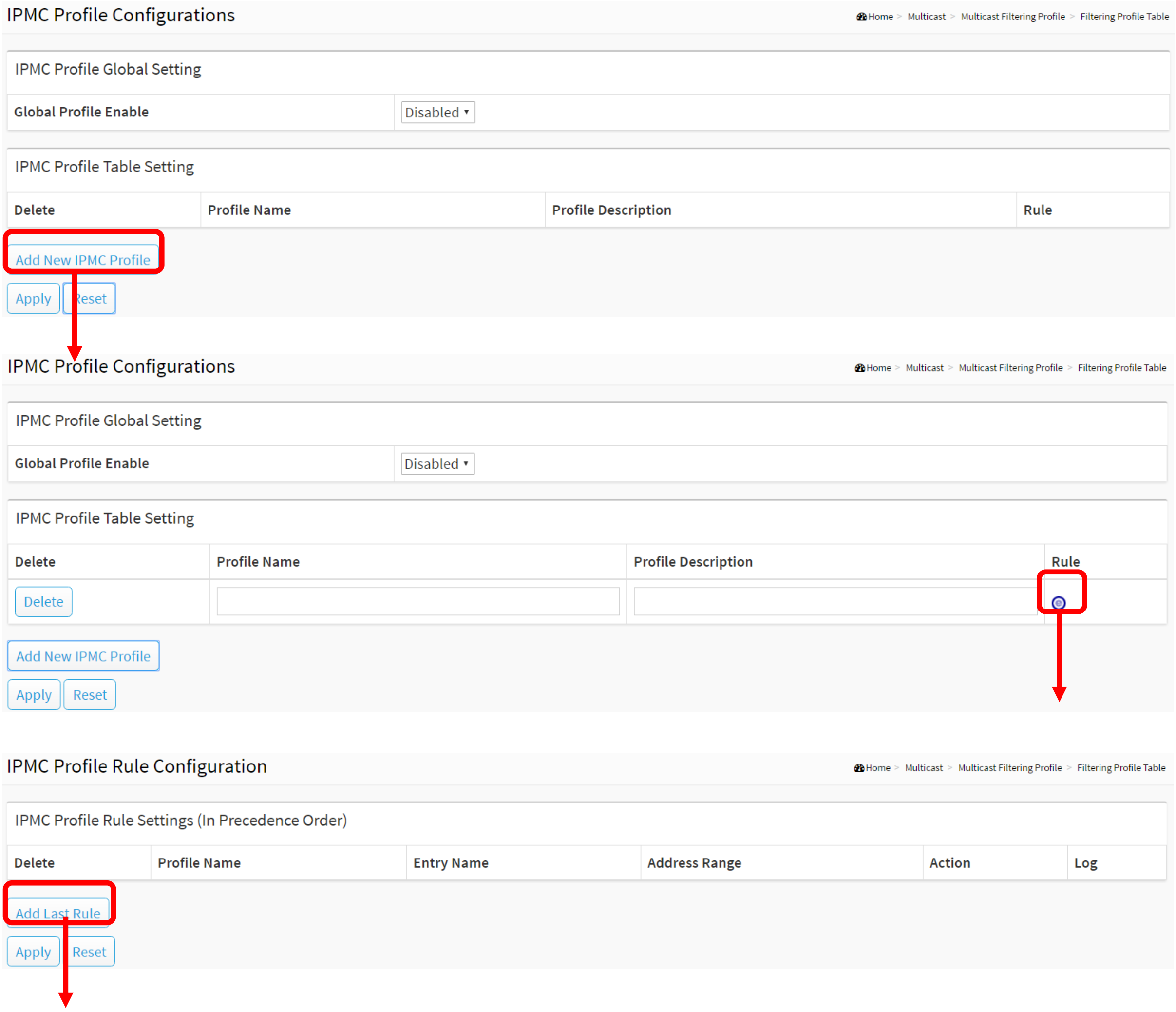
This page provides Multicast Filtering Profile related configurations.

10-3.1 Filtering Profile Table

The IPMC profile is used to deploy the access control on IP multicast streams. It is allowed to create at maximum 64 Profiles with at maximum 128 corresponding rules for each.

Web Interface

To configure the IPMC Profile Configuration in the web interface:



IPMC Profile Configurations

Home > Multicast > Multicast Filtering Profile > Filtering Profile Table

IPMC Profile Global Setting

Global Profile Enable	Disabled ▾

IPMC Profile Table Setting

Delete	Profile Name	Profile Description	Rule

Add New IPMC Profile

Apply Reset

IPMC Profile Configurations

Home > Multicast > Multicast Filtering Profile > Filtering Profile Table

IPMC Profile Global Setting

Global Profile Enable	Disabled ▾

IPMC Profile Table Setting

Delete	Profile Name	Profile Description	Rule
Delete			◎

Add New IPMC Profile

Apply Reset

IPMC Profile Rule Configuration

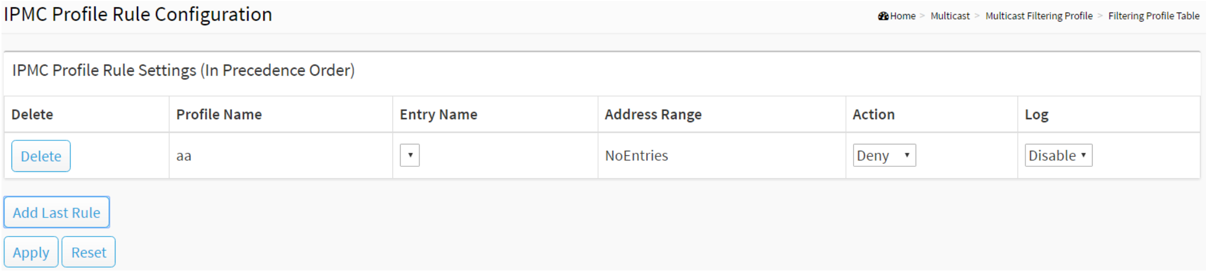
Home > Multicast > Multicast Filtering Profile > Filtering Profile Table

IPMC Profile Rule Settings (In Precedence Order)

Delete	Profile Name	Entry Name	Address Range	Action	Log

Add Last Rule

Apply Reset



IPMC Profile Rule Configuration

Home > Multicast > Multicast Filtering Profile > Filtering Profile Table

IPMC Profile Rule Settings (In Precedence Order)

Delete	Profile Name	Entry Name	Address Range	Action	Log
Delete	aa	▾	NoEntries	Deny ▾	Disable ▾

Figure 10-3.1: The IPMC Profile Configuration

Parameter description:

- **Global Profile Mode :**

  Enable/Disable the Global IPMC Profile.
  System starts to do filtering based on profile settings only when the global profile mode is enabled.

- **Profile Name :**

  The name used for indexing the profile table.
  Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters.

- **Profile Description :**

  Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile.
  No blank or space characters are permitted as part of description. Use "_" or "-" to seperate the description sentence.

- **Rule :**

  When the profile is created, click the edit button to enter the rule setting page of the designated profile. Summary about the designated profile will be shown by clicking the view button. You can manage or inspect the rules of the designated profile by using the following buttons:
  👁: List the rules associated with the designated profile.
  ⓔ: Adjust the rules associated with the designated profile.

- **Profile Name :**

  The name of the designated profile to be associated. This field is not editable.

- **Entry Name :**

  The name used in specifying the address range used for this rule.
  Only the existing profile address entries will be chosen in the selected box. This field is not allowed to be selected as none ("-") while the Rule Settings Table is committed.

- **Address Range :**

  The corresponding address range of the selected profile entry. This field is not editable and will be adjusted automatically according to the selected profile entry.

- **Action :**

  Indicates the learning action upon receiving the Join/Report frame that has the group address matches the address range of the rule.

  Permit: Group address matches the range specified in the rule will be learned.
  Deny: Group address matches the range specified in the rule will be dropped.

- **Log :**

  Indicates the logging preference upon receiving the Join/Report frame that has the group address matches the address range of the rule.

  Enable: Corresponding information of the group address, that matches the range specified in the rule, will be logged.
  Disable: Corresponding information of the group address, that matches the range specified in the rule, will not be logged.

Buttons

- **Add New IPMC Profile** :

  Click to add new IPMC profile. Specify the name and configure the new entry. Click "Save".

- **Delete :**

  Check to delete the entry.
  The designated entry will be deleted during the next save.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

- **Add Last Rule :**

  Click to add a new rule in the end of the specific profile's rule list. Specify the address entry and configure the new entry. Click "Apply"

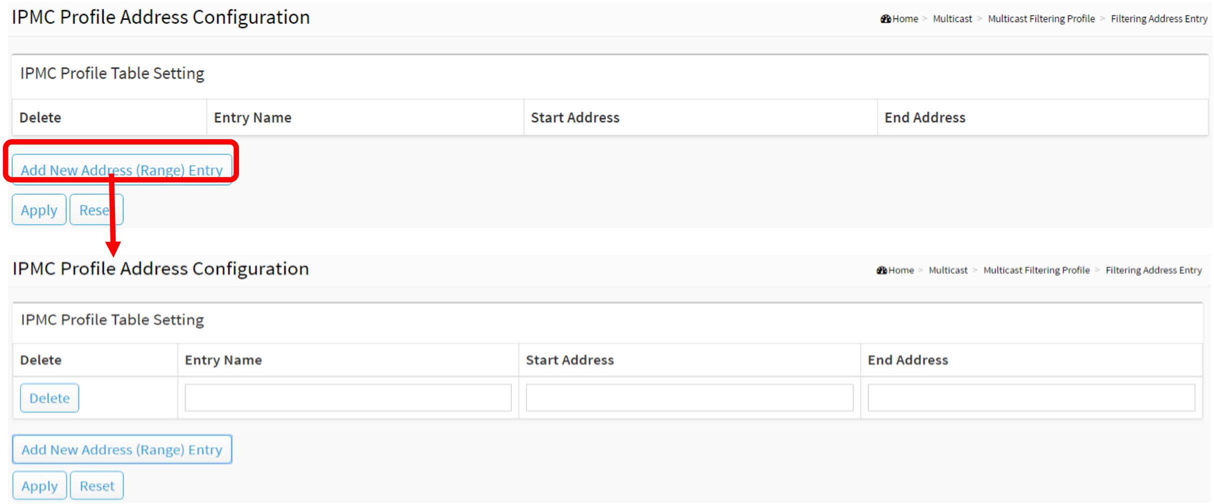
10-3.2 Filtering Address Entry

This page provides address range settings used in IPMC profile.

The address entry is used to specify the address range that will be associated with IPMC Profile. It is allowed to create at maximum 128 address entries in the system.

Web Interface

To configure the IPMC Profile Address Configuration in the web interface:



IPMC Profile Address Configuration

Home > Multicast > Multicast Filtering Profile > Filtering Address Entry

IPMC Profile Table Setting

Delete	Entry Name	Start Address	End Address

Add New Address (Range) Entry

Apply Reset

IPMC Profile Address Configuration

Home > Multicast > Multicast Filtering Profile > Filtering Address Entry

IPMC Profile Table Setting

Delete	Entry Name	Start Address	End Address
Delete			

Add New Address (Range) Entry

Apply Reset

Figure 10-3.2: The IPMC Profile Address Configuration

Parameter description:

- **Entry Name :**

  The name used for indexing the address entry table.
  Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters.

- **Start Address :**

  The starting IPv4/IPv6 Multicast Group Address that will be used as an address range.

- **End Address :**

  The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.

Buttons

- **Add New Address (Range) Entry** :

  Click to add new address range. Specify the name and configure the addresses. Click "Apply"

- **Delete :**

  Check to delete the entry.
  The designated entry will be deleted during the next save.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

Chapter 11 MVR

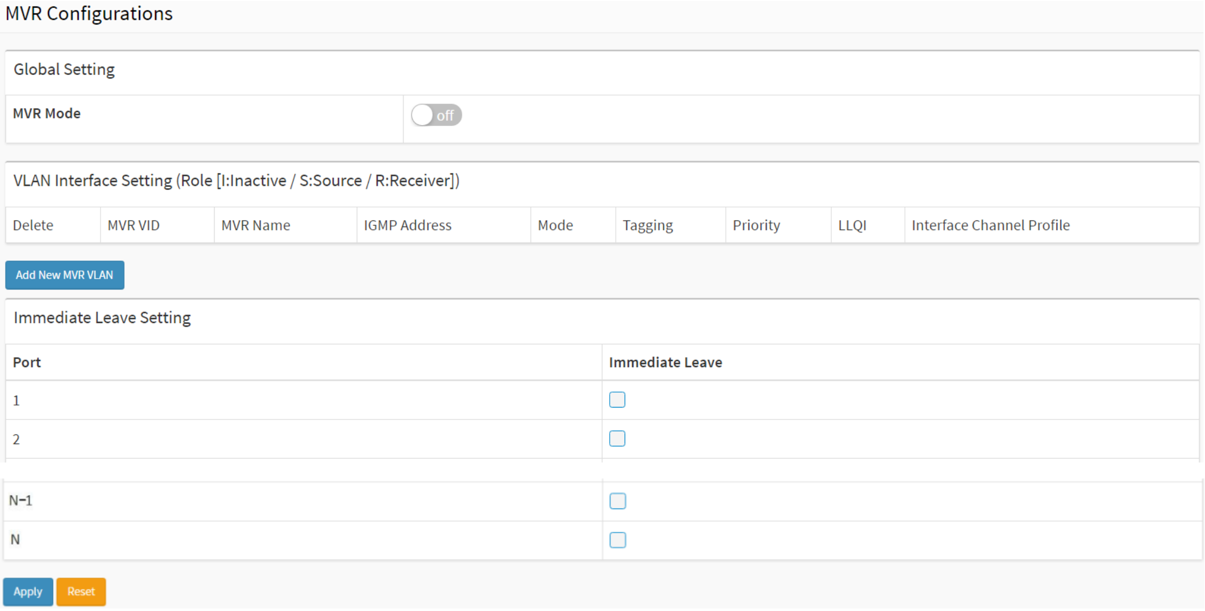
The MVR feature enables multicast traffic forwarding on the Multicast VLAN. In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP join message to Switch A to join the appropriate multicast. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

11-3.1 Basic Configuration

Web Interface

To configure the MVR Configuration in the web interface:

1. Click MVR and Basic Configuration.
2. Scroll the MVR mode to enable or disable and Scroll to set all parameters.
3. Click “Add New MVR VLAN”.
4. Specify MVR VID, MVR Name, IGMP Address, Mode, Tagging, Priority, LLQI, Interface, Channel Profile.
5. Select which port to Click Immediate Leave.
6. Click the apply to save the setting
7. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values



MVR Configurations

Global Setting

MVR Mode	off

VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver])

Delete	MVR VID	MVR Name	IGMP Address	Mode	Tagging	Priority	LLQI	Interface Channel Profile

Immediate Leave Setting

Port	Immediate Leave
1	□
2	□
N-1	□
N	□

Figure 11-3.1: The MVR Configuration

Parameter description:

- **MVR Mode :**

  Enable/Disable the Global MVR.

  The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping. It is suggested to enable Unregistered Flooding control when the MVR group table is full.

- **MVR VID :**

  Specify the Multicast VLAN ID.

  Be Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.

- **MVR Name :**

  MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 32. MVR VLAN Name can only contain alphabets or numbers. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.

- **IGMP Address :**

  Define the IPv4 address as source address used in IP header for IGMP control frames.

  The default IGMP address is not set (0.0.0.0).

  When the IGMP address is not set, system uses IPv4 management address of the IP interface associated with this VLAN.

When the IPv4 management address is not set, system uses the first available IPv4 management address.

Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

- **Mode :**

  Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode.

- **Tagging :**

  Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is tagged.

- **Priority :**

  Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.

- **LLQI :**

  Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a seconds. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second.

- **Interface Channel Profile :**

  When the MVR VLAN is created, select the profile to expand the corresponding multicast channel settings for the specific MVR VLAN. The file established on Filtering Profile Table.

- **Port :**

  The logical port for the settings.

- **Port Role :**

  Configure an MVR port of the designated MVR VLAN as one of the following roles.

  Inactive: The designated port does not participate MVR operations.

  Source: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports.

  Receiver: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages.

Be Caution: MVR source ports are not recommended to be overlapped with management VLAN ports. Select the port role by clicking the Role symbol to switch the setting. I indicates Inactive; S indicates Source; R indicates Receiver. The default Role is Inactive.

- **Immediate Leave :**

  Enable the fast leave on the port.

Buttons

- **Add New MVR VLAN** :

  Click to add new mvr vlan. Specify MVR VID, MVR Name, IGMP Address, Mode, Tagging, Priority, LLQI, Interface Channel Profile. Click "Apply"

- **Delete :**

  Check to delete the entry. The designated entry will be deleted during the next save.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

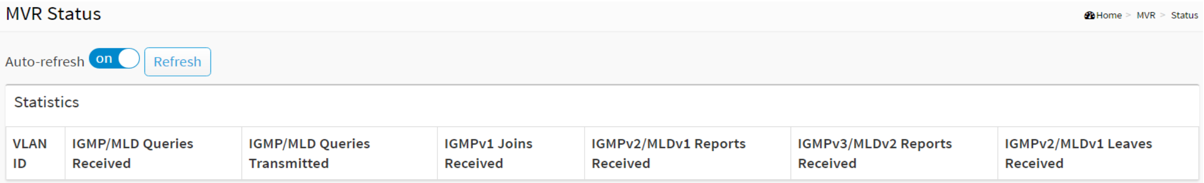
11-3.2 Status

The section describes the switch will display the MVR detail Statistics after you had configured MVR on the switch. It provides the detail MVR Statistics Information

Web Interface

To display the MVR Statistics Information in the web interface:

1. Click MVR and Status.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. To click the "Refresh" to refresh an entry of the MVR Statistics Information.



MVR Status

Home > MVR > Status

Auto-refresh on Refresh

Statistics

VLAN ID	IGMP/MLD Queries Received	IGMP/MLD Queries Transmitted	IGMPv1 Joins Received	IGMPv2/MLDv1 Reports Received	IGMPv3/MLDv2 Reports Received	IGMPv2/MLDv1 Leaves Received

Figure 11-3.2: The MVR Statistics Information

Parameter description:

- **VLAN ID :**

  The Multicast VLAN ID.

- **IGMP/MLD Queries Received :**

  The number of Received Queries for IGMP and MLD, respectively.

- **IGMP/MLD Queries Transmitted :**

  The number of Transmitted Queries for IGMP and MLD, respectively.

- **IGMPv1 Joins Received :**

  The number of Received IGMPv1 Join's.

- **IGMPv2/MLDv1 Report's Received :**

  The number of Received IGMPv2 Join's and MLDv1 Report's, respectively.

- **IGMPv3/MLDv2 Report's Received :**

  The number of Received IGMPv3 Join's and MLDv2 Report's, respectively.

- **IGMPv2/MLDv1 Leave's Received :**

  The number of Received IGMPv2 Leave's and MLDv1 Done's, respectively.

Buttons

Figure 11-3.2: The MVR Statistics Information buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

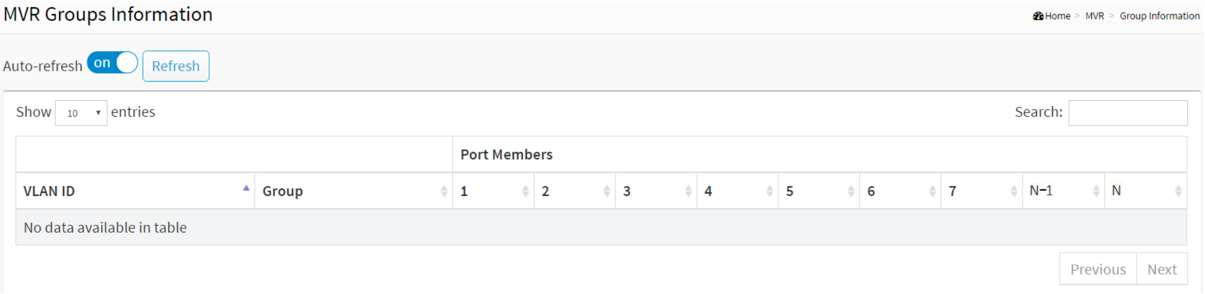
11-3.3 MVR Groups Information

The section describes user could display the MVR Groups detail information on the switch. Entries in the MVR Group Table are shown on this page. The MVR Group Table is sorted first by VLAN ID, and then by group

Web Interface

To display the MVR Groups Information in the web interface:

1. Click MVR and Groups Information.
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. To click the “Refresh” to refresh an entry of the MVR Groups Information.
4. Click Previous/next to change page.



		Port Members								
VLAN ID	Group	1	2	3	4	5	6	7	N-1	N
No data available in table										

Figure 11-3.3: The MVR Groups Information

Parameter description:

Navigating the MVR Channels (Groups) Information Table

Each page shows up to many entries from the MVR Group table, default being 10, selected through the "entries per page" input field. When first visited, the web page will show the first 10 entries from the beginning of the MVR Channels (Groups) Information Table.

The "Search" input fields allow the user to select the starting point in the MVR Channels (Groups) Information Table. It will update the displayed table starting from that or the closest next MVR Channels (Groups) Information Table match.

The will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over

MVR Channels (Groups) Information Table Columns

- **Show entries :**

  You can choose how many items you want to show up.

- **Search :**

  You can search for the information that you want to see.

- **VLAN ID :**

  VLAN ID of the group.

- **Groups :**

  Group ID of the group displayed.

- **Port Members :**

  Ports under this group.

Buttons

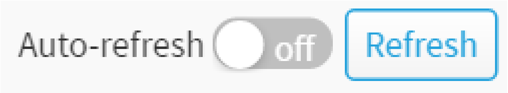


Figure 11-3.3: The MVR Groups Information buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

- **Next :**

  Updates the system log entries, turn to the next page.

- **Previous :**

  Updates the system log entries, turn to the previous page.

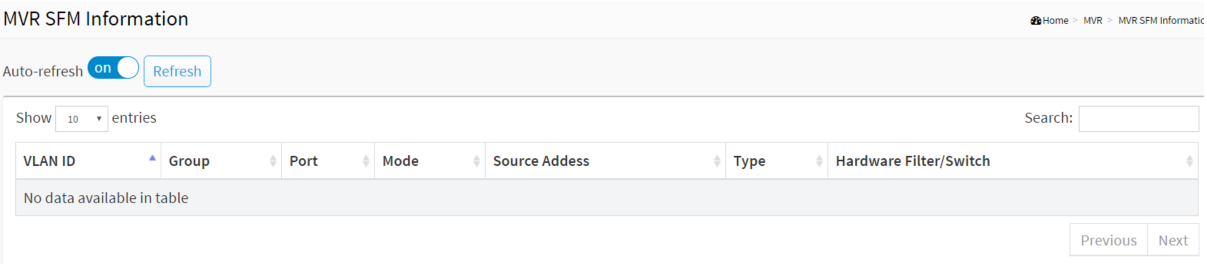
11-3.4 MVR SFM Information

The MVR SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Web Interface

To display the MVR SFM Information in the web interface:

1. Click MVR and MVR SFM Information.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. To click the "Refresh" to refresh an entry of the MVR Groups Information.
4. Click Previous/next to change page.



MVR SFM Information

VLAN ID	Group	Port	Mode	Source Addess	Type	Hardware Filter/Switch
No data available in table						

Figure 11-3.4: The MVR SFM Information

Parameter description:

Navigating the MVR SFM Information Table

Each page shows up to many entries from the MVR SFM Information Table, default being 10, selected through the "entries per page" input field. When first visited, the web page will show the first 10 entries from the beginning of the MVR SFM Information Table.

The "Search " input fields allow the user to select the starting point in the MVR SFM Information Table. It will update the displayed table starting from that or the closest next MVR SFM Information Table match.

The will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

MVR SFM Information Table Columns

- **Show entries :**

  You can choose how many items you want to show up.

- **Search :**

  You can search for the information that you want to see.

- **VLAN ID :**

  VLAN ID of the group.

- **Group :**

  IP Multicast Group address.

- **Port :**

  Switch port number.

- **Mode :**

  Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

- **Source Address :**

  IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. When there is not any source filtering address, the text "None" is shown in the Source Address field.

- **Type :**

  Indicates the Type. It can be either Allow or Deny.

- **Hardware Filter/Switch :**

  Indicates whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by chip or not.

Buttons

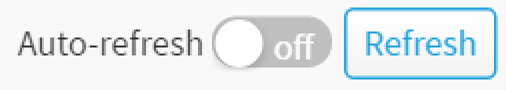


Figure 11-3.4: The MVR SFM Information buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

- **Next :**

  Updates the system log entries, turn to the next page.

- **Previous :**

  Updates the system log entries, turn to the previous page.

Chapter 12 DHCP

The section describes to configure and display the DHCP Snooping parameters of the switch. The DHCP Snooping can prevent attackers from adding their own DHCP servers to the network.

12-1 Snooping

12-1.1 Configuration

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.

The section describes to configure the DHCP Snooping parameters of the switch. The DHCP Snooping can prevent attackers from adding their own DHCP servers to the network.

Web Interface

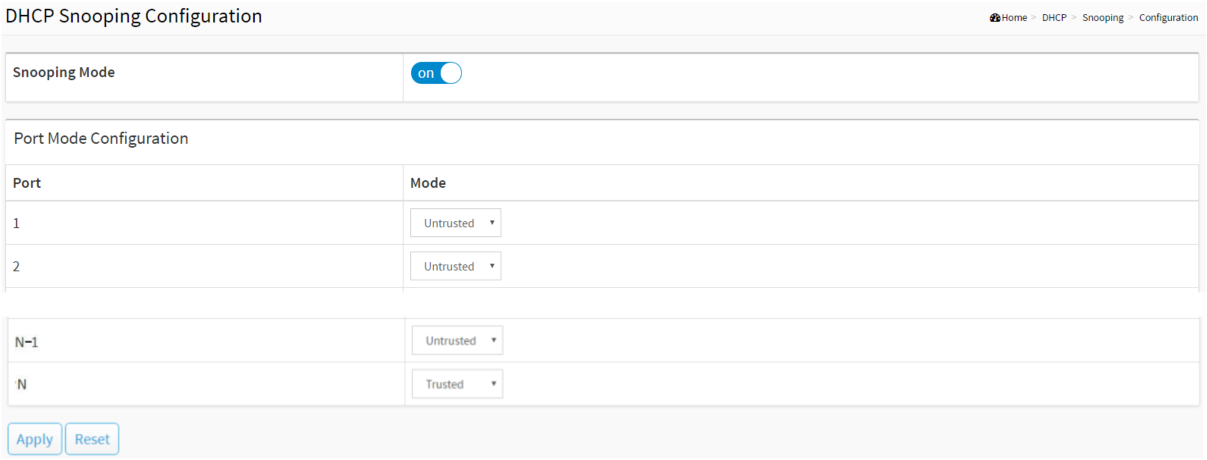
To configure DHCP snooping in the web interface:

1. Click DHCP, Snooping and Configuration.

2. Select “on” in the Mode of DHCP Snooping Configuration.

3. Select “Trusted” of the specific port in the Mode of Port Mode Configuration.

4. Click Apply.



DHCP Snooping Configuration

Home > DHCP > Snooping > Configuration

Snooping Mode	on

Port Mode Configuration

Port	Mode
1	Untrusted
2	Untrusted
N-1	Untrusted
N	Trusted

Figure 12-1.1: The DHCP Snooping Configuration

Parameter description:

- **Snooping Mode :**

  Indicates the DHCP snooping mode operation. Possible modes are:

  on: Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.

  off: Disable DHCP snooping mode operation.

- **Port Mode Configuration**

  Indicates the DHCP snooping port mode. Possible port modes are:

  Trusted: Configures the port as trusted source of the DHCP messages. Trusted port can forward DHCP packets normally.

  Untrusted: Configures the port as untrusted source of the DHCP messages. Untrusted port will discard the packets when it receive DHCP packets.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

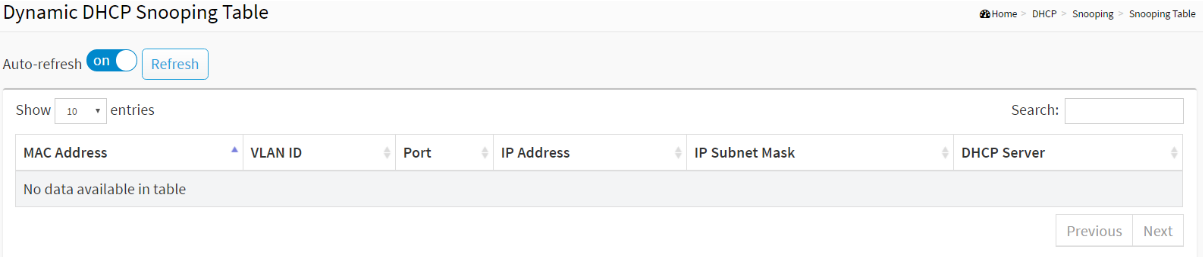
12-1.2 Snooping Table

This page display the dynamic IP assigned information after DHCP Snooping mode is enabled. All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page.

Web Interface

To monitor a DHCP in the web interface:

1. Click DHCP, Snooping and Snooping table.



Dynamic DHCP Snooping Table

MAC Address	VLAN ID	Port	IP Address	IP Subnet Mask	DHCP Server
No data available in table					

Figure 12-1.2: The DHCP snooping table

Parameter description:

- **Show entries :**

  You can choose how many items you want to show up.

- **Search :**

  You can search for the information that you want to see.

- **MAC Address :**

  User MAC address of the entry.

- **VLAN ID :**

  VLAN-ID in which the DHCP traffic is permitted.

- **Port:**

  Switch Port Number for which the entries are displayed.

- **IP Address :**

  User IP address of the entry.

- **IP Subnet Mask :**

  User IP subnet mask of the entry.

- **DHCP Server :**

  DHCP Server address of the entry.

Buttons

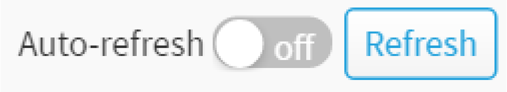


Figure 12-1.2: The DHCP snooping table buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

- **Next :**

  Updates the system log entries, turn to the next page.

- **Previous :**

  Updates the system log entries, turn to the previous page.

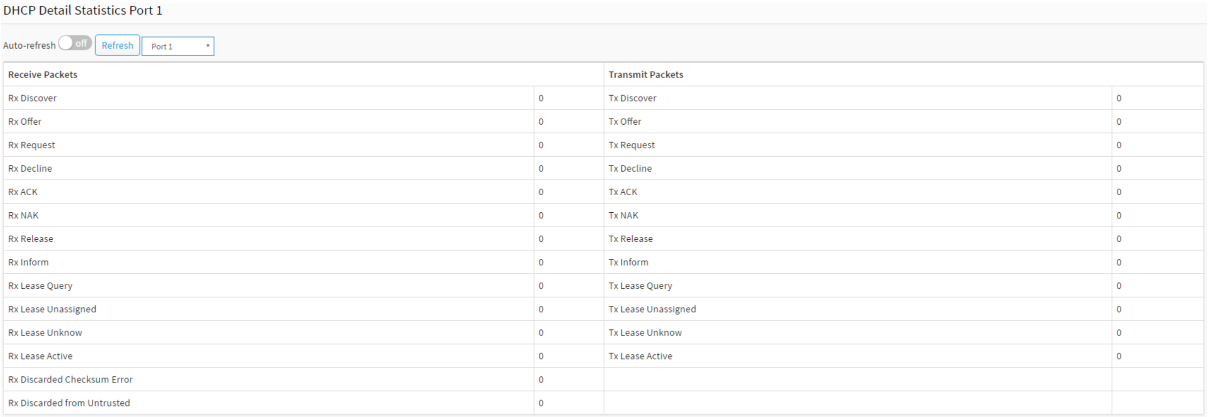
12-1.3 Detailed Statistics

This page provides statistics for DHCP snooping. Notice that the normal forward per-port TX statistics isn't increased if the incoming DHCP packet is done by L3 forwarding mechanism. And clear the statistics on specific port may not take effect on global statistics since it gathers the different layer overview.

Web Interface

To display an DHCP Relay statistics in the web interface:

1. Click DHCP, Snooping and Detailed Statistics.
2. Select port that you want to display the DHCP Detailed Statistics.
3. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
4. To click the "Refresh" to refresh an entry of the DHCP Detailed Statistics.



DHCP Detail Statistics Port 1

Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	0
Rx Offer	0	Tx Offer	0
Rx Request	0	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknow	0	Tx Lease Unknow	0
Rx Lease Active	0	Tx Lease Active	0
Rx Discarded Checksum Error	0		
Rx Discarded from Untrusted	0		

Figure 12-1.3: The DHCP Detailed Statistics

Parameter description:

Server Statistics

- **Rx and Tx Discover :**

  The number of discover (option 53 with value 1) packets received and transmitted.

- **Rx and Tx Offer :**

The number of offer (option 53 with value 2) packets received and transmitted.

- **Rx and Tx Request :**

  The number of request (option 53 with value 3) packets received and transmitted.

- **Rx and Tx Decline :**

  The number of decline (option 53 with value 4) packets received and transmitted.

- **Rx and Tx ACK :**

  The number of ACK (option 53 with value 5) packets received and transmitted.

- **Rx and Tx NAK :**

  The number of NAK (option 53 with value 6) packets received and transmitted.

- **Rx and Tx Release :**

  The number of release (option 53 with value 7) packets received and transmitted.

- **Rx and Tx Inform :**

  The number of inform (option 53 with value 8) packets received and transmitted.

- **Rx and Tx Lease Query :**

  The number of lease query (option 53 with value 10) packets received and transmitted.

- **Rx and Tx Lease Unassigned :**

  The number of lease unassigned (option 53 with value 11) packets received and transmitted.

- **Rx and Tx Lease Unknown :**

  The number of lease unknown (option 53 with value 12) packets received and transmitted. Rx and Tx Lease Active

- **Rx and Tx Lease Active :**

  The number of lease active (option 53 with value 13) packets received and transmitted.

- **Rx Discarded checksum error :**

  The number of discard packet that IP/UDP checksum is error.

- **Rx Discarded from Untrusted :**

  The number of discarded packet that are coming from untrusted port.

Buttons

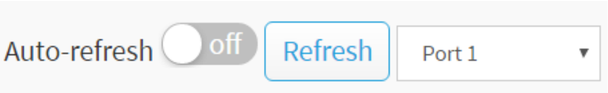


Figure 12-1.3: The DHCP Detailed Statistics buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

- **Port 1 :**

  Select port that you want to display the DHCP Detailed Statistics.

12-2 Relay

12-2.1 Configuration

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

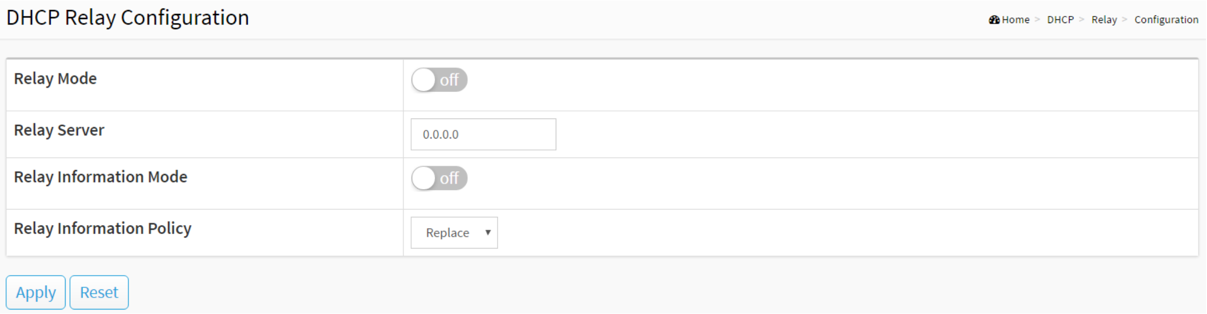
Web Interface

To configure DHCP Relay in the web interface:

1. Click DHCP, Relay and Configuration.

2. Specify the Relay Mode, Relay server, Relay Information Mode, Relay Information Policy.

3. Click Apply.



DHCP Relay Configuration

Relay Mode	off
Relay Server	0.0.0.0
Relay Information Mode	off
Relay Information Policy	Replace

Figure 12-2.1: The DHCP Relay Configuration

Parameter description:

- **Relay Mode :**

  Indicates the DHCP relay mode operation.

  Possible modes are:

  on: Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.

off: Disable DHCP relay mode operation.

- **Relay Server :**

  Indicates the DHCP relay server IP address.

- **Relay Information Mode :**

  Indicates the DHCP relay information mode option operation. The option 82 circuit ID format as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID(in standalone device it always equal 0, in stackable device it means switch ID), and the last two characters are the port number. For example, "00030108" means the DHCP message receive form VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal the switch MAC address.

  Possible modes are:

  Enabled: Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.

  Disabled: Disable DHCP relay information mode operation.

- **Relay Information Policy :**

  Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' policy is invalid when relay information mode is disabled.
  Possible policies are:
  Replace: Replace the original relay information when a DHCP message that already contains it is received.
  Keep: Keep the original relay information when a DHCP message that already contains it is received.
  Drop: Drop the package when a DHCP message that already contains relay information is received.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

12-2.2 Statistics

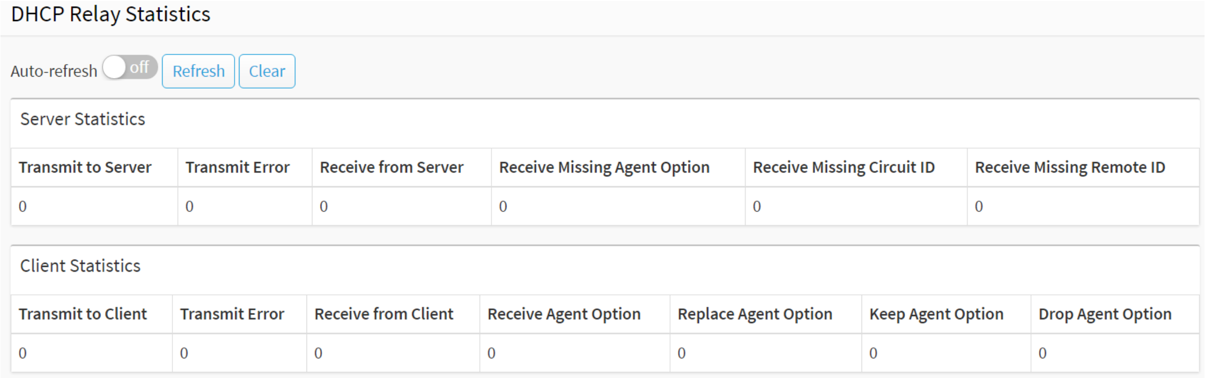
This page provides statistics for DHCP relay.

Web Interface

To monitor a DHCP Relay statistics in the web interface:

1. Click DHCP, Relay and Relay Statistics.

2. To display DHCP relay statistics.



DHCP Relay Statistics

Server Statistics

Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID
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

Figure 12-2.2: The DHCP relay statistics

Parameter description:

Server Statistics

- **Transmit to Server :**

  The number of packets that are relayed from client to server.

- **Transmit Error :**

  The number of packets that resulted in errors while being sent to clients.

- **Receive from Server :**

  The number of packets received from server.

- **Receive Missing Agent Option:**

  The number of packets received without agent information options.

- **Receive Missing Circuit ID :**

The number of packets received with the Circuit ID option missing.

- **Receive Missing Remote ID :**

  The number of packets received with the Remote ID option missing.

Client Statistics

- **Transmit to Client :**

  The number of relayed packets from server to client.

- **Transmit Error :**

  The number of packets that resulted in error while being sent to servers.

- **Receive from Client :**

  The number of received packets from server.

- **Receive Agent Option :**

  The number of received packets with relay agent information option.

- **Replace Agent Option :**

  The number of packets which were replaced with relay agent information option.

- **Keep Agent Option :**

  The number of packets whose relay agent information was retained.

- **Drop Agent Option :**

  The number of packets that were dropped which were received with relay agent information.

Buttons

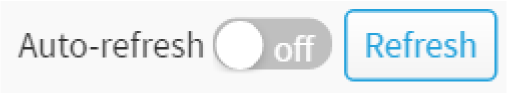


Figure 12-2.2: The DHCP relay statistics buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

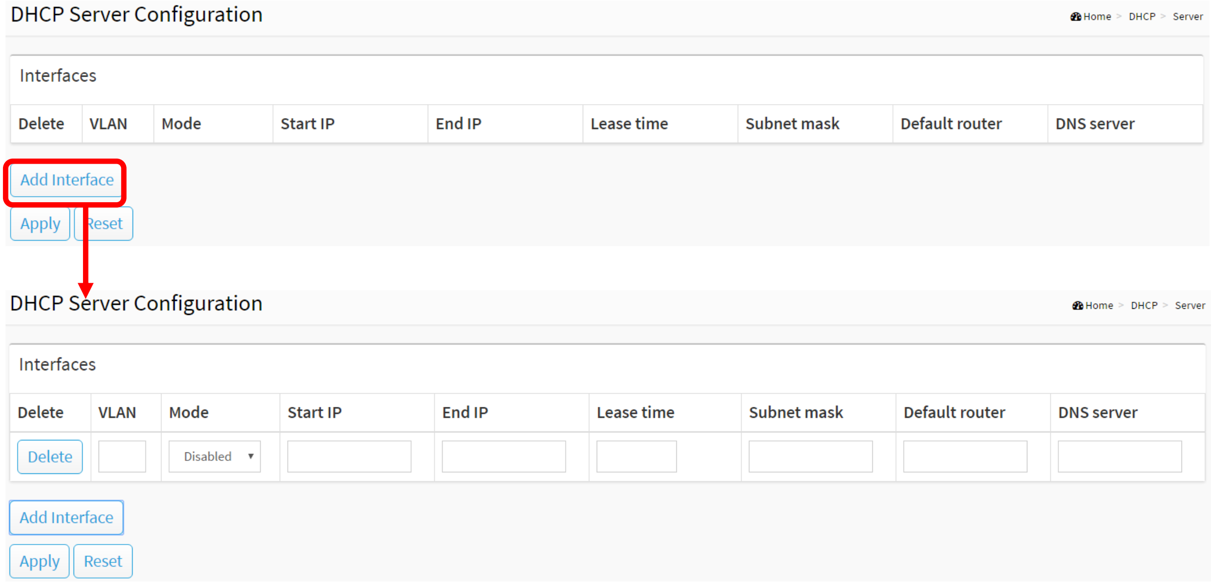
12-3 Server

This page configures mode to enable/disable DHCP server per system and per VLAN. And configures Start IP and End IP addresses. DHCP server will allocate these IP addresses to DHCP client. And deliver configuration parameters to DHCP client.

Web Interface

To configure DHCP server Configuration in the web interface:

1. Click DHCP and Server.
2. Click “Add Interface”.
3. Specify VLAN, Mode, Start IP, End IP, Lease time, Subnet mask, Default router, DNS server.
4. Click Apply.



DHCP Server Configuration

Home > DHCP > Server

Interfaces

Delete	VLAN	Mode	Start IP	End IP	Lease time	Subnet mask	Default router	DNS server

DHCP Server Configuration

Home > DHCP > Server

Interfaces

Delete	VLAN	Mode	Start IP	End IP	Lease time	Subnet mask	Default router	DNS server
Delete		Disabled						

Figure 12-3: The DHCP server configuration

Parameter description:

- **VLAN:**

  Configure the VLAN in which DHCP server is enabled or disabled. Allowed VLAN are in the range 1 through 4095

- **Mode :**

Indicate the operation mode per VLAN. Possible modes are:

Enable: Enable DHCP server per VLAN.

Disable: Disable DHCP server pre VLAN.

- **Start IP and End IP :**

  Define the IP range. The Start IP must be smaller than or equal to the End IP.

- **Lease Time :**

  Display lease time of the pool.

- **Subnet Mask :**

  Configure subnet mask of the DHCP address.

- **Default router :**

  Configure the destination IP network or host address of this route.

- **DNS Server :**

  Specify DNS server.

Buttons

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **Add Interface :**

  Click to add a new DHCP server.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

Chapter 13 Security

This section shows you to configure the Port Security settings of the Switch. You can use the Port Security feature to restrict input to an interface by limiting and identifying MAC addresses.

13-1 Management

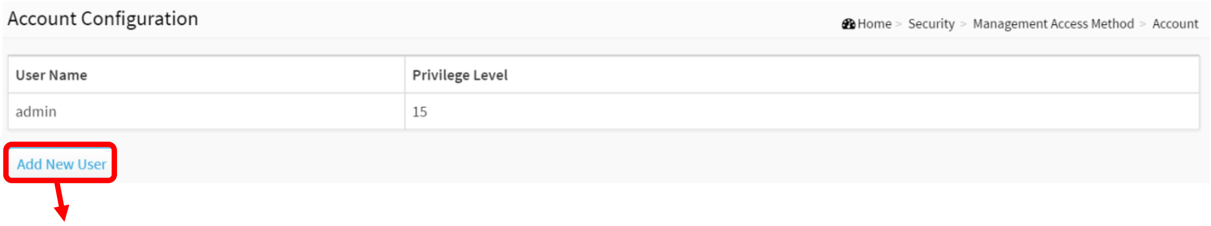
13-1.1 Account

This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser

Web Interface

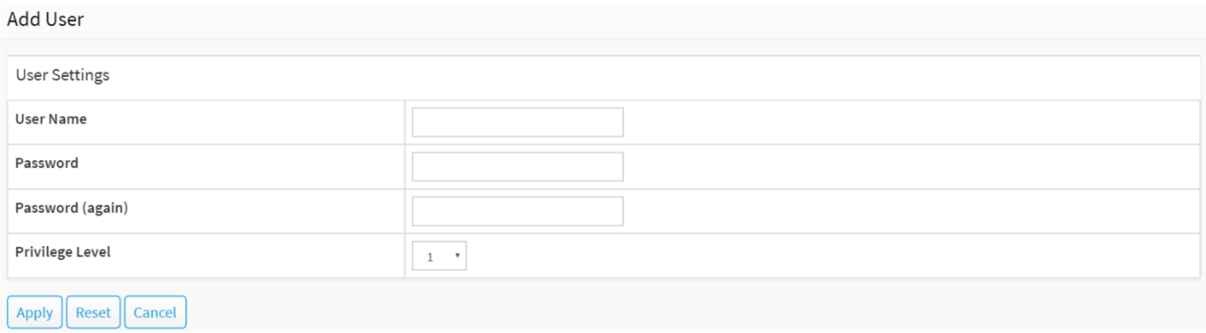
To configure User in the web interface:

1. Click Security, Management and Account.
2. Click Add new user
3. Specify the User Name parameter.
4. Click Apply.



Account Configuration

User Name	Privilege Level
admin	15



Add User

User Settings

User Name	
Password	
Password (again)	
Privilege Level	1

Figure 13-1.1: The Account configuration

Parameter description:

- **User Name :**

  The name identifying the user. The field can be input 31 characters. This is also a link to Add/Edit User.

- **Password :**

  To type the password. The field can be input 31 characters, and the allowed content is the ASCII characters from 32 to 126.

- **Password (again) :**

  To type the password again. You must type the same password again in the field.

- **Privilege Level :**

  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.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

- **Cancel :**

Click to undo any changes made locally and return to the Users.

- **Delete User :**

  Delete the current user. This button is not available for new configurations (Add new user)

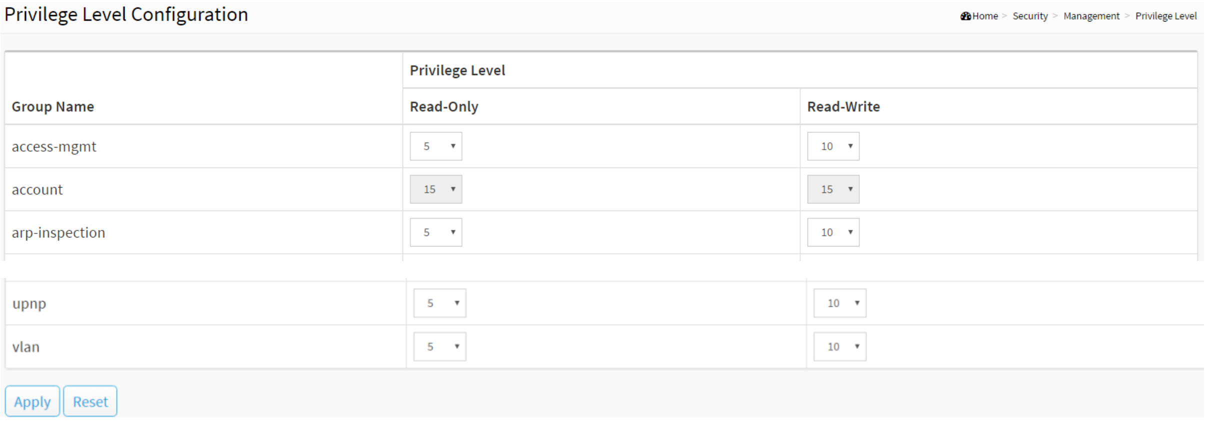
13-1.2 Privilege Levels

This page provides an overview of the privilege levels. The switch provides user set Account, Aggregation, Diagnostics, EEE, GARP, GVRP,IP, IPMC Snooping LACP LLDP LLDP MED MAC Table MRP MVR MVRP Maintenance Mirroring POE Ports Private VLANs QoS SMTP SNMP Security Spanning Tree System Trap Event VCL VLANs Voice VLAN Privilege Levels from 1 to 15 .

Web Interface

To configure Privilege Level in the web interface:

1. Click Security, Management and Privilege Level.
2. Specify the Privilege parameter.
3. Click Apply.



Privilege Level Configuration

Home > Security > Management > Privilege Level

Group Name	Privilege Level Read-Only	Read-Write
access-mgmt	5	10
account	15	15
arp-inspection	5	10
upnp	5	10
vlan	5	10

Figure13-1.2: The Privilege Level configuration

Parameter description:

- **Group Name :**

The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details:

System: Contact, Name, Location, Timezone, Daylight Saving Time, Log.

Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard.

IP: Everything except 'ping'.

Port: Everything except 'VeriPHY'.

Diagnostics: 'ping' and 'VeriPHY'.

Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.

- **Privilege Levels :**

  Every group has an authorization Privilege level for the following sub groups: configuration read-only, configuration/execute read-write. User Privilege should be same or greater than the authorization Privilege level to have the access to that group.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

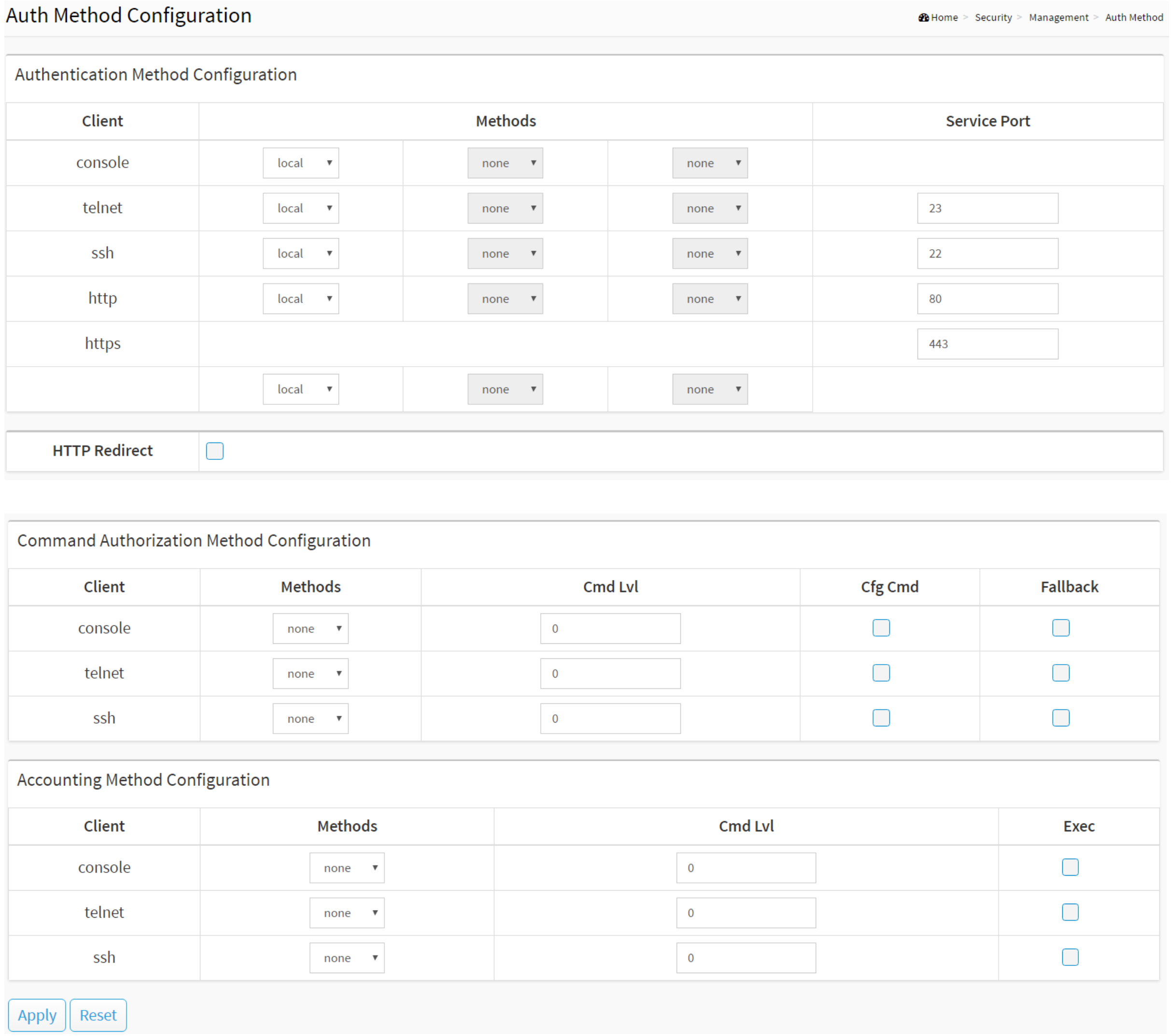
13-1.3 Auth Method

This page shows how to configure a user with auth method when he logs into the switch via one of the management client interfaces.

Web Interface

To configure an Auth Method Configuration in the web interface:

1. Click Security, Management and Auth Method.
2. Specify the Client (console, telent, ssh, web) which you want to monitor.
3. Specify the Methods (none, local, radius, tacacs), Service port, Cmd Lvl, Cfg Cmd, Fallback, Exec.
4. Click Apply.



Auth Method Configuration

Authentication Method Configuration

Client	Methods			Service Port
console	local	none	none	
telnet	local	none	none	23
ssh	local	none	none	22
http	local	none	none	80
https				443
	local	none	none	

HTTP Redirect	□

Command Authorization Method Configuration

Client	Methods	Cmd Lvl	Cfg Cmd	Fallback
console	none	0	□	□
telnet	none	0	□	□
ssh	none	0	□	□

Accounting Method Configuration

Client	Methods	Cmd Lvl	Exec
console	none	0	□
telnet	none	0	□
ssh	none	0	□

Figure 13-1.3: The Authentication Method Configuration

Parameter description:

Authentication Method Configuration

- **Client :**

  The management client for which the configuration below applies.

- **Method :**

  Authentication Method can be set to one of the following values:

  - none : authentication is disabled and login is not possible.
  - local : use the local user database on the switch for authentication.
  - radius : use a remote RADIUS server for authentication.
  - tacacs : use a remote TACACS server for authentication.

  Methods that involves remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.

- **Service Port :**

  The TCP port for each client service. The valid port number is 1 ~ 65534.

- **HTTP Redirect :**

  Enable http Automatic Redirect.

Command Authorization Method Configuration

- **Client :**

  The management client for which the configuration below applies.

- **Method :**

  Authorization Method can be set to one of the following values:

  - none : authorization is disabled and login is not possible.
  - tacacs+ : use a remote TACACS+ server for authorization.

- **Cmd Lvl :**

  Runs authorization for all commands at the specified privilege level. Specific command level that should be authorized. Valid entries are 0 through 15.

- **Cfg Cmd :**

  Enable or disable the configure command.

- **Fallback :**

  The local database can act as a fallback method for several functions. This behavior is designed to help you prevent accidental lockout from the security appliance.

  Accounting Method Configuration

- **Client :**

  The management client for which the configuration below applies.

- **Method :**

  Accounting Method can be set to one of the following values:

  - none : accounting is disabled and login is not possible.
  - tacacs+ : use a remote TACACS+ server for accounting.

- **Cmd Lvl :**

  Runs accounting for all commands at the specified privilege level. Specific command level that should be authorized. Valid entries are
  0 through 15.

- **Exec :**

  Runs accounting to determine if the user is allowed to run an EXEC shell. This facility might return user profile information such as autocommand information.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

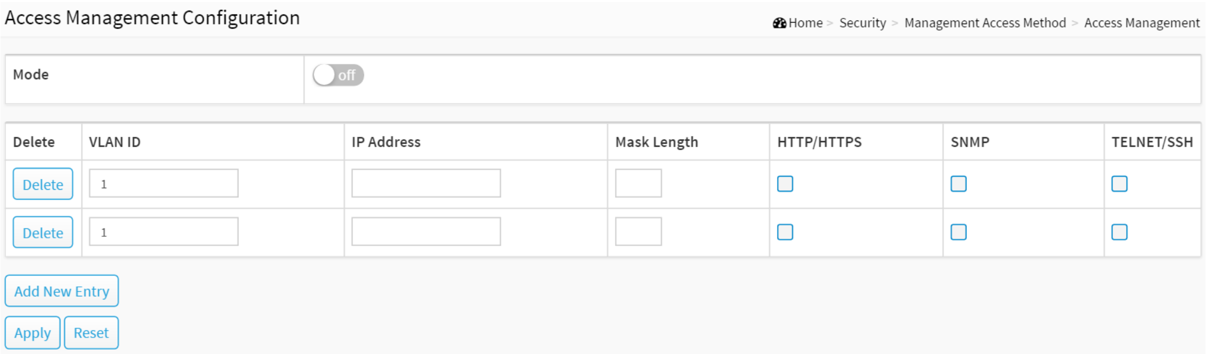
13-1.4 Access Management

This section shows you to configure access management table of the Switch including HTTP/HTTPS, SNMP, and TELNET/SSH. You can manage the Switch over an Ethernet LAN, or over the Internet.

Web Interface

To configure an Access Management Configuration in the web interface:

1. Click Security, Management and Access Management.
2. Select "on" in the Mode of Access Management Configuration.
3. Click "Add new entry".
4. Specify the IP Address, Mask Length.
5. Checked Access Management method (HTTP/HTTPS, SNMP, and TELNET/SSH) in the entry.
6. Click Apply.



Access Management Configuration

Home > Security > Management Access Method > Access Management

Mode	off

Delete	VLAN ID	IP Address	Mask Length	HTTP/HTTPS	SNMP	TELNET/SSH
Delete	1			□	□	□
Delete	1			□	□	□

Add New Entry
Apply
Reset

Figure 13-1.4: The Access Management Configuration

Parameter description:

- **Mode :**

  Indicates the access management mode operation. Possible modes are:

  On : Enable access management mode operation.

  Off : Disable access management mode operation.

- **VLAN ID :**

Indicates the VLAN ID for the access management entry.

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **IP address :**

  Enter the source IP address.

- **Mask Length :**

  Enter the Mask Length.

- **HTTP/HTTPS :**

  Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.

- **SNMP :**

  Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.

- **TELNET/SSH :**

  Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.

Buttons

- **Add New Entry :**

  Click to add a new access management entry.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

13-2 SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. The SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. SNMP agent is running on the switch to response the request issued by SNMP manager.

Basically, it is passive except issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP “Enable”, SNMP agent will be started up. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field SNMP is set “Disable”, SNMP agent will be de-activated, the related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

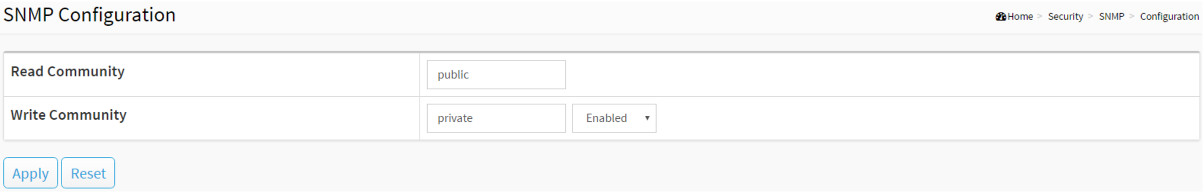
13-2.1 Configuration

This section describes how to configure SNMP System on the switch. This function is used to configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP. A SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So, both parties must have the same community name. Once completing the setting, click <Apply> button, the setting takes effect.

Web Interface

To configure the configure SNMP System in the web interface:

1. Click Security, SNMP and configuration.
2. Evoke SNMP State to enable or disable the SNMP function.
3. Specify the Read Community, Write Community.
4. Click Apply.



SNMP Configuration

Read Community	public
Write Community	private Enabled

Figure 13-2.1: The SNMP Configuration

Parameter description:

- **Read Community :**

  Indicates the community read access string to permit access to SNMP agent. The allowed string length is 1 to 31, and the allowed content is the ASCII characters from 33 to 126.

  The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

- **Write Community :**

  Indicates the community write access string to permit access to SNMP agent. The allowed string length is 1 to 31, and the allowed content is the ASCII characters from 33 to 126.

  The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

13-2.2 SNMPv3

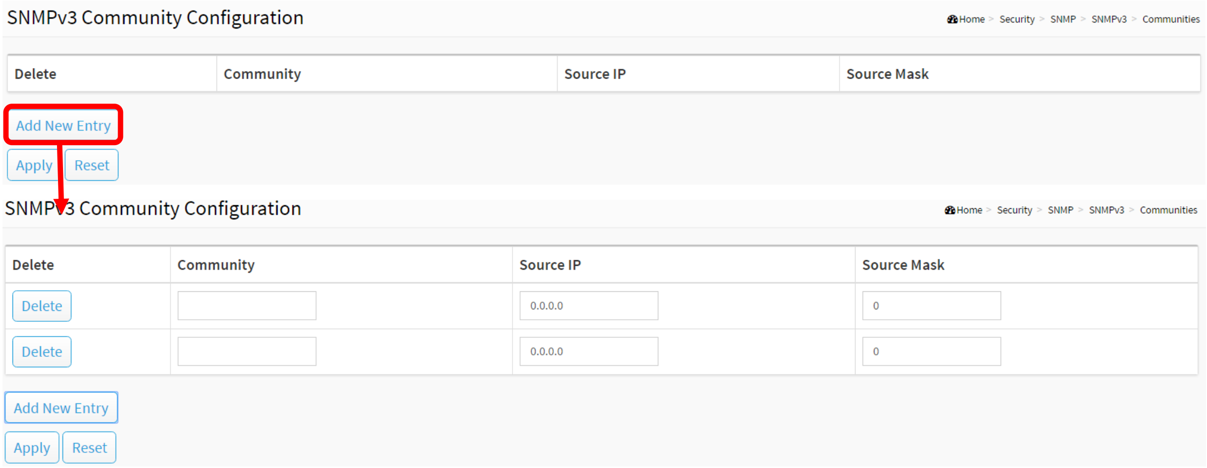
13-2.2.1 Communities

The function is used to configure SNMPv3 communities. The Community is unique. To create a new community account, please check <Add new community> button, and enter the account information then check <Save>. Max Group Number: 6.

Web Interface

To configure the configure SNMP Communities in the web interface:

1. Click Security, SNMP, SNMPv3 and Communities.
2. Click Add new community.
3. Specify the SNMP communities parameters.
4. Click Apply.
5. If you want to modify or clear the setting then click Reset.



SNMPv3 Community Configuration

Home > Security > SNMP > SNMPv3 > Communities

Delete	Community	Source IP	Source Mask

SNMPv3 Community Configuration

Home > Security > SNMP > SNMPv3 > Communities

Delete	Community	Source IP	Source Mask
Delete		0.0.0.0	0
Delete		0.0.0.0	0

Figure 13-2.2.1: The SNMPv3 Communities Configuration

Parameter description:

- **Community**

  Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.

- **Source IP**

  Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.

- **Source Mask**

  Indicates the SNMP access source address mask

Buttons

- **Add New Entry :**

  Click to add new entry. Specify the name and configure the new entry. Click "Save".

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

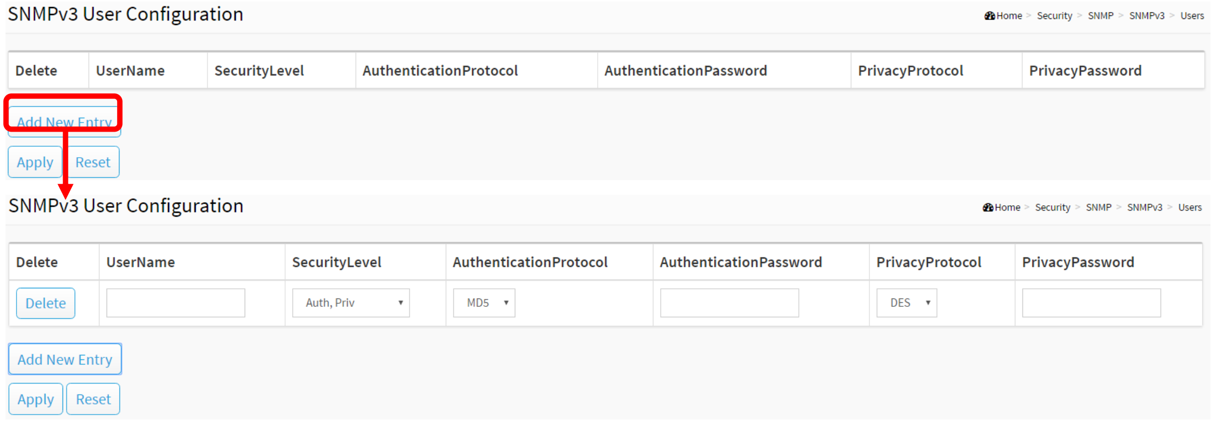
13-2.2.2 Users

The function is used to configure SNMPv3 user. The Entry index key is UserName. To create a new UserName account, please check <Add new user> button, and enter the user information then check <Apply>. Max Group Number: 6.

Web Interface

To configure SNMP Users in the web interface:

1. Click Security, SNMP, SNMPv3 and Users.
2. Click Add new entry.
3. Specify the SNMPv3 Users parameter.
4. Click Apply.



SNMPv3 User Configuration

Home > Security > SNMP > SNMPv3 > Users

Delete	UserName	SecurityLevel	AuthenticationProtocol	AuthenticationPassword	PrivacyProtocol	PrivacyPassword

Add New Entry

Apply Reset

SNMPv3 User Configuration

Home > Security > SNMP > SNMPv3 > Users

Delete	UserName	SecurityLevel	AuthenticationProtocol	AuthenticationPassword	PrivacyProtocol	PrivacyPassword
Delete		Auth, Priv	MD5		DES	

Add New Entry

Apply Reset

Figure 13-2.2.2: The SNMP Users Configuration

Parameter description:

- **User Name :**

  A string identifying the user name that this entry should belong to. The allowed string length is 1 to 31, and the allowed content is ASCII characters from 33 to 126.

- **Security Level :**

  Indicates the security model that this entry should belong to. Possible security models are:

  NoAuth, NoPriv: No authentication and no privacy.

  Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.

- **Authentication Protocol :**

  Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:

  MD5: An optional flag to indicate that this user uses MD5 authentication protocol.

  SHA: An optional flag to indicate that this user uses SHA authentication protocol.

  The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.

- **Authentication Password :**

  A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 39. For SHA authentication protocol, the allowed string length is 8 to 39. The allowed content is ASCII characters from 33 to 126.

- **Privacy Protocol :**

  Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:

  DES: An optional flag to indicate that this user uses DES authentication protocol.

  AES: An optional flag to indicate that this user uses AES authentication protocol.

- **Privacy Password :**

  A string identifying the privacy password phrase. The allowed string length is 8 to 31, and the allowed content is ASCII characters from 33 to 126.

Buttons

- **Add New Entry :**

  Click to add new entry. Specify the name and configure the new entry. Click "Apply".

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

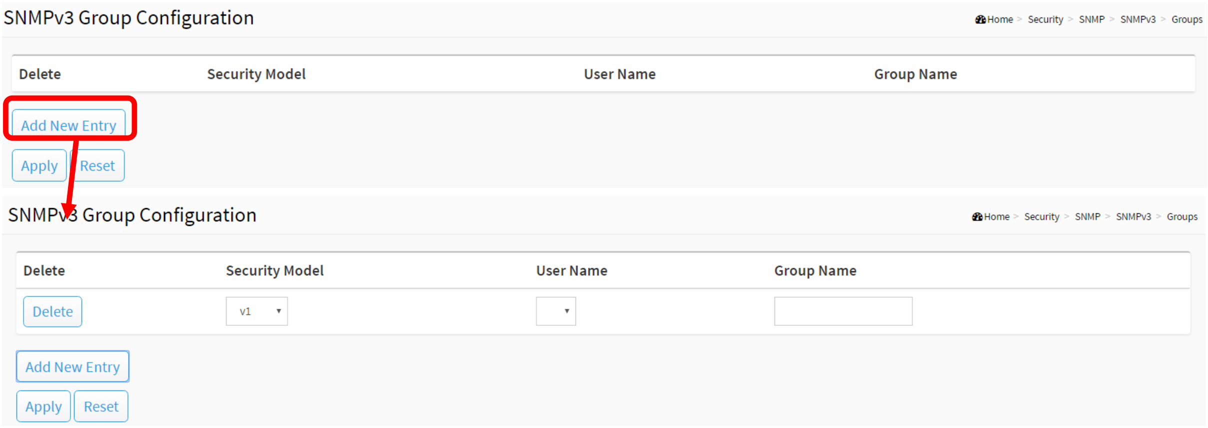
13-2.2.3 Groups

The function is used to configure SNMPv3 group. The Entry index key are Security Model and Security Name. To create a new group account, please check <Add new group> button, and enter the group information then check <Save>. Max Group Number:12.

Web Interface

To configure SNMP Groups in the web interface:

1. Click Security, SNMP, SNMPv3 and Groups.
2. Click Add new entry.
3. Specify the SNMP group parameter.
4. Click Apply.



SNMPv3 Group Configuration

Home > Security > SNMP > SNMPv3 > Groups

Delete	Security Model	User Name	Group Name

Add New Entry

Apply Reset

SNMPv3 Group Configuration

Home > Security > SNMP > SNMPv3 > Groups

Delete	Security Model	User Name	Group Name
Delete	v1		

Add New Entry

Apply Reset

Figure 13-2.2.3: The SNMP Groups Configuration

Parameter description:

- **Security Model :**

  Indicates the security model that this entry should belong to. Possible security models are:

  v1: Reserved for SNMPv1.

  v2c: Reserved for SNMPv2c.

  usm: User-based Security Model (USM).

- **Security Name :**

  A string identifying the security name that this entry should belong to. The allowed string length is 1 to 31, and the allowed content is ASCII characters from 33 to 126.

- **Group Name :**

  A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons

- **Add New Entry :**

  Click to add new entry. Specify the name and configure the new entry. Click "Apply".

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

13-2.2.4 Views

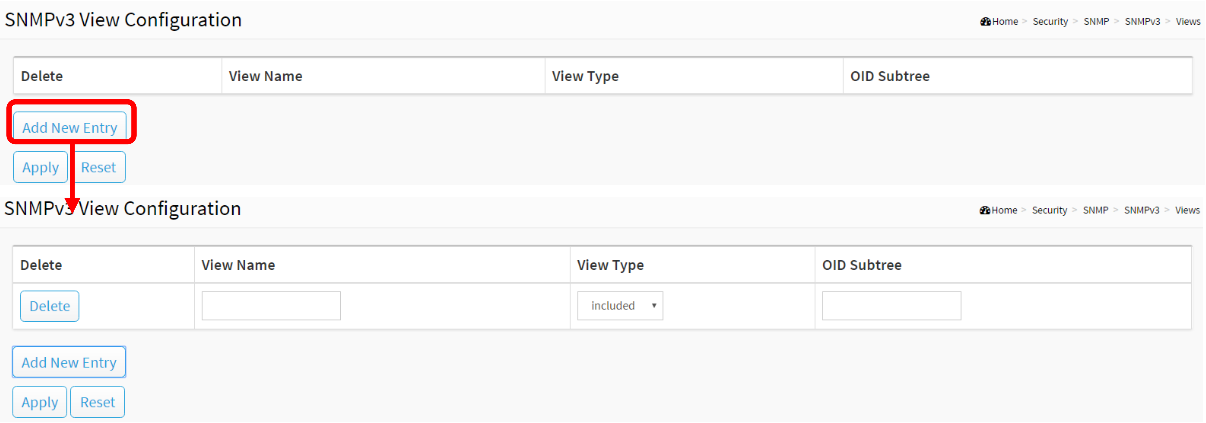
The function is used to configure SNMPv3 view. The Entry index keys are OID Subtree and View Name. To create a new view account, please check <Add new view> button, and enter the view information then click <Apply>. Max Group Number: 12.

Configure SNMPv3 view table on this page. The entry index keys are View Name and OID Subtree.

Web Interface

To configure SNMP views in the web interface:

1. Click Security, SNMP, SNMPv3 and Views.
2. Click Add new entry.
3. Specify the SNMP View parameters.
4. Click Apply.
5. If you want to modify or clear the setting then click Reset.



SNMPv3 View Configuration

Home > Security > SNMP > SNMPv3 > Views

Delete	View Name	View Type	OID Subtree

SNMPv3 View Configuration

Home > Security > SNMP > SNMPv3 > Views

Delete	View Name	View Type	OID Subtree
Delete		included ▾	

Figure 13-2.2.4: The SNMP Views Configuration

Parameter description:

- **View Name :**

  A string identifying the view name that this entry should belong to. The allowed string length is 1 to 31, and the allowed content is ASCII characters from 33 to 126.

- **View Type :**

Indicates the view type that this entry should belong to. Possible view types are:

Included: An optional flag to indicate that this view subtree should be included.

Excluded: An optional flag to indicate that this view subtree should be excluded.

In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and it's OID subtree should overstep the 'excluded' view entry.

- **OID Subtree :**

  The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

Buttons

- **Add New Entry :**

  Click to add new entry. Specify the name and configure the new entry. Click "Save".

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

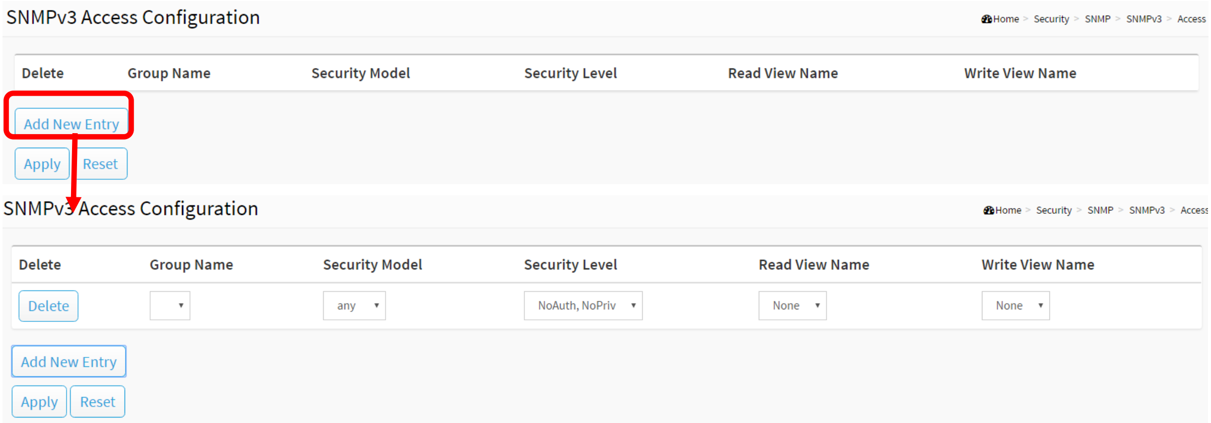
13-2.2.5 Access

The function is used to configure SNMPv3 accesses. The Entry index key are Group Name, Security Model and Security level. To create a new access account, please check <Add new access> button, and enter the access information then check <Apply>. Max Group Number : 12.

Web Interface

To display the configure SNMP Access in the web interface:

1. Click Security, SNMP, SNMPv3 and Accesses.
2. Click Add new entry.
3. Specify the SNMP Access parameters.
4. Click Apply.
5. If you want to modify or clear the setting then click Reset.



SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name

SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
Delete		any	NoAuth, NoPriv	None	None

Home > Security > SNMP > SNMPv3 > Access
Add New Entry
Apply
Reset
Home > Security > SNMP > SNMPv3 > Access
Add New Entry
Apply
Reset

Figure 13-2.2.5: The SNMP Accesses Configuration

Parameter description:

- **Group Name :**

  A string identifying the group name that this entry should belong to. The allowed string length is 1 to 31, and the allowed content is ASCII characters from 33 to 126.

- **Security Model :**

Indicates the security model that this entry should belong to. Possible security models are:

Any: Any security model accepted(v1|v2c|usm).

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: User-based Security Model (USM).

- **Security Level :**

  Indicates the security model that this entry should belong to. Possible security models are:

  NoAuth, NoPriv: No authentication and no privacy.

  Auth, NoPriv: Authentication and no privacy.

  Auth, Priv: Authentication and privacy.

- **Read View Name :**

  The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 31, and the allowed content is ASCII characters from 33 to 126.

- **Write View Name :**

  The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 31, and the allowed content is ASCII characters from 33 to 126.

Buttons

- **Add New Entry :**

  Click to add new entry. Specify the name and configure the new entry. Click "Apply".

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

13-2.3 Trap Event Severity

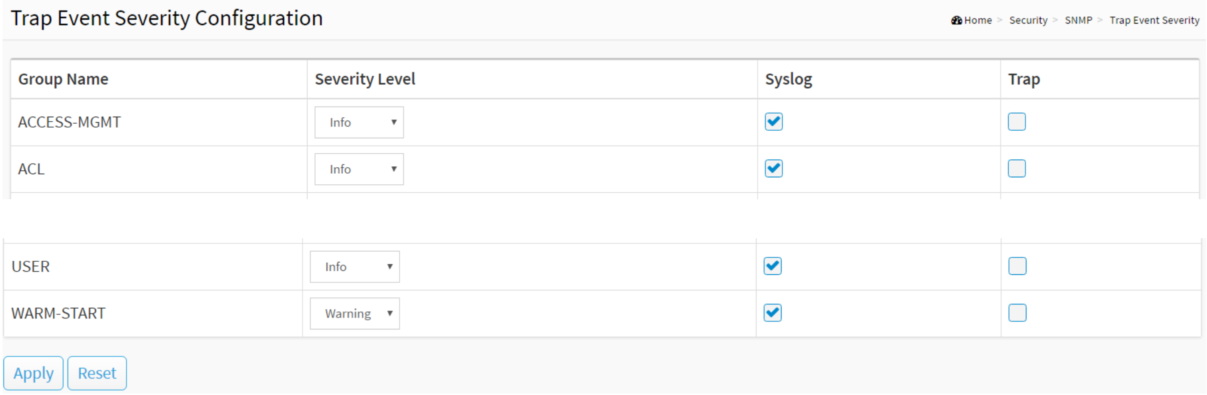
This page displays current trap event severity configurations. Trap event severity can also be configured here.

Web Interface

To display the configure Trap Event Severity in the web interface:

1. Click Security, SNMP and Trap Event Severity.
2. Scroll to select the Group name and Severity Level
3. Click the Apply to save the setting
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

.



Trap Event Severity Configuration

Group Name	Severity Level	Syslog	Trap
ACCESS-MGMT	Info	☑	□
ACL	Info	☑	□
USER	Info	☑	□
WARM-START	Warning	☑	□

Figure 13-2.3: The Trap Event Severity Configuration

Parameter description:

- **Group Name :**

  The name identifying the severity group.

- **Severity Level :**

  Every group has an severity level. The following level types are supported:

  <0> Emergency: System is unusable.

  <1> Alert: Action must be taken immediately.

  <2> Critical: Critical conditions.

<3> **Error:** Error conditions.

<4> **Warning:** Warning conditions.

<5> **Notice:** Normal but significant conditions.

<6> **Information:** Information messages.

<7> **Debug:** Debug-level messages.

- **Syslog :**

  Enable - Select this Group Name in Syslog.

- **Trap :**

  Enable - Select this Group Name in Trap.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

13-3 RMON Configuration

An RMON implementation typically operates in a client/server model. Monitoring devices contain RMON software agents that collect information and analyze packets. These probes act as servers and the Network Management applications that communicate with them act as clients.

13-3.1 Statistics

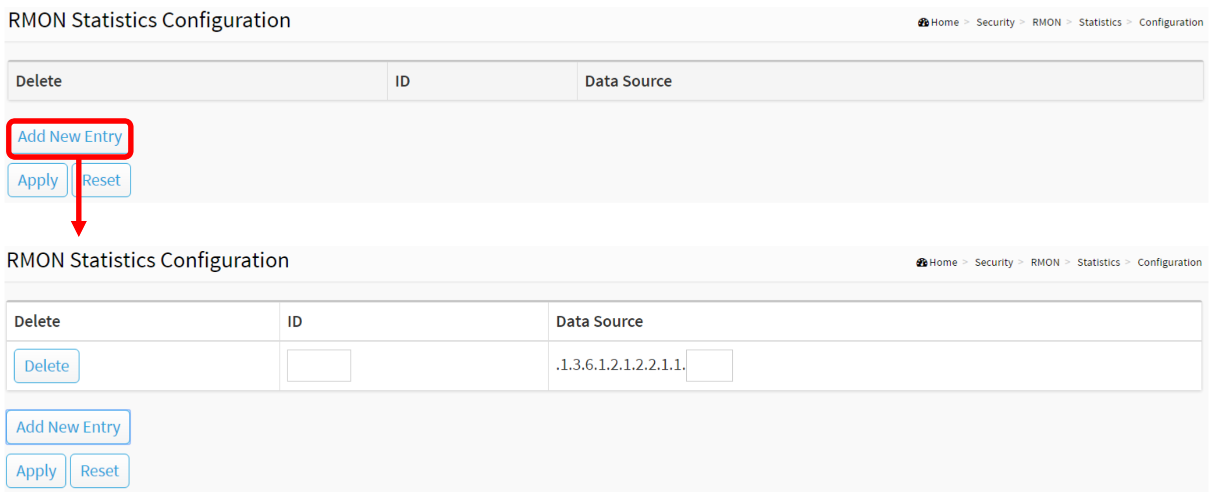
13-3.1.1 Configuration

Configure RMON Statistics table on this page. The entry index key is **ID.**

Web Interface

To configure the RMON Statistics Configuration in the web interface:

1. Click Security, RMON, Statistics and Configuration.
2. Click Add New Entry.
3. Specify the ID parameters.
4. Click Apply.



RMON Statistics Configuration

Home > Security > RMON > Statistics > Configuration

Delete	ID	Data Source

RMON Statistics Configuration

Home > Security > RMON > Statistics > Configuration

Delete	ID	Data Source
Delete		.1.3.6.1.2.1.2.2.1.1.

Figure 13-3.1.1: The RMON Statistics Configuration

Parameter description:

These parameters are displayed on the RMON Statistics Configuration page:

- **ID :**

  Indicates the index of the entry. The range is from 1 to 65535.

- **Data Source :**

  Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005

Buttons

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **Add New Entry :**

  Click to add a new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

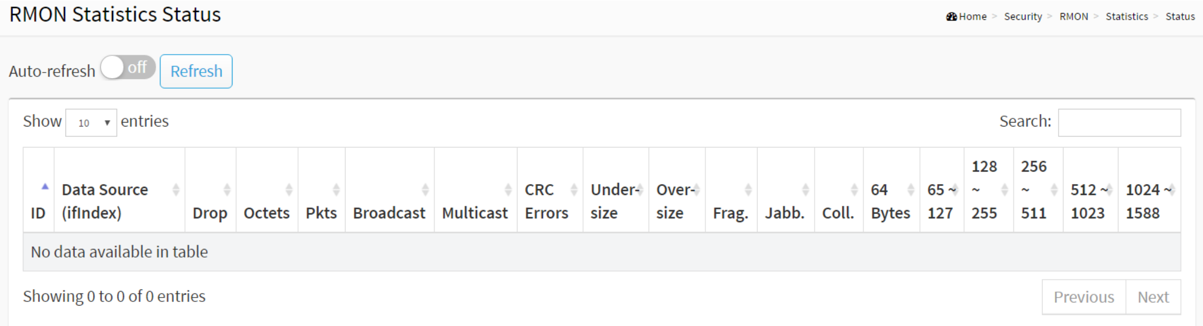
13-3.1.2 Status

This section provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.

Web Interface

To display a RMON Statistics Status in the web interface:

1. Click Security, RMON, Statistics and Status.
2. Specify Port which want to check.
3. Checked "Auto-refresh".
4. Click "Refresh" to refresh the port detailed statistics.



RMON Statistics Status

ID	Data Source (ifIndex)	Drop	Octets	Pkts	Broadcast	Multicast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
No data available in table																		

Showing 0 to 0 of 0 entries

Figure 13-3.1.2: The RMON Statistics Status

Parameter description:

- **ID :**

  Indicates the index of Statistics entry.

- **Data Source(if Index) :**

  The port ID which wants to be monitored.

- **Drop :**

  The total number of events in which packets were dropped by the probe due to lack of resources.

- **Octets :**

  The total number of octets of data (including those in bad packets) received on the network.

- **Pkts :**

  The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

- **Broad-cast :**

  The total number of good packets received that were directed to the broadcast address.

- **Multi-cast :**

  The total number of good packets received that were directed to a multicast address.

- **CRC Errors :**

  The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

- **Under-size :**

  The total number of packets received that were less than 64 octets.

- **Over-size :**

  The total number of packets received that were longer than 1518 octets.

- **Frag. :**

  The number of frames which size is less than 64 octets received with invalid CRC.

- **Jabb. :**

  The number of frames which size is larger than 64 octets received with invalid CRC.

- **Coll. :**

  The best estimate of the total number of collisions on this Ethernet segment.

- **64 Bytes :**

  The total number of packets (including bad packets) received that were 64 octets in length.

- **65~127 :**

The total number of packets (including bad packets) received that were between 65 to 127 octets in length.

- **128~255 :**

  The total number of packets (including bad packets) received that were between 128 to 255 octets in length.

- **256~511 :**

  The total number of packets (including bad packets) received that were between 256 to 511 octets in length.

- **512~1023 :**

  The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.

- **1024~1588 :**

  The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.

- **Search :**

  You can search for the information that you want to see.

- **Show entries :**

  You can choose how many items you want to show off.

Buttons

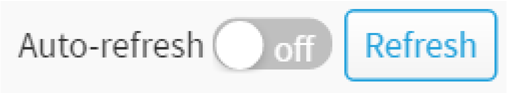


Figure 13-3.1.2: The RMON Statistics Status buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

- **Next :**

  Updates the system log entries, turn to the next page.

- **Previous :**

  Updates the system log entries, turn to the previous page.

13-3.2 History

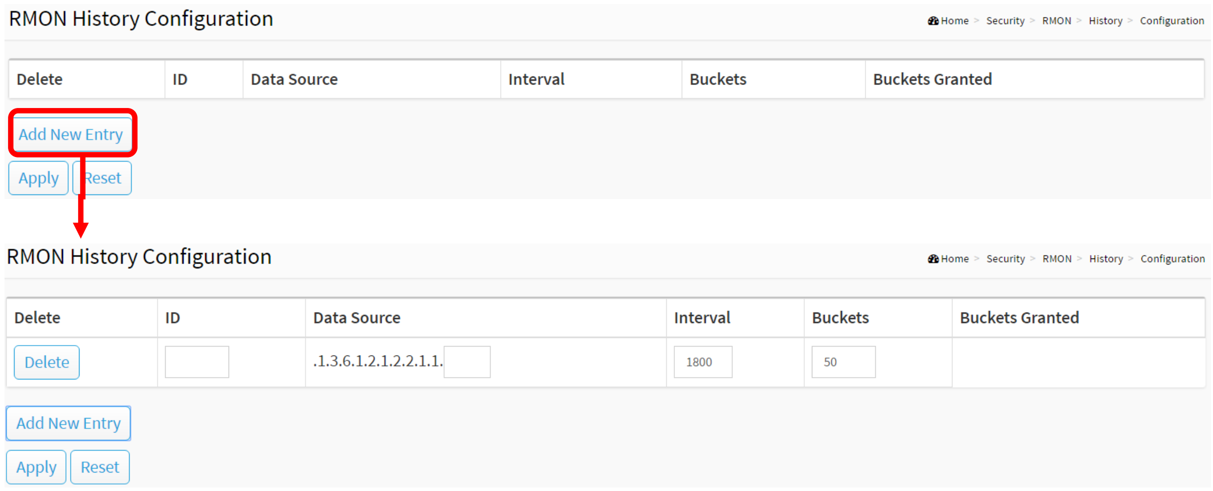
13-3.2.1 Configuration

Configure RMON History table on this page. The entry index key is **ID.**

Web Interface

To configure the RMON History Configuration in the web interface:

1. Click Security, RMON, History and Configuration.
2. Click Add New Entry.
3. Specify the ID parameters.
4. Click Apply.


RMON History Configuration
Home > Security > RMON > History > Configuration
Add New Entry
Apply
Reset
RMON History Configuration
Home > Security > RMON > History > Configuration
Delete
Add New Entry
Apply
Reset

Delete	ID	Data Source	Interval	Buckets	Buckets Granted

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
Delete		.1.3.6.1.2.1.2.2.1.1.	1800	50	

Figure 13-3.2.1: The RMON History Configuration

Parameter description:

These parameters are displayed on the RMON History Configuration page:

- **ID :**

  Indicates the index of the entry. The range is from 1 to 65535.

- **Data Source :**

  Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005

- **Interval :**

  Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.

- **Buckets :**

  Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600, default value is 50.

- **Buckets Granted :**

  The number of data shall be saved in the RMON.

Buttons

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **Add New Entry :**

  Click to add a new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

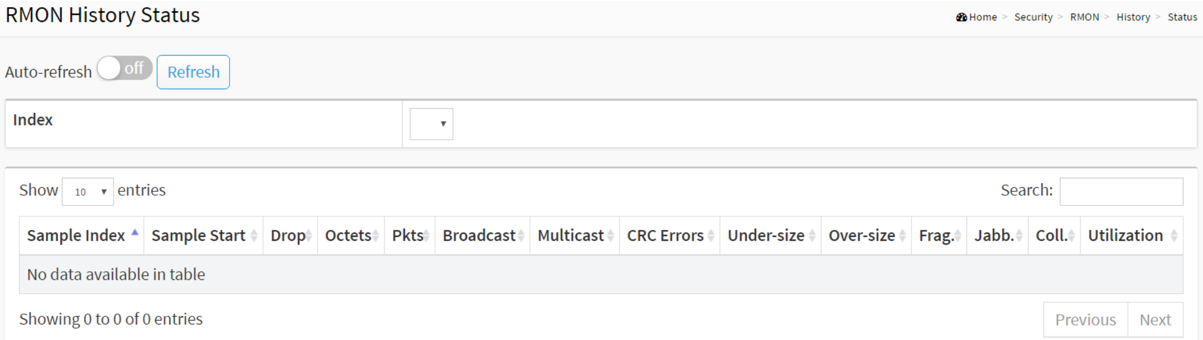
13-3.2.2 Status

This section provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table.

Web Interface

To display a RMON History Status in the web interface:

1. Click Security, RMON, History and Status.
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.



RMON History Status

Sample Index	Sample Start	Drop	Octets	Pkts	Broadcast	Multicast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
No data available in table													

Showing 0 to 0 of 0 entries

Figure 13-3.2.2: The RMON History Status

Parameter description:

- **Index :**

  Indicates the index of History control entry.

- **Sample Index :**

  Indicates the index of the data entry associated with the control entry.

- **Sample Start :**

  The value of sysUpTime at the start of the interval over which this sample was measured.

- **Drop :**

  The total number of events in which packets were dropped by the probe due to lack of resources.

- **Octets :**

  The total number of octets of data (including those in bad packets) received on the network.

- **Pkts :**

  The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

- **Broadcast :**

  The total number of good packets received that were directed to the broadcast address.

- **Multicast :**

  The total number of good packets received that were directed to a multicast address.

- **CRC Errors :**

  The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

- **Under-size :**

  The total number of packets received that were less than 64 octets.

- **Over-size :**

  The total number of packets received that were longer than 1518 octets.

- **Frag. :**

  The number of frames which size is less than 64 octets received with invalid CRC.

- **Jabb. :**

  The number of frames which size is larger than 64 octets received with invalid CRC.

- **Coll. :**

  The best estimate of the total number of collisions on this Ethernet segment.

- **Utilization :**

The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

- **Search :**

  You can search for the information that you want to see.

- **Show entries :**

  You can choose how many items you want to show off.

Buttons

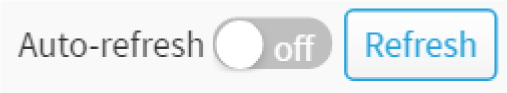


Figure 13-3.2.2: The RMON History Status buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

- **Next :**

  Updates the system log entries, turn to the next page.

- **Previous :**

  Updates the system log entries, turn to the previous page.

13-3.3 Alarm

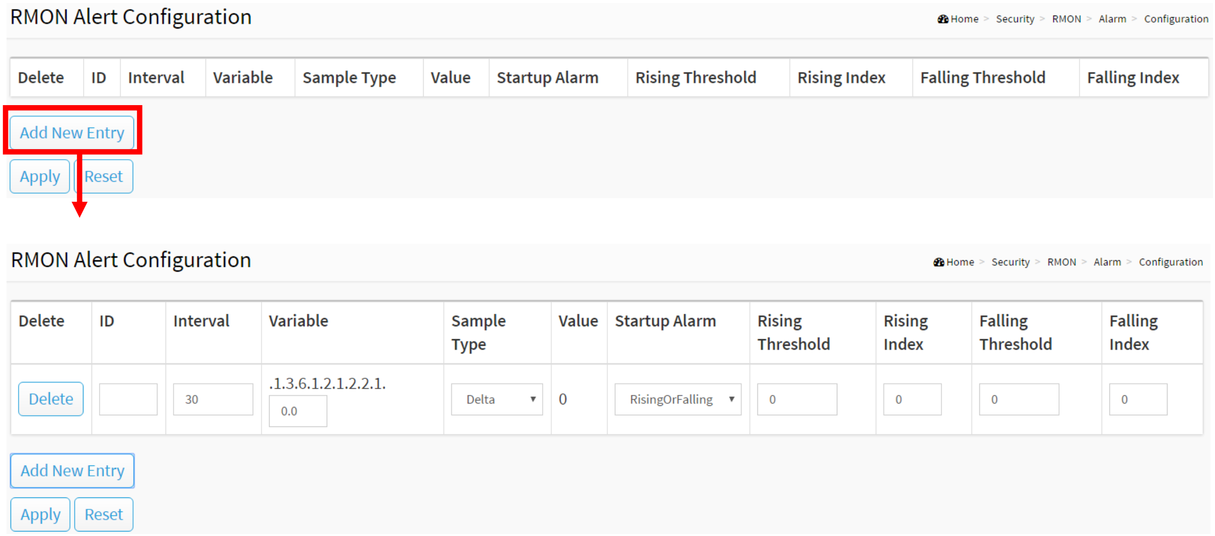
13-3.3.1 Configuration

Configure RMON Alarm table on this page. The entry index key is **ID.**

Web Interface

To configure the RMON Alarm Configuration in the web interface:

1. Click Security, RMON, Alarm and Configuration.
2. Click Add New Entry.
3. Specify the ID parameters.
4. Click Apply.



RMON Alert Configuration

Home > Security > RMON > Alarm > Configuration

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index

RMON Alert Configuration

Home > Security > RMON > Alarm > Configuration

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
Delete		30	.1.3.6.1.2.1.2.2.1. 0.0	Delta	0	RisingOrFalling	0	0	0	0

Figure 13-3.3.1: The RMON Alarm Configuration

Parameter description:

These parameters are displayed on the RMON Alarm Configuration page:

- **ID :**

  Indicates the index of the entry. The range is from 1 to 65535.

- **Interval :**

  Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^31-1.

- **Variable :**

  Indicates the particular variable to be sampled, the possible variables are:

  InOctets:
  The total number of octets received on the interface, including framing characters.

  InUcastPkts:
  The number of uni-cast packets delivered to a higher-layer protocol.

  InNUcastPkts:
  The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.

  InDiscards:
  The number of inbound packets that are discarded even the packets are normal.

  InErrors:
  The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

  InUnknownProtos:
  the number of the inbound packets that were discarded because of the unknown or un-support protocol.

  OutOctets:
  The number of octets transmitted out of the interface , including framing characters.

  OutUcastPkts:
  The number of uni-cast packets that request to transmit.

  OutNUcastPkts:
  The number of broad-cast and multi-cast packets that request to transmit.

  OutDiscards:
  The number of outbound packets that are discarded event the packets is normal.

  OutErrors:
  The The number of outbound packets that could not be transmitted because of errors.

  OutQLen:
  The length of the output packet queue (in packets).

- **Sample Type :**

  The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:

  Absolute: Get the sample directly.

  Delta: Calculate the difference between samples (default).

- **Value :**

  The value of the statistic during the last sampling period.

- **Startup Alarm :**

  The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:

  RisingTrigger alarm when the first value is larger than the rising threshold.

  FallingTrigger alarm when the first value is less than the falling threshold.

  RisingOrFallingTrigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).

- **Rising Threshold :**

  Rising threshold value (-2147483648-2147483647).

- **Rising Index :**

  Rising event index (1-65535).

- **Falling Threshold :**

  Falling threshold value (-2147483648-2147483647)

- **Falling Index :**

  Falling event index (1-65535).

Buttons

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **Add New Entry :**

  Click to add a new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

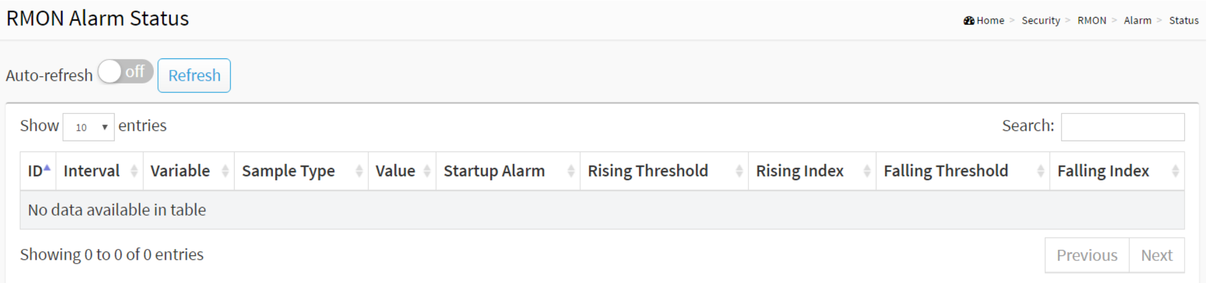
13-3.3.2 Status

This page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table

Web Interface

To display a RMON Alarm Status in the web interface:

1. Click Security, RMON, Alarm and Status.
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.



RMON Alarm Status

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
No data available in table									

Showing 0 to 0 of 0 entries

Figure 13-3.3.2: RMON Alarm Status

Parameter description:

- **ID :**

  Indicates the index of Alarm control entry.

- **Interval :**

  Indicates the interval in seconds for sampling and comparing the rising and falling threshold.

- **Variable :**

  Indicates the particular variable to be sampled

- **Sample Type :**

  The method of sampling the selected variable and calculating the value to be compared against the thresholds.

- **Value :**

  The value of the statistic during the last sampling period.

- **Startup Alarm :**

  The alarm that may be sent when this entry is first set to valid.

- **Rising Threshold :**

  Rising threshold value.

- **Rising Index :**

  Rising event index.

- **Falling Threshold :**

  Falling threshold value.

- **Falling Index :**

  Falling event index.

- **Search :**

  You can search for the information that you want to see.

- **Show entries :**

  You can choose how many items you want to show off.

Buttons

Figure 13-3.3.2: RMON Alarm Status buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

- **Next :**

  Updates the system log entries, turn to the next page.

- **Previous :**

Updates the system log entries, turn to the previous page.

13-3.4 Event

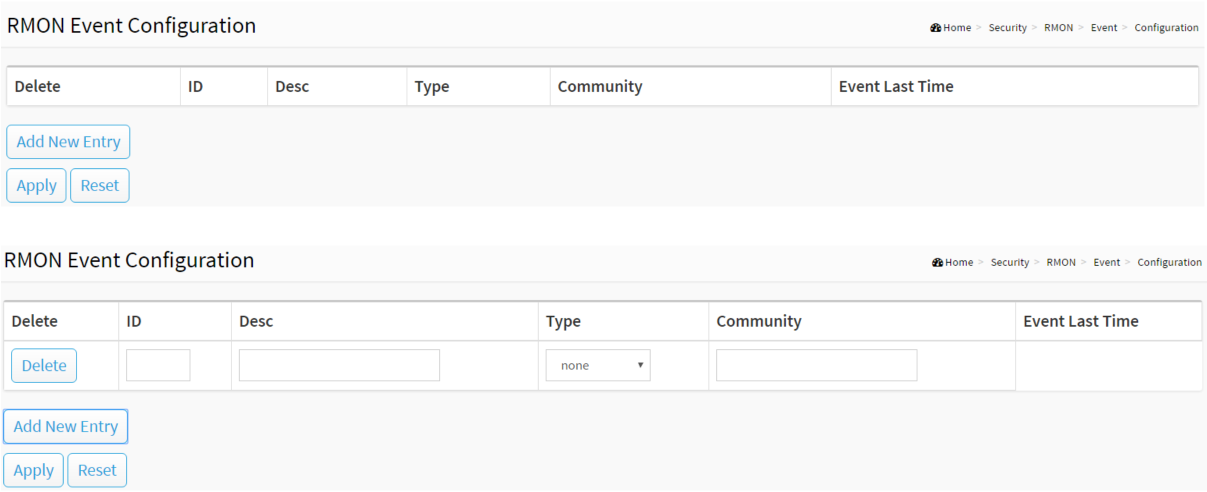
13-3.4.1 Configuration

Configure RMON Event table on this page. The entry index key is **ID.**

Web Interface

To configure the RMON Event Configuration in the web interface:

1. Click Security, RMON, Event and Configuration.
2. Click Add New Entry.
3. Specify the ID parameters.
4. Click Apply.


RMON Event Configuration

Delete	ID	Desc	Type	Community	Event Last Time

RMON Event Configuration

Delete	ID	Desc	Type	Community	Event Last Time
Delete			none		

Home > Security > RMON > Event > Configuration
Add New Entry
Apply
Reset
Home > Security > RMON > Event > Configuration
Add New Entry
Apply
Reset

Figure 13-3.4.1: The RMON Event Configuration

Parameter description:

These parameters are displayed on the RMON History Configuration page:

- **ID :**

  Indicates the index of the entry. The range is from 1 to 65535.

- **Desc :**

Indicates this event, the string length is from 0 to 127, default is a null string.

- **Type :**

  Indicates the notification of the event, the possible types are:

  None: No SNMP log is created, no SNMP trap is sent.

  Log: Create SNMP log entry when the event is triggered.

  Snmp trap: Send SNMP trap when the event is triggered.

  Log and trap: Create SNMP log entry and sent SNMP trap when the event is triggered.

- **Community :**

  Specify the community when trap is sent, the string length is from 0 to 127, default is "public".

- **Event Last Time :**

  Indicates the value of sysUpTime at the time this event entry last generated an event.

Buttons

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **Add New Entry :**

  Click to add a new entry.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

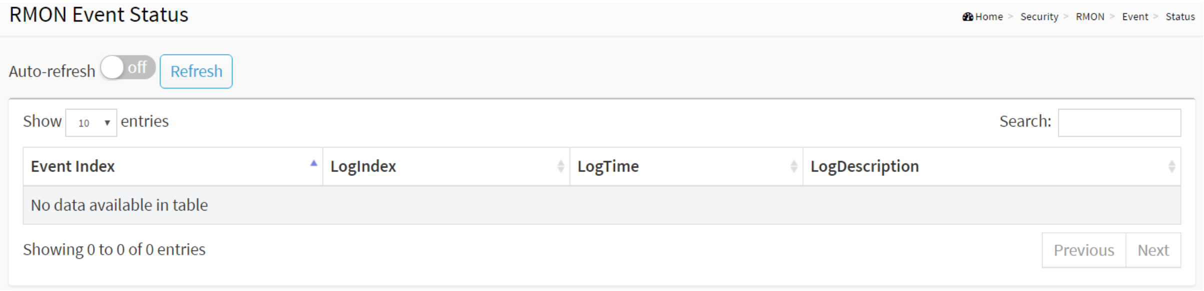
13-3.4.2 Status

This page provides an overview of RMON Event table entries. Each page shows up to 99 entries from the Event table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table.

Web Interface

To display a RMON Event Status in the web interface:

1. Click Security, RMON, Event and Status.
2. Checked "Auto-refresh".
3. Click " Refresh" to refresh the port detailed statistics
4. Specify Port which wants to check.



Event Index	LogIndex	LogTime	LogDescription
No data available in table			

Showing 0 to 0 of 0 entries

Figure 13-3.4.2: RMON Event Status

Parameter description:

- **Event Index :**

  Indicates the index of the event entry.

- **Log Index :**

  Indicates the index of the log entry.

- **LogTIme :**

  Indicates Event log time

- **LogDescription :**

Indicates the Event description.

- **Search :**

  You can search for the information that you want to see.

- **Show entries :**

  You can choose how many items you want to show off.

Buttons

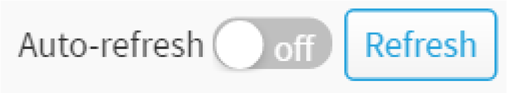


Figure 13-3.4.2: RMON Event Status buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

- **Next :**

  Updates the system log entries, turn to the next page.

- **Previous :**

  Updates the system log entries, turn to the previous page.

13-3 IEEE 802.1X

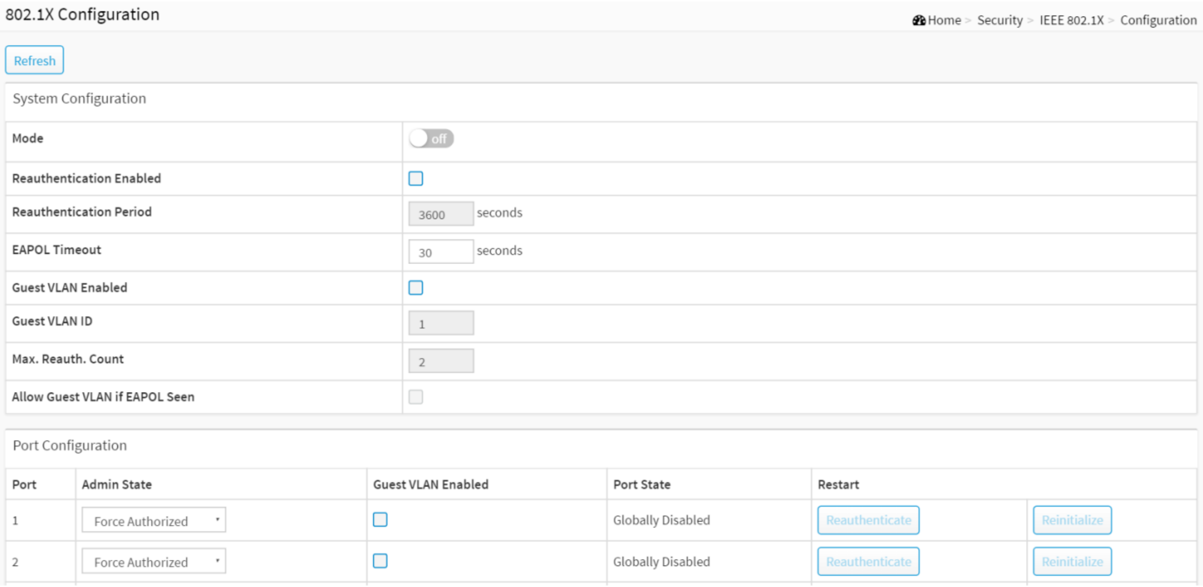
13-3.1 Configuration

The section describes to configure the 802.1X parameters of the switch. The 802.1X can be employed to connect users to a variety of resources including Internet access, conference calls, printing documents on shared printers, or by simply logging on to the Internet.

Web Interface

To configure the IEEE 802.1X in the web interface:

1. Click Security, IEEE 802.1X and Configuration.
2. Select “on” in the Mode of IEEE 802.1X Configuration.
3. Checked Reauthentication Enabled.
4. Set Reauthentication Period (Default is 3600 seconds).
5. Select Admin State and displays Port State.
6. Click the Apply to save the setting.
7. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



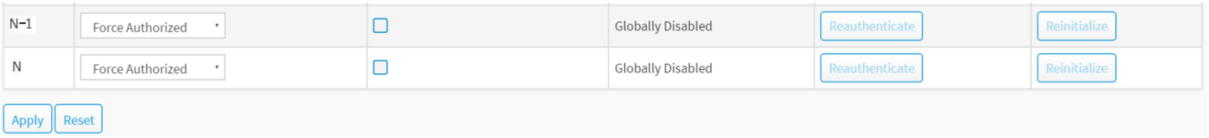
802.1X Configuration

System Configuration

Mode	off
Reauthentication Enabled	□
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Guest VLAN Enabled	□
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	□

Port Configuration

Port	Admin State	Guest VLAN Enabled	Port State	Restart	
1	Force Authorized	□	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized	□	Globally Disabled	Reauthenticate	Reinitialize



N-1	Force Authorized	□	Globally Disabled	Reauthenticate	Reinitialize
N	Force Authorized	□	Globally Disabled	Reauthenticate	Reinitialize

Figure 13-3.1: The IEEE 802.1X Configuration

Parameter description:

System Configuration

- **Mode :**

  on or off.

  Indicates if IEEE 802.1X is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.

- **Reauthentication Enabled :**

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

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

- **Reauthentication Period :**

  Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.

- **EAPOL Timeout :**

  Determines the time for retransmission of Request Identity EAPOL frames.

  Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports.

- **Guest VLAN Enabled**

  A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below.
  The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN

functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

- **Guest VLAN ID**

  This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled.
  Valid values are in the range [1; 4094].

- **Max. Reauth. Count**

  The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled.
  Valid values are in the range [1; 255].

- **Allow Guest VLAN if EAPOL Seen**

  The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port.
  The value can only be changed if the Guest VLAN option isglobally enabled.

Port Configuration

- **Port :**

  The port number for which the configuration below applies.

- **Admin State :**

  If 802.1X is globally enabled, this selection controls the port's authentication mode. The following modes are available:

  - **Force Authorized :**

    In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.

  - **Force Unauthorized :**

    In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.

- **Port-based 802.1X :**

In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant

NOTE: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead).

Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant.

And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

- **Guest VLAN Enabled**

When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below.

This option is only available for EAPOL-based modes, i.e.:

• Port-based 802.1X

• Single 802.1X

• Multi 802.1X

For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

Guest VLAN Operation:

When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.

Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.

While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.

- **Port State :**

The current state of the port. It can undertake one of the following values:

Globally Disabled: IEEE 802.1X is globally disabled.

Link Down: IEEE 802.1X is globally enabled, but there is no link on the port.

Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.

Unauthorized: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.

X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.

- **Restart :**

Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode.

Clicking these buttons will not cause settings changed on the page to take effect.

Re-authenticate: Schedules a re-authentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, re-authentication will be attempted immediately.

The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.

Reinitialize: Forces a re-initialization of the clients on the port and thereby a re-authentication immediately. The clients will transfer to the unauthorized state while the re-authentication is in progress.

Buttons

- **Apply :**

Click to save changes.

- **Reset :**

Click to undo any changes made locally and revert to previously saved values.

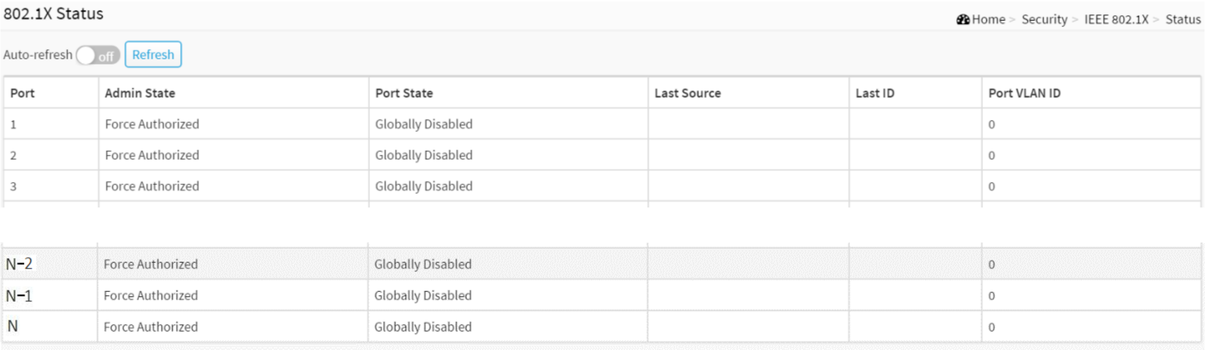
13-3.2 Status

The section describes to show the each port 802.1X status information of the switch. The status includes Admin State, Port State, Last Source, Last ID and Port VLAN ID.

Web Interface

To displays 802.1X Status in the web interface:

1. Click Security, IEEE 802.1X and Status.
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.
4. You can select which port that you want display 802.1X Statistics.



802.1X Status

Port	Admin State	Port State	Last Source	Last ID	Port VLAN ID
1	Force Authorized	Globally Disabled			0
2	Force Authorized	Globally Disabled			0
3	Force Authorized	Globally Disabled			0
N-2	Force Authorized	Globally Disabled			0
N-1	Force Authorized	Globally Disabled			0
N	Force Authorized	Globally Disabled			0

Figure 13-3.2: The IEEE 802.1X Status

Parameter description:

802.1X Status

- **Port :**

  The switch port number. Click to navigate to detail 802.1X statistics for this port.

- **Admin State :**

  The port's current administrative state. Refer to 802.1X Admin State for a description of possible values.

- **Port State :**

  The current state of the port. Refer to 802.1X Port State for a description of the individual states.

- **Last Source :**

  The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

- **Last ID :**

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

- **Port VLAN ID :**

  The VLAN ID that 802.1X has put the port in. The field is blank, if the Port VLAN ID is not overridden by 802.1X.

  If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here.

  If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Buttons

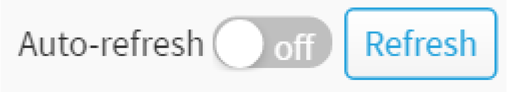


Figure 13-3.2: The IEEE 802.1X Status buttons

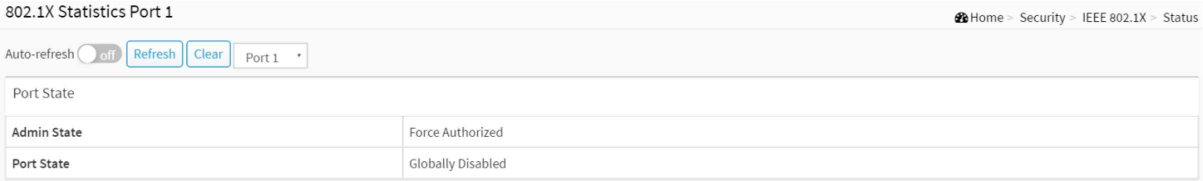
- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

- **If you select port1 to display 802.1X Statistics.**


802.1X Statistics Port 1

Home > Security > IEEE 802.1X > Status

Auto-refresh off Refresh Clear Port 1

Port State	
Admin State	Force Authorized
Port State	Globally Disabled

Figure 13-3.2: The 802.1X Statistics Port 1

Parameter description:

- **Port :**

  You can select which port that you want display 802.1X Statistics.

- **Admin State :**

  The port's current administrative state. Refer to 802.1X Admin State for a description of possible values.

- **Port State :**

  The current state of the port. Refer to 802.1X Port State for a description of the individual states.

Buttons

Figure 13-3.2: The IEEE 802.1X Statistics Port buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page.

- **Clear :**

  Clears the counters for the selected port.

13-4 IP Source Guard

The section describes to configure the IP Source Guard detail parameters of the switch. You could use the IP Source Guard configure to enable or disable with the Port of the switch.

13-4.1 Configuration

This section describes how to configure IP Source Guard setting including：

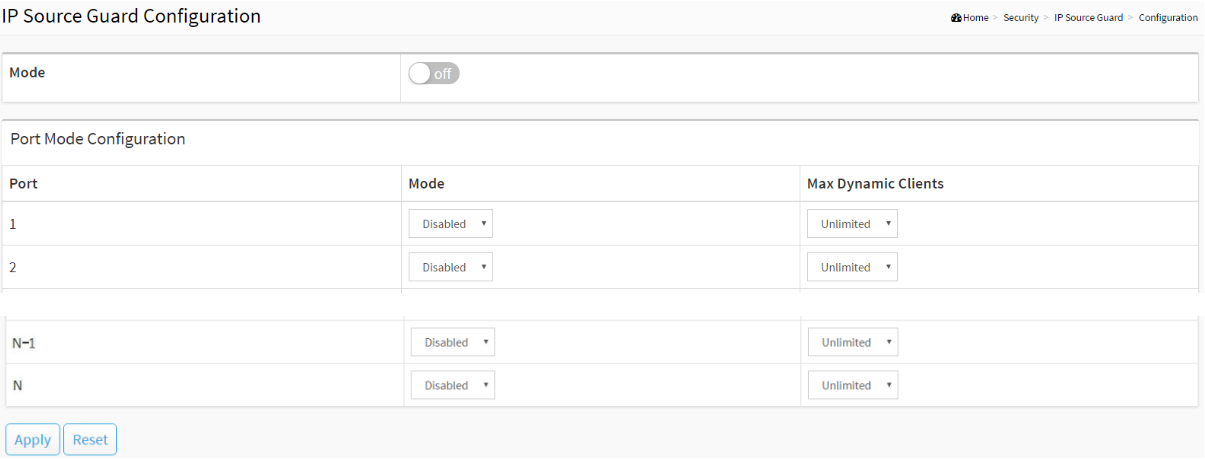
Mode (Enabled and Disabled)

Maximum Dynamic Clients (0, 1, 2, Unlimited)

Web Interface

To configure an IP Source Guard Configuration in the web interface:

1. Click Security, IP Source Guard and Configuration.
2. Select "on" in the Mode of IP Source Guard Configuration.
3. Select "Enabled" of the specific port in the Mode of Port Mode Configuration.
4. Select Maximum Dynamic Clients (0, 1, 2, Unlimited) of the specific port in the Mode of Port Mode Configuration.
5. Click Apply.



IP Source Guard Configuration

Mode	off

Port Mode Configuration

Port	Mode	Max Dynamic Clients
1	Disabled	Unlimited
2	Disabled	Unlimited
N-1	Disabled	Unlimited
N	Disabled	Unlimited

Figure 13-4.1: The IP Source Guard Configuration

Parameter description :

- **Mode of IP Source Guard Configuration :**

Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.

- **Port Mode Configuration :**

  Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.

- **Max Dynamic Clients :**

  Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

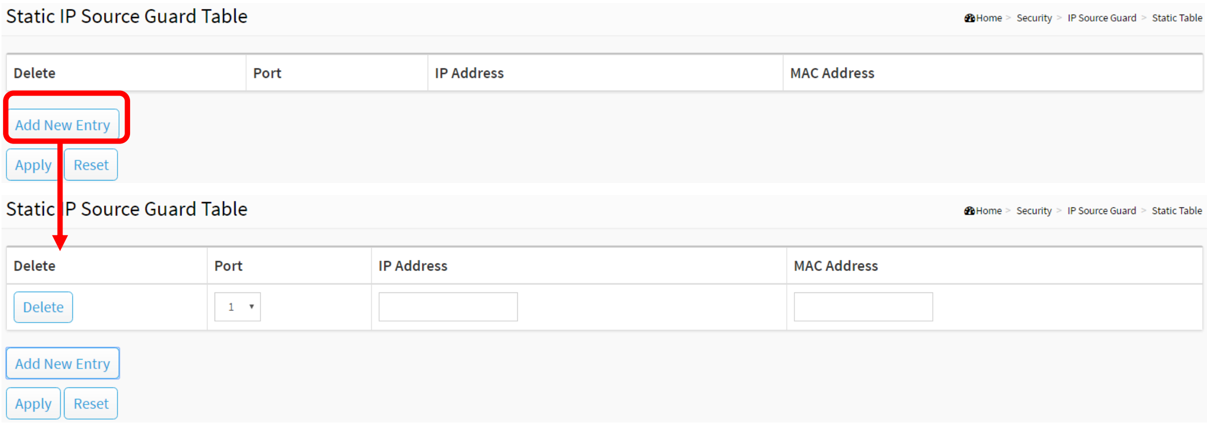
13-4.2 Static Table

The section describes to configure the Static IP Source Guard Table parameters of the switch. You could use the Static IP Source Guard Table configure to manage the entries.

Web Interface

To configure a Static IP Source Guard Table Configuration in the web interface:

1. Click Security, IP Source Guard and Static Table.
2. Click "Add New Entry".
3. Specify the Port, IP Address, and MAC address in the entry.
4. Click Apply.



Static IP Source Guard Table

Delete	Port	IP Address	MAC Address

Static IP Source Guard Table

Delete	Port	IP Address	MAC Address
Delete	1		

Home > Security > IP Source Guard > Static Table
Add New Entry
Apply
Reset
Home > Security > IP Source Guard > Static Table
Add New Entry
Apply
Reset

Figure 13-4.2: The Static IP Source Guard Table

Parameter description:

- **Port :**

  The logical port for the settings.

- **IP Address :**

  Allowed Source IP address.

- **MAC address :**

  Allowed Source MAC address.

Buttons

- **Add New Entry :**

  Click to add a new entry to the Static IP Source Guard table. Specify the Port, VLAN ID, IP address, and IP Mask for the new entry. Click "Apply".

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

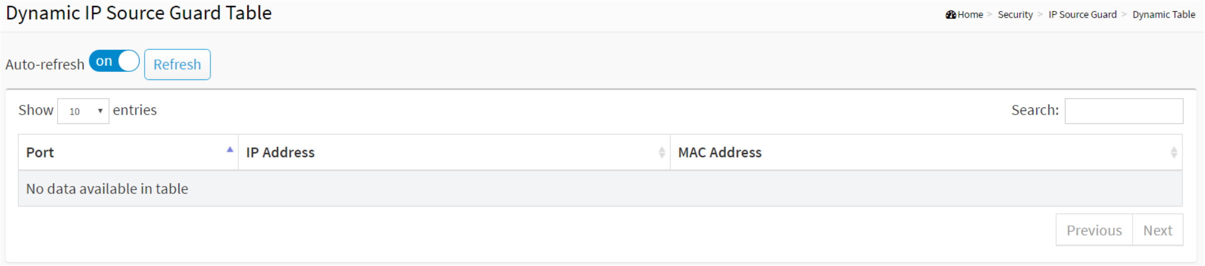
13-4.3 Dynamic Table

Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by IP address, and then by MAC address.

Web Interface

To configure a Dynamic IP Source Guard Table Configuration in the web interface:

1. Click Security, IP Source Guard and Dynamic Table.
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.
4. Specify the Start from port, IP Address, and entries per page.



Dynamic IP Source Guard Table

Home > Security > IP Source Guard > Dynamic Table

Auto-refresh on Refresh

Show 10 entries

Search:

Port	IP Address	MAC Address
No data available in table		

Previous Next

Figure 13-4.3: The Dynamic IP Source Guard Table

Parameter description:

- **Port :**

  Switch Port Number for which the entries are displayed.

- **IP Address :**

  User IP address of the entry.

- **MAC Address :**

  Source MAC address.

- **Search :**

  You can search for the information that you want to see.

- **Show entries :**

  You can choose how many items you want to show off.

Buttons

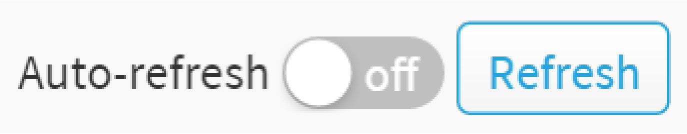


Figure 13-4.3: The Dynamic IP Source Guard Table buttons

- **Next :**

  Updates the system log entries, turn to the next page.

- **Previous :**

  Updates the system log entries, turn to the previous page.

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

13-5 ARP Inspection

The section describes to configure the ARP Inspection parameters of the switch. You could use the ARP Inspection configure to manage the ARP table.

13-5.1 Configuration

This section describes how to configure ARP Inspection setting including：

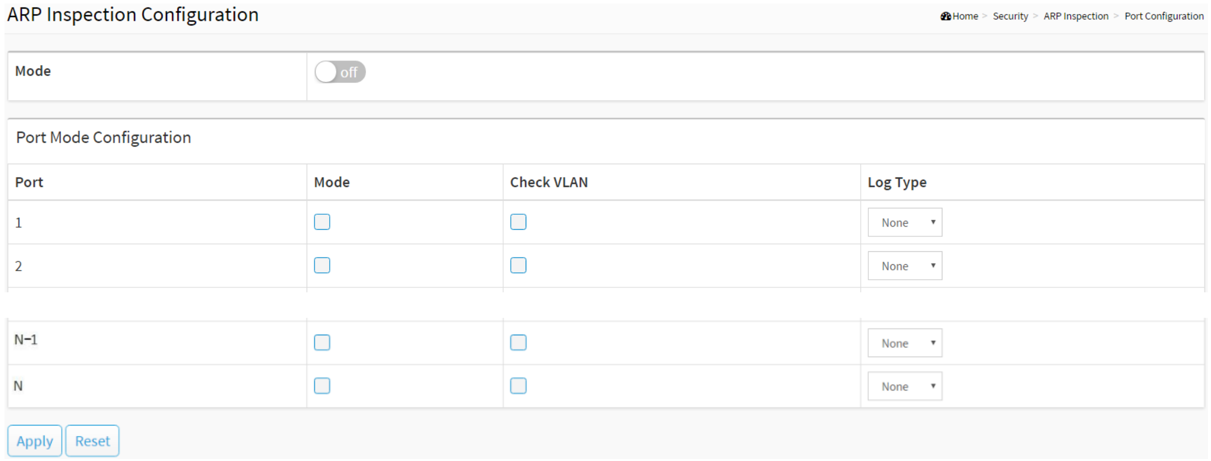
Mode (on and off)

Port (Enabled and Disabled)

Web Interface

To configure an ARP Inspection Configuration in the web interface:

1. Click Security, ARP Inspection and Port Configuration.
2. Select “on” in the Mode of ARP Inspection Configuration.
3. Select “Enabled” of the specific port in the Mode of Port Mode Configuration.
4. Click Apply.



ARP Inspection Configuration

Home > Security > ARP Inspection > Port Configuration

Mode	off

Port Mode Configuration

Port	Mode	Check VLAN	Log Type
1	□	□	None ▾
2	□	□	None ▾
N-1	□	□	None ▾
N	□	□	None ▾

Figure 13-5.1: The ARP Inspection Configuration

Parameter description:

- **Mode of ARP Inspection Configuration :**

  Enable the Global ARP Inspection or disable the Global ARP Inspection.

- **Port Mode Configuration :**

  Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Possible modes are:
  Enabled: Enable ARP Inspection operation.
  Disabled: Disable ARP Inspection operation.
  If you want to inspect the VLAN configuration, you have to enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of "Check VLAN" are:
  Enabled: Enable check VLAN operation.
  Disabled: Disable check VLAN operation.
  Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. There are four log types and possible types are:
  None: Log nothing.
  Deny: Log denied entries.
  Permit: Log permitted entries.
  ALL: Log all entries.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

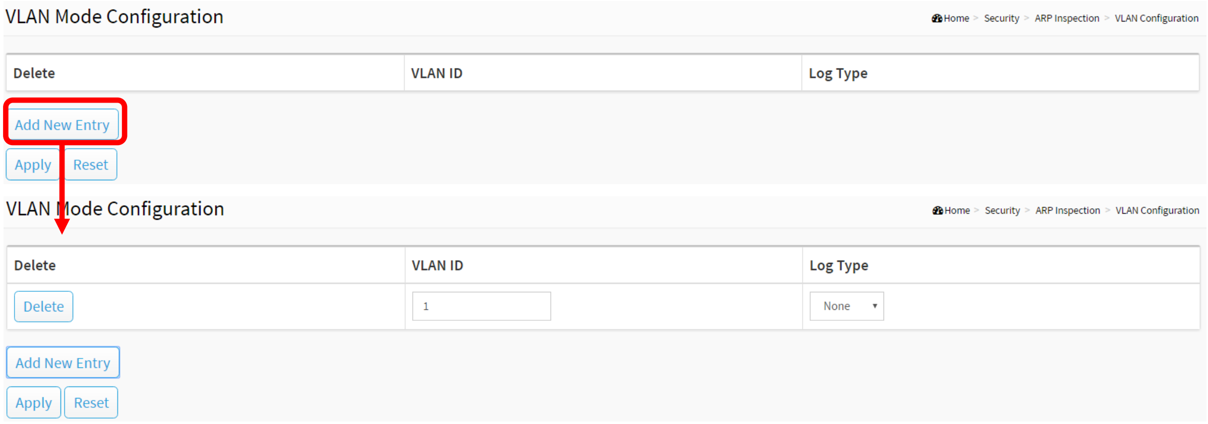
13-5.2 VLAN Configuration

Specify ARP Inspection is enabled on which VLANs

Web Interface

To configure a VLAN Mode Configuration in the web interface:

1. Click Security, ARP Inspection and VLAN Configuration.
2. Click "Add new entry".
3. Specify the VLAN ID, Log Type
4. Click Apply.



VLAN Mode Configuration

Home > Security > ARP Inspection > VLAN Configuration

Delete	VLAN ID	Log Type

VLAN Mode Configuration

Home > Security > ARP Inspection > VLAN Configuration

Delete	VLAN ID	Log Type
Delete	1	None

Figure 13-5.2: The VLAN Mode Configuration

Parameter description:

- **VLAN Mode Configuration :**

  Specify ARP Inspection is enabled on which VLANs. First, you have to enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on VLAN mode configuration web page. The log type also can be configured on per VLAN setting.

  Possible types are:

  None: Log nothing.

  Deny: Log denied entries.

Permit: Log permitted entries.

ALL: Log all entries.

Buttons

- **Add New Entry :**

  Click to add a new VLAN to the ARP Inspection VLAN table.

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

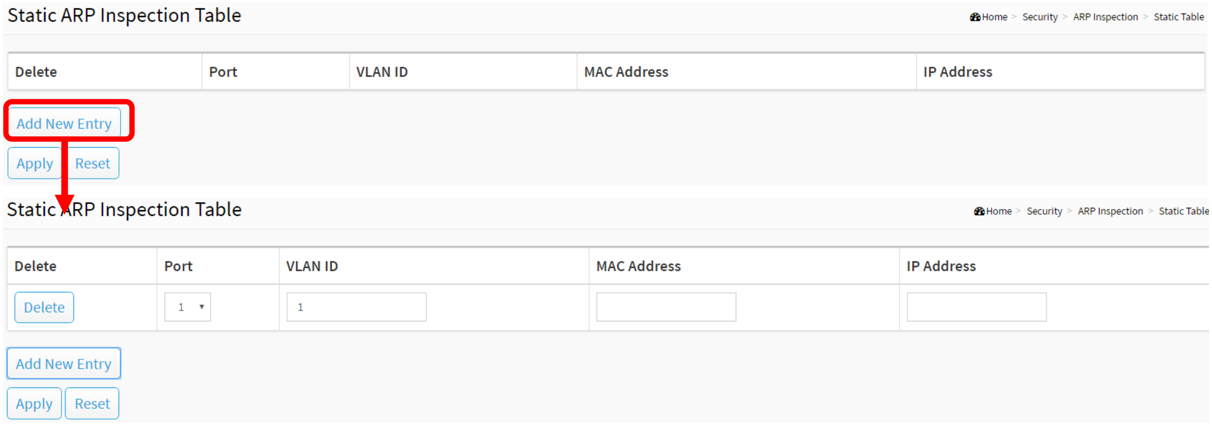
13-5.3 Static Table

The section describes to configure the Static ARP Inspection Table parameters of the switch. You could use the Static ARP Inspection Table configure to manage the ARP entries.

Web Interface

To configure a Static ARP Inspection Table Configuration in the web interface:

1. Click Security, ARP Inspection and Static Table.
2. Click “Add new entry”.
3. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
4. Click Apply.



Static ARP Inspection Table

Home > Security > ARP Inspection > Static Table

Delete	Port	VLAN ID	MAC Address	IP Address

Static ARP Inspection Table

Home > Security > ARP Inspection > Static Table

Delete	Port	VLAN ID	MAC Address	IP Address
Delete	1 ▾	1		

Figure13-5.3: The Static ARP Inspection Table

Parameter description:

- **Port :**

  The logical port for the settings.

- **VLAN ID :**

  The vlan id for the settings.

- **MAC Address :**

  Allowed Source MAC address in ARP request packets.

- **IP Address :**

  Allowed Source IP address in ARP request packets.

- **Adding new entry :**

  Click to add a new entry to the Static ARP Inspection table. Specify the Port, VLAN ID, MAC address, and IP address for the new entry. Click "Apply".

Buttons

- **Add New Entry :**

  Click to add a new VLAN to the ARP Inspection VLAN table.

- **Delete :**

  Check to delete the entry. It will be deleted during the next save.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

13-5.4 Dynamic Table

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

Navigating the ARP Inspection Table

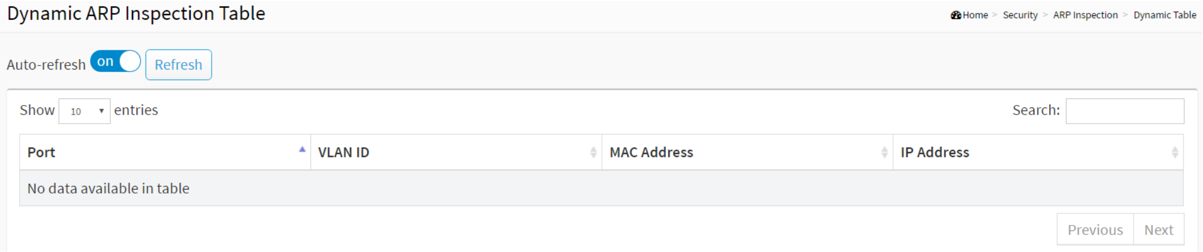
Each page shows up to many entries from the Dynamic ARP Inspection table, default being 10, selected through the "entries per page" input field. When first visited, the web page will show the first 10 entries from the beginning of the Dynamic ARP Inspection Table.

The "Search" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. It will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match.

This will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

Web Interface

To configure a Dynamic ARP Inspection Table Configuration in the web interface:



Dynamic ARP Inspection Table

Port	VLAN ID	MAC Address	IP Address
No data available in table			

Figure 13-5.4: The Dynamic ARP Inspection Table

Parameter description:

ARP Inspection Table Columns

- **Port :**

  Switch Port Number for which the entries are displayed.

- **VLAN ID :**

  VLAN-ID in which the ARP traffic is permitted.

- **MAC Address :**

  User MAC address of the entry.

- **IP Address :**

  User IP address of the entry.

- **Search :**

  You can search for the information that you want to see.

- **Show entries :**

  You can choose how many items you want to show up.

Buttons

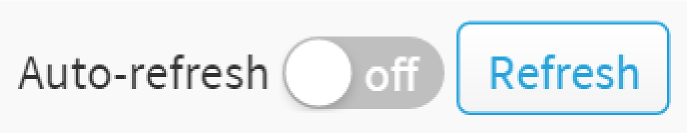


Figure 13-5.4: The Dynamic ARP Inspection Table buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

- **Next :**

  Updates the system log entries, turn to the next page.

- **Previous :**

  Updates the system log entries, turn to the previous page.

13-6 Port Security

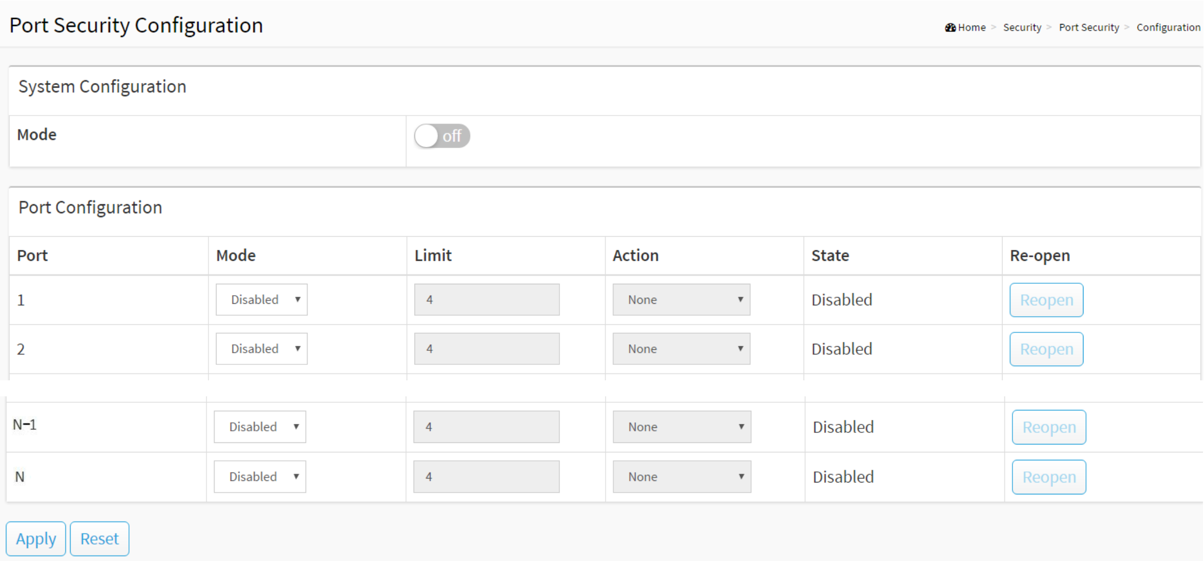
13-6.1 Configuration

This section shows you to configure the Port Security settings of the Switch. You can use the Port Security feature to restrict input to an interface by limiting and identifying MAC addresses.

Web Interface

To configure a Port Security Configuration in the web interface:

1. Click Security, Port Security and Configuration.
2. Select "Enabled" in the Mode of System Configuration.
3. Set Mode(Enabled, Disabled), Limit, Action (Trap, Shutdown, Trap & Shutdown) for each port.
4. Click the Apply to save the setting.
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



Port Security Configuration

Home > Security > Port Security > Configuration

System Configuration

Mode	off

Port Configuration

Port	Mode	Limit	Action	State	Re-open
1	Disabled	4	None	Disabled	Reopen
2	Disabled	4	None	Disabled	Reopen
N-1	Disabled	4	None	Disabled	Reopen
N	Disabled	4	None	Disabled	Reopen

Figure 13-6.1: The Port Security Configuration

Parameter description:

System Configuration

- **Mode :**

Indicates if Limit Control is globally enabled or disabled on the switch. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

Port Configuration

The table has one row for each port on the selected switch and a number of columns, which are:

- **Port :**

The port number to which the configuration below applies.

- **Mode :**

Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.

- **Limit :**

The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.
The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

- **Action :**

If Limit is reached, the switch can take one of the following actions:

None: Do not allow more than Limit MAC addresses on the port, but take no further action.

Trap: If Limit + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded.

Shutdown: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:

1) Boot the switch,

2) Disable and re-enable Limit Control on the port or the switch,

3) Click the Reopen button.

Trap & Shutdown: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the

"Shutdown" actions described above will be taken.

- **State :**

  This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values:

  Disabled: Limit Control is either globally disabled or disabled on the port.

  Ready: The limit is not yet reached. This can be shown for all actions.

  Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if Action is set to none or Trap.

  Shutdown: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown.

- **Re-open Button :**

  If a port is shut down by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to shut down in the Action section.

NOTE: That clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost

Buttons

- **Apply**

  Click to save changes.

- **Reset**

  Click to undo any changes made locally and revert to previously saved values.

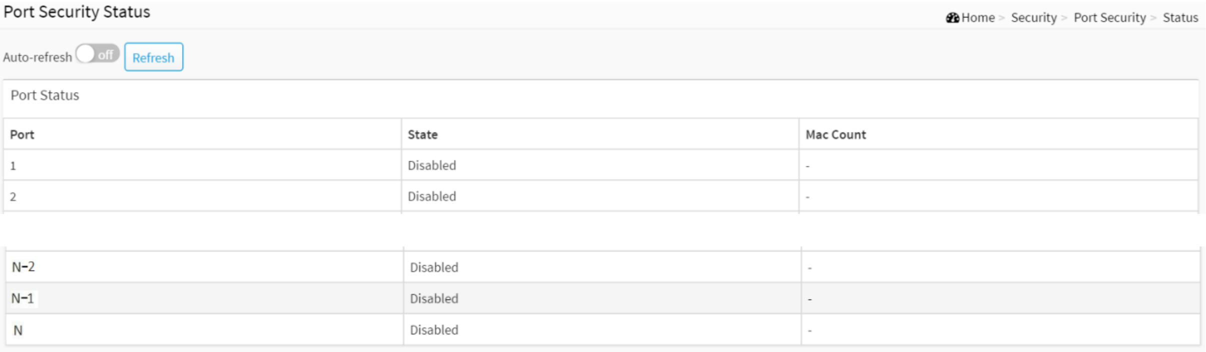
13-6.2 Status

This section shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise. The status page is divided into two sections - one with a legend of user modules and one with the actual port status.

Web Interface

To displays a Port Security Status in the web interface:

1. Click Security, Port Security and status.
2. Checked "Auto-refresh".
3. Click "Refresh" to refresh the port detailed statistics.
4. Click the port number to see the status for this particular port.



Port	State	Mac Count
1	Disabled	-
2	Disabled	-
N-2	Disabled	-
N-1	Disabled	-
N	Disabled	-

Figure 13-6.2: The Port Security Status

Parameter description:

- **Port :**

  The port number for which the status applies. Click the port number to see the status for this particular port.

- **State :**

  Shows the current state of the port. It can take one of four values:

  Disabled: No user modules are currently using the Port Security service.

  Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.

  Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.

  Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.

- **MAC Count (Current Learned) :**

  The columns indicates the number of currently learned MAC addresses (forwarding as well as blocked) and the number of MAC addresses that can be learned on the port, respectively.

  If no user modules are enabled on the port, the Current column will show a dash (-).

Buttons

Figure 13-6.2: The Port Security Status buttons

- **Auto-refresh :**

  Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

- **Refresh :**

  Click to refresh the page immediately.

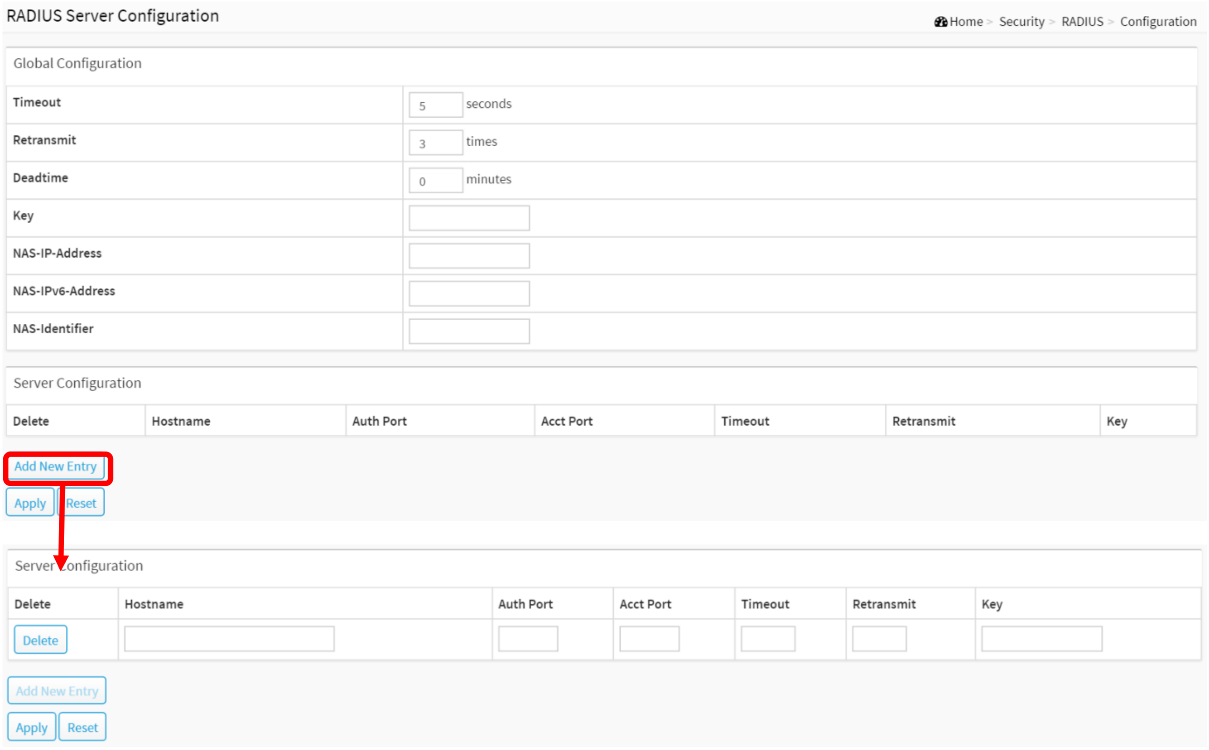
13-7 RADIUS

13-7.1 Configuration

Web Interface

To configure a RADIUS in the web interface:

1. Click Security, RADIUS and Configuration.
2. Set Timeout, Retransmit, Deadtime, Key, NAS-IP-Address, NAS IPv6-Address,NAS-Identifier.
3. Click "Add New Entry".
4. Set Hostname, Auth Port, Acct Port, Timeout, Retransmit, Key.
5. Click the Apply to save the setting.
6. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.



RADIUS Server Configuration

Home > Security > RADIUS > Configuration

Global Configuration

Timeout	5 seconds
Retransmit	3 times
Deadtime	0 minutes
Key	
NAS-IP-Address	
NAS-IPv6-Address	
NAS-Identifier	

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key

Add New Entry

Apply Reset

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
Delete						

Add New Entry

Apply Reset

Figure 13-7.1: The RADIUS Configuration

Parameter description:

Global Configuration

These setting are common for all of the RADIUS servers.

- **Timeout :**

  Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.

- **Retransmit :**

  Retransmit is the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.

- **Deadtime :**

  Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.
  Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

- **Key :**

  The secret key - up to 63 characters long - shared between the RADIUS server and the switch.

- **NAS-IP-Address :**

  The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

- **NAS-IPv6-Address :**

  The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

- **NAS-Identifier :**

  The identifier - up to 255 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.

Server Configuration

The table has one row for each RADIUS server and a number of columns, which are:

- **Delete :**

To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.

- **Hostname :**

  The IP address or hostname of the RADIUS server.

- **Auth Port :**

  The UDP port to use on the RADIUS server for authentication.

- **Acct Port :**

  The UDP port to use on the RADIUS server for accounting.

- **Timeout :**

  This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

- **Retransmit :**

  This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.

- **Key :**

  This optional setting overrides the global key. Leaving it blank will use the global key.

Buttons

- **Adding New Server Entry :**

  Click to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported.
  The button can be used to undo the addition of the new server.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

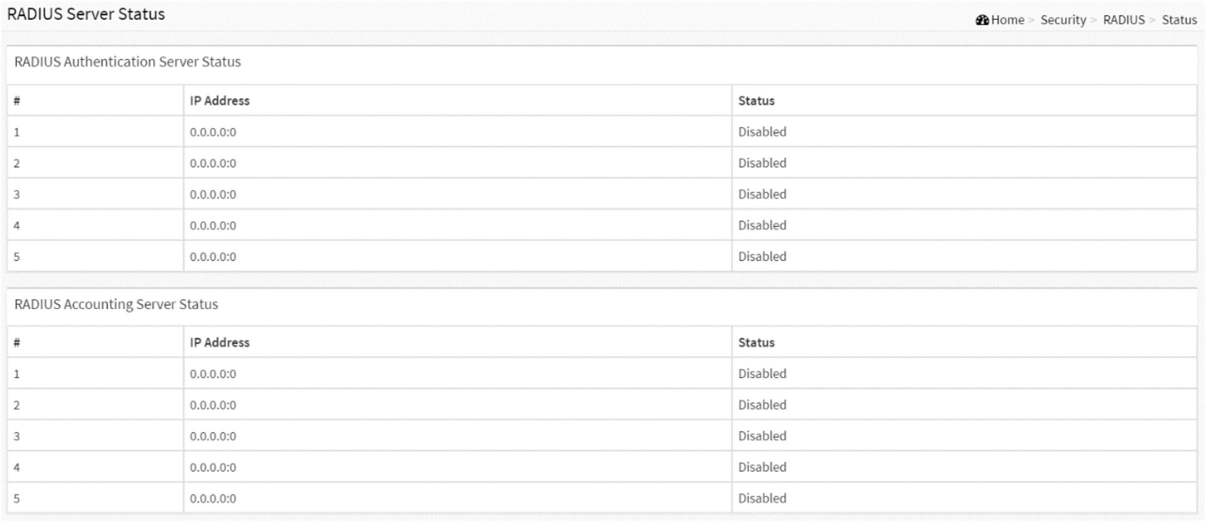
13-7.2 Status

This section shows you an overview/detail of the RADIUS Authentication and Accounting servers' status to ensure the function is workable.

Web Interface

To display a RADIUS Status in the web interface:

1. Click Security, RADIUS and Status.
2. Select server to display the detail statistics for a particular RADIUS



RADIUS Server Status

RADIUS Authentication Server Status

#	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

#	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

Figure 13-7.2: The RADIUS Server Status Overview

Parameter description:

RADIUS Authentication Server Status

- **# :**

  The RADIUS server number. Click to navigate to detailed statistics for this server.

- **IP Address :**

  The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

- **State :**

  The current state of the server. This field takes one of the following values:

  - **Disabled :**

    The server is disabled.

  - **Not Ready :**

    The server is enabled, but IP communication is not yet up and running.

  - **Ready :**

    The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

  - **Dead (X seconds left) :**

    Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

RADIUS Accounting Server Status

- **# :**

  The RADIUS server number. Click to navigate to detailed statistics for this server.

- **IP Address :**

  The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

- **State :**

  The current state of the server. This field takes one of the following values:

  - **Disabled:**

    The server is disabled.

  - **Not Ready:**

    The server is enabled, but IP communication is not yet up and running.

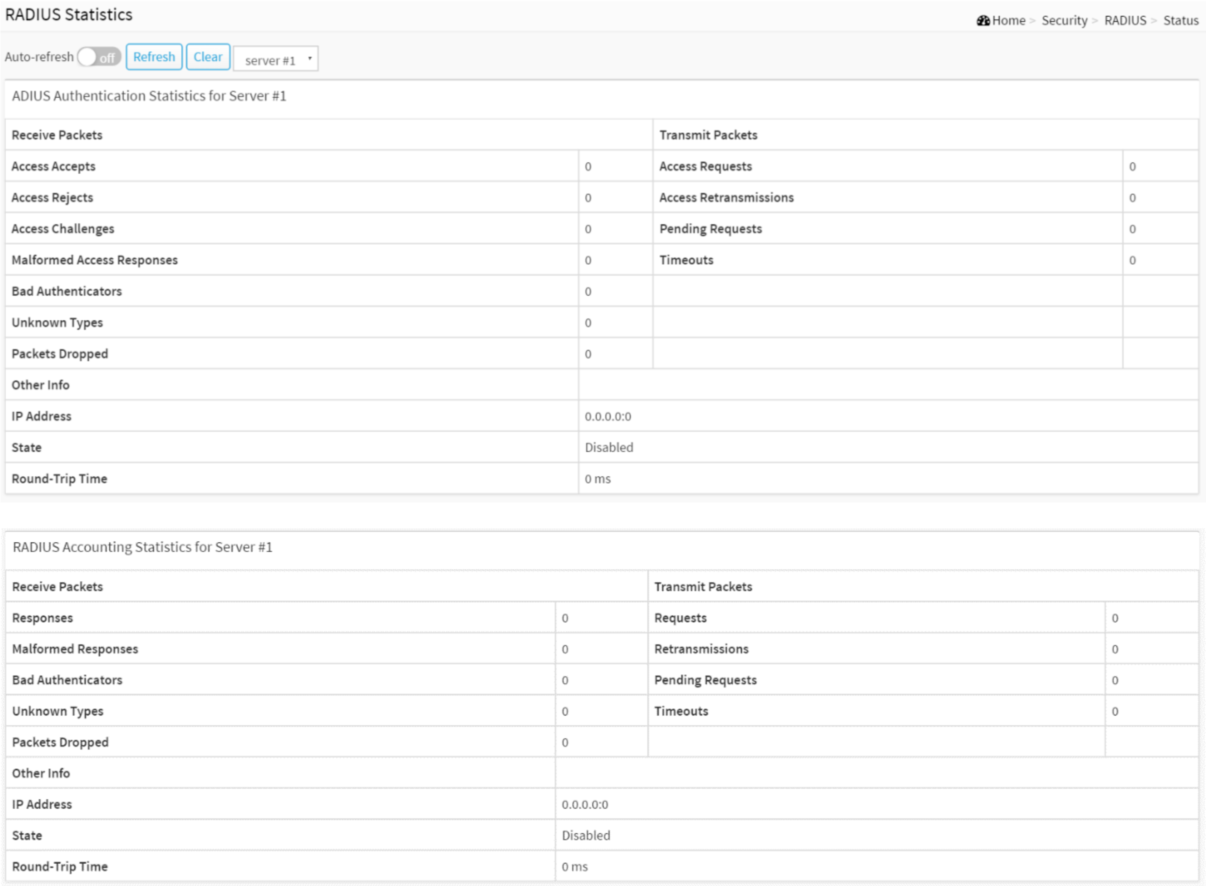
  - **Ready:**

    The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.

- **Dead (X seconds left):**

  Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

- **If you select Server#1 to display RADIUS Statistics**



ADIUS Authentication Statistics for 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		

Figure 13-7.2: The RADIUS Statistics Server

Parameter description:

- **server :**

  You can select which server that you want to display RADIUS.

RADIUS Authentication Statistics for Server #1

The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB. Use the server select box to switch between the backend servers to show details for.

- **Access Accepts :**

  The number of RADIUS Access-Accept packets (valid or invalid) received from the server.

- **Access Rejects :**

  The number of RADIUS Access-Reject packets (valid or invalid) received from the server.

- **Access Challenges :**

  The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.

- **Malformed Access Responses :**

  The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.

- **Bad Authenticators :**

  The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.

- **Unknown Types :**

  The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.

- **Packets Dropped :**

  The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.

- **Access Requests :**

  The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.

- **Access Retransmissions :**

  The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.

- **Pending Requests :**

The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.

- **Timeouts :**

  The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

- **IP Address :**

  IP address and UDP port for the authentication server in question.

- **State :**

  Shows the state of the server. It takes one of the following values:

  - **Disabled :**

    The selected server is disabled.

  - **Not Ready :**

    The server is enabled, but IP communication is not yet up and running.

  - **Ready :**

    The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

  - **Dead (X seconds left) :**

    Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

- **Round-Trip Time :**

  The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

RADIUS Accounting Statistics for Server #1

The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB.
Use the server select box to switch between the backend servers to show details for.

- **Responses :**

  The number of RADIUS packets (valid or invalid) received from the server.

- **Malformed Responses :**

  The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.

- **Bad Authenticators :**

  The number of RADIUS packets containing invalid authenticators received from the server.

- **Unknown Types :**

  The number of RADIUS packets of unknown types that were received from the server on the accounting port.

- **Packets Dropped :**

  The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.

- **Requests :**

  The number of RADIUS packets sent to the server. This does not include retransmissions

- **Retransmissions :**

  The number of RADIUS packets retransmitted to the RADIUS accounting server.

- **Pending Requests :**

  The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.

- **Timeouts :**

  The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

- **IP Address :**

  IP address and UDP port for the accounting server in question.

- **State :**

  Shows the state of the server. It takes one of the following values:

  - **Disabled :**

    The selected server is disabled.

  - **Not Ready :**

    The server is enabled, but IP communication is not yet up and running.

  - **Ready :**

    The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.

  - **Dead (X seconds left) :**

    Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

- **Round-Trip Time :**

  The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

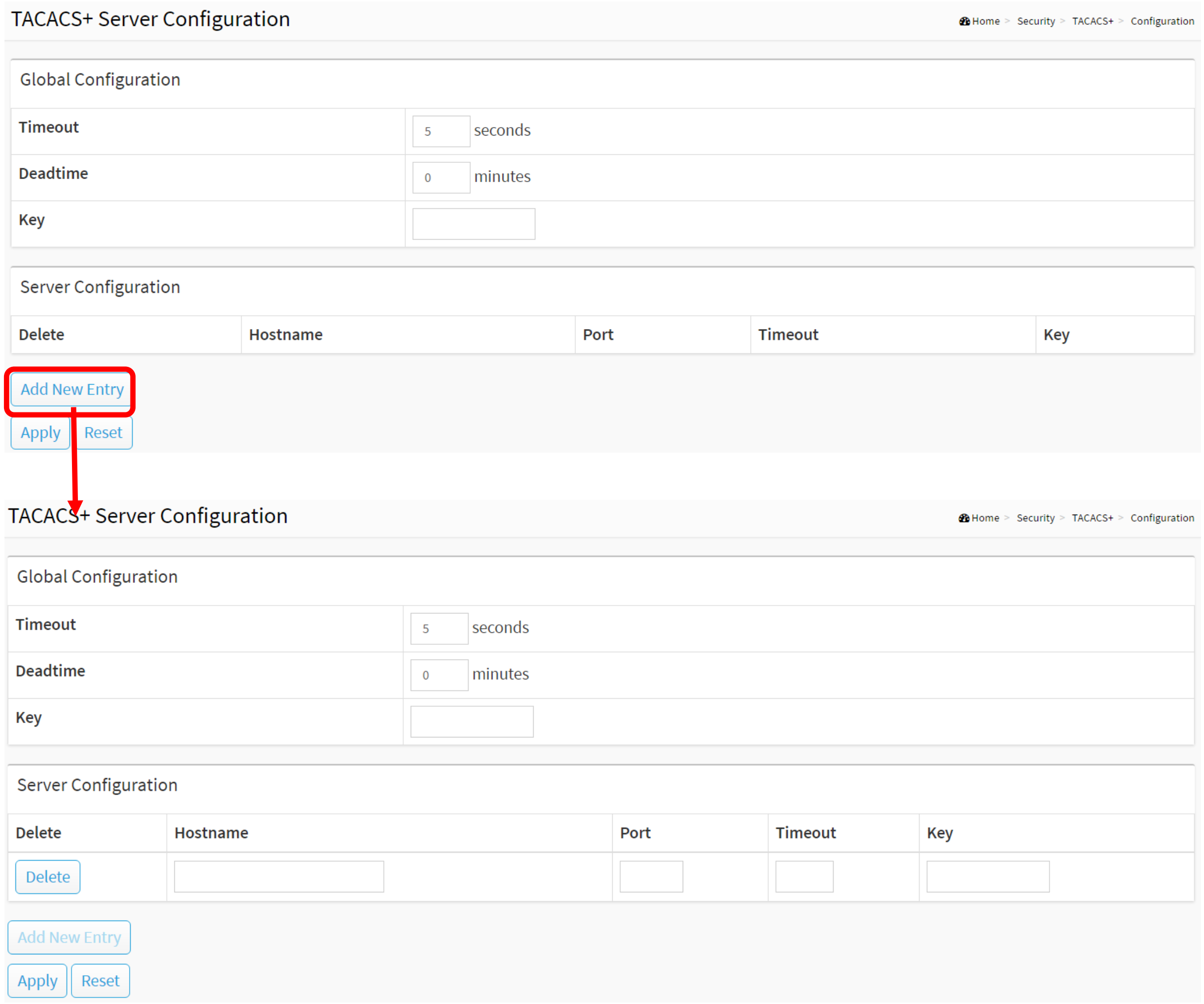
13-8 TACACS+

13-8.1 Configuration

Web Interface

To configure the TACACS+ servers in the web interface:

1. Click Security and TACACS+.
2. Click "Add New Entry".
3. Specify the Timeout, Deadtime, Key.
4. Specify the Hostname, Port, Timeout and Key in the server.
5. Click Apply.



TACACS+ Server Configuration

Home > Security > TACACS+ > Configuration

Global Configuration

Timeout	5 seconds
Deadtime	0 minutes
Key	

Server Configuration

Delete	Hostname	Port	Timeout	Key

Add New Entry
Apply
Reset

TACACS+ Server Configuration

Home > Security > TACACS+ > Configuration

Global Configuration

Timeout	5 seconds
Deadtime	0 minutes
Key	

Server Configuration

Delete	Hostname	Port	Timeout	Key
Delete				

Add New Entry
Apply
Reset

Figure 13-8.1: The TACACS+ Server Configuration

Parameter description:

Global Configuration

These setting are common for all of the TACACS+ servers.

- **Timeout :**

  Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead.

- **Deadtime :**

  Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.
  Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

- **Key :**

  The secret key - up to 63 characters long - shared between the TACACS+ server and the switch.

Server Configuration

The table has one row for each TACACS+ server and a number of columns, which are:

- **Delete :**

  To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save.

- **Hostname :**

  The IP address or hostname of the TACACS+ server.

- **Port :**

  The TCP port to use on the TACACS+ server for authentication.

- **Timeout :**

  This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

- **Key :**

  This optional setting overrides the global key. Leaving it blank will use the global key.

Buttons

- **Delete :**

  This button can be used to undo the addition of the new server.

- **Add New Server :**

  Click to add a new TACACS+ server. An empty row is added to the table, and the TACACS+ server can be configured as needed. Up to 5 servers are supported.

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

Chapter 14 Access Control

14-1 Access Control List

The section describes how to configure Access Control List rule. An Access Control List (ACL) is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the frame is accepted. Other actions can also be invoked when a matching packet is found, including rate limiting, copying matching packets to another port or to the system log, or shutting down a port.

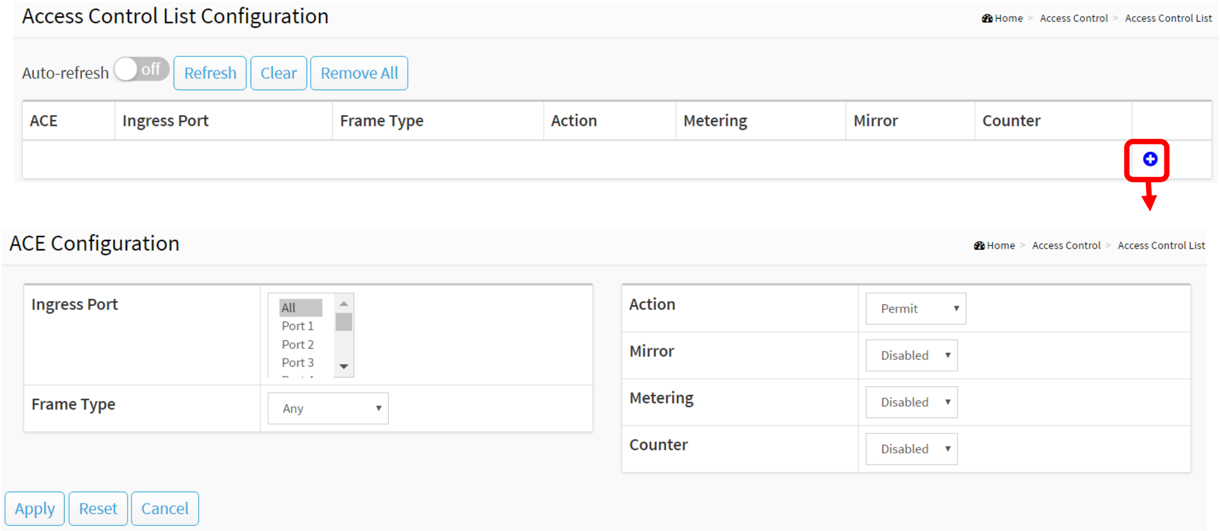
This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 256 on each switch. Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed the priority is highest.

Web Interface

To configure Access Control List in the web interface:

1. Click Access Control and Access Control List.
2. Click the ⊕ button to add a new ACL, or use the other ACL.
3. modification buttons to specify the editing action (i.e., edit, delete, or moving the relative position of entry in the list).
4. To specific the parameter of the ACE.
5. Click Apply.
6. If you want to cancel the setting then you need to click the reset button. It will revert to previously saved values.

7. When editing an entry on the ACE Configuration page, note that the Items displayed depend on various selections, such as Frame Type and IP Protocol Type. Specify the relevant criteria to be matched for this rule, and set the actions to take when a rule is matched.



Access Control List Configuration

Home > Access Control > Access Control List

Auto-refresh off Refresh Clear Remove All

ACE	Ingress Port	Frame Type	Action	Metering	Mirror	Counter	
							⊕

ACE Configuration

Home > Access Control > Access Control List

Ingress Port	All Port 1 Port 2 Port 3
Frame Type	Any

Action	Permit
Mirror	Disabled
Metering	Disabled
Counter	Disabled

Apply Reset Cancel

Figure 14-1: The Access Control List Configuration & ACE Configuration

Parameter description:

- **ACE :**

  The ACE number for the Access Control List.

- **Ingress Port :**

  Indicates the ingress port of the ACE.

- **Frame Type :**

  Indicates the frame type of the ACE. Possible values are:

  Any: The ACE will match any frame type.

  Ethernet Type: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.

  IPv4: The ACE will match all IPv4 frames.

- **Action :**

  Indicates the forwarding action of the ACE.

  Permit: Frames matching the ACE may be forwarded and learned.

Deny: Frames matching the ACE are dropped.

Shutdown: Specify the port shut down operation of the ACE.

- **Metering :**

  Select metering mode, enable or disable.

- **Mirror:**

  Select mirror mode, enable or disable.

- **Counter :**

  The counter indicates the number of times the ACE was hit by a frame.

  Modification Buttons

  You can modify each ACE (Access Control Entry) in the table using the following buttons:

  ⊕ : Inserts a new ACE before the current row.

  ✎ : Edits the ACE row.

  ⊗ : Deletes the ACE.

  ⊕ : The lowest plus sign adds a new entry at the bottom of the ACE listings.

ACE Configuration

An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type selected.

A frame that hits this ACE matches the configuration that is defined here.

- **Ingress Port :**

  Select the ingress port for which this ACE applies.
  All: The ACE applies to all port.
  Port n: The ACE applies to this port number, where n is the number of the switch port.

- **Frame Type :**

  Select the frame type for this ACE. These frame types are mutually exclusive.
  Any: Any frame can match this ACE.

Ethernet Type: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal).

IPv4: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type.

- **Action :**

Specify the action to take with a frame that hits this ACE.

Permit: The frame that hits this ACE is granted permission for the ACE operation.

Deny: The frame that hits this ACE is dropped.

Shutdown : Specify the port shut down operation of the ACE.

Note: The shutdown feature only works when the packet length is less than 1518(without VLAN tags).

- **Metering :**

Select metering mode, enable or disable.

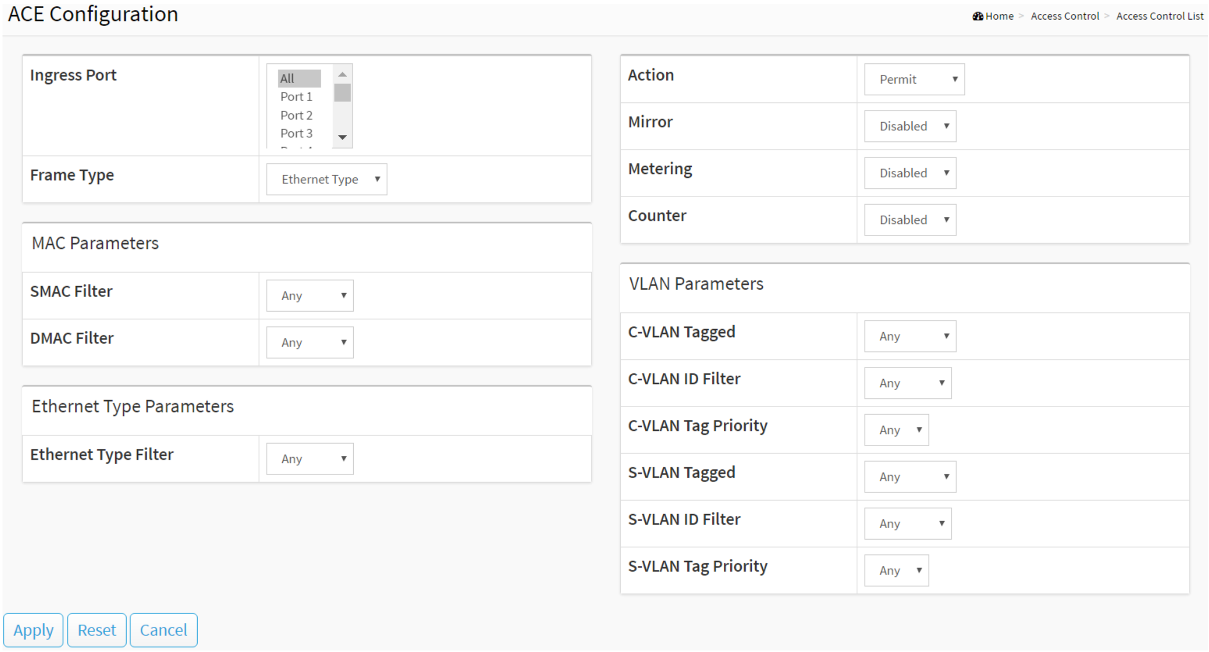
- **Mirror:**

Select mirror mode, enable or disable.

- **Counter :**

The counter indicates the number of times the ACE was hit by a frame.

■ Select Frame Type to Ethernet Type:



ACE Configuration

Ingress Port	All Port 1 Port 2 Port 3
Frame Type	Ethernet Type

MAC Parameters

SMAC Filter	Any
DMAC Filter	Any

Ethernet Type Parameters

Ethernet Type Filter	Any

Action	Permit
Mirror	Disabled
Metering	Disabled
Counter	Disabled

VLAN Parameters

C-VLAN Tagged	Any
C-VLAN ID Filter	Any
C-VLAN Tag Priority	Any
S-VLAN Tagged	Any
S-VLAN ID Filter	Any
S-VLAN Tag Priority	Any

Figure 14-1: The ACE Configuration (Select Frame Type to Ethernet Type)

MAC Parameters

- **SMAC Filter :**

Specify the destination MAC filter for this ACE.

Any: No SMAC filter is specified. (SMAC filter status is "don't-care".)

Specific: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a SMAC value appears.

- **DMAC Filter :**

Specify the destination MAC filter for this ACE.

Any: No DMAC filter is specified. (DMAC filter status is "don't-care".)

MC: Frame must be multicast.

BC: Frame must be broadcast.

UC: Frame must be unicast.

Specific: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.

Ethernet Type Parameters

- **Ethernet Type Filter :**

Specify the destination Ethernet Type filter for this ACE.

Any: No Ethernet Type filter is specified. (Ethernet Type filter status is "don't-care".)

Specific: If you want to filter a specific destination Ethernet Type with this ACE, choose this value. A field for entering a Ethernet Type value appears.

VLAN Parameters

- **C-VLAN Tagged :**

Indicates tag type. Possible values are:
Any: Match tagged and untagged frames.
Enable: Match C-VLAN Tagged frames.
Disable: disable C-VLAN Tagged frames.

- **C-VLAN ID Filter :**

  Specify the C-VLAN ID filter for this ACE.
  Any: No C-VLAN ID filter is specified. (C-VLAN ID filter status is "don't-care".)
  Specific: If you want to filter a specific C-VLAN ID with this ACE, choose this value. A field for entering a C-VLAN ID number appears.

- **C-VLAN Tag Priority :**

  Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7 or range 0-1, 2-3, 4-5, 6-7, 0-3 and 4-7. The value any means that no tag priority is specified (tag priority is "don't-care".)

- **S-VLAN Tagged :**

  Indicates tag type. Possible values are:
  Any: Match tagged and untagged frames.
  Enable: Match S-VLAN Tagged frames.
  Disable: disable S-VLAN Tagged frames.

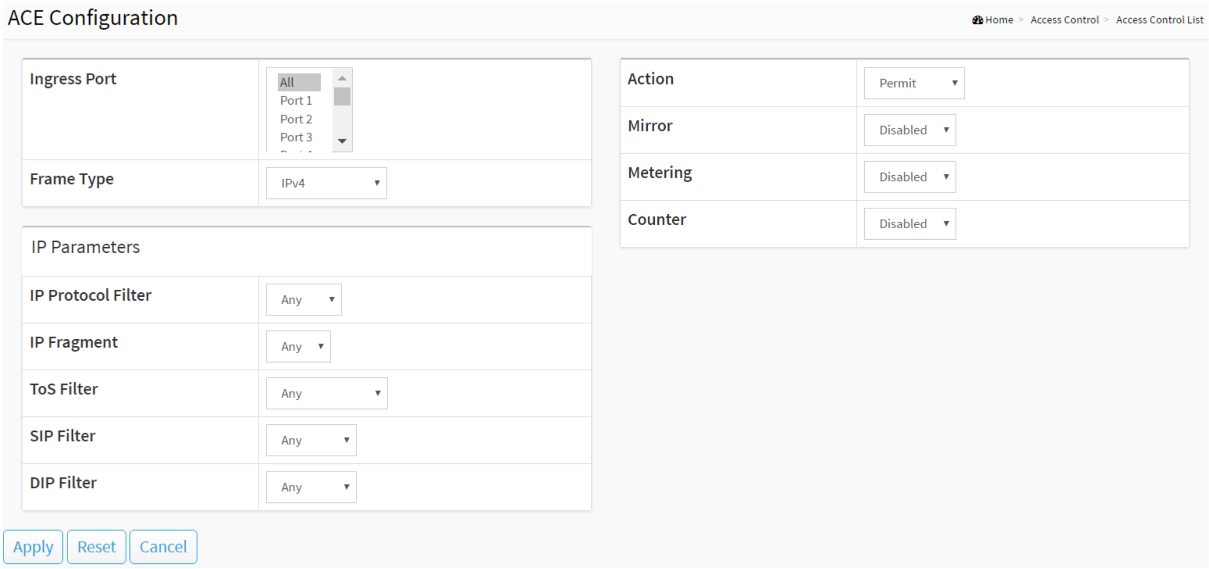
- **S-VLAN ID Filter :**

  Specify the S-VLAN ID filter for this ACE.
  Any: No S-VLAN ID filter is specified. (S-VLAN ID filter status is "don't-care".)
  Specific: If you want to filter a specific S-VLAN ID with this ACE, choose this value. A field for entering a S-VLAN ID number appears.

- **S-VLAN Tag Priority :**

  Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7 or range 0-1, 2-3, 4-5, 6-7, 0-3 and 4-7. The value any means that no tag priority is specified (tag priority is "don't-care".)

- Select Frame Type to IPv4:



ACE Configuration

Home > Access Control > Access Control List

Ingress Port	All Port 1 Port 2 Port 3
Frame Type	IPv4

Action	Permit
Mirror	Disabled
Metering	Disabled
Counter	Disabled

IP Parameters

IP Protocol Filter	Any
IP Fragment	Any
ToS Filter	Any
SIP Filter	Any
DIP Filter	Any

Figure 14-1: The ACE Configuration (Select Frame Type to Ipv4)

IP Parameters

- **IP Protocol Filter :**

  Any: The ACE will match any frame type.

  ICMP: The ACE will match IPv4 frames with ICMP protocol.

  UDP: The ACE will match IPv4 frames with UDP protocol.

  TCP: The ACE will match IPv4 frames with TCP protocol.

  Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.

- **IP Fragment :**

  IP Fragment IPv4 frame fragmented option: yes, no, any.

- **ToS Filter :**

  ToS Filter option: Any,DSCP, IP Precedence.

- **SIP Filter :**

  SIP Filte option: Any, Host, Network.

- **DIP Filter :**

  DIP Filte option: Any, Host, Network

Buttons

- **Apply :**

Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

- **Auto-refresh :**

  To evoke the auto-refresh to refresh the information automatically.

- **Refresh, clear, Remove All :**

  You can click them for refresh the ACL configuration or clear them by manual. Others remove all to clean up all ACL configurations on the table.

- **Cancel :**

  Return to the previous page.

Chapter 15 Event Notification

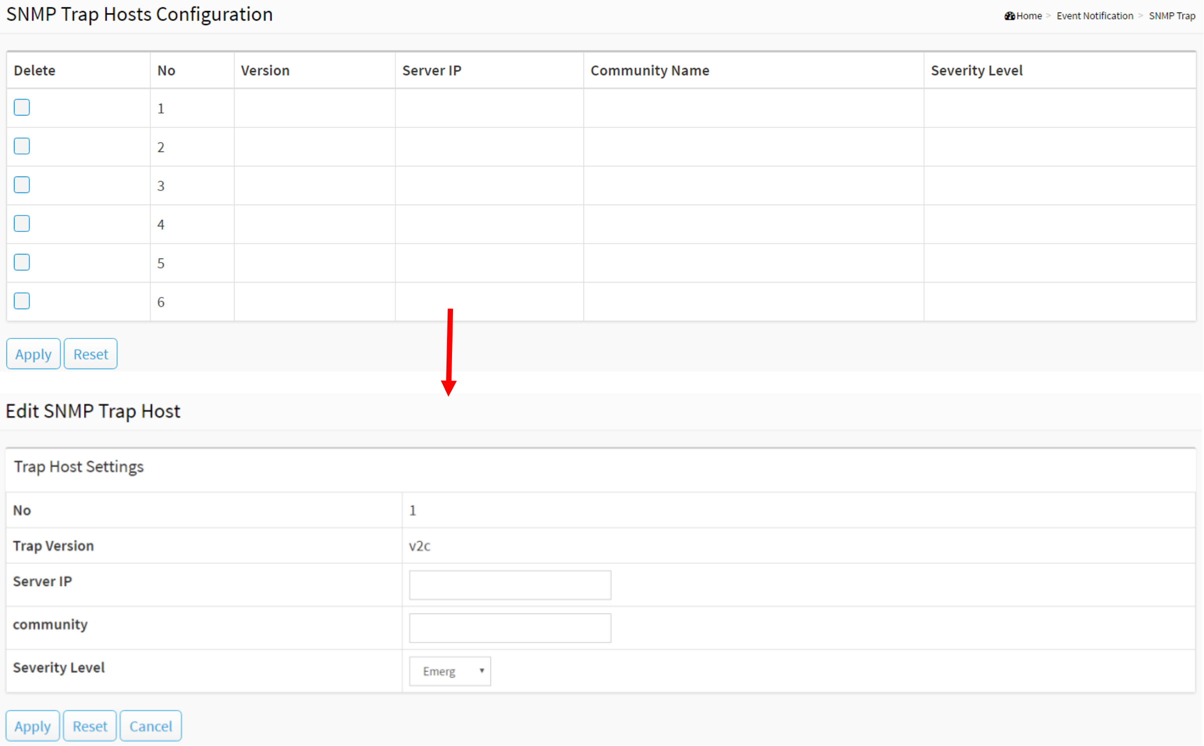
15-1 SNMP Trap

Configure Trap on this page.

Web Interface

To configure SNMP Trap Configuration in the web interface:

1. Click Event Notification and SNMP Trap.
2. Click any entry then you can create new SNMP Trap on the switch.
3. Specify Server IP Community, Severity Level.
4. Click Apply



SNMP Trap Hosts Configuration

Delete	No	Version	Server IP	Community Name	Severity Level
□	1				
□	2				
□	3				
□	4				
□	5				
□	6				

Edit SNMP Trap Host

Trap Host Settings

No	1
Trap Version	v2c
Server IP	
community	
Severity Level	Emerg

Figure 15-1: The SNMP Trap Configuration

Parameter description:

- **No :**

  The index of the trap host entry.

- **Version :**

  Indicates the SNMP trap supported version. Possible versions are:
  SNMP v2c: Set SNMP trap supported version 2c.

- **Server IP :**

  This is the IP of the trap host.

- **Community Name :**

  Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 33 to 126.

- **Severity Level :**

  Indicates what kind of message will send to trap server. Possible modes are:
  Emerg: System is unusable.
  Alert: Action must be taken immediately.
  Crit: Critical conditions.
  Error: Error conditions.
  Warning: Warning conditions.
  Notice: Normal but significant conditions.
  Info: Information messages.
  Debug: Debug-level messages.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

Chapter 16 Diagnostics

This chapter provides a set of basic system diagnosis. These includes Ping, Traceroute, Cable Diagnostics and port mirror.

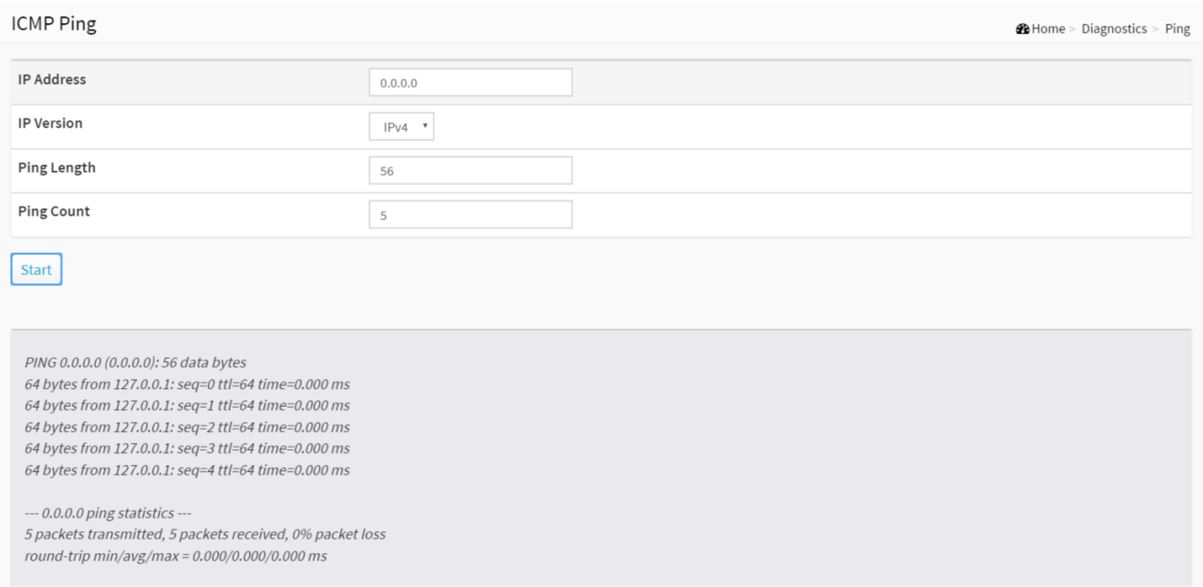
16-1 Ping

This section allows you to issue ICMP Echo packets to troubleshoot Ipv4/6 connectivity issues.

Web Interface

To configure a PING in the web interface:

1. Click Diagnostics and Ping.
2. Specify IP Address, IP Version, Ping Length and Ping Count.
3. Click Start.



ICMP Ping

IP Address	0.0.0.0
IP Version	IPv4
Ping Length	56
Ping Count	5

```
PING 0.0.0.0 (0.0.0.0): 56 data bytes
64 bytes from 127.0.0.1: seq=0 ttl=64 time=0.000 ms
64 bytes from 127.0.0.1: seq=1 ttl=64 time=0.000 ms
64 bytes from 127.0.0.1: seq=2 ttl=64 time=0.000 ms
64 bytes from 127.0.0.1: seq=3 ttl=64 time=0.000 ms
64 bytes from 127.0.0.1: seq=4 ttl=64 time=0.000 ms

--- 0.0.0.0 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.000/0.000/0.000 ms
```

Figure 16-1: The ICMP Ping

Parameter description:

- **IP Address :**

  To specify the target IP Address of the Ping.

- **IP Version :**

  To select the IP Version.

- **Ping Length :**

  The payload size of the ICMP packet. Values range from 1 bytes to 1452 bytes.

- **Ping Count :**

  The count of the ICMP packet. Values range from 1 time to 60 times.

- **Start:**

  Click the "Start" button to start to ping the target IP Address.

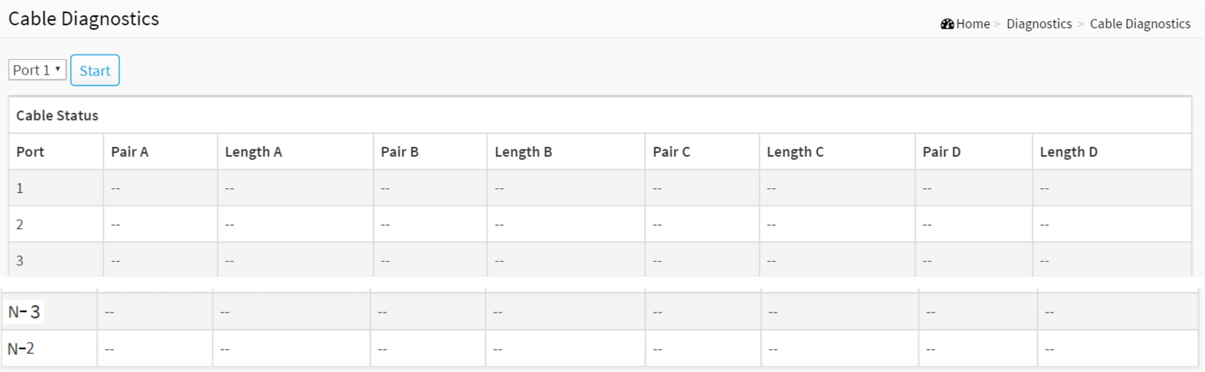
16-2 Cable Diagnostics

This section shows how to run Cable Diagnostics for copper ports.

Web Interface

To configure a Cable Diagnostics Configuration in the web interface:

1. Click Diagnostics and Cable Diagnostics.
2. Specify Port which want to check.
3. Click Start.



Cable Status

Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--
N-3	--	--	--	--	--	--	--	--
N-2	--	--	--	--	--	--	--	--

Figure 16-2: The Cable Diagnostics

Parameter description:

- **Port :**

  The port where you are requesting Cable Diagnostics.

Cable Status

- **Port :**

  Port number.

- **Pair :**

  The status of the cable pair.

- **Length :**

  The length (in meters) of the cable pair.

Button

- **Start :**

  Start to cable diagnostics the port that you selected.

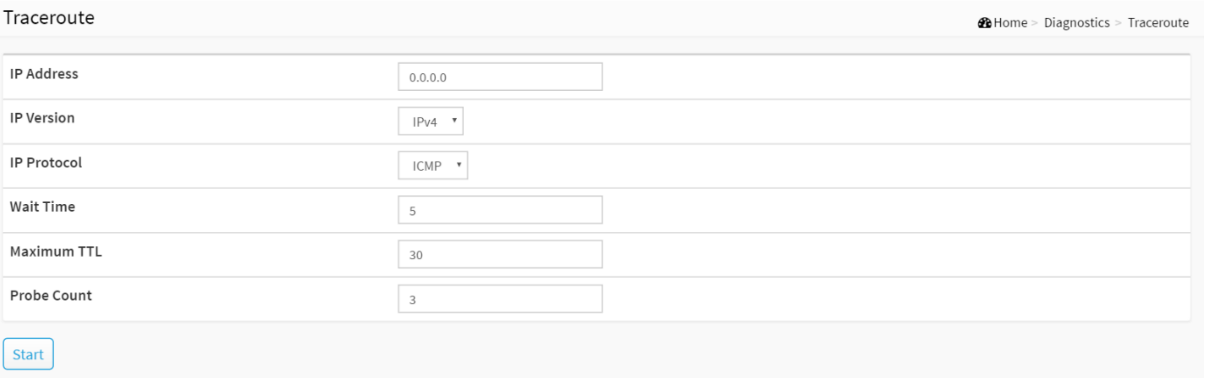
16-3 Traceroute

This page allows you to issue ICMP, TCP, or UDP packets to diagnose network connectivity issues.

Web Interface

To start a Traceroute in the web interface:

1. Click Diagnostics and Traceroute.
2. Specify IP Address, IP Version, IP Protocol, traceroute Size.
3. Click Start.



Traceroute

Home > Diagnostics > Traceroute

IP Address	0.0.0.0
IP Version	IPv4
IP Protocol	ICMP
Wait Time	5
Maximum TTL	30
Probe Count	3

Figure 16-3: The Traceroute

Parameter description:

- **IP Address :**

  The destination IP Address.

- **IP Version :**

  To set the IP Version what you want.

- **Protocol :**

  The protocol(ICMP, UDP, TCP) packets to send.

- **Wait Time :**

Set the time (in seconds) to wait for a response to a probe (default 5.0 sec). Values range from 1 to 60.

- **Maximum TTL :**

  Specifies the maximum number of hops (max time-to-live value) traceroute will probe. Values range from 1 to 255. The default is 30.

- **Probe Count :**

  Sets the number of probe packets per hop. Values range from 1 to 10. The default is 3.

16-4 Mirror

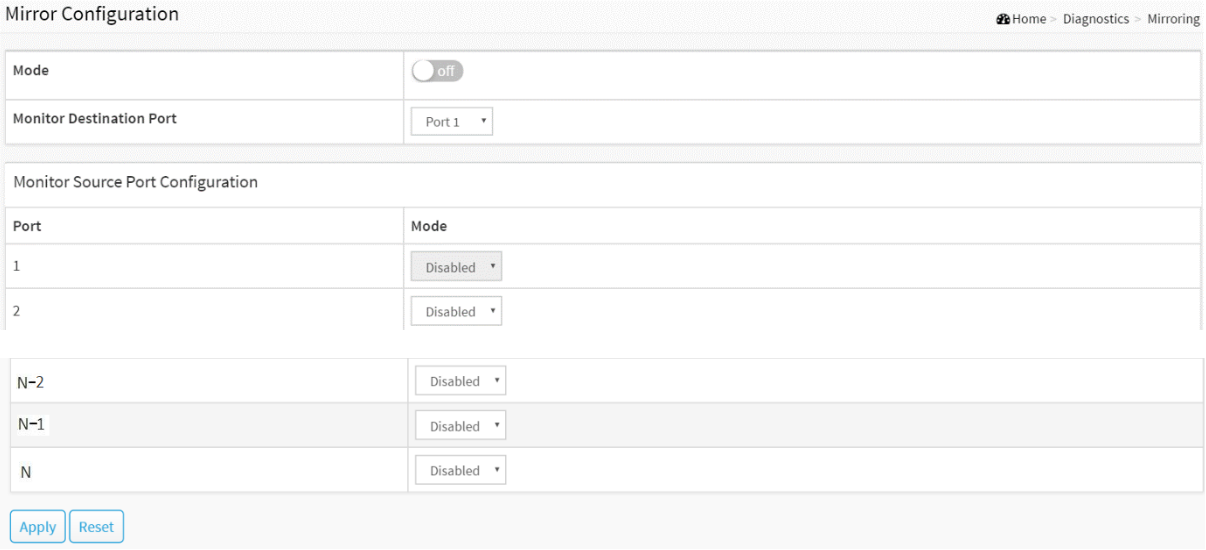
You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Mirror Configuration is to monitor the traffic of the network. For example, we assume that Port A and Port B are Monitoring Port and Monitored Port respectively, thus, the traffic received by Port B will be copied to Port A for monitoring.

Web Interface

To configure the Port Mirror function in the web interface:

1. Click Diagnostics and Mirroring.
2. Select the Monitor Destination Port (Mirror Port).
3. Select mode (disabled, enable, TX Only and RX only) for each monitored port.
4. Click the Apply button to save the setting.
5. If you want to cancel the setting then you need to click the Reset button to revert to previously saved values.



Mirror Configuration

Home > Diagnostics > Mirroring

Mode	off
Monitor Destination Port	Port 1

Monitor Source Port Configuration

Port	Mode
1	Disabled
2	Disabled
N-2	Disabled
N-1	Disabled
N	Disabled

Figure 16-4: The Mirror Configuration

Parameter description:

- **Mode :**

  Indicates the Mirror mode operation. Possible modes are:

  on: Enable Mirror mode operation.

  off: Disable Mirror mode operation.

- **Monitor Destination Port :**

  Port to output the mirrored traffic. Also known as the mirror port. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port.

Mirror Source Port Configuration

The following table is used for Rx and Tx enabling.

- **Port :**

  The logical port for the settings contained in the same row.

- **Mode :**

  Select mirror mode.

  Rx only : Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored.

  Tx only : Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored.

  Disabled : neither frames transmitted nor frames received are mirrored.

  Enabled : Frames received and frames transmitted are mirrored on the mirror port.

Buttons

- **Apply :**

  Click to save changes.

- **Reset :**

  Click to undo any changes made locally and revert to previously saved values.

Chapter 17 Maintenance

This chapter describes the entire Maintenance configuration tasks including Save/Backup/Restore/Activate/Delete Restart Device, Factory Defaults, Firmware upgrade.

17-1 Configuration

The switch stores its configuration in a number of files in text format. The files are either virtual (RAM-based) or stored in flash on the switch.

There are three system files:

- running-config: A virtual file that represents the currently active configuration on the switch. This file is volatile.
- startup-config: The startup configuration for the switch, read at boot time.
- default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

17-1.1 Save startup-config

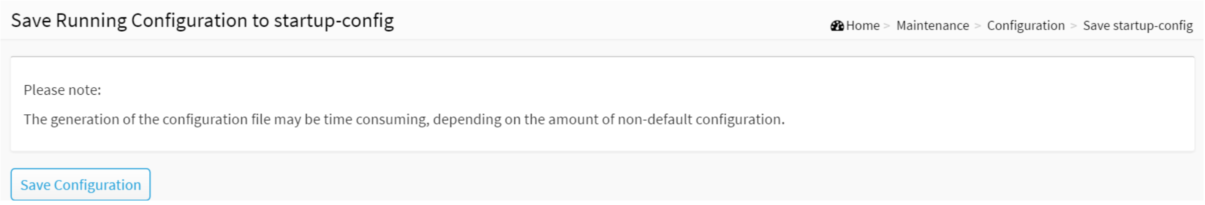
This copy running-config to startup-config, thereby ensuring that the current active configuration will be used at the next reboot.

Web Interface

To save running configuration in the web interface:

1. Click Maintenance, Configuration and Save startup-config.

2. Click Save Configuration.



Save Running Configuration to startup-config

Please note:

The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

Figure 17-1.1: The Save Startup Configuration

Parameter description:

Button

- **Save Configuration :**

Click to save configuration, the running configuration will be written to flash memory for system boot up to load this startup configuration file.

17-1.2 Backup

This section describes how to export the Switch Configuration for maintenance needs. Any current configuration files will be exported as text format.

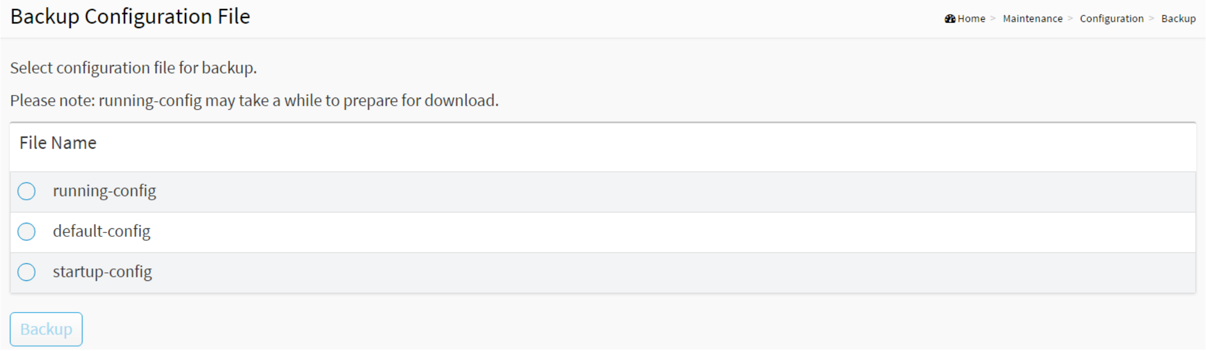
The configuration files on the switch can be backed up and saved on the station running the web browser.

It is possible to transfer any of the files on the switch to the web browser. Select the running-config may take a little while to complete, as the file must be prepared before backup.

Web Interface

To backup configuration in the web interface:

1. Click Maintenance, Configuration and Backup.
2. Click Backup.


Backup Configuration File

Select configuration file for backup.

Please note: running-config may take a while to prepare for download.

File Name
○ running-config
○ default-config
○ startup-config

Figure 17-1.2: Backup

Parameter description:

- **running-config :**

  A virtual file that represents the currently active configuration on the switch. This file is volatile.

- **startup-config :**

  The startup configuration for the switch, read at boot time.

- **default-config :**

  A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

Button

- **Backup :**

  Click the "Backup" button then the switch will start to transfer the configuration file to your workstation.

17-1.3 Restore

It is possible to import a file from the web browser to all the files on the switch, except default-config, which is read-only.

Select the source file to restore, and select the destination file on the target.

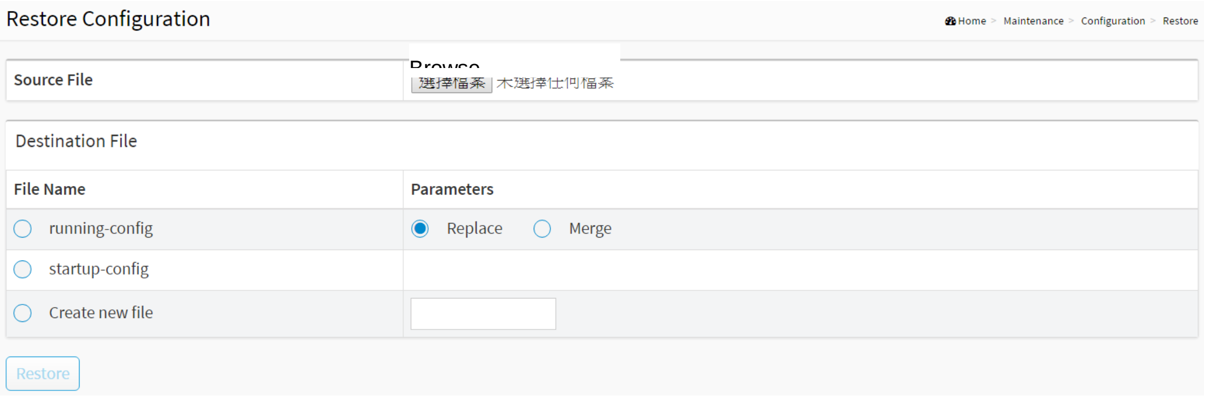
If the destination is running-config, the file will be applied to the switch configuration. This can be done in two ways:

- Replace mode: The current configuration is fully replaced with the configuration specified in the source file.
- Merge mode: The source file configuration is merged into running-config.

Web Interface

To restore configuration in the web interface:

1. Click Maintenance, Configuration and Restore.
2. Click Restore.



Restore Configuration

Source File	選擇檔案 未選擇任何檔案

Destination File

File Name	Parameters
○ running-config	● Replace ○ Merge
○ startup-config	
○ Create new file	

Figure 17-1.3: Restore Config

There are three system files:

1. running-config: A virtual file that represents the currently active configuration on the switch. This file is volatile.

2. startup-config: The startup configuration for the switch, read at boot time.

Parameter description:

Buttons

- **Browse :**

  Click the "browse." button to search the configuration text file and filename

- **Restore :**

  Click the "Restore" button to start transfer the source file to the destination file.

17-1.4 Activate config

It is possible to activate any of the configuration files present on the switch, except for running-config which represents the currently active configuration.

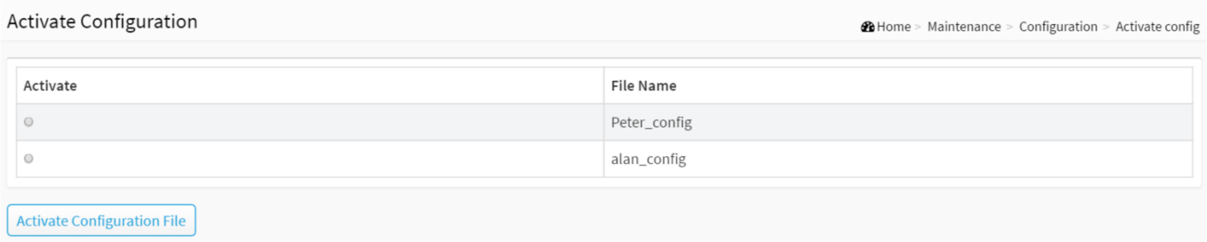
Select the file to activate and click. This will initiate the process of completely replacing the existing configuration with that of the selected file.

Web Interface

To activate configuration in the web interface:

1. Click Maintenance, Configuration and Activate config..

2. Click Activate Select.



Activate Configuration

Home > Maintenance > Configuration > Activate config

Activate	File Name
○	Peter_config
○	alan_config

Activate Configuration File

Figure 17-1.4: Configuration Activation

System files:

startup-config: The startup configuration for the switch, read at boot time.

Parameter description:

- **Activate**

You can select the file that you want to activate**.**

Buttons

- **Activate Configuration File:**

Click the "Activate Configuration File" button then the selected file will be activated to be the switch's running configuration.

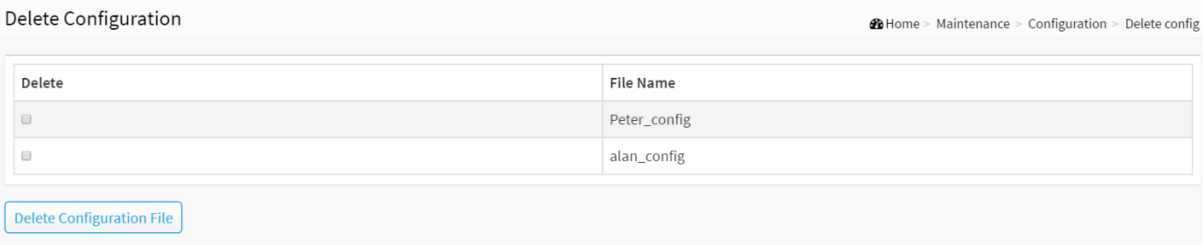
17-1.5 Delete config

It is possible to delete any of the writable files stored in flash, including startup-config. If this is done and the switch is rebooted without a prior save operation, this effectively resets the switch to default configuration.

Web Interface

To delete configuration in the web interface:

1. Click Maintenance, Configuration and Delete config.
2. Click Delete Select.



Delete Configuration

Home > Maintenance > Configuration > Delete config

Delete	File Name
□	Peter_config
□	alan_config

Delete Configuration File

Figure 17-1.5: Delete Configuration

Parameter description:

- **Delete**

  You can select the file that you want to delete**.**

Buttons

- **Delete Configuration File:**

  Click the "Delete Configuration File" button then the selected file will be deleted.

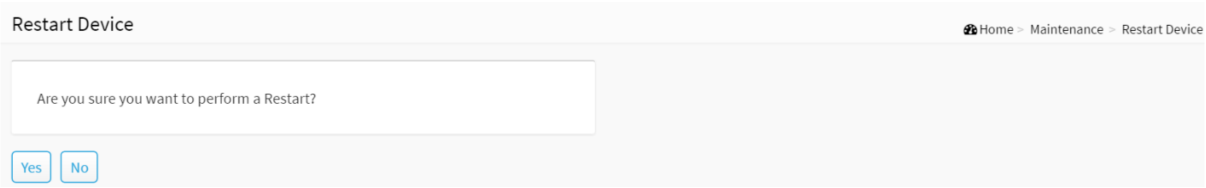
17-2 Restart Device

This section describes how to restart the device for any maintenance needs. Any configuration files or scripts that you saved in the switch should still be available afterwards.

Web Interface

To Restart Device in the web interface:

1. Click Maintenance and Restart Device.
2. Click Yes.



Restart Device

Are you sure you want to perform a Restart?

Figure 17-2: Restart Device

Parameter description:

Restart Device :

You can restart the switch on this page. After restart, the switch will boot normally.

Buttons

- **Yes :**

  Click to “Yes” then the device will restart.

- **No :**

  Click to cancel the opeation.

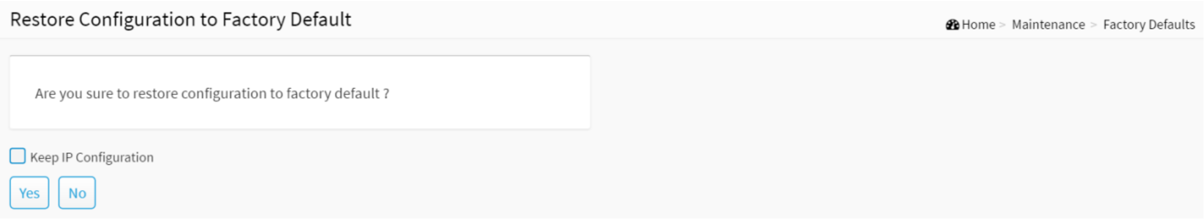
17-3 Factory Defaults

This section describes how to restore the Switch configuration to Factory Defaults.

Web Interface

To restore a Factory Defaults in the web interface:

1. Click Maintenance and Factory Defaults.
2. You can choose if you want to keep ip configuration or not.
3. Click Yes.



Restore Configuration to Factory Default

Home > Maintenance > Factory Defaults

Are you sure to restore configuration to factory default ?

□ Keep IP Configuration

Figure 17-3: The Factory Defaults

Parameter description:

Buttons

- **Keep IP Configuration :**

  Choose if you want to keep ip configuration or not.

- **Yes :**

  Click to "Yes" button to reset the configuration to Factory Defaults.

- **No :**

  Click to cancel the operation.

17-4 Firmware

This section describes how to upgrade (or update) Firmware.

17-4.1 Firmware Upgrade

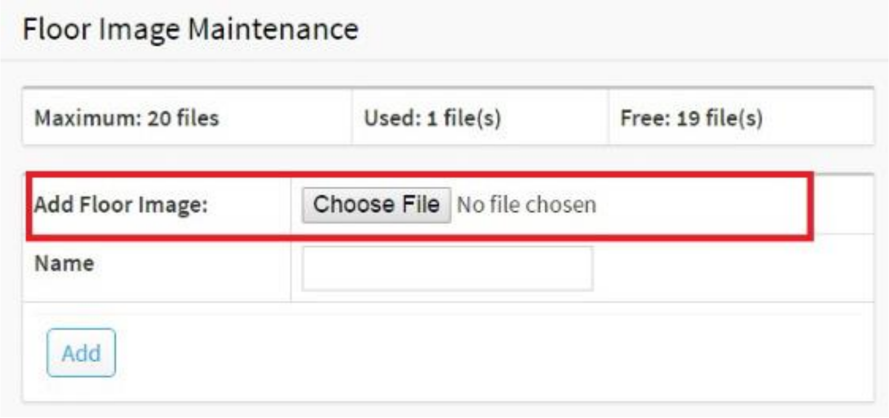
This page facilitates an update of the firmware controlling the switch..

Web Interface

To update firmware of the device in the web interface:

1. Click Maintenance, Firmware and Firmware Upgrade.
2. Click Upload.

Figure 17-4.1 The firmware upgrade



Floor Image Maintenance

Maximum: 20 files	Used: 1 file(s)	Free: 19 file(s)

Add Floor Image: Choose File No file chosen

Name

Parameter description:

- **Browse :**

  Click the “Browse” button to search the Firmware URL and filename.

17-4.2 Firmware Selection

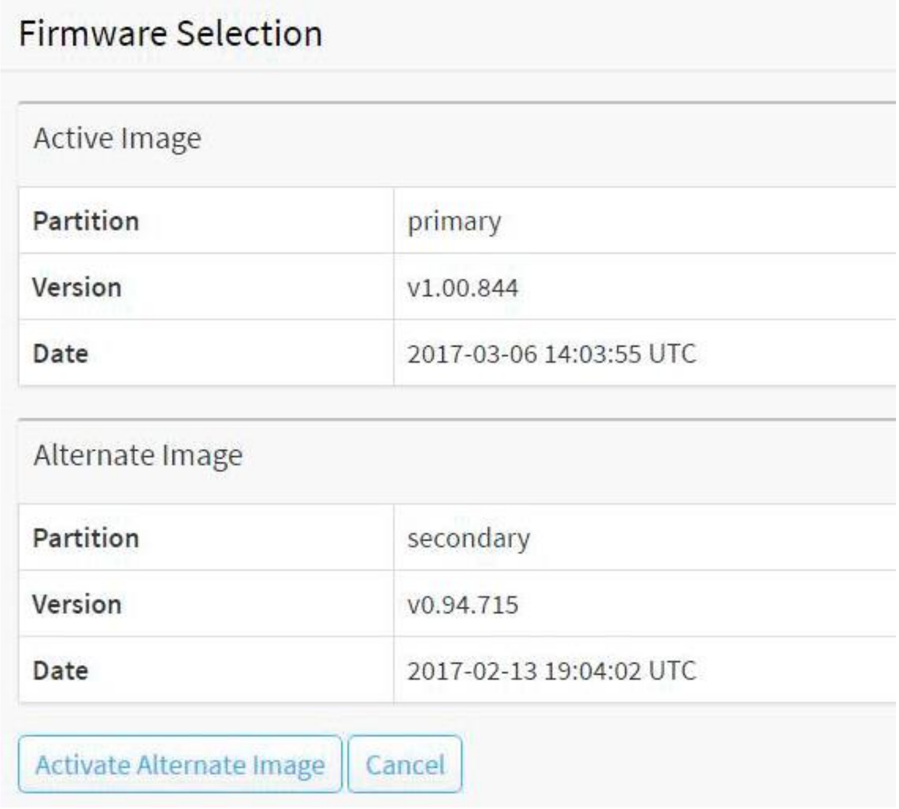
This page provides information about the active and alternate (backup) firmware images in the device, and allows you to activate the alternate image.

The web page displays two tables with information about the active and alternate firmware images.

Web Interface

To show the Firmware information or swap booting firmware in the web interface:

1. Click Maintenance, Firmware and Firmware Selection.
2. Click Activate Alternate Image



Firmware Selection

Active Image

Partition	primary
Version	v1.00.844
Date	2017-03-06 14:03:55 UTC

Alternate Image

Partition	secondary
Version	v0.94.715
Date	2017-02-13 19:04:02 UTC

Figure 17-4.2 The Firmware selection

Image Information

- **Partition :**

Indicate whether primary or secondary partition in the flash is used for storing the firmware image.

- **Version :**

  The version of the firmware image.

- **Date :**

  The date where the firmware was produced.

Buttons

- **Activate Alternate Image :**

  Click to use the "Activate Alternate Image". This button may be disabled depending on system state.

- **Cancel :**

  Cancel activating the alternate image. Navigates away from this page.

Chapter 18 Device Management System

18-1 DMS Overview

1. DMS is an intelligent management tool embedded in switches to intuitively help IT/TS reduce support cost/time/effort.
2. All devices connected to the switches can be discovered and displayed by DMS automatically using standard networking protocols such as LLDP, UPnP, ONVIF, Bonjour, etc.
3. Users can operate the features below via an intuitive web GUI.
   - Power down, remotely, the IP cameras, NVRs, or any PoE devices.
   - Identify where exactly the broken cable is, remotely.
   - Detect abnormal traffic issues on IP cameras/NVR.
   - Monitor devices status intuitively, e.g. link up, PoE power, traffic, etc.
   - Configure VLAN/QoS intuitively for better solution quality/reliability.
4. DMS supports up to 1,000 devices within 4 subnets.

The embedded Device Managed System is designed to be extremely easy-to-use/manage/install IP Phone, IP Cam, or Wifi-AP for enterprise applications. User can deploy IP Device through Topology/ Floor/ Map View to installation location, and through Diagnostics and Traffic Monitor, they may also check link status and monitor throughput as well.

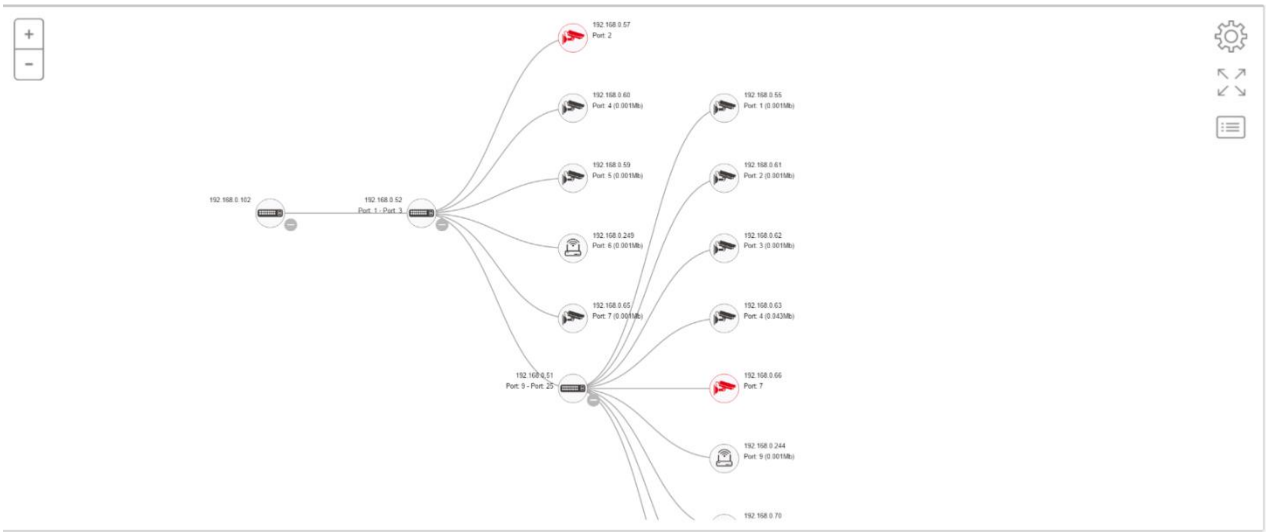
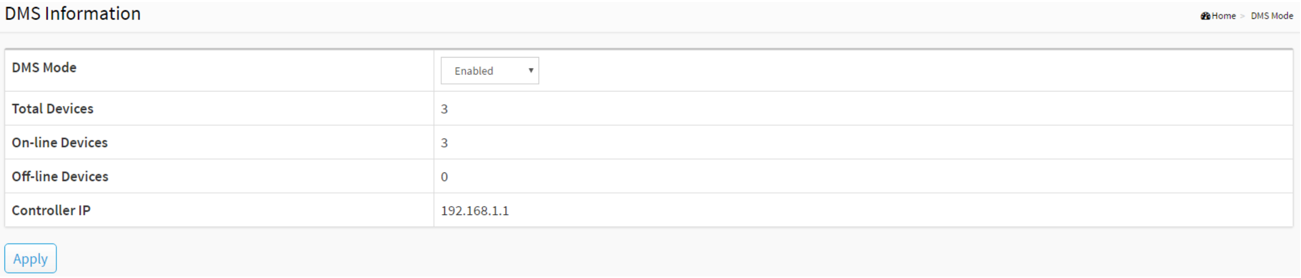


Figure 1: The DMS Overview

18-2 DMS Mode

DMS Information



DMS Information

DMS Mode	Enabled
Total Devices	3
On-line Devices	3
Off-line Devices	0
Controller IP	192.168.1.1

Figure 2: The DMS Information

- DMS Mode: Enable/ Disable the DMS function.
- Total Device: Here will show how many IP devices are detected and displayed in the topology view.
- On-Line Devices: Here will show how many IP devices on-line in the topology view.
- Off-Line Device: Here will show how many IP devices off-line in the topology view.
- Controller IP: It show the Master IP.

18-3 Graphical Monitoring

Topology View

DMS can automatically discover all IP devices and display the devices by graphic networking topology view. User could manage and monitor them by the Topology View, such as to remotely diagnose the cable connection status, auto alarm notifications on critical events, remotely reboot PoE device when it's not alive. Therefore, the user can apply DMS platform to solve the abnormal issues anytime and anywhere by tablet or smart phone, and keep the network works smoothly.

Click Graphical Monitoring Topology View, you can see a visual view of the network topology.

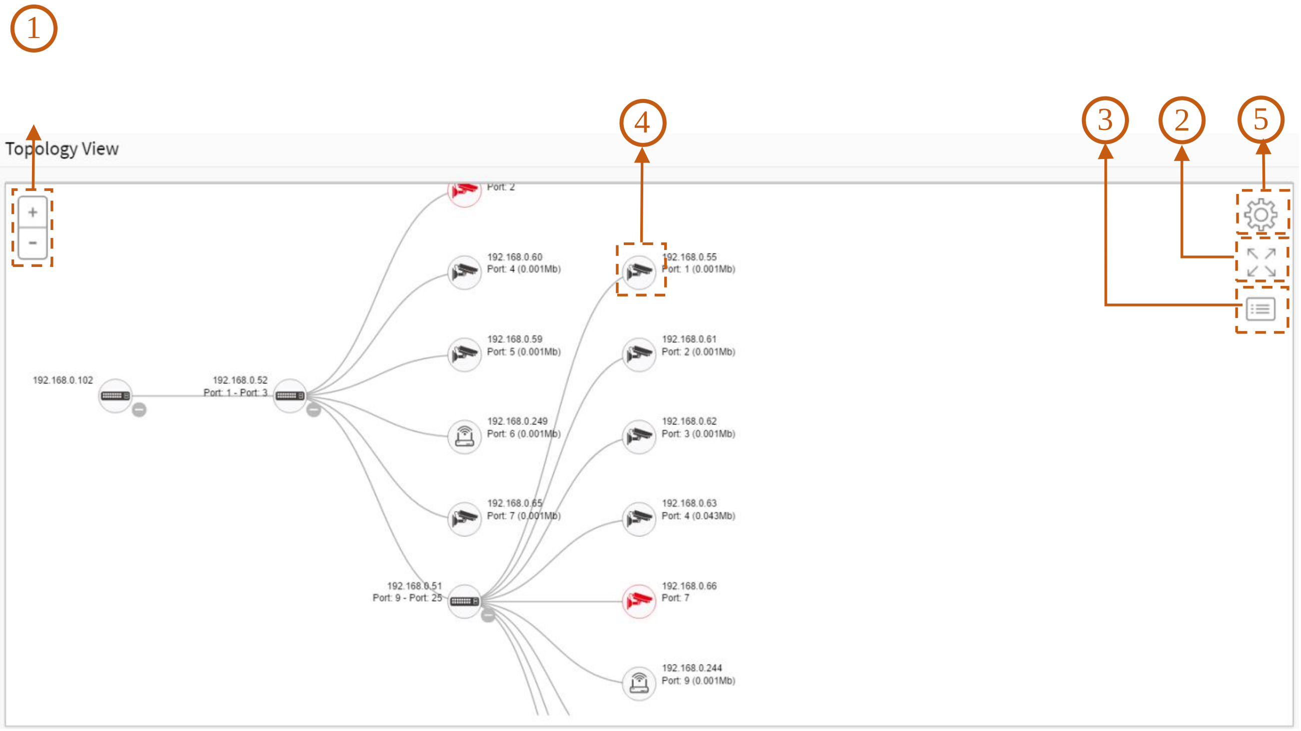


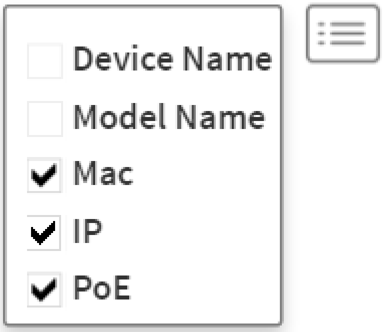
Figure 3: The Topology View

Parameter description:

1. + − Icon with plus and minus marks: Zoom in and zoom out the topology view, user can scroll up/down with mouse to achieve the same purpose.

2. ↖ ↗ ↙ ↘ Icon with screen view type: Click it to change to Full Screen View of Topology or return to the Normal View.

3. Icon with information list: User can select what kind of information should be shown on the topology view of each device. Up to 3 items can be selected.



- ☐ Device Name
- ☐ Model Name
- ☑ Mac
- ☑ IP
- ☑ PoE

Figure 4: The Information List

4. Device icon

   A. Device category

   - : It means the device is Switch.
   - : It means the device is PC.
   - : It means the device is IP Cam.
   - : It means the device is IP Phone.
   - : It means the device is AP.
   - : It means the device is Router.

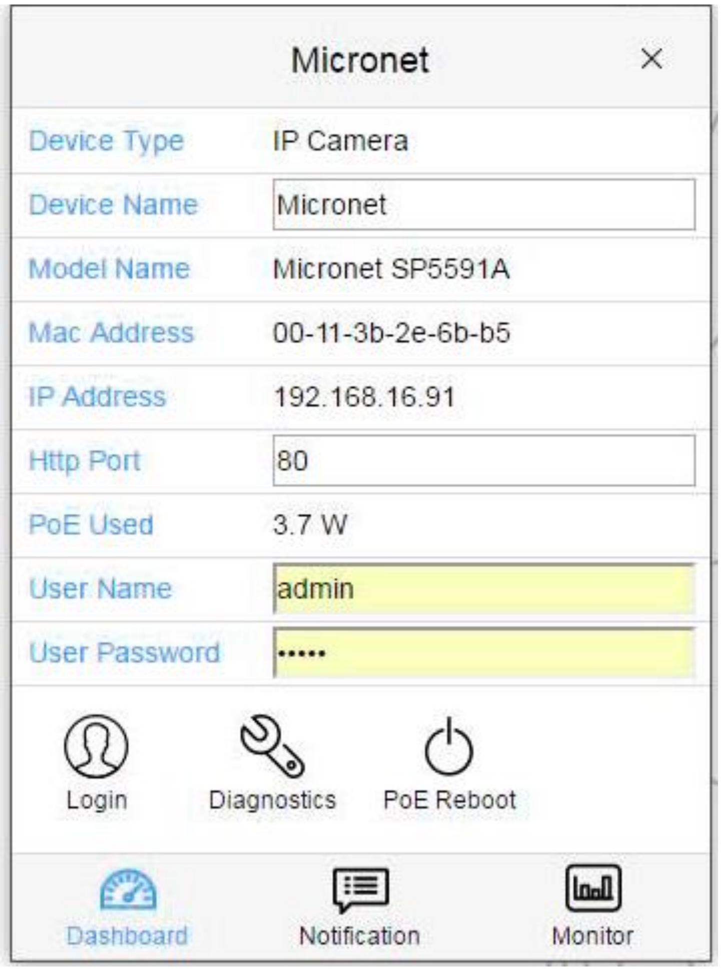
   B. Device Status

   - Icon with black mark: Device link up. User can select function and check issues.
   - Icon with red mark: Device link down. User can diagnose the link status.
   - Icon with numbers: It means some events happened (e.g. Device Off-line, IP Duplicate…etc.) on the IP device, user can click on the device icon to check events in Notification.

- ? Icon with question: It means the IP device is detected by DMS, but the device type can’t be recognized which will be classified as an unknown device type.

C. Device consoles

- To left-click any device icon to display the device consoles for further actions:



Micronet ×

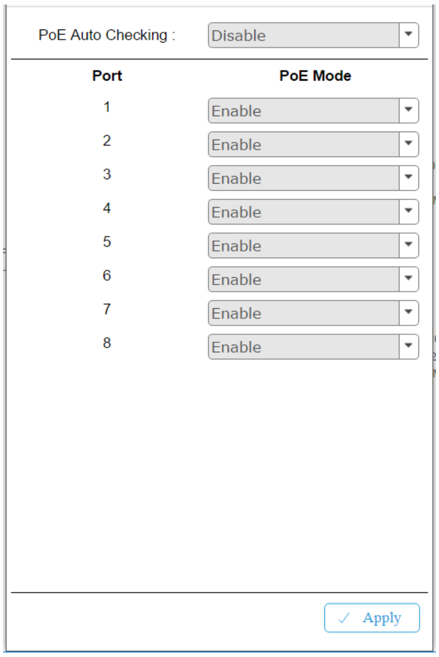
Device Type: IP Camera
Device Name: Micronet
Model Name: Micronet SP5591A
Mac Address: 00-11-3b-2e-6b-b5
IP Address: 192.168.16.91
Http Port: 80
PoE Used: 3.7 W
User Name: admin
User Password: •••••

Figure 5: The Device Console

- Dashboard Console: it displays device info and related actions for the device.
  - ■ Different device type supports different function:
  - - If an IP device is recognized as DMS switch, it will support “Upgrade“, “PoE Config“ and “Find Switch” function.
  - - If an IP device is recognized as PoE device, it will support more “PoE Reboot” function in addition to “Upgrade” and “Find Switch”.
  - ■ Device Type: It can be displayed automatically. If an unknown type is detected, user can still select type from a pre-defined list.
  - ■ Device Name: Create your own Device Name or alias for easy management such as,

1F_Lobby_Cam1.

- Model Name, MAC Address, IP Address, PoE Supply and PoE Used are displayed automatically by DMS.
- Http Port: Re-assign http port number to the device for better security.
- Login Login: Click the Login Action Icon to log in the device via http for further configuration or status monitoring.
- Upgrade Upgrade: Click it to upgrade software version.
- Find Switch Find Switch: When this feature is activated, the switch LED will all lighten up and flicker for 15 seconds.
- PoE Config PoE Config: Click it to configure the PoE function, enable/disable PoE Auto Checking or enable/disable PoE mode for per port.



PoE Auto Checking : Disable

Port	PoE Mode
1	Enable
2	Enable
3	Enable
4	Enable
5	Enable
6	Enable
7	Enable
8	Enable

Figure 6: The PoE Configure

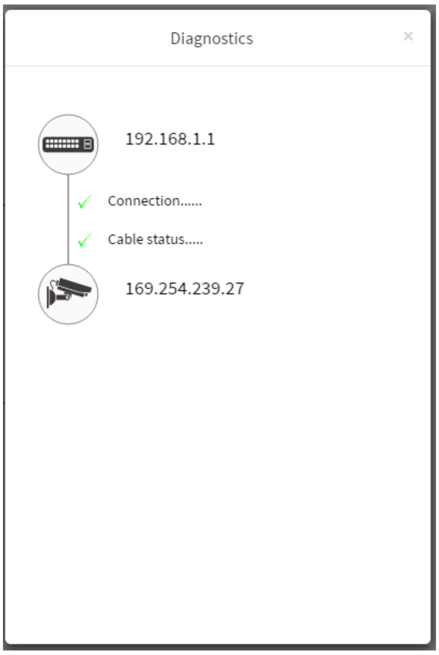
- Diagnostics Diagnostics: Click Diagnostic Action Icon to perform the cable diagnostics, to exam where the broken cable is, and, check if the device connection is alive or not by ping.

- Cable Status:

◆ Green icon: Cable is connected correctly.

◆ Red icon: Cable is not connected correctly. User can check the distance info (XX meters) to identify the broken cable location.

- Connection:
  - ◆ Green icon: Device is pinged correctly.
  - ◆ Red icon: Device is not transmitted /receiving data correctly. Which means it might not be pinged successfully.



Diagnostics ×

192.168.1.1

✓ Connection......

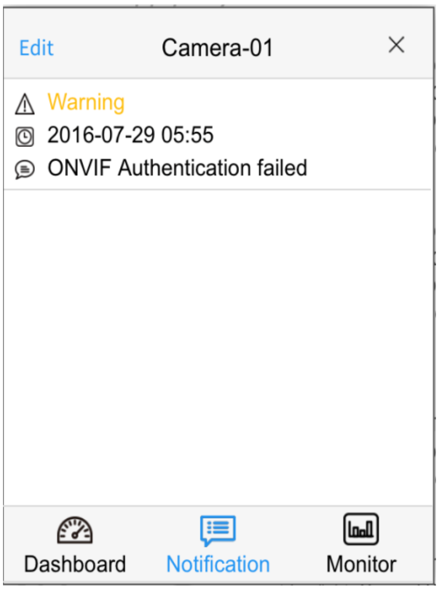
✓ Cable status.....

169.254.239.27

Figure 7: The Diagnostics

- ■ PoE Reboot PoE Reboot: Click Reboot Action Icon to reboot the device remotely so as recover the device back to its normal operation.
- ■ Streaming Streaming: Click Streaming Action Icon to display the video images streaming, if the device supports this feature.
- ■ Parent Node Icon with blank node: When DMS switch detects more than two IP devices from the same port, switch can’t resolve this IP device’s layout, and instead, it will show a blank node to present this situation. User can use “Parent Node” function to adjust layout in Dashboard.

● Notification Console: It displays alarms and logs triggered by events.



Edit Camera-01

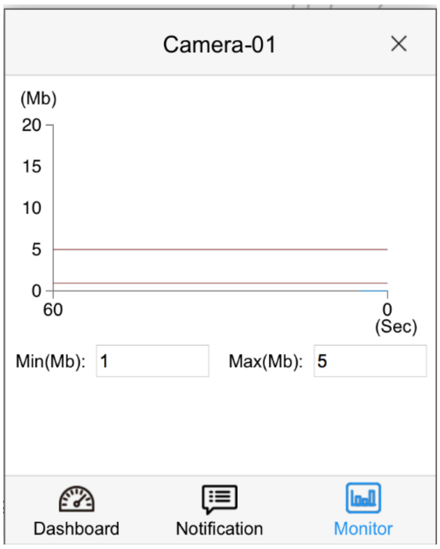
Warning

2016-07-29 05:55

ONVIF Authentication failed

Figure 8: The Notification Console

- Monitor Console: It displays the traffics for device health check purpose.
  - For each IP device except DMS switches, User can set a threshold of throughput for IP devices, and get notification when throughput is lower or higher than settings.
  - If both values are “0”, it means the function is disabled.
  - Polling interval is 1 second, when the page is closed; the Polling interval will change to around 5 seconds.



Camera-01

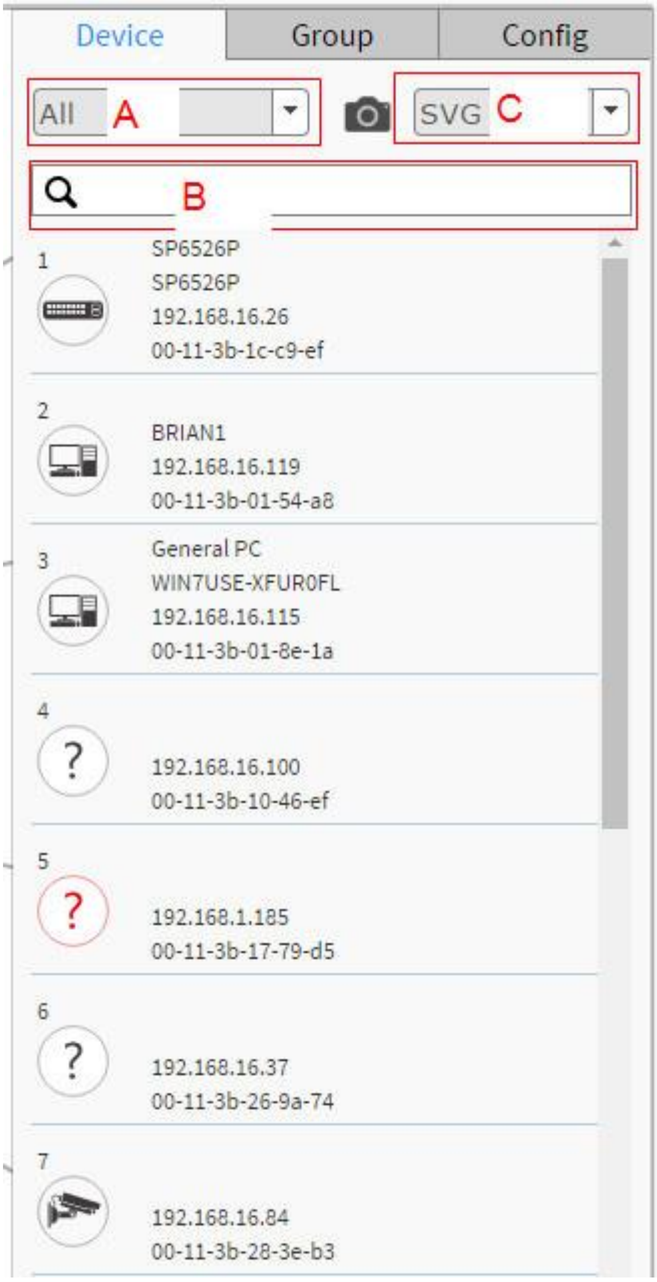
Min(Mb): 1

Max(Mb): 5

Figure 9: The Monitor Console

5. ⚙ In the upper right corner, there is a “Setting icon”. When user clicks the icon, it will pop-up Device, Group, Config, export topology view and advanced search functions for the topology.

- **Device Search Console**
  All devices and info. It will show on the list.



1
SP6526P
SP6526P
192.168.16.26
00-11-3b-1c-c9-ef

2
BRIAN1
192.168.16.119
00-11-3b-01-54-a8

3
General PC
WIN7USE-XFUR0FL
192.168.16.115
00-11-3b-01-8e-1a

4
192.168.16.100
00-11-3b-10-46-ef

5
192.168.1.185
00-11-3b-17-79-d5

6
192.168.16.37
00-11-3b-26-9a-74

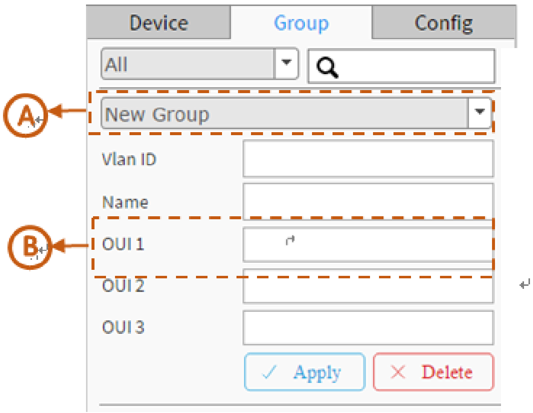
7
192.168.16.84
00-11-3b-28-3e-b3

	Function
A.	Filter devices by Device Type
B.	Search devices by key words full text search
C.	Save the whole View to SVG, PNG or PDF

Figure 10: The Device Search Console

Group Setting Console

- User can set VLAN group for each IP device by OUI or clicking device icon, and configure traffic priority (0~7) for each VLAN group.
- Using Mac Based VLAN to isolate groups.
- One IP device only can join one VLAN group.



All

New Group

Vlan ID

Name

OUI 1

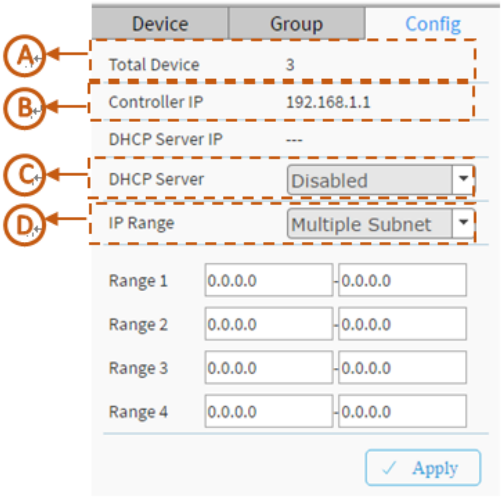
OUI 2

OUI 3

	Function
A.	Group devices by filtering, searching, clicking device icons, or specifying OUI.
B.	Assign VLAN ID or Name to Group.

Figure 11: The Group Setting Console

System Setting Console



Total Device 3

Controller IP 192.168.1.1

DHCP Server IP ---

DHCP Server Disabled

IP Range Multiple Subnet

Range 1 0.0.0.0 - 0.0.0.0

Range 2 0.0.0.0 - 0.0.0.0

Range 3 0.0.0.0 - 0.0.0.0

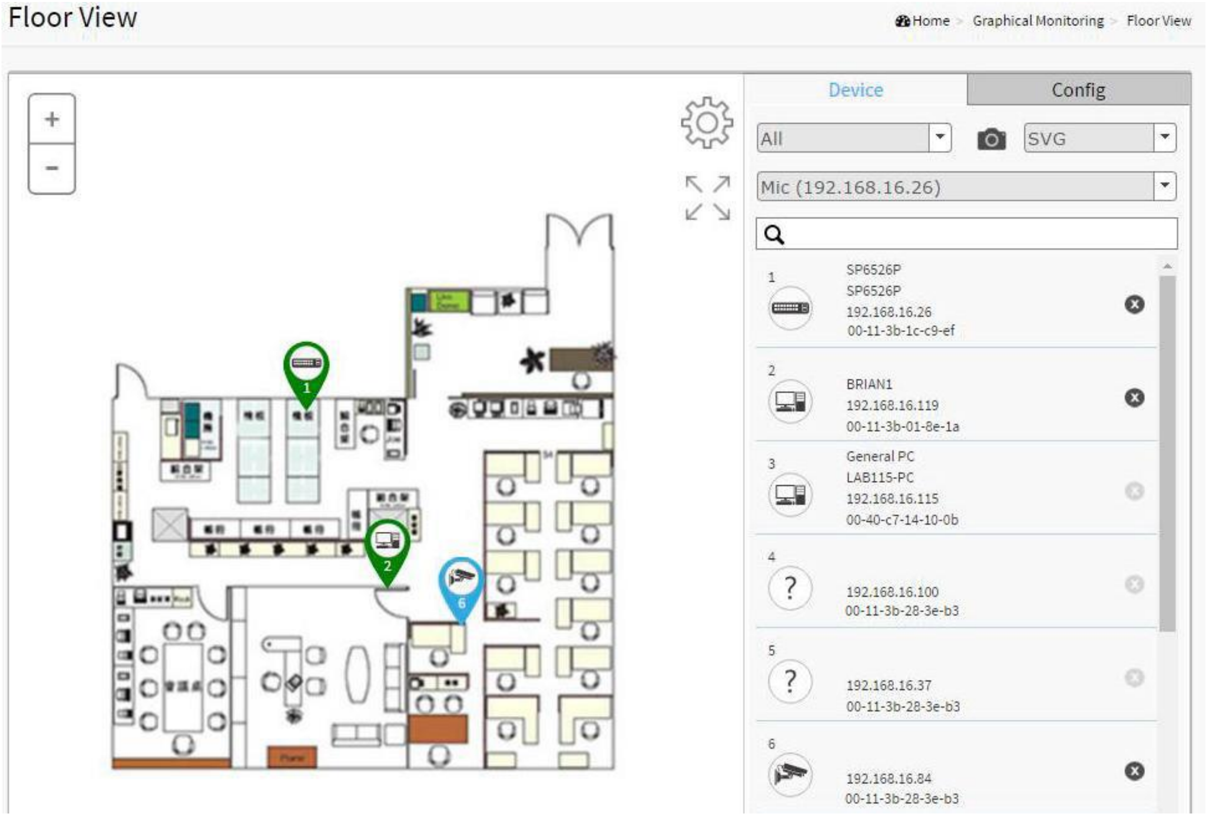
Range 4 0.0.0.0 - 0.0.0.0

	Function
A.	Here will show how many IP devices are detected and displayed in the topology view.
B.	It show the Master IP.
C.	You can enable/disable DHCP server
D.	- Single Subnet: DMS will base on the master switch's IP address. Here the subnet means "255.255.255.0". - Multiple Subnet: To provide 4 ranges for inputting manually.(In the case, we will suggest user to adjust switch's subnet mask to "255.255.0.0" also to avoid IP devices can't be recognized.)

Figure 12: The System Setting Console

Floor View

User can easily plan IP devices installation location onto the custom uploaded floor images.



1 SP6526P SP6526P 192.168.16.26 00-11-3b-1c-c9-ef

2 BRIAN1 192.168.16.119 00-11-3b-01-8e-1a

3 General PC LAB115-PC 192.168.16.115 00-40-c7-14-10-0b

4 ? 192.168.16.100 00-11-3b-28-3e-b3

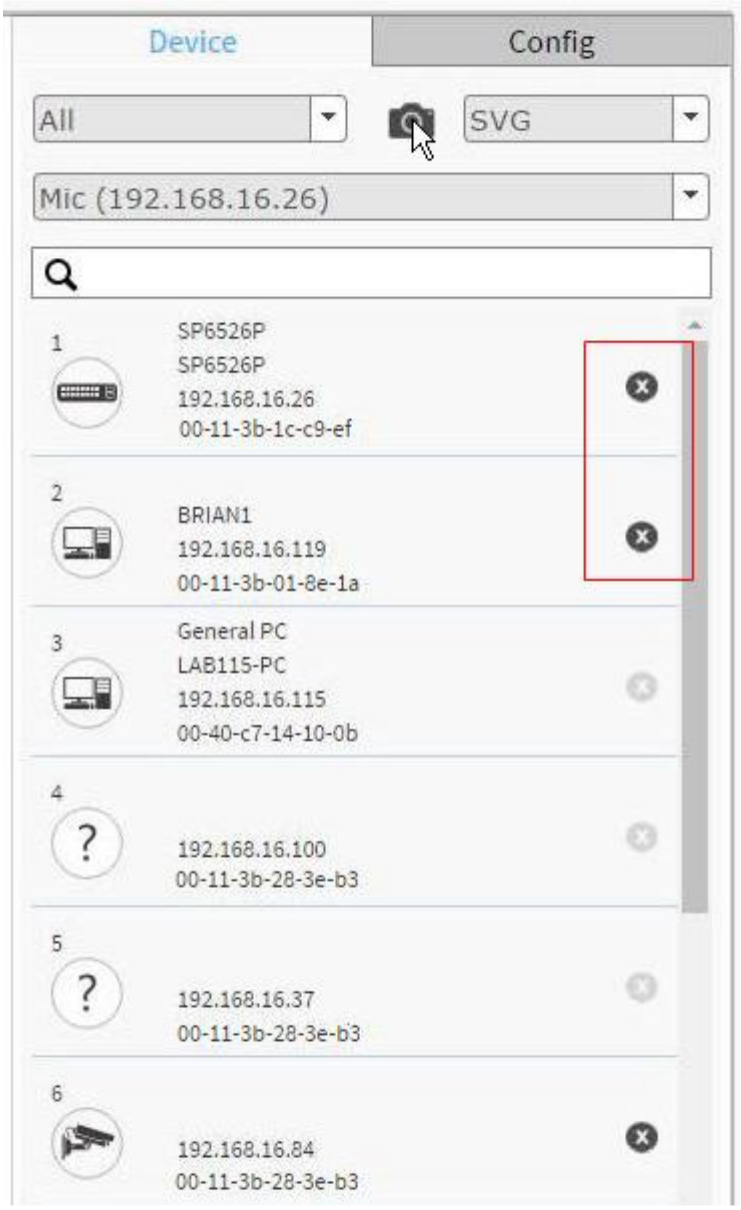
5 ? 192.168.16.37 00-11-3b-28-3e-b3

6 192.168.16.84 00-11-3b-28-3e-b3

Figure 13: The Floor View

- Anchor Devices onto Floor Maps
- Find Device Location Instantly
- 10 Maps can be Stored in Each Switch
- IP Surveillance/VoIP/WiFi Applications
- Other Feature same as Topology View
- To place and remove a device icon:
  - To select a device and click its icon from the device list.

- The device icon will show on the floor image’s default location.
- To click and hold left mouse by dragging-and-dropping the icon to the correct location on the floor view.
- To click cross sign on the right side of device icon to remove a device from all floor view images.



All
SVG
Mic (192.168.16.26)

1
SP6526P
SP6526P
192.168.16.26
00-11-3b-1c-c9-ef

2
BRIAN1
192.168.16.119
00-11-3b-01-8e-1a

3
General PC
LAB115-PC
192.168.16.115
00-40-c7-14-10-0b

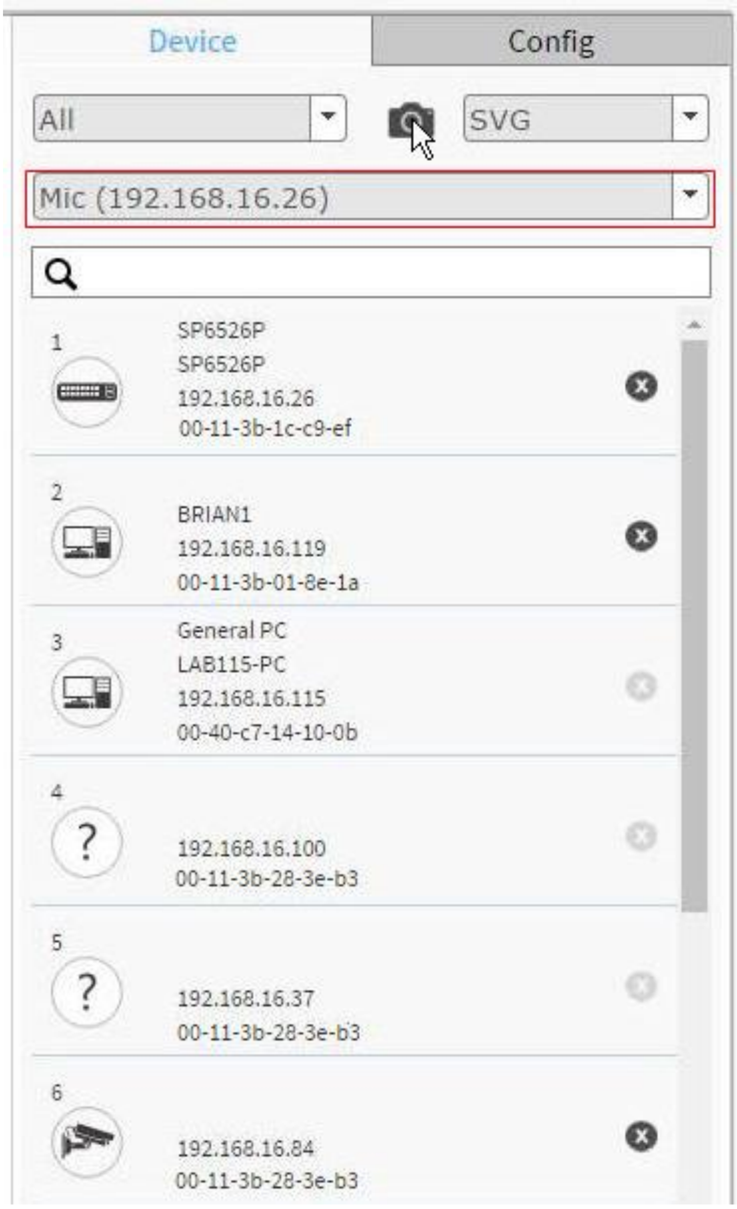
4
192.168.16.100
00-11-3b-28-3e-b3

5
192.168.16.37
00-11-3b-28-3e-b3

6
192.168.16.84
00-11-3b-28-3e-b3

Figure 14: The Device Icon to Remove a Device

If there are more than two floor images, it can be selected from the field.



All

SVG

Mic (192.168.16.26)

1
SP6526P
SP6526P
192.168.16.26
00-11-3b-1c-c9-ef

2
BRIAN1
192.168.16.119
00-11-3b-01-8e-1a

3
General PC
LAB115-PC
192.168.16.115
00-40-c7-14-10-0b

4
192.168.16.100
00-11-3b-28-3e-b3

5
192.168.16.37
00-11-3b-28-3e-b3

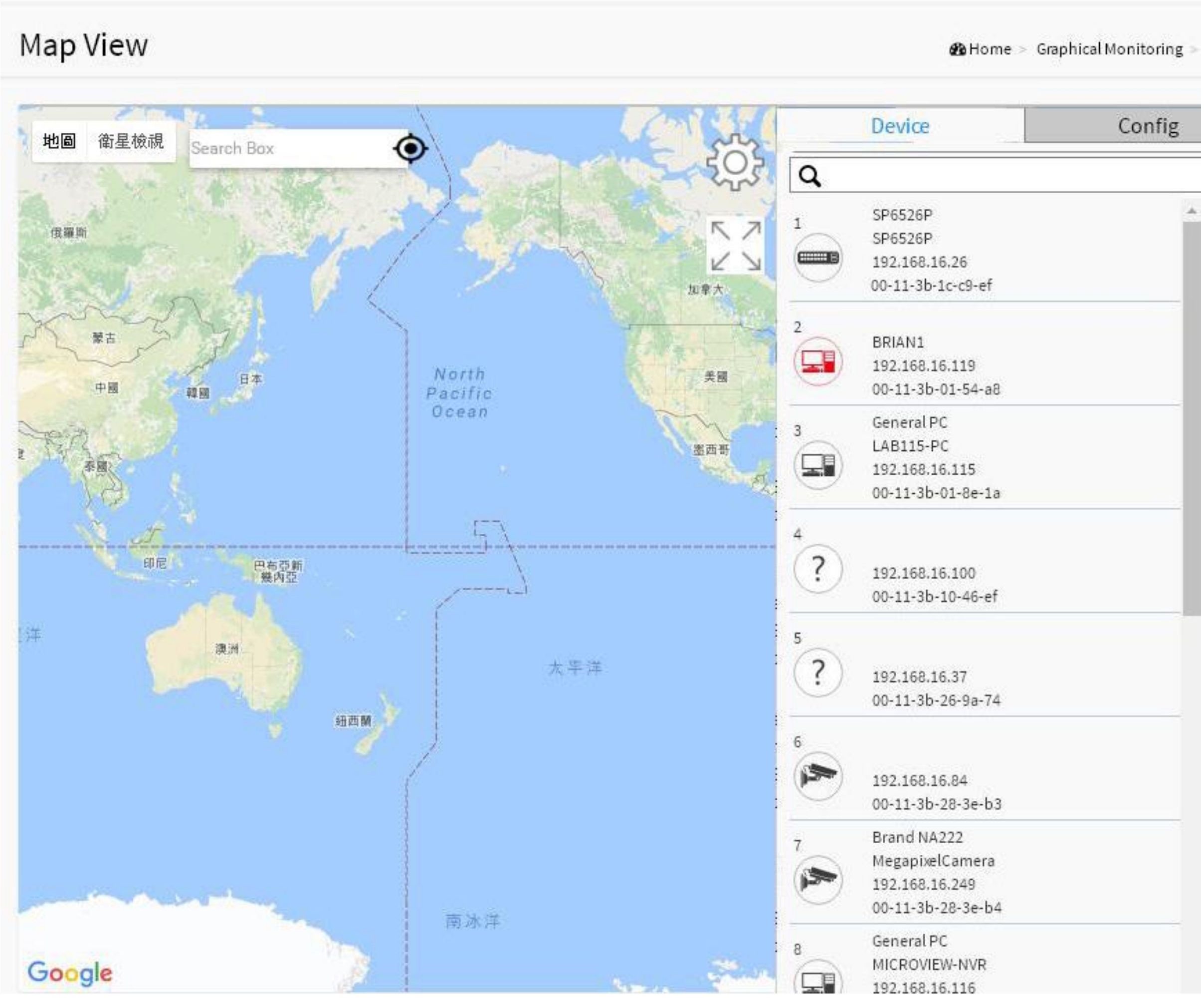
6
192.168.16.84
00-11-3b-28-3e-b3

Figure 15: The Device Icon to Select floor

Map View

It can help to find the location of the devices even they are installed in different building.

User can place the device icon on the Map View of which navigated by Google map.



1
SP6526P
SP6526P
192.168.16.26
00-11-3b-1c-c9-ef

2
BRIAN1
192.168.16.119
00-11-3b-01-54-a8

3
General PC
LAB115-PC
192.168.16.115
00-11-3b-01-8e-1a

4
192.168.16.100
00-11-3b-10-46-ef

5
192.168.16.37
00-11-3b-26-9a-74

6
192.168.16.84
00-11-3b-28-3e-b3

7
Brand NA222
MegapixelCamera
192.168.16.249
00-11-3b-28-3e-b4

8
General PC
MICROVIEW-NVR
192.168.16.116

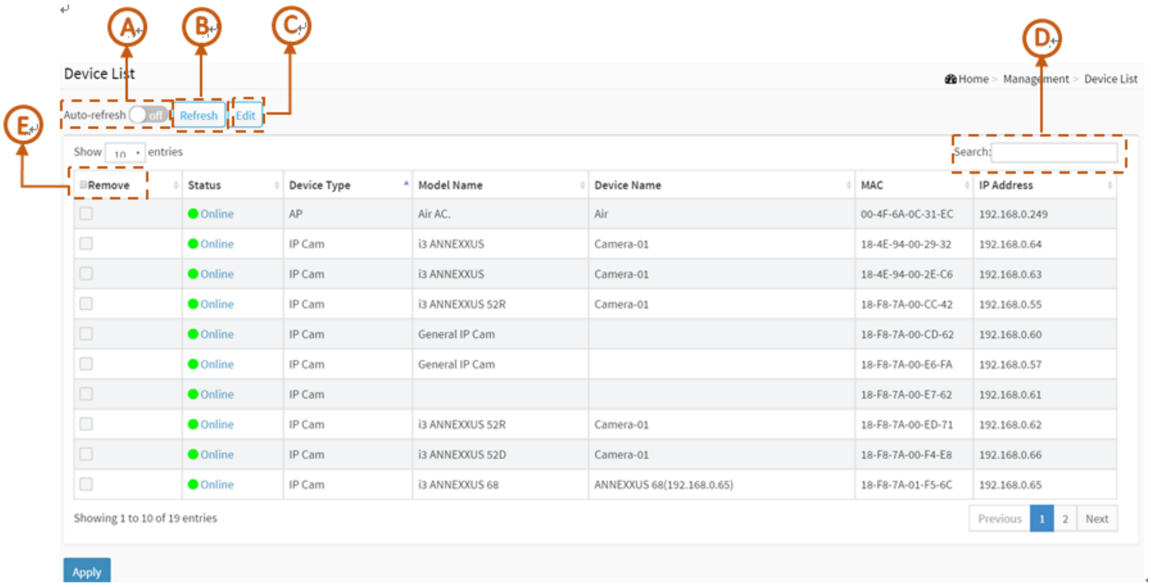
Figure 16: The Map View

- Anchor Devices onto Google Map.
- Find Devices Instantly from Map.
- On-Line Search Company/Address.
- Outdoor IP Cam/WiFi Applications.
- Other Feature same as Topology View.

18-4 Management

Device List

It will show all devices and their information which are detected by DMS.



Device List

Home > Management > Device List

Auto-refresh off Refresh Edit

Show 10 entries

Search:

□Remove	Status	Device Type	Model Name	Device Name	MAC	IP Address
□	● Online	AP	Air AC.	Air	00-4F-6A-0C-31-EC	192.168.0.249
□	● Online	IP Cam	i3 ANNEXXUS	Camera-01	18-4E-94-00-29-32	192.168.0.64
□	● Online	IP Cam	i3 ANNEXXUS	Camera-01	18-4E-94-00-2E-C6	192.168.0.63
□	● Online	IP Cam	i3 ANNEXXUS 52R	Camera-01	18-F8-7A-00-CC-42	192.168.0.55
□	● Online	IP Cam	General IP Cam		18-F8-7A-00-CD-62	192.168.0.60
□	● Online	IP Cam	General IP Cam		18-F8-7A-00-E6-FA	192.168.0.57
□	● Online	IP Cam			18-F8-7A-00-E7-62	192.168.0.61
□	● Online	IP Cam	i3 ANNEXXUS 52R	Camera-01	18-F8-7A-00-ED-71	192.168.0.62
□	● Online	IP Cam	i3 ANNEXXUS 52D	Camera-01	18-F8-7A-00-F4-E8	192.168.0.66
□	● Online	IP Cam	i3 ANNEXXUS 68	ANNEXXUS 68(192.168.0.65)	18-F8-7A-01-F5-6C	192.168.0.65

Showing 1 to 10 of 19 entries

Previous 1 2 Next

Apply

Figure 17: The Devices List

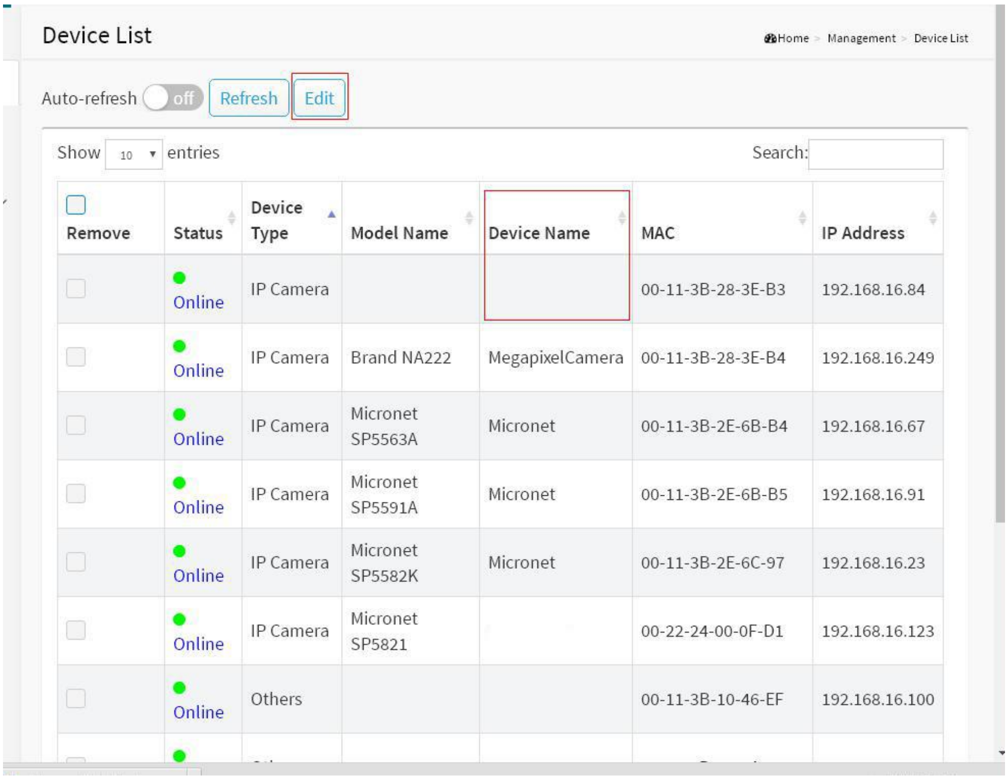
A. Auto-refresh off If you want to auto-refresh the information then you need to evoke the “Auto refresh”.

B. Refresh Click this icon to refresh the status of all devices.

C. Edit Click this icon to Edit Device Name and http Port.

- User can press “Edit” icon to edit device name for each IP device. This function can also be configured in the Dashboard of Topology view.

- There is no HTTP connection function for Unknown Device and PC type devices, so UI doesn’t provide “Edit HTTP port” function for configuring it.



Device List

Home > Management > Device List

□ Remove	Status	Device Type	Model Name	Device Name	MAC	IP Address
□	● Online	IP Camera			00-11-3B-28-3E-B3	192.168.16.84
□	● Online	IP Camera	Brand NA222	MegapixelCamera	00-11-3B-28-3E-B4	192.168.16.249
□	● Online	IP Camera	Micronet SP5563A	Micronet	00-11-3B-2E-6B-B4	192.168.16.67
□	● Online	IP Camera	Micronet SP5591A	Micronet	00-11-3B-2E-6B-B5	192.168.16.91
□	● Online	IP Camera	Micronet SP5582K	Micronet	00-11-3B-2E-6C-97	192.168.16.23
□	● Online	IP Camera	Micronet SP5821		00-22-24-00-0F-D1	192.168.16.123
□	● Online	Others			00-11-3B-10-46-EF	192.168.16.100

Figure 18: The Edit of Devices List

D Search: Search devices by key words with full text search.

E □ Remove Only Offline devices provide “Remove” function to remove from DMS device list.

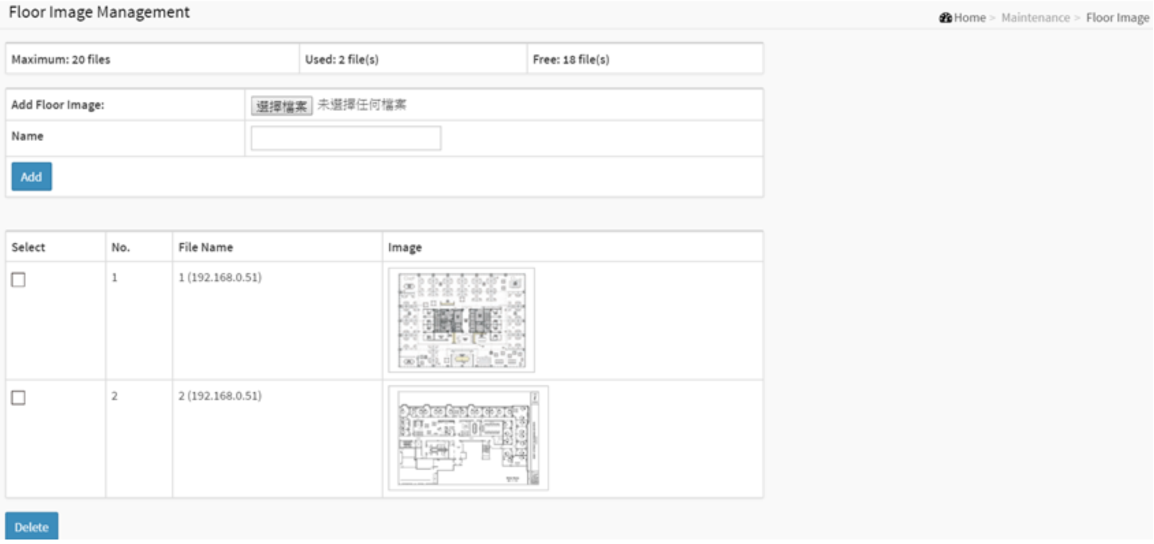
Note:

The device name will not save until you click Apply button. Please do not click refresh, auto-refresh or edit button before you apply new device name.

18-5 Maintenance

Floor Image

In this page, user can add or delete a floor image.



Floor Image Management

Maximum: 20 files	Used: 2 file(s)	Free: 18 file(s)

Add Floor Image:	選擇檔案 未選擇任何檔案
Name	

Select	No.	File Name	Image
□	1	1 (192.168.0.51)	
□	2	2 (192.168.0.51)	

Figure 19: The Floor Image

- Each DMS switch provides 10 files space for uploading.
- Only support JPG and PNG formats.
- File size is limited to 256KB.
- All DMS switches' floor image in the same network can be shared together.
  - For example:
  - If Switch1 has uploaded 10 floor images, Switch2 uploaded 5 images, the total 15 floor images can be shared and selected on all DMS switches in the same network.
- File name will attach IP address to let user know the floor image is stored on which DMS switch.

Chapter 19 Command Line Interface

The following description is the brief of the network connection.

-- Attach the RJ45 serial port on the switch’s front panel which used to connect to the switch for telnet configuration

-- At “Com Port Properties” Menu, configure the parameters as below: (see the next section)

Baud rate	115200
Stop bits	1
Data bits	8
Parity	N
Flow control	none

19-1 Login

The command-line interface (CLI) is a text-based interface. User can access the CLI through either a direct serial connection to the device or a Telnet session (Default IP address: **192.168.1.1**). The default user and password to login into the Managed Switch are listed below:

Username: **admin**

Password: **admin**

Note: <none> means empty string

After login successfully, the prompt will be shown as "<sys_name>#". See the following figures. It means you behave as an administrator and have the privilege for setting the Managed Switch. If log as not the administrator, the prompt will be shown as "<sys_name>", it means you behave as a guest and are only allowed for setting the system under the administrator. Each CLI command has its privilege

```
Username: admin
Password: admin
SP6526P#
```

19-2 Commands of CLI

The CLI is divided into several modes. If a user has enough privilege to run a particular command, the user has to run the command in the correct mode. To see the commands of the mode, please input “**?**” after the system prompt, then all commands will be listed in the screen. The command modes are listed as bellows:

Command Modes

MODE	**PROMPT**	**COMMAND FUNCTION IN THIS MODE**
exec	<sys_name>#	Display current configuration, diagnostics, maintenance
config	<sys_name>(config)#	Configure features other than those below
Config-if	<sys_name>(config-interface)#	Configure ports
Config-if-vlan	<sys_name>(config-if-vlan)#	Configure static vlan
Config-line	<sys_name>(config-line)#	Line Configuration
Config-impc-profile	<sys_name>(config-impc-profile)#	IPMC Profile
Config-snmp-host	<sys_name>(config-snmp-host)#	SNMP Server Host
Config-stp-aggr	<sys_name>(config-stp-aggr)#	STP Aggregation
Config-dhcp-pool	<sys_name>(config-dhcp-pool)#	DHCP Pool Configuration
Config-rfc2544-profile	<sys_name>(config-rfc2544-profile)#	RFC2544 Profile

Commands reside in the corresponding modes could run only in that mode. If a user wants to run a particular command, the user has to change to the appropriate mode. The command modes are organized as a tree, and users start to in enable mode. The following table explains how to change from one mode to another.

Change between Command Modes

MODE	ENTER MODE	LEAVE MODE
exec	--	--
config	Configure terminal	exit
config-interfcae	Interface <port-type> <port-type-list>	exit
config-vlan	Interface vlan <vlan_list>	exit

19-3 Global Commands of CLI

```
SP6526P# ?
    !              Comment
    clear          Reset functions
    configure      Enter configuration mode
    copy           Copy from source to destination
    delete         Delete one file in flash file system
    diagnostics    diagnostics
    dir            Directory of all files in flash file system
    exit           Exit from the CLI
    find-switch    Turn on and off all LED light 3 times in 15 seconds
    firmware       Firmware
    logout         Exit from EXEC mode
    more           Display file
    ping           Send ICMP echo messages
    reload         Reload system
    show           Show running system information
    ssl            Setup SSL certificate
    terminal       Set terminal line parameters
    traceroute    Trace the route to HOST
```

Exit

Exit from EXEC mode.

Syntax:

exit

Parameter:

None.

Example:

```
SP6526P(config)# exit

SP6526P#
```

logout

Exit from EXEC mode.

Syntax:

logout

Parameter:

none

Example:

```
SP6526P# logout

Username:
```

Chapter 20 CLEAR of CLI

Table : CLEAR Commands

Command	Function
access-list	Access list
ip	Clear DHCP Relay statistics
lldp	Clear LLDP statistics for one or more given
logging	Syslog
mac	MAC Address Table
spanning-tree	Execute protocol migration check on interfaces
statistics	Clear statistics for one or more given interface

20-1 access-list

Access list.

Syntax:

Clear access-list ace statistics

Parameter:

ace	Access list entry
statistics	Traffic statistics

Example:

```
SP6526P# clear access-list ace statistics
SP6526P#
```

20-2 ip

Clear DHCP Relay statistics.

Syntax

clear ip dhcp relay statistics

Parameter

dhcp	Clear DHCP Relay statistics
relay	Clear DHCP Relay statistics

statistics	Clear DHCP Relay statistics

EXAMPLE

```
SP6526P# clear  ip dhcp relay statistics

SP6526P#
```

20-3 lldp

Clear LLDP statistics for one or more given interface.

Syntax

Clear lldp statistics { global | (interface [* | GigabitEthernet <port_list>]) }

Parameter

statistics	Clear LLDP statistics
global	Clear global counters
interface	Interface
GigabitEthernet	GigabitEthernet
*****	All ports
<port_list>	Port List S/X-Y,Z (1/1-26)

EXAMPLE

```
SP6526P# clear lldp statistics interface *

SP6526P#
```

20-4 logging

Syslog.

Syntax

clear logging [info] [warning] [error]

Parameter

error	Error
info	Information
warning	Warning

EXAMPLE

```
SP6526P# clear logging info error warning

SP6526P#
```

20-5 mac

MAC Address Table.

Syntax

Clear mac address-table

Parameter

address-table	Flush MAC Address table.

EXAMPLE

```
SP6526P# clear mac address-table
SP6526P#
```

20-6 spanning-tree

Execute protocol migration check on interfaces.

Syntax

clear spanning-tree detected-protocols interface (* | GigabitEthernet <port_list>)

Parameter

detected-protocols	Clear spanning-tree detected protocols, i.e. mcheck.
interface	Interface
GigabitEthernet	GigabitEthernet
*****	All ports
<port_type_list>	Port List S/X-Y,Z (1/1-26)

EXAMPLE

```
SP6526P# clear spanning-tree detected-protocols interface *
SP6526P#
```

20-7 statistics

Clear statistics for a given interface.

Syntax

clear statistics interface (* | GigabitEthernet <port_list>)

Parameter

interface	Interface
GigabitEthernet	GigabitEthernet
*****	All switches or All ports

<port__list> Port List S/X-Y,Z (1/1-26)

EXAMPLE

```
SP6526P# clear statistics GigabitEthernet 1/1-26

SP6526P#
```

Chapter 21 CONFIGURE Commands of CLI

Table : CONFIGURE Commands

Command	Function
terminal	Configure from the terminal
!	Comments
aaa	Authentication, Authorization and Accounting
access	Access management
access-list	Access list
aggregation	Aggregation mode
clock	Configure time-of-day clock
dms	DMS Mode
do	To run exec commands in config mode
dot1x	IEEE Standard for port-based Network Access Control
end	Go back to EXEC mode
event	Trap event level
exit	Exit from Configuration mode
interface	Select an interface to configure
ip	Internet Protocol
ipmc	IPv4/IPv6 multicast configuration
ipv6	IPv6 configuration commands
lacp	Lacp system configuration
lldp	LLDP configurations.

logging	Syslog
loop-protect	Loop protection configuration
mac	MAC table entries/configuration
monitor	Monitoring different system events
mvr	MVR multicast VLAN list
no	Negate a command or set its defaults
ntp	Configure NTP
poe	power over Ethernet
port-security	Enable/disable port security globally
Privilege	Privilege level
qos	Quality of Service
radius-server	Configure RADIUS
rmon	Remote Monitoring
snmp-server	Set SNMP server's configurations
spanning-tree	Spanning Tree protocol
system	Set the SNMP server's configurations
tacacs-server	Configure TACACS+
trap	Trap
upnp	Set UPnP's configurations
username	Establish User Name Authentication
vlan	VLAN commands
voice	Vlan for voice traffic

21-1 terminal

Configure from the terminal.

Syntax

configure terminal

Parameter

terminal	Configure from the terminal

EXAMPLE

```
SP6526P# configure terminal
SP6526P(config)#
```

21-1.1 aaa

Authentication, Authorization and Accounting.

SYNTAX

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

aaa authentication service-port [ssh | telnet | http | https] <0-65535>

aaa authentication redirect

aaa authorization (ssh | telnet) tacacs commands <0-15> fallback

aaa authorization (ssh | telnet) tacacs commands <0-15> config-commands fallback

aaa accounting (ssh | telnet) tacacs

aaa accounting (ssh | telnet) tacacs commands <0-15> [exec]

Parameter

authentication	Authentication
authorization	Authorization
accounting	Accounting
login	Login
service-port	Service port
redirect	HTTP redirect HTTPS
ssh	Configure SSH

telnet	Configure Telnet
http	Configure HTTP
local	Use local database for authentication
radius	Use RADIUS for authentication
tacacs	Use TACACS+ for authentication
https	Configure HTTPS
<0-65535>	Service port (0..65535)
telnet	telnet
ssh	ssh
tacacs	Configure Telnet
commands	Cmd Lvl (0..15)
<0-15>	Cmd Lvl (0..15)
config-commands	config-commands
fallback	fallback
tacacs	Configure SSH
exec	config-commands

EXAMPLE

```
SP6526P(config)# aaa authentication login http radius
SP6526P(config)#
```

21-1.2 !

Comments

21-1.3 access

Access management.

SYNTAX

access management <1..16> <1..4095> A.B.C.D[/mask] { [web] [snmp] [telnet] | all }

access management <1..16> <1..4095> A.B.C.D[/mask] { [web] | [snmp] | [telnet] | [all] }

Parameter

management	Access management configuration
< 1-16>	ID of access management entry (1..16)
<1..4095>	VID of access management entry (1..4095)
A.B.C.D[/mask]	A valid IPv4 unicast address
all	All services
snmp	SNMP service
telnet	TELNET/SSH service
web	Web service

EXAMPLE

```
SP6526P(config)# access management 10 3 192.168.1.1 all
SP6526P(config)#
```

21-1.4 access-list

Access list.

Table : configure – access-list Commands

Command	Function
ace	Access list entry

21-1.4.1 ace

Access list entry.

SYNTAX

access-list ace <1-384> action [deny | permit | shutdown]

access-list ace <1-384> action { (deny | permit | shutdown) [ingress | mirror | metering | counter | frame-type] }

access-list ace <1-384> action { (deny | permit | shutdown) ingress [any | interface] [mirror | metering | counter

| frame-type] }

access-list ace <1-384> action { (deny | permit | shutdown) ingress any mirror [disable | metering | counter | frame-type] }

access-list ace <1-384> action { (deny | permit | shutdown) ingress any metering [disable | <16-1000000>] [mirror | counter | frame-type] }

access-list ace <1-384> action { (deny | permit | shutdown) ingress any counter [disable | mirror | metering | frame-type] }

access-list ace <1-384> action { (deny | permit | shutdown) ingress any frame-type any [mirror | metering | counter] }

access-list ace <1-384> action { (deny | permit | shutdown) ingress any frame-type any mirror [disable | metering | counter] }

access-list ace <1-384> action { (deny | permit | shutdown) ingress any frame-type any metering [disable | <16-1000000>] [mirror | counter] }

access-list ace <1-384> action { (deny | permit | shutdown) ingress any frame-type any counter [disable | mirror | metering] }

access-list ace <1-384> action { (deny | permit | shutdown) ingress any frame-type etype [mirror | metering | counter | ctag | ctag-priority | ctag-vid | stag | stag-priority | stag-vid | dmac-type | dmac | smac | etype-value] }

access-list ace <1-384> action { (deny | permit | shutdown) ingress any frame-type ipv4 [mirror | metering | counter | dip | sip | ip-protocol | ip-flag | tos] }

access-list ace <1-384> action { (deny | permit | shutdown) ingress any frame-type ipv4-icmp [mirror | metering | counter | dip | sip | ip-flag | tos | icmp-code | icmp-type] }

access-list ace <1-384> action { (deny | permit | shutdown) ingress any frame-type ipv4-tcp [mirror | metering | counter | dip | sip | ip-flag | tos | dport | sport | tcp-flag] }

access-list ace <1-384> action { (deny | permit | shutdown) ingress any frame-type ipv4-udp [mirror | metering | counter | dip | sip | ip-flag | tos | dport | sport] }

access-list ace <1-384> ingress { any | interface [* | GigabitEthernet <port_list>] }

access-list ace <1-384> ingress any [action | mirror | metering | counter | frame-type]

access-list ace <1-384> ingress interface { * [<port_list> | action | mirror | metering | counter | frame-type] | GigabitEthernet <port_list> }

access-list ace <1-384> mirror disable

```
access-list ace <1-384> mirror [ disable | action | ingress | metering | counter | frame-type ]

access-list ace <1-384> metering [disable | <16-1000000000>]

access-list ace <1-384> metering { ( disable | <16-1000000000> ) [ action | ingress | mirror | counter | frame-type ] }

access-list ace <1-384> counter disable

access-list ace <1-384> counter [ disable | action | ingress | mirror | metering | frame-type ]

access-list ace <1-384> frame-type any

access-list ace <1-384> frame-type any [ action | ingress | mirror | metering | counter ]

access-list ace <1-384> frame-type etype [ action | ingress | mirror | metering | counter | ctag | ctag-priority | ctag-vid | stag | stag-priority | stag-vid | dmac-type | dmac | smac | etype-value ]

access-list ace <1-384> frame-type etype [ ctag | stag ] [ any | tagged | untagged ]

access-list ace <1-384> frame-type etype [ ctag-priority | stag-priority ] [ any | 0-1 | 0-3 | 2-3 | 4-5 | 4-7 | 6-7 | <0-7> ]

access-list ace <1-384> frame-type etype [ ctag-vid | stag-vid ] [ any | <vlan_id> ]

access-list ace <1-384> frame-type etype dmac-type [ any | broadcast | multicast | unicast ]

access-list ace <1-384> frame-type etype [ dmac | smac ] [ any | <mac_addr> ]

access-list ace <1-384> frame-type etype etype-value [ any | <0x0000-0xFFFF> ]

access-list ace <1-384> frame-type ipv4 [ action | ingress | mirror | metering | counter | dip | sip | ip-protocol | ip-flag | tos ]

access-list ace <1-384> frame-type ipv4-icmp [ action | ingress | mirror | metering | counter | dip | sip | ip-flag | tos | icmp-code | icmp-type ]

access-list ace <1-384> frame-type ipv4-tcp [ action | ingress | mirror | metering | counter | dip | sip | ip-flag | tos | dport | sport | tcp-flag ]

access-list ace <1-384> frame-type ipv4-udp [ action | ingress | mirror | metering | counter | dip | sip | ip-flag | tos | dport | sport ]
```

Parameter

<1-384>	ACE ID (1..384)
action	Access list action

ingress	Ingress Port
mirror	Mirror frame to destination mirror port
metering	Bandwidth limitation on the traffic flow
counter	Count the packet if the ACE rule is matched
frame-type	Frame type
deny	Deny
permit	Permit
shutdown	Shutdown the interface
any	Don't-care the ingress interface
interface	Select an interface to configure
*	All switches or All ports
GigabitEthernet	GigabitEthernet
<port_list>	Port list in (1/1-26)
disable	Disable metering
disable	Disable mirror
disable	Disable counter
<16-1000000000>	Metering bandwidth in Kbps (16..1000000000)
any	Don't-care the frame type
etype	Frame type of etype
ipv4	Frame type of IPv4
ipv4-icmp	Frame type of IPv4 ICMP
ipv4-tcp	Frame type of IPv4 TCP
ipv4-udp	Frame type of IPv4 UDP
dip	Destination IP address field
sip	Source IP address field
ip-protocol	IP protocol

ip-flag	IP flag
tos	IPv4 traffic class field
icmp-code	ICMP code field
icmp-type	ICMP type field
ctag	C-VLAN Tag
ctag-priority	C-VLAN Tag-priority
ctag-vid	C-VLAN ID field
stag	S-VLAN Tag
stag-priority	S-VLAN Tag-priority
stag-vid	S-VLAN ID field
dmac-type	The type of destination MAC address
dmac	Destination MAC address field
smac	Source MAC address field
etype-value	Ether type value
dport	TCP/UDP destination port field
sport	TCP/UDP source port field
cp-flag	TCP flag
any	Don't-care tagged or untagged
tagged	Tagged
untagged	Untagged
any	Don't-care the value of tag priority field
0-1	The range of tag priority
0-3	The range of tag priority
2-3	The range of tag priority
4-5	The range of tag priority
4-7	The range of tag priority

6-7	The range of tag priority
<0-7>	The value of tag priority (0..7)
any	Don't-care the value of VID field
<vlan_id>	The value of VID field (1-4095)
any	Don't-care the type of destination MAC address
broadcast	Broadcast destination MAC address
multicast	Multicast destination MAC address
unicast	Unicast destination MAC address
any	Don't-care the value of destination MAC address field
<mac_addr>	The value of destination MAC address field
any	Don't-care the value of source MAC address field
<mac_addr>	The value of source MAC address field
any	Don't-care the value of etype field
<0x0000-0xFFFF>	The value of etype field

```
SP6526P(config)# access-list ace 10 action deny
SP6526P(config)#
```

21-1.5 aggregation

Aggregation mode.

SYNTAX

aggregation mode [dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac]

Parameter

mode	Traffic distribution mode
dst-ip	Destination IP address affects the distribution
dst-mac	Destination MAC affects the distribution

src-dst-ip	Source and Destination IP affect the distribution
src-dst-mac	Source and Destination MAC affect the distribution
src-ip	Source IP address affects the distribution
src-mac	Source MAC affects the distribution

EXAMPLE

```
SP6526P(config)# aggregation mode dst-ip

SP6526P(config)#
```

21-1.6 clock

Configure time-of-day clock.

SYNTAX

clock set date date

clock timezone { [acronym <word16>] | [clock_offset <-12:00-12:00>] }

clock summer-time mode_type <1-12> <1-5> <1-7> <0-23> <1-12> <1-5> <1-7> <0-23> <1-1440>

Parameter

set	set clock
summer-time	Configure summer (daylight savings) time
timezone	Configure time zone
date	yyyy/mm/dd
date	hh:mm:ss
acronym	name of time zone
clock_offset	Offset from UTC
word16	name of time zone. (word16)
<-12 :00-12 :00>	Hours offset from UTC.
mode_type	Enable or Disable time zone in summer. (disable/enable)
<1-12>	Month to start. (1..12)

<1-5>	Week number to start. (1..5)
<1-7>	Weekday to start. (1..7)
<0-23>	Hour to start. (0..23)
<1-12>	Month to end. (1..12)
<1-5>	Week number to end. (1..5)
<1-7>	Weekday to end. (1..7)
<0-23>	Hour to end. (0..23)
<1-1440>	Offset to add in minutes. (1..1440)

EXAMPLE

```
SP6526P(config)# clock set 2016/11/04 10:22:03
2016-11-04T10:22:03+00:00
SP6526P(config)# do show clock
System Time     : 2016-11-04T10:22:48+00:00
```

21-1.7 dms

DMS mode.

SYNTAX

dms mode

dms mode [high-priority | enabled | disabled]

Parameter

mode	DMS mode
high-priority	High Priority
enabled	Enabled
disabled	Disabled

EXAMPLE

```
SP6526P(config)# dms mode disabled
SP6526P(config)#
```

21-1.8 do

To run exec commands in config mode.

SYNTAX

do   < LINE >{[< LINE >]}

do clear access-list ace statistics

do clear ip dhcp relay statistics

do clear lldp statistics { global | [interface (GigabitEthernet <port_list> | *)] }

do clear logging [error | info | warning]

do clear spanning-tree detected-protocols interface (GigabitEthernet <port_list> | *)

do clear statistics interface (GigabitEthernet <port_list> | * <port_list>)

Parameter

Clear	Reset functions
configure	Enter configuration mode
copy	Copy from source to destination
delete	Delete one file in flash file system
diagnostics	diagnostics
dir	Directory of all files in flash file system
find-switch	Turn on and off all LED light 3 times in 15 seconds
firmware	firmware
logout	Exit from EXEC mode
more	Display file
ping	Send ICMP echo messages

reload	Reload system
show	Show running system information
ssl	Setup SSL certificate
terminal	Set terminal line parameters
traceroute	Trace the route to HOST
access-list	Access list
ip	Clear DHCP Relay statistics
lldp	Clear LLDP statistics for one or more given interface
logging	Syslog
mac	MAC Address Table
spanning-tree	Execute protocol migration check on interfaces
statistics	Clear statistics for one or more given interface
ace	Access list entry
statistics	Traffic statistics
dhcp	Clear DHCP Relay statistics
relay	Clear DHCP Relay statistics
statistics	Clear DHCP Relay statistics
statistics	Clear LLDP statistics
global	Clear global counters
interface	Interface
GigabitEthernet	GigabitEthernet
*	All ports
<port_list>	Port List S/X-Y,Z (1/1-26)
Error	Error
info	Information
warning	Warning

address-table	Flush MAC Address table
detected-protocols	Clear spanning-tree detected protocols, i.e. mcheck.
interface	Interface
*	All switches or All ports

EXAMPLE

```
SP6526P(config)# do clear statistics interface GigabitEthernet 1/1-26
SP6526P(config)#
```

21-1.9 dot1x

IEEE Standard for port-based Network Access Control.

SYNTAX

dot1x authentication timer re-authenticate <1-3600>

dot1x feature guest-vlan

dot1x guest-vlan [<1-4095> | supplicant]

dot1x max-reauth-req <1-255>

dot1x re-authentication

dot1x system-auth-control

dot1x timeout tx-period <1-65535>

Parameter

authentication	Authentication
feature	Globally enables/disables a dot1x feature functionality
guest-vlan	Guest VLAN
max-reauth-req	The number of times a Request Identity EAPOL frame is sent without response before considering entering the Guest VLAN
re-authentication	Set Re-authentication state
system-auth-control	Set the global NAS state

timeout	timeout
timer	timer
re-authenticate	The period between re-authentication attempts in seconds
<1-3600>	seconds (1..3600)
guest-vlan	Globally enables/disables state of guest-vlan
<1-4095>	Guest VLAN ID used when entering the Guest VLAN (1..4095)
supplicant	The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest
<1-255>	number of times (1..255)
tx-period	the time between EAPOL retransmissions.
<1-65535>	seconds (1..65535)

EXAMPLE

```
SP6526P(config)# dot1x authentication timer re-authenticate 1000
SP6526P(config)# dot1x feature guest-vlan
SP6526P(config)# dot1x guest-vlan 33
SP6526P(config)# dot1x max-reauth-req 3
SP6526P(config)# dot1x re-authentication
SP6526P(config)# dot1x system-auth-control
SP6526P(config)# dot1x timeout tx-period 3000
```

21-1.10 end

Go back to EXEC mode.

Syntax:

end

Example:

```
SP6526P (config)# end
SP6526P#
```

21-1.11 event

Trap event level.

SYNTAX

event group [aclaccess-mgmt | arp-inspection | auth-failed | bsc-protection | cold-start | dhcp | dhcp-snooping | ip-source-guard | lacp | link-updown | login | logout | loop-protection | mac-table | maintenance | mgmt-ip-change | nas | port | port-security | rmon | sfp | spanning-tree | system | user | warm-start] { [level < 0-7 >] | { syslog [enable | disable] } | { trap [enable | disable] } }

event group [acl | aclaccess-mgmt | arp-inspection | auth-failed | bsc-protection | cold-start | dhcp | dhcp-snooping | ip-source-guard | lacp | link-updown | login | logout | loop-protection | mac-table | maintenance | mgmt-ip-change | nas | port | port-security | rmon | sfp | spanning-tree | system | user | warm-start] [level | syslog | trap]

event group [acl | aclaccess-mgmt | arp-inspection | auth-failed | bsc-protection | cold-start | dhcp | dhcp-snooping | ip-source-guard | lacp | link-updown | login | logout | loop-protection | mac-table | maintenance | mgmt-ip-change | nas | port | port-security | rmon | sfp | spanning-tree | system | user | warm-start] [level | syslog | trap] < 0-7 > { syslog [enable | disable] [trap] } | { trap [enable | disable] [syslog] }

Parameter

group	Trap Event group name
acl	Group ID ACL
access-mgmt	Group ID ACCESS-MGMT
arp-inspection	Group ID ARP-INSPECTION
auth-failed	Group ID AUTH-FAILED
bsc-protection	Group ID BCS-PROTECTION
cold-start	Group ID COLD-START
dhcp	Group ID DHCP
dhcp-snooping	Group ID DHCP-SNOOPING
ip-source-guard	Group ID IP-SOURCE-GUARD

lacp	Group ID LACP
link-updown	Group ID LINK-UPDOWN
login	Group ID LOGIN
logout	Group ID LOGOUT
loop-protection	Group ID LOOP-PROTECTION
mac-table	Group ID MAC-TABLE
maintenance	Group ID MAINTENANCE
mgmt-ip-change	Group ID MGMT-IP-CHANGE
nas	Group ID NAS
port	Group ID PORT
port-security	Group ID PORT-SECURITY
rmon	Group ID RMON
sfp	Group ID SFP
spanning-tree	Group ID SPANNING-TREE
system	Group ID SYSTEM
user	Group ID USER
warm-start	Group ID WARM-START
level	event group level
syslog	syslog mode
trap	trap mode
<0-7>	<0> Emergency ,<1> Alert ,<2> Critical ,<3> Error ,<4> Warning ,<5> Notice ,<6> Informationl ,<7> Debug (0..7)
enable	syslog mode enable
disable	syslog mode disable
enable	trap mode enable
disable	trap mode disable

EXAMPLE

```
SP6526P(config)# event group lacp trap enable
SP6526P(config)#
```

21-1.12 interface

Select an interface to configure.

SYNTAX

interface vlan <vlan_list>

interface vlan <vlan_list> end

interface vlan <vlan_list> exit

interface vlan <vlan_list> ip (address | dhcp | igmp) <ipv4_addr> <ipv4_netmask>

interface vlan <vlan_list> ip address dhcp

interface vlan <vlan_list> ip address dhcp fallback <ipv4_addr> <ipv4_netmask>

interface vlan <vlan_list> ip address dhcp fallback <ipv4_addr> <ipv4_netmask> timeout

interface vlan <vlan_list> ip address dhcp fallback <ipv4_addr> <ipv4_netmask> timeout <0-4294967295>

interface GigabitEthernet <port_list>

Parameter

vlan	VLAN interface configurations
GigabitEthernet	1 Gigabit Ethernet Port
<vlan_list>	List of VLAN interface numbers, 1~4094 (1-4095)
!	Comments
end	Go back to EXEC mode
exit	Exit from current mode
ip	Interface Internet Protocol config commands
ipv6	Interface IPv6 config commands
no	Negate a command or set its defaults

Address	Address configuraton
dhcp	Dynamic Host Configuration Protocol
igmp	ip mode
<ipv4_addr>	IP address (X.X.X.X)
dhcp	Enable DHCP client
<ipv4_netmask>	IP netmask (X.X.X.X)
fallback	DHCP fallback settings
timeout	DHCP fallback timeout
<0-4294967295>	DHCP fallback timeout in seconds (0..4294967295)
address	Address configuraton
mld	ipv6 mode
<port_list>	Port List S/X-Y,Z (1/1-26)

EXAMPLE

```
SP6526P(config)# interface GigabitEthernet 1/1-26
SP6526P(config-if)#
SP6526P(config-if)#  interface vlan 3
SP6526P(config-if-vlan)#
```

21-1.13 ip

Internet Protocol.

SYNTAX

ip arp inspection

ip arp inspection entry interface [* | GigabitEthernet <port_id>] <vlan_id> <mac_ucast> <ipv4_ucast>

ip arp inspection vlan <vlan_list>

ip arp inspection vlan <vlan_list> logging [deny | permit | all]

ip dhcp pool <vlan_id>

ip dhcp relay

ip dhcp relay information option

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

ip dhcp snooping

ip helper-address <ipv4_ucast>

ip igmp snooping

ip igmp host-proxy

ip igmp ssm-range <ipv4_mcast> <4-32>

ip igmp unknown-flooding

ip name-server { <ipv4_ucast> | [dhcp interface vlan <vlan_id>] }

ip route <ipv4_addr> <ipv4_netmask> <ipv4_ucast>

ip source binding interface [* | GigabitEthernet <port_id>] <ipv4_ucast> <mac_ucast>

ip verify source

Parameter

arp	Address Resolution Protocol
dhcp	Dynamic Host Configuration Protocol
helper-address	DHCP helper server address
igmp	Internet Group Management Protocol
name-server	Domain Name System
route	Add IP route
source	source command
verify	verify command
inspection	ARP inspection
entry	arp inspection entry
vlan	arp inspection vlan setting
interface	Select an interface to configure

*****	All switches or All ports
GigabitEthernet	GigabitEthernet
<port_id>	Port ID in (1/1-26)
<vlan_id>	Select a VLAN id to configure (1-4095)
<mac_ucast>	Select a MAC address to configure
<ipv4_ucast>	Select an IP Address to configure (X.X.X.X)
<vlan_list>	arp inspection vlan list (1-4095)
logging	ARP inspection vlan logging mode config
all	log all entries
deny	log denied entries
permit	log permitted entries
pool	DHCP server pool
relay	DHCP relay
snooping	DHCP snooping
<vlan_id>	VLAN id of DHCP server pool (1-4095)
information	DHCP information option <Option 82>
option	DHCP option 82
policy	Policy for handling the receiving DHCP packet already include the information option
drop	Drop the package
keep	Keep the original relay information
replace	Replace the original relay information
<ipv4_ucast>	IP Address (X.X.X.X)
snooping	Snooping IGMP
host-proxy	IGMP proxy configuration
unknown-flooding	Flooding unregistered IPv4 multicast traffic
ssm-range	IPv4 address range of Source Specific Multicast

<ipv4_mcast>	Valid IPv4 multicast address (X.X.X.X)
<4-32>	Prefix length ranges from 4 to 32
<ipv4_ucast>	A valid IPv4 unicast address (X.X.X.X)
dhcp	Dynamic Host Configuration Protocol
interface	Select an interface to configure
vlan	VLAN Interface
<vlan_id>	VLAN identifier(s): VID (1-4095)
<ipv4_addr>	Network (X.X.X.X)
<ipv4_netmask>	Netmask (X.X.X.X)
<ipv4_ucast>	Gateway (X.X.X.X)
binding	ip source binding
interface	ip source binding entry interface config
<ipv4_ucast>	Select an unicast IP address to configure (X.X.X.X)
<mac_ucast>	Select an unicast MAC address to configure
source	verify source

EXAMPLE

```
SP6526P(config)# ip arp inspection
SP6526P(config)# ip dhcp relay
SP6526P(config)# ip helper-address 192.168.1.1
SP6526P(config)# ip name-server 192.168.1.6
SP6526P(config)# ip route 192.168.1.1 255.255.255.0 192.168.1.100
SP6526P(config)# ip verify source
IP Source Guard:
      Translate 0 dynamic entries into static entries.
```

21-1.14 ipmc

IPv4/IPv6 multicast configuration.

SYNTAX

ipmc profile word16

ipmc range word16 [<ipv4_mcast> | <ipv6_mcast>]

ipmc mode

Parameter

profile	Ipmc profile provides the rules for specific group addresses.
range	A range of IPv4/IPv6 multicast addresses for the profile
mode	IPMC profile mode
word16	Profile name in 16 char's (word16)
word16	Range entry name in 16 char's (word16)
<ipv4_mcast>	Valid IPv4 multicast address
<ipv6_mcast>	Valid IPv6 multicast address

EXAMPLE

```
SP6526P(config)# ipmc profile test
SP6526P(config-ipmc-profile)#
```

21-1.15 ipv6

IPv6 configuration commands.

SYNTAX

ipv6 mld host-proxy

ipv6 mld snooping

ipv6 mld ssm-range <ipv6_mcast> Unsigned integer

ipv6 mld unknown-flooding

Parameter

mld	Multicasat Listener Discovery
host-proxy	MLD proxy configuration
snooping	Snooping MLD

ssm-range	IPv6 address range of Source Specific Multicast
unknown-flooding	Flooding unregistered IPv6 multicast traffic
<ipv6_mcast>	Valid IPv6 multicast address (X:X:X:X:X:X:X:X)
Unsigned integer	Prefix length ranges from 4 to 32

EXAMPLE

```
SP6526P(config)# ipv6 mld host-proxy
SP6526P(config)# ipv6 mld snooping
SP6526P(config)#
```

21-1.16 lacp

Lacp system configuration.

SYNTAX

lacp system-priority <1-65535>

Parameter

system-priority	System priority
<1-65535>	Aggregation group number (1..65535)

EXAMPLE

```
SP6526P(config)# lacp system-priority 333
SP6526P(config)#
```

21-1.17 lldp

LLDP configurations.

SYNTAX

lldp holdtime <2-10>

lldp med datum [wgs84 | nad83_navd88 | nad83_mllw]

lldp med fast <1-10>

lldp med location-tlv altitude [meters | floors] <-32767-32767>

lldp med location-tlv civic-addr [country | state | county | city | district | block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark | additional-info | name | zip-code | building | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code] [word50 | word2]

lldp med location-tlv elin-addr <phone_call_str>

lldp med location-tlv latitude [north | south] <0-90>

lldp med location-tlv longitude [west | east] <0-180>

lldp med media-vlan-policy <0-31> { voice | voice-signaling | guest-voice-signaling | guest-voice | softphone-voice | video-conferencing | streaming-video | video-signaling } { tagged <1-4095> | untagged } [l2-priority <0-7>] [dscp <0-63>]

lldp reinit <1-10>

lldp timer <5-32768>

lldp transmission-delay <1-8192>

Parameter

holdtime	Sets LLDP hold time
med	Media Endpoint Discovery.
reinit	Sets LLDP reinit time
timer	Sets LLDP TX interval
transmission-delay	Sets LLDP transmision-delay.
<2-10>	The neighbor switch will discarded the LLDP information after hold time multiplied with timer seconds (2..10)
datum	Datum type
fast	Number of times to repeat LLDP frame transmission at fast start
location-tlv	LLDP-MED Location Type Length Value parameter

media-vlan-policy	Use the media-vlan-policy to create a policy, which can be assigned to an interface
nad83_mllw	Mean lower low water datum 1983
nad83_navd88	North American vertical datum 1983
wgs84	World Geodetic System 1984
<1-10>	Fast start repeat count (1..10)
altitude	Altitude parameter
civic-addr	Civic address information and postal information
elin-addr	Emergency Location Identification Number
latitude	Latitude parameter
longitude	Longitude parameter
meter	Specify the altitude in meters
floors	Specify the altitude in floor
<-32767-32767>	Specify the altitude in floor (-32767..32767)
<-32767-32767>	Specify the altitude in meters (-32767..32767)
country	The two-letter ISO 3166 country code in capital ASCII letters
word2	Example: DK, DE or US (word2) (for **country**)
state	National subdivisions
word50	state, canton, region, province, prefecture (word50) (for **state**)
county	County, parish, gun (Japan), district
word50	County, parish, gun (Japan), district (word50) (for **county**)
city	City, township, shi (Japan) - Example: Copenhagen
word50	City, township, shi (Japan) - Example:Copenhagen (word50) (for **city**)
district	City division, borough, city district, ward, chou (Japan)
word50	City division, borough, city district, ward, chou (Japan) (word50) (for **district**)
block	Neighbourhood, block

word50	Neighborhood, block (word50) (for **block**)
street	Street
word50	Example: Poppelvej (word50) (for **street**)
leading-street-direction	Leading street direction
word50	Example: N (word50) (for **leading-street-direction**)
trailing-street-suffix	Trailing street suffix
word50	Example: SW (word50) (for **trailing-street-suffix**)
street-suffix	Street suffix – Example
word50	Example: Ave, Platz (word50) (for **street-suffix**)
house-no	House number
word50	Example: 21 (word50) (for **house-no**)
house-no-suffix	House number suffix
word50	Example: A, 1/2 (word50) (for **house-no-suffix**)
landmark	Landmark or vanity address
word50	Example: Columbia University (word50) (for **landmark**)
additional-info	Additional location info
word50	Example: South Wing (word50) (for **additional-info**)
name	Name (residence and office occupant)
word50	Example: Flemming Jahn (word50) (for **name**)
zip-code	Postal/zip code
word50	Example: 2791 (word50) (for **zip-code**)
building	Building (structure)
word50	Example: Low Library (word50) (for **building**)
apartment	Unit (Apartment, suite)
word50	Example: Apt 42 (word50) (for **apartment**)
floor	Floor

word50	Example: 4 (word50) (for **floor**)
room-number	Room number
word50	Example: 450F (word50) (for **room-number**)
place-type	Place type
word50	Example: Office (word50) (for **place-type**)
postal-community-name	Postal community name
word50	Example: Leonia. (word50) (for **postal-community-name**)
p-o-box	Post office box (P.O. BOX)
word50	Example: 12345 (word50) (for **p-o-box**)
additional-code	Additional code
word50	Example: 1320300003 (word50) (for **additional-code**)
<phone_call_str>	ELIN value
north	Setting latitude direction to north
south	Setting latitude direction to south
<0-90>	Setting latitude direction to south (0..90)
east	Setting longitude direction to east
west	Setting longitude direction to west
<0-180>	Setting longitude direction to east (0..180)
<0-31>	Policy id for the policy which is created.
voice	Create a voice policy.
voice-signaling	Create a voice signaling policy.
guest-voice-signaling	Create a guest voice signaling policy.
guest-voice	Create a guest voice policy.
softphone-voice	Create a softphone voice policy.
video-conferencing	Create a video conferencing policy.
streaming-video	Create a streaming video policy.

video-signaling	Create a video signaling policy.
tagged	The policy uses tagged frames.
untagged	The policy uses un-tagged frames
<1-4095>	The VLAN the policy uses tagged frames (1..4095)
l2-priority	Layer 2 priority
<0-7>	Priority 0-7 (0..7)
dscp	Differentiated Services Code Point
<0-63>	DSCP value 0-63 (0..63)
<1-10>	LLDP tx reinitialization delay in seconds (1..10)
<5-32768>	The time between each LLDP frame transmitted in seconds (5..32768)
<1-8192>	LLDP transmission delay (1..8192)

EXAMPLE

```
SP6526P(config)# lldp holdtime 5
SP6526P(config)# lldp med fast 5
SP6526P(config)# lldp reinit 3
SP6526P(config)# lldp timer 555
SP6526P(config)# lldp transmission-delay 333
Note: According to IEEE 802.1AB-clause 10.5.4.2 the transmission-delay must not
be larger than LLDP timer * 0.25. LLDP timer changed to 13332
```

21-1.18 logging

Syslog.

SYNTAX

logging host <1-6> { <ipv4_ucast> | <hostname> }

logging on

Parameter

host	host

on	Enable syslog server
<1-6>	host number (1..6)
<hostname>	Donain name of the log server
<ipv4_ucast>	IP address of the log server (X.X.X.X)

EXAMPLE

```
SP6526P(config)# logging host 3 192.155.3.2
SP6526P(config)#
SP6526P(config)# logging on
SP6526P(config)#
```

21-1.19 loop-protect

Loop protection configuration.

SYNTAX

loop-protect

loop-protect shutdown-time <10-604800>

loop-protect transmit-time <1-10>

Parameter

shutdown-time	Loop protection shutdown time interval
transmit-time	Loop protection transmit time interval
<10-604800>	Shutdown time in second (10..604800)
<1-10>	Transmit time in second (1..10)

EXAMPLE

```
SP6526P(config)# loop-protect
SP6526P(config)# loop-protect shutdown-time 333
SP6526P(config)# loop-protect transmit-time 3
SP6526P(config)#
```

21-1.20 mac

MAC table entries/configuration.

SYNTAX

mac address-table aging-time <10-1000000>

mac address-table static <mac_addr> vlan <vlan_id> { (interface [* | GigabitEthernet <port_id>]) | block }

Parameter

address-table	MAC table entries/configuration
aging-time	Mac address aging time
static	Static MAC address
<10-1000000>	Aging time in seconds (10..1000000)
<mac_addr>	48 bit MAC address: xx:xx:xx:xx:xx:xx
vlan	VLAN keyword
<vlan_id>	VLAN IDs 1-4095 (1-4095)
block	Drop the packet which MAC Address and VLAN ID is match
interface	Select an interface to configure
*****	All switches or All ports
Gigabitethernet	1 Gigabit Ethernet port
<port_id>	Port ID in (1/1-26)

EXAMPLE

```
SP6526P(config)# mac address-table aging-time 3333
SP6526P(config)#
```

21-1.21 monitor

Monitoring different system events.

SYNTAX

monitor session 1

monitor session 1 destination interface [* | GigabitEthernet] <port_id>

monitor session 1 source interface [* | GigabitEthernet] <port_list> [both | rx | tx]

monitor session 1 source interface [* | GigabitEthernet] [both | rx | tx]

Parameter

session	Configure a MIRROR session
<1>	MIRROR session number (1..1)
destination	MIRROR destination interface
source	MIRROR source interface
interface	MIRROR destination interface
*****	All switches or All ports
GigabitEthernet	GigabitEthernet
<port_id>	Port ID in (1/1-26)
Interface	MIRROR source interface
<port_list>	Port List S/X-Y,Z (1/1-26)
both	Mirror both ingress and egress traffic.
rx	Mirror ingress traffic.
tx	Mirror egress traffic.

EXAMPLE

```
SP6526P(config)# monitor session 1 destination interface GigabitEthernet 1/9
SP6526P(config)# monitor session 1 source interface GigabitEthernet 1/5 both
SP6526P(config)#
```

21-1.22 mvr

MVR multicast VLAN list

SYNTAX

mvr

mvr vlan <vlan_list> name word16

mvr vlan <vlan_list> channel word16

mvr vlan <vlan_list> frame priority <Priority : 0-7>

mvr vlan <vlan_list> frame tagged untagged/tagged

mvr vlan <vlan_list> igmp-address <ipv4_addr>

mvr vlan <vlan_list> last-member-query-interval <Range : 0-31744 tenths of seconds>

mvr vlan <vlan_list> mode [dynamic | compatible]

Parameter

vlan	MVR multicast vlan list
<vlan_list>	MVR multicast VLAN list (1-4095)
name	MVR multicast name
frame	MVR control frame in TX
mode	MVR mode of operation
last-member-query-interval	Last Member Query Interval in tenths of seconds
channel	MVR channel configuration
igmp-address	MVR address configuration used in IGMP
word16	Range entry name in 16 char's (word16)
word16	Profile name in 16 char's (word16)
priority	Interface CoS priority
tagged	Tagged IGMP/MLD frames will be sent
<Priority : 0-7>	Range : 0-7 (0..7)
untagged/tagged	tagged mode
<ipv4_addr>	A valid IPv4 unicast address (X.X.X.X)
<Range : 0-31744 tenths of seconds>	Last Member Query Interval in tenths of seconds (0..31744)
compatible	Compatible MVR operation mode

dynamic	Dynamic MVR operation mode	MVR mode of operation

EXAMPLE

```
SP6526P(config)# mvr vlan 10 mode dynamic
SP6526P(config)#
```

21-1.23 no

Negate a command or set its defaults.

Table : configure – no Commands

Command	Function
aaa	Authentication, Authorization and Accounting
access	Access management
access-list	Access list
aggregation	Aggregation mode
clock	Configure time-of-day clock
dot1x	IEEE Standard for port-based Network Access Control
interface	Select an interface to configure
ip	Internet Protocol
ipmc	IPv4/IPv6 multicast configuration
ipv6	IPv6 configuration commands
lacp	LACP system configuration
lldp	LLDP configurations
logging	Syslog
loop-protect	Loop protection configuration
mac	MAC table entries/configuration
monitor	Monitoring different system events
mvr	Multicast VLAN Registration configuration
ntp	Configure NTP
poe	Power Over Ethernet
port-security	Enable/disable port security globally
Privilege	Privilege level
qos	Quality of Service
radius-server	Configure RADIUS
rmon	Remote Monitoring
snmp-server	Enable SNMP server
spanning-tree	Spanning Tree protocol
system	Set the SNMP server's configurations

tacacs-server	Configure TACACS+
trap	Trap
upnp	Set UPnP's configurations
username	Establish User Name Authentication
vlan	Vlan commands
voice	Voice appliance attributes

21-1.23.1 aaa

Authentication, Authorization and Accounting.

SYNTAX

no aaa authentication login [telnet | ssh | http]

no aaa authentication service-port [ssh | telnet | http | https]

no aaa authentication redirect

no aaa authorization [ssh | telnet]

no aaa accounting [ssh | telnet]

Parameter

authentication	Authentication
authorization	Authorization
accounting	Accounting
login	Login
service-port	Service port
redirect	HTTP redirect HTTPS
http	Configure HTTP
ssh	Configure SSH
telnet	Configure Telnet
https	Configure HTTPS
telnet	telnet

ssh	ssh

EXAMPLE

```
SP6526P(config)# no aaa authentication  login ssh
SP6526P(config)#
```

21-1.23.2 access

Access management.

SYNTAX

no access management <1~16>]

no access management

Parameter

management	Access management configuration
<1~16>	ID of access management entry (1..16)

EXAMPLE

```
SP6526P(config)# no access management
SP6526P(config)#
```

21-1.23.3 access-list

Access list.

SYNTAX

no access-list ace <1~384>

Parameter

ace	Access list entry
<1-384>	ACE ID (1-384)

EXAMPLE

```
SP6526P(config)# access-list ace 1
SP6526P(config)#
```

21-1.23.4 aggregation

Aggregation mode.

SYNTAX

no aggregation mode

Parameter

mode	Traffic distribution mode

EXAMPLE

```
SP6526P(config)# no aggregation mode
SP6526P(config)#
```

21-1.23.5 clock

Configure time-of-day clock.

SYNTAX

no clock summer-time

no clock timezone

Parameter

summer-time	Configure summer (daylight savings) time
timezone	Configure time zone

EXAMPLE

```
SP6526P(config)# no clock summer-time
SP6526P(config)# no clock timezone
SP6526P(config)#
```

21-1.23.6 dot1x

IEEE Standard for port-based Network Access Control.

SYNTAX

no dot1x authentication timer re-authenticate

no dot1x feature guest-vlan

no dot1x guest-vlan

no dot1x guest-vlan supplicant

no dot1x max-reauth-req

no dot1x re-authentication

no dot1x system-auth-control

no dot1x timeout tx-period

Parameter

authentication	Authentication
feature	Globally enables/disables a dot1x feature functionality
guest-vlan	Guest VLAN
max-reauth-req	The number of time a Request Identity EAPOL frame is sent without response before considering entering the Guest VLAN
re-authentication	Set Re-authentication state
system-auth-control	Set the global NAS state
timeout	timeout
timer	timer
re-authenticate	The period between re-authentication attempts in seconds
guest-vlan	Globally enables/disables state of guest-vlan
supplicant	The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest
tx-period	The time between EAPOL retransmissions

EXAMPLE

```
SP6526P(config)# no dot1x authentication timer re-authenticate

SP6526P(config)# no dot1x guest-vlan supplicant

SP6526P(config)# no dot1x max-reauth-req

SP6526P(config)# no dot1x re-authentication

SP6526P(config)# no dot1x system-auth-control

SP6526P(config)# no dot1x timeout tx-period

SP6526P(config)#
```

21-1.23.7 interface

Select an interface to configure.

SYNTAX

no interface vlan <vlan_list>

Parameter

vlan	Vlan interface configurations
<vlan_list>	List of VLAN interface numbers, 1~4094 (1-4095)

EXAMPLE

```
SP6526P(config)# no interface vlan 10

SP6526P(config)#
```

21-1.23.8 Ip

Internet Protocol.

SYNTAX

no ip arp inspection

no ip arp inspection entry interface { * | [Gigabitethernet <port_id>] } <vlan_id> <mac_ucast> <ipv4_ucast>

no ip arp inspection vlan <vlan_list> logging

no dhcp pool <vlan_id>

no ip dhcp relay information [option | policy]

no ip dhcp relay

no ip dhcp snooping

no ip helper-address

no ip igmp host-proxy

no ip igmp snooping

no ip igmp unknown-flooding

no ip name-server

no ip route <ipv4_addr> <ipv4_netmask> <ipv4_ucast>

no ip source binding interface { [* | Gigabitethernet] <port_id> <ipv4_ucast> <mac_ucast> }

no ip verify source

Parameter

arp	Address Resolution Protocol
dhcp	Dynamic Host Configuration Protocol
helper-address	DHCP helper server address
igmp	set igmp
name-server	Domain Name System
route	Add IP route
source	source command
verify	verify command
inspection	ARP inspection
entry	arp inspection entry
vlan	arp inspection vlan setting
interface	Select an interface to configure
GigabitEthernet	GigabitEthernetPort
*****	All switches or All ports
<port_id>	Port ID in (1/1-26)

<vlan_id>	Select a VLAN id to configure (1-4095)
<mac_ucast>	Select a MAC address to configure
<ipv4_ucast>	Select an IP Address to configure (X.X.X.X)
<vlan_list>	arp inspection vlan list (1-4095)
logging	ARP inspection vlan logging mode config
pool	DHCP server pool
relay	DHCP relay
snooping	DHCP snooping
<vlan_id>	VLAN id of DHCP server pool (1-4095)
information	DHCP information option(Option 82)
option	DHCP option 82
policy	Policy for handling the receiving DHCP packet already include the information option
host-proxy	IGMP proxy configuration
snooping	Snooping IGMP
unknown-flooding	Flooding unregistered IPv4 multicast traffic
<ipv4_addr>	Network (X.X.X.X)
<ipv4_netmask>	Netmask (X.X.X.X)
<ipv4_ucast>	Gateway (X.X.X.X)
binding	ip source binding
interface	ip source binding entry interface config
<ipv4_ucast>	Select an unicast IP address to configure (X.X.X.X)
<mac_ucast>	Select an unicast MAC address to configure
source	verify source

EXAMPLE

```
SP6526P(config)# no ip arp inspection vlan 3 logging
SP6526P(config)# no ip helper-address
SP6526P(config)# no ip igmp snooping
SP6526P(config)# no ip name-server
SP6526P(config)# no ip verify source
SP6526P(config)#
```

21-1.23.9 ipmc

IPv4/IPv6 multicast configuration.

SYNTAX

no mode

no ipmc profile word16

no ipmc range word16

Parameter

profile	IPMC profile configuration
range	A range of IPv4/IPv6 multicast addresses for the profile
mode	IPMC profile mode
word16	Range entry name in 16 char's (word16)
word16	Profile name in 16 char's (word16)

EXAMPLE

```
SP6526P(config)# no ipmc profile aa
SP6526P(config)#
```

21-1.23.10 ipv6

IPv6 configuration commands.

SYNTAX

no ipv6 mld host-proxy

no ipv6 mld snooping

no ipv6 mld unknown-flooding

Parameter

mld	Multicasat Listener Discovery
host-proxy	MLD proxy configuration
snooping	Snooping MLD
unknown-flooding	Flooding unregistered IPv6 multicast traffic

EXAMPLE

```
SP6526P(config)# no ipv6 mld snooping
SP6526P(config)#
```

21-1.23.11 lacp

Lacp system configuration.

SYNTAX

no lacp system-priority

Parameter

system-priority	System priority

EXAMPLE

```
SP6526P(config)# no lacp system-priority
SP6526P(config)#
```

21-1.23.12 lldp

LLDP configurations.

SYNTAX

no lldp holdtime

no lldp med datum

no lldp med fast

no lldp med location-tlv altitude

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

no lldp med location-tlv elin-addr

no lldp med location-tlv latitude

no lldp med location-tlv longitude

no lldp med media-vlan-policy <0~31>

no lldp reinit

no lldp timer

no lldp transmission-delay

Parameter

holdtime	LLDP hold time
med	Media Endpoint Discovery
reinit	LLDP reinit time
timer	LLDP TX interval
transmission-delay	LLDP transmision-delay
datum	datum typa
fast	Number of times to repeat LLDP frame transmission at fast start
location-tlv	LLDP-MED Location Type Length Value parameter
media-vlan-policy	Use the media-vlan-policy to create a policy, which can be assigned to an interface
altitude	Altitude parameter
latitude	Latitude parameter
longitude	Longitude parameter

elin-addr	Emergency Location Identification Number
civic-addr	Civic address information and postal information
country	The two-letter ISO 3166 country code in capital ASCII letters
state	National subdivisions
county	County, parish, gun (Japan), district
city	City, township, shi (Japan) - Example: Copenhagen
district	City division, borough, city district, ward, chou (Japan)
block	Neighbourhood, block
street	Street
leading-street-direction	Leading street direction
trailing-street-suffix	Trailing street suffix
street-suffix	Street suffix
house-no	House number
house-no-suffix	House number suffix
landmark	Landmark or vanity address
additional-info	Additional location info
name	Name (residence and office occupant)
zip-code	Postal/zip code
building	Building (structure)
apartment	Unit (Apartment, suite)
floor	Floor
room-number	Room number
place-type	Place type
postal-community-name	Postal community name
p-o-box	Post office box (P.O. BOX)

additional-code	Additional code
<0~31>	Policy id for the policy which is created (0..31)

EXAMPLE

```
SP6526P(config)# no lldp holdtime
SP6526P(config)# no lldp med location-tlv civic-addr floor
SP6526P(config)# no lldp reinit
SP6526P(config)# no lldp timer
SP6526P(config)# no lldp transmission-delay
SP6526P(config)#
```

21-1.23.13 logging

Syslog.

SYNTAX

no logging host <1-6>

no logging on

Parameter

host	host
on	Enable syslog server
<1-6>	host number (1..6)

EXAMPLE

```
SP6526P(config)# no logging host 3
SP6526P(config)# no logging on
SP6526P(config)#
```

21-1.23.14 loop-protect

Loop protection configuration.

SYNTAX

no loop-protect

no loop-protect shutdown-time

no loop-protect transmit-time

Parameter

shutdown-time	Loop protection shutdown time interval
transmit-time	Loop protection transmit time interval

EXAMPLE

```
SP6526P(config)# no loop-protect shutdown-time
SP6526P(config)# no loop-protect transmit-time
SP6526P(config)#
```

21-1.23.15 mac

MAC table entries/configuration.

SYNTAX

no mac address-table aging-time

no mac address-table static <mac_addr> vlan <vlan_id>

no mac address-table static <mac_addr>

Parameter

address-table	Mac table entries configuration/table
aging-time	Mac address aging time
static	Static MAC address
<mac_addr>	48 bit MAC address: xx:xx:xx:xx:xx:xx
vlan	VLAN keyword
<vlan_id>	VLAN IDs 1-4095 (1-4095)

EXAMPLE

```
SP6526P(config)# no mac address-table aging-time
SP6526P(config)# no mac address-table static <mac_addr>
SP6526P(config)#
```

21-1.23.16 monitor

Monitoring different system events.

SYNTAX

no monitor session <1>

no monitor session <1> destination

no monitor session <1> source interface [* | Gigabitethernet] <port_list> [both | rx | tx]

Parameter

session	Configure a MIRROR session
<1>	MIRROR session number (1..1)
destination	MIRROR destination interface
source	MIRROR source interface
interface	Mirror source Interface
*	All switches or All ports
Gigabitethernet	GigabitEthernet
<port_list>	Port List S/X-Y,Z (1/1-26)
both	Mirror both ingress and egress traffic.
rx	Mirror ingress traffic.
tx	Mirror egress traffic.

EXAMPLE

```
SP6526P(config)# no monitor session 1 destination
SP6526P(config)# no monitor session 1 source interface GigabitEthernet
1/5 both
SP6526P(config)#
```

21-1.23.17 mvr

Multicast VLAN Registration configuration.

SYNTAX

no mvr

EXAMPLE

```
SP6526P(config)# no mvr
SP6526P(config)#
```

21-1.23.18 ntp

Configure NTP.

SYNTAX

no ntp

no ntp server <1-6>

no ntp interval

Parameter

server	Configure NTP server
interval	Configure NTP interval
<1-6>	index number (1..6)

EXAMPLE

```
SP6526P(config)# no ntp server 2
SP6526P(config)#
```

21-1.23.19 port-security

Enable/disable port security globally.

SYNTAX

no port-security

EXAMPLE

```
SP6526P(config)# no port-security
SP6526P(config)#
```

21-1.23.20 Privilege

Privilege level

SYNTAX

no privilege group [access-mgmt | arp-inspection | auth-method | dhcp-relay | dhcp-snooping | diagnostic | dot1x | eee | event | forward-failure | ip | ipmc | ip-source-guard | lacp | lldp | loop-protection | mac-table | mirror | mvr | poe | port | port-security | qos | radius | snmp | stp | system | upnp | vlan] level

no privilege group level

Parameter

group	Privilege group name
<group>	Privilege group name (access-mgmt / arp-inspection / auth-method / dhcp-relay / dhcp-snooping / diagnostic / dot1x / eee / event / forward-failure / ip / ipmc / ip-source-guard / lacp / lldp / loop-protection / mac-table / mirror / mvr / poe / port / port-security / qos / radius / snmp / stp / system / upnp / vlan)
level	Privilege group level

EXAMPLE

```
SP6526P(config)# no privilege group access-mgmt level
SP6526P(config)#
```

21-1.23.21 Qos

Quality of Service.

SYNTAX

no qos map cos-queue

no qos map cos-queue <0-7>

no qos map dscp-queue

no qos map dscp-queue <0-63>

no qos map precedence-queue

no qos map precedence-queue <0-7>

no qos map queue-cos

no qos map queue-cos <0-7>

no qos map queue-dscp

no qos map queue-dscp <0-7>

no qos map queue-precedence

no qos map queue-precedence <0-7>

no qos trust

Parameter

map	QoS Global Map/Table
trust	Restore global trust mode to default value
cos-queue	Map for CoS to queue
dscp-queue	Map for DSCP to queue
precedence-queue	Map for IP Precedence to queue
queue-cos	Map for queue to CoS
queue-dscp	Map for queue to DSCP
queue-precedence	Map for queue to IP Precedence
<0-7>	Specify class of service (0..7)

<0-63>	Specify DSCP (0..63)
<0-7>	Specify IP Precedence (0..7)
<0-7>	The queue number for mapping to a specific CoS value (0..7)
<0-7>	The queue number for maaping to a specific DSCP value (0..7)
<0-7>	The queue number for mapping to a specific IP Precedence value (0..7)

EXAMPLE

```
SP6526P(config)# no qos map cos-queue 3
SP6526P(config)#
```

21-1.23.22 radius-server

Configure RADIUS.

SYNTAX

no radius-server attribute [32 | 4 | 95]

no radius-server deadtime

no radius-server host word255

no radius-server host word255 [acct-port <AcctPort : 0-65535>]

no radius-server host word255 [auth-port <AuthPort : 0-65535>]

no radius-server host word255 [auth-port <AuthPort : 0-65535>] [acct-port <AcctPort : 0-65535>]

no radius-server key

no radius-server retransmit

no radius-server timeout

Parameter

attribute	
deadtime	Time to stop using a RADIUS server that doesn't respond
host	Specify a RADIUS server
key	Set RADIUS encryption key

retransmit	Specify the number of retries to active server
timeout	Time to wait for a RADIUS server to reply
32	
4	
95	
word255	Hostname or IP address (word255)
acct-port	UDP port for RADIUS accounting server
auth-port	UDP port for RADIUS authentication server
<AcctPort : 0-65535>	UDP port number (0..65535)
<AuthPort : 0-65535>	UDP port number (0..65535)

EXAMPLE

```
SP6526P(config)# no radius-server attribute 4
SP6526P(config)# no radius-server deadtime
SP6526P(config)# no radius-server key
SP6526P(config)# no radius-server retransmit
SP6526P(config)# no radius-server timeout
SP6526P(config)# no radius-server host aa auth-port 3 acct-port 3
SP6526P(config)#
```

21-1.23.23 rmon

Remote Monitoring.

SYNTAX

no rmon (alarm | event) <1-65535>

Parameter

alarm	Configure an RMON alarm
event	Configure an RMON event
<1-65535>	Alarm entry ID (1..65535)

<1-65535>	Event entry ID (1..65535)

EXAMPLE

```
SP6526P(config)# no rmon alarm 1000
SP6526P(config)#
```

21-1.23.24 snmp-server

Set SNMP server's configurations.

SYNTAX

no snmp-server access <Groupname : word32> model [v1 | v2c | v3 | any] level [auth | noauth | priv]

no snmp-server community { v2c | write-mode | [v3 <Community : word127>] }

no snmp-server security-to-group model { v1 | v2c | v3 } name <Securityname : word32>

no snmp-server user <Username : word32>

no snmp-server view <Viewname : word32> <Oidsubtree : word128>

Parameter

access	access configuration
community	Set the SNMP community
security-to-group	security-to-group configuration
user	Set the SNMPv3 user's configurations
view	MIB view configuration
<Groupname : word32>	group name (word32)
model	security model
v1	v1 security model
v2c	v2c security model
v3	v3 security model
any	any security model
level	security level

auth	authNoPriv Security Level
noauth	noAuthNoPriv Security Level
priv	authPriv Security Level
write-mode	SNMPv2c write mode
v2c	SNMPv2c
v3	SNMPv3
<Community : word32>	Specify community name (word32)
model	security model
v1	v1 security model
v2c	v2c security model
v3	v3 security model
name	security user
<SecurityName : word32>	security user name (word32)
<Username : word32>	Security user name (word32)
<Viewname : word32>	MIB view name (word32)
<Oidsubtree : word128>	MIB view OID (word128)

EXAMPLE

```
SP6526P(config)# no snmp-server access 333 model any level auth

SP6526P(config)# no snmp-server community v2c

SP6526P(config)# no snmp-server security-to-group model v2c name 132

SP6526P(config)# no snmp-server View aa a

SP6526P(config)#
```

21-1.23.25 spanning-tree

Spanning Tree protocol.

SYNTAX

no spanning-tree

no spanning-tree mode

no spanning-tree mst <0-4094> [priority | vlan]

no spanning-tree mst forward-time

no spanning-tree mst max-age

no spanning-tree mst max-hops

no spanning-tree mst name

Parameter

mode	STP protocol mode
mst	STP bridge instance
<0-4094>	MST instance ID , 0 is for CIST (0..4094)
forward-time	Delay between port states
max-age	Max bridge age before timeout
max-hops	MSTP bridge max hop count
name	Name keyword
priority	Priority of the instance
vlan	VLAN keyword

EXAMPLE

```
SP6526P(config)# no spanning-tree mode
SP6526P(config)# no spanning-tree mst max-age
SP6526P(config)#
```

21-1.23.26 system

Set the SNMP server's configurations.

SYNTAX

no system name

no system contact

no system location

Parameter

name	Clear the SNMP server's system model name string
contact	Clear the SNMP server's contact string
location	Clear the SNMP server's location string

EXAMPLE

```
SP6526P(config)# no system name

SP6526P(config)# no system contact

SP6526P(config)# no system location

SP6526P(config)#
```

21-1.23.27 tacacs-server

Configure TACACS+.

SYNTAX

no tacacs-server deadtime

no tacacs-server host word255

no tacacs-server host word255 port <AcctPort : 0-65535>

no tacacs-server key

no tacacs-server timeout

Parameter

deadtime	Time to stop using a TACACS+ server that doesn't respond
host	Specify a TACACS+ server
key	Set TACACS+ encryption key
timeout	Time to wait for a TACACS+ server to reply
word255	Hostname or IP address (word255)
port	UDP port for TACACS+ accounting server

<AcctPort : 0-65535>	UDP port number (0..65535)

EXAMPLE

```
SP6526P(config)# no tacacs-server deadtime
SP6526P(config)# no tacacs-server host 192.168.1.1 port 10000
SP6526P(config)# no tacacs-server key
SP6526P(config)# no tacacs-server timeout
SP6526P(config)#
```

21-1.23.28 upnp

Set UPnP's configurations.

SYNTAX

no upnp

no upnp advertising-duration

no upnp interface-vlan

no upnp ttl

Parameter

advertising-duration	Set advertising duration
interface-vlan	Set ip-interface vlan
ttl	Set TTL value

EXAMPLE

```
SP6526P(config)# no upnp advertising-duration
SP6526P(config)# no upnp interface-vlan
SP6526P(config)# no upnp ttl
SP6526P(config)#
```

21-1.23.29 username

Establish User Name Authentication.

SYNTAX

no username word31

Parameter

word31	User name allows letters, numbers and underscores (word31)

EXAMPLE

```
SP6526P(config)# username aaa
SP6526P(config)#
```

21-1.23.30 vlan

Vlan commands.

SYNTAX

no vlan ethertype s-custom-port

no vlan <vlan_list>

no vlan ip-subnet <ipv4_addr> <ipv4_netmask> vlan <vlan_id>

no vlan mac <mac_ucast> vlan <vlan_id>

no vlan protocol eth2 <ethernet value> group word16

no vlan protocol llc <dsap value > <ssap vlaue> group word16

no vlan protocol snap <snap oui> <pid value> group word16

Parameter

<vlan_list>	List of VLAN interface numbers, 1~4094 (1-4095)
ethertype	Ether type for Custom S-ports
ip-subnet	IP subnet based VLAN configuration
mac	MAC-based VLAN commands
protocol	Protocol-based VLAN commands
s-custom-port	Custom S-ports configuration
<ipv4_addr>	The specific ip-subnet to set. (X.X.X.X)
<ipv4_netmask>	Source IP address (X.X.X.X)

vlan	vlan keyword
<vlan_id>	VLAN ID required for the group to VLAN mapping. (1-4095)
<mac_ucast>	48 bit unicast MAC address: xx:xx:xx:xx:xx:xx
eth2	Ethernet protocol based VLAN status
llc	LLC-based VLAN group
snap	SNAP-based VLAN group
<ethernet vlaue>	Ether Type(Range: 0x600 - 0xFFFF)
group	Protocol-based VLAN group commands
word16>	Group Name (Range: 1 - 16 characters) (word16)
<dsap value>	DSAP(Range: 0x00 - 0xFF)
<ssap value>	SSAP(Range: 0x00 - 0xFF)
<snap oui>	SNAP OUI (must be 0x000000)
<pid oui>	PID (Range: 0x0000 - 0xFFFFFF)

EXAMPLE

```
SP6526P(config)# no vlan 3

SP6526P(config)# no vlan ethertype s-custom-port

SP6526P(config)#
```

21-1.23.31 voice

Vlan for voice traffic.

SYNTAX

no voice vlan

no voice vlan aging-time

no voice vlan class

no voice vlan oui <oui>

no voice vlan vid <vlan_id>

Parameter

vlan	voice_vlan_mode help
oui	OUI configuration
vid	Set VLAN ID
<oui>	OUI configuration
<vlan_id>	VLAN IDs 1-4095 (1-4095)

EXAMPLE

```
SP6526P(config)# no voice vlan vid 3
SP6526P(config)#
```

21-1.24 poe

Configure poe.

SYNTAX

poe capacitor-detect

poe auto-check

poe profile id <1-16> (Mon | Tue | Wed | Thr | Fri | Sat | Sun | name) <0-23> <0-55> <0-23> <0-55>

Parameter

capacitor-detect	Enable capacitor detection
auto-check	Enable Ping Check
profile	poe scheduling profile
id	poe scheduling profile id, from 1 to 16
<1-16>	Profile id (1..16)
Mon	Monday
Tue	Tuesday
Wed	Wednesday

Thr	Thursday
Fri	Friday
Sat	Saturday
Sun	Sunday
name	name
<0-23>	Start hour (0..23)
<0-55>	Start miniute (0..55)
<0-23>	End hour (0..23)
<0-55>	End miniute (0..55)

EXAMPLE

```
SP6526P(config)# poe capacitor-detect
SP6526P(config)# poe auto-check
SP6526P(config)# poe profile id 4 Mon 0 0 0 0
SP6526P(config)#
```

21-1.25 ntp

Configure NTP.

SYNTAX

ntp

ntp interval <10-2880>

ntp server <1-6> ip-address <hostname>

ntp server <1-6> ip-address <ipv4_ucast>

Parameter

server	Configure NTP server
interval	Configure NTP interval
<1-6>	index number (1..6)
ip-address	ip address
<ipv4_ucast>	ipv4 address (x.x.x.x)
<hostname>	domain name

<10-2880> interval val range from 10 to 2880 min. (10..2880)

EXAMPLE

```
SP6526P(config)# ntp server 3 ip-address 192.168.1.1

SP6526P(config)#
```

21-1.26 port-security

Enable/disable port security globally.

SYNTAX

port-security

EXAMPLE

```
SP6526P(config)# port-security

SP6526P(config)#
```

21-1.27 privilege

Command privilege parameters.

SYNTAX

privilege group <group> level ro <0-15> rw <0-15>

Parameter

group Privilege group name

<group> Privilege group name (access-mgmt / arp-inspection / auth-method / dhcp-relay / dhcp-snooping / diagnostic / dot1x / eee / event / forward-failure / ip / ipmc / ip-source-guard / lacp / lldp / loop-protection / mac-table / mirror / mvr / poe / port / port-security / qos / radius / snmp / stp / system / upnp / vlan)

level Privilege group level

ro Read-only level

<0-15> Privilege level (0..15)

rw	Read-write level

EXAMPLE

```
SP6526P(config)# privilege group access-mgmt level ro 3 rw 5
SP6526P(config)#
```

21-1.28 qos

Quality of Service.

SYNTAX

qos map cos-dscp <0-7> to <0-7>

qos map dscp-queue <0-63> to <0-7>

qos map precedence-queue <0-7> to <0-7>

qos map queue-cos <0-7> to <0-7>

qos map queue-dscp <0-7> to <0-63>

qos map queue-precedence <0-7> to <0-7>

qos trust cos

qos trust cos-dscp

qos trust dscp

qos trust ip-precedence

Parameter

map	QoS Global Map/Table
trust	Global trust mode configuration
cos-queue	Map for CoS to queue
dscp-queue	Map for DSCP to queue
precedence-queue	Map for IP Precedence to queue
queue-cos	Map for queue to CoS
queue-dscp	Map for queue to DSCP

queue-precedence	Map for queue to IP Precedence
<0-7>	Specify class of service (0..7)
to	Specify the queue to which the CoS will be mapped
<0-7>	The queue number to which the following CoS values are mapped (0..7)
<0-63>	Specify DSCP (0..63)
to	Specify the queue to which the DSCP will be mapped
<0-7>	The queue number to which the following DSCP values are mapped (0..7)
<0-7>	Specify IP Precedence (0..7)
to	Specify the queue to which the IP Precedence will be mapped
<0-7>	The queue number to which the following IP Precedence values are mapped (0..7)
<0-7>	The queue number for mapping to a specific CoS value (0..7)
to	Specify the CoS to which the queue will be mapped
<0-7>	Specify class of service (0..7)
<0-7>	The queue number for maaping to a specific DSCP value (0..7)
to	Specify the DSCP to which the queue will be mapped
<0-63>	Specify DSCP (0..63)
<0-7>	The queue number for mapping to a specific IP Precedence value (0..7)
to	Specify the IP Precedence to which the queue will be mapped
<0-7>	Specify IP Precedence (0..7)
cos	Prioritize packet based on the CoS/802.1p field in the VLAN tag
cos-dscp	Uses the CoS mode for non-IP packet and DSCP mode for IP packet
dscp	Prioritize packet based on the DSCP field in the IP header
ip-precedence	Prioritize packet based on the ip precedence

EXAMPLE

```
SP6526P(config)# qos map cos-queue 3 to 5
SP6526P(config)#
```

21-1.29 radius-server

Configure RADIUS.

SYNTAX

radius-server attribute 32 word255

radius-server attribute 4 <ipv4_ucast>

radius-server attribute 95 <ipv6_addr>

radius-server deadtime <Minutes : 1-1440>

radius-server host word255 [auth-port <Authport : 0-65535>] [acct-port <Acctport : 0-65535>] [timeout <Seconds : 1-1000>] [retransmit <Retries :1-1000>] [key word63]

radius-server key word63

radius-server retransmit <Retries : 1-1000>

radius-server timeout <Seconds : 1-1000>

Parameter

Attribute	
deadtime	Time to stop using a RADIUS server that doesn't respond
host	Specify a RADIUS server
key	Set RADIUS encryption key
retransmit	Specify the number of retries to active server
timeout	Time to wait for a RADIUS server to reply
32	
4	

95	
word255	(word255)
<ipv4_ucast>	(X.X.X.X)
<ipv6_addr>	(X:X:X:X:X:X:X:X)
<Minutes : 1-1440>	Time in minutes (1..1440)
word255	Hostname or IP address (word255)
acct-port	UDP port for RADIUS accounting server
auth-port	UDP port for RADIUS authentication server
key	Server specific key (overrides default)
retransmit	Specify the number of retries to active server (overrides default)
timeout	Time to wait for this RADIUS server to reply (overrides default)
<AuthPort : 0-65535>	UDP port number (0..65535)
<AcctPort : 0-65535>	UDP port number (0..65535)
<Seconds : 1-1000>	Wait time in seconds (1..1000)
<Retries : 1-1000>	Number of retries for a transaction (1..1000)
word63	The shared key (word63)

EXAMPLE

```
SP6526P(config)# radius-server host device key 12
SP6526P(config)#
```

21-1.30 rmon

Remote Monitoring.

SYNTAX

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] }

rmon event <1-65535> [log] [trap <word31>] { [description <word127>] }

Parameter

alarm	Configure an RMON alarm
event	Configure an RMON event
<1-65535>	Alarm entry ID (1..65535)
ifInOctets	The total number of octets received on the interface, including framing characters
ifInUcastPkts	The number of uni-cast packets delivered to a higher-layer protocol
ifInNUcastPkts	The number of broad-cast and multi-cast packets delivered to a higher-layer protocol
ifInDiscards	The number of inbound packets that are discarded even the packets are normal
ifInErrors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol
ifInUnknownProtos	The number of the inbound packets that were discarded because of the unknown or un-support protocol
ifOutOctets	The number of octets transmitted out of the interface , including framing characters
ifOutUcastPkts	The number of uni-cast packets that request to transmit
ifOutNUcastPkts	The number of broad-cast and multi-cast packets that request to transmit
ifOutDiscards	The number of outbound packets that are discarded event the packets is normal
ifOutErrors	The The number of outbound packets that could not be transmitted because of errors
<uint>	ifIndex(1..9)
<1-2147483647>	Sample interval(1.. 2147483647)
absolute	Test each sample directly
delta	Test delta between samples
rising-threshold	Configure the rising threshold
<-2147483648-2147483647>	rising threshold value(-2147483648..2147483647)
<0-65535>	Event to fire on rising threshold crossing(0..65535)
falling-threshold	Configure the falling threshold

<-2147483648-2147483647>	falling threshold value(-2147483648..2147483647)
rising	Trigger alarm when the first value is larger than the rising threshold
falling	Trigger alarm when the first value is less than the falling threshold
both	Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default)
<1-65535>	Event entry ID (1..65535)
description	Specify a description of the event
log	Generate RMON log when the event fires
trap	Generate SNMP trap when the event fires
word127	Event description (word127)
word31	SNMP community string (word31)

EXAMPLE

```
SP6526P(config)# rmon alarm 10000 ifInErrors 6 9999 absolute rising-threshold 0
falling-threshold 0 both
SP6526P(config)#
```

21-1.31 snmp-server

Set SNMP server's configurations.

SYNTAX

snmp-server

Table : configure –snmp-server Commands

Command	Function
access	access configuration
community	Set the SNMP community
security-to-group	security-to-group configuration
user	Set the SNMPv3 user's configurations
view	MIB view configuration

21-1.31.1 access

access configuration.

SYNTAX

snmp-server access <GroupName : word32> model [v1 | v2c | v3 | any] level [auth | noauth | priv]

Parameter

<GroupName : word32>	group name (word32)
model	security model
any	any security model
v1	v1 security model
v2c	v2c security model
v3	v3 security model
level	security level
auth	authNoPriv Security Level
noauth	noAuthNoPriv Security Level
priv	authPriv Security Level

EXAMPLE

```
SP6526P(config)# snmp-server access text model v2c level noauth write
text
SP6526P(config)#
```

21-1.31.2 community

Set the SNMP community.

SYNTAX

snmp-server community write-mode

snmp-server community v2c <Community : word32> [ro | rw]

snmp-server community v3 <Community : word32> <ipv4_ucast> <0-32>

Parameter

write-mode	SNMPv2c write mode
v3	SNMPv3
v2c	SNMPv2c
<Community : word32>	Specify community name (word32)
ro	Read only
rw	Read write
<ipv4_ucast>	IPv4 address (X.X.X.X)
<0-32>	IPv4 netmask (0..32)

EXAMPLE

```
SP6526P(config)# snmp-server community v2c text ro
SP6526P(config)#
```

21-1.31.3 security-to-group

security-to-group configuration.

SYNTAX

snmp-server security-to-group model [v1 | v2c | v3] name <SecurityName : word32> group <GroupName : word32>

Parameter

model	security model
v1	v1 security model
v2c	v2c security model
v3	v3 security model
name	security user
<SecurityName : word32>	security group name (word32)
group	security use
<GroupName : word32>	group name (word32)

EXAMPLE

```
SP6526P(config)# snmp-server security-to-group model v2c name text group
text
SP6526P(config)#
```

21-1.31.4 user

Set the SNMPv3 user's configurations.

SYNTAX

snmp-server user <Username : word32>

snmp-server user <Username : word32> { [md5 <Md5Passwd : word8-32> | [sha <ShaPasswd : word8-40>] }

snmp-server user <Username : word32> { [md5 <Md5Passwd : word8-32> | [sha <ShaPasswd : word8-40>] } priv [des | aes] <word8-32>

Parameter

<Username : word32>	Security user name (word32)
md5	Set MD5 protocol
sha	Set SHA protocol
<Md5Passwd : word8-32>	MD5 password (word8-32)
<ShaPasswd word8-40>	SHA password (word8-40)
priv	Set Privacy
des	Set DES protocol
aes	Set AES protocol
<word8-32>	Set AES protocol (word8-32)

EXAMPLE

```
SP6526P(config)# snmp-server user text md5 12345678 priv aes 12345678
SP6526P(config)#
```

21-1.31.5 view

MIB view configuration.

SYNTAX

snmp-server view <ViewName : word32> <OidSubtree : word255> [include | exclude]

Parameter

<ViewName : word32>	MIB view name (word32)
<OidSubtree : word255>	MIB view OID (word128)
include	Ixcluded type from the view
exclude	Excluded type from the view

EXAMPLE

```
SP6526P(config)# snmp-server view text .1 include
SP6526P(config)#
```

21-1.32 spanning-tree

Spanning Tree protocol.

Table : configure –spanning-tree Commands

Command	Function
mode	STP protocol mode
mst	STP bridge instance

21-1.32.1 mode

STP protocol mode.

SYNTAX

spanning-tree mode [stp | rstp | mstp]

Parameter

mstp	Multiple Spanning Tree (802.1s)
rstp	Rabid Spanning Tree (802.1w)
stp	802.1D Spanning Tree

EXAMPLE

```
SP6526P(config)# spanning-tree mode stp
SP6526P(config)#
```

21-1.32.2 mst

STP bridge instance.

SYNTAX

spanning-tree mst <0-4094> priority <0-61440>

spanning-tree mst <0-4094> vlan <vlan_list>

spanning-tree mst forward-time <4-30>

spanning-tree mst max-age < 6-40>

spanning-tree mst max-hops <6-40>

spanning-tree mst name <word32> revision <0-65535>

Parameter

<0-4094>	MST instance ID , 0 is for CIST (0..4094)
forward-time	Delay between port states
max-age	Max bridge age before timeout
max-hops	MSTP bridge max hop count
name	Name keyword
priority	Priority of the instance
vlan	VLAN keyword
<0-61440>	Priority value (0..61440)
<vlan_list>	Range of VLANs (1-4095)
<4-30>	Range in seconds (4..30)
<6-40>	Range in seconds (6..40)
<6-40>	Hop count range (6..40)

<word32>	Name of the bridge (word32)
revision	Revision keyword
<0-65535>	Revision number (0..65535)

EXAMPLE

```
SP6526P(config)# spanning-tree mst 7 vlan 10
SP6526P(config)#
```

21-1.33 system

Set the SNMP server's configurations.

SYNTAX

system contact word128

system location word128

system name word128

Parameter

contact	Set the SNMP server's contact string
location	Set the SNMP server's location string
name	Set the SNMP server's system model name string
word128	name string (word128)
word128	contact string (word128)
word128	location string (word128)

EXAMPLE

```
SP6526P(config)# system contact 222
SP6526P(config)# system location 333
SP6526P(config)# system name GE
SP6526P(config)#
```

21-1.34 tacacs-server

Configure TACACS+.

SYNTAX

tacacs-server deadtime <Minutes : 1-1440>

tacacs-server host word255

tacacs-server host word255 [port <AcctPort : 0-65535>] [timeout <Seconds : 1-1000>] [key word63]

tacacs-server key word63

tacacs-server timeout <Seconds : 1-1000>

Parameter

deadtime	Time to stop using a TACACS+ server that doesn't respond
host	Specify a TACACS+ server
key	Set TACACS+ encryption key
timeout	Time to wait for a TACACS+ server to reply
<Minutes : 1-1440>	Time in minutes (0..1440)
word255	Hostname or IP address (word255)
port	UDP port for TACACS+ accounting server
timeout	Time to wait for this TACACS+ server to reply (overrides default)
key	Server specific key (overrides default)
<AcctPort : 0-65535>	TCP port number (0..65535)
<Seconds : 1-1000>	Wait time in seconds(0..1000)
word63	The shared key (word63)

EXAMPLE

```
SP6526P(config)# tacacs-server deadtime 300

SP6526P(config)# tacacs-server key 33

SP6526P(config)# tacacs-server timeout 300

SP6526P(config)#
```

21-1.35 trap

Trap.

SYNTAX

trap <1..6> v2c <ipv4_ucast> <0..7> word32

Parameter

<1..6>	ID of Trap entry (1..6)
v2c	v2c
<ipv4_ucast>	ipv4 address (X.X.X.X)
<0..7>	Trap severity (0..7)
word32	trap community (word32)

EXAMPLE

```
SP6526P(config)# trap 3 v2c 192.168.1.1 2 test
SP6526P(config)#
```

21-1.36 upnp

Set UPnP's configurations.

SYNTAX

upnp

upnp advertising-duration <advertising duration>

upnp interface-vlan <vlan_id>

upnp ttl <TTL value>

Parameter

advertising-duration	Set advertising duration
interface-vlan	Set ip-interface vlan
ttl	Set TTL value
<advertising duration>	value is 66..86400 (66..86400)

<vlan_id>	value is 1..4095 (1-4095)
<TTL value>	value is 1..255 (1..255)

EXAMPLE

```
SP6526P(config)# upnp advertising-duration 88
SP6526P(config)# upnp ttl 25
SP6526P(config)#
```

21-1.37 username

Establish User Name Authentication.

SYNTAX

username word31 privilege <privilegeLevel : 0-15> password encrypted word4-44

username word31 privilege <privilegeLevel : 0-15> password none

username word31 privilege <privilegeLevel : 0-15> password unencrypted word31

Parameter

word31	User name allows letters, numbers and underscores (word31)
privilege	Set user privilege level
<privilegeLevel : 0-15>	User privilege level (0..15)
password	Specify the password for the user
encrypted	Specifies an ENCRYPTED password will follow
none	NULL password
unencrypted	Specifies an UNENCRYPTED password will follow
word4-44	The ENCRYPTED (hidden) user password. Notice the ENCRYPTED password will be decoded by system internally. You cannot directly use it as same as the Plain Text and it is not human-readable text normally. (word4-44)
word31	The UNENCRYPTED (Plain Text) user password. Any printable characters including space is accepted. Notice that you have no chance to get the Plain

Text password after this command. The system will always display the ENCRYPTED password. (word31)

EXAMPLE

```
SP6526P(config)# username jefferson privilege 15 password
none
SP6526P(config)# (config)#
```

21-1.38 vlan

VLAN commands.

SYNTAX

vlan <vlan_list>

vlan ethertype s-custom-port <ethernet value>

vlan protocol eth2 <ethernet value> group word16

vlan protocol llc <dsap value> <ssap value> group word16

vlan protocol snap <snap oui> <pid value> group word16

vlan ip-subnet <ipv4_addr> <ipv4_netmask> vlan <vlan_id>

vlan mac <mac_ucast> vlan <vlan_id>

Parameter

<vlan_list>	List of VLAN interface numbers, 1~4094 (1-4095)
ethertype	Ether type for Custom S-ports
protocol	Protocol-based VLAN status
ip-subnet	ip-subnet VLAN configuration.
mac	MAC-based VLAN commands
s-custom-port	Custom S-ports configuration
<ethernet value>	Ether Type(Range: 0x600 - 0xFFFF)
eth2	Ethernet-based VLAN commands

llc	LLC-based VLAN group
snap	SNAP-based VLAN group
group	Protocol-based VLAN group commands
<word16>	Group Name (Range: 1 - 16 characters) (word16)
<dsap value>	DSAP(Range: 0x00 - 0xFF)
<ssap value>	SSAP(Range: 0x00 - 0xFF)
<snap oui>	SNAP OUI(must be 0x000000)
<pid value>	PID(Range: 0x0000 - 0XFFFF)
<ipv4_addr>	Source IP address (X.X.X.X)
<ipv4_netmask>	Source IP address (X.X.X.X)
vlan	vlan keyword
<vlan_id>	VLAN ID required for the group to VLAN mapping (1-4095)
<mac_ucast>	48 bit unicast MAC address: xx:xx:xx:xx:xx:xx

EXAMPLE

```
SP6526P(config)# vlan ethertype s-custom-port 0x1111
SP6526P(config)# vlan protocol eth2 0x6000 group aa
SP6526P(config)#
```

21-1.39 voice

Vlan for voice traffic.

SYNTAX

voice vlan oui <oui>

voice vlan oui <oui> description word32

voice vlan vid <vlan_id>

voice vlan vid <vlan_id> aging-time <AgingTime : 10-10000000>

voice vlan vid <vlan_id> aging-time <AgingTime : 10-10000000> class <class : 0-7>

Parameter

vlan	voice_vlan_mode help
vid	Set a entry VLAN ID
oui	OUI configuration
<vlan_id>	VLAN IDs 1-4095 (1-4095)
aging-time	Set a entry secure learning aging time
class	Set a entry traffic class
<AgingTime : 10-10000000>	Aging time, 10-10000000 seconds (10..10000000)
<0-7>	Traffic class value (0..7)
<oui>	OUI value
description	Set description for the OUI
word32	Description line (word32)

EXAMPLE

```
SP6526P(config)# voice vlan aging-time 3333
SP6526P(config)# voice vlan class 7
SP6526P(config)# voice vlan vid 3333
SP6526P(config)#
```

Chapter 22 COPY Commands of CLI

Copy from source to destination.

SYNTAX

copy running-config [startup-config | flash:filename | tftp://server/path-to-file]

copy startup-config [running-config | flash:filename | tftp://server/path-to-file]

copy flash:filename [startup-config | running-config | tftp://server/path-to-file]

copy tftp://server/path-to-file [startup-config | running-config | flash:filename]

Parameter

running-config	Current running configuration
startup-config	Startup configuration
flash:filename	File in FLASH
tftp://server/path-to-file	File on TFTP server

EXAMPLE

```
SP6526P# copy startup-config  running-config
SP6526P#
```

Chapter 23 DELETE Commands of CLI

Delete one file in flash file system.

SYNTAX

delete string

Parameter

String	File in FLASH

EXAMPLE

```
SP6526P# delete text
SP6526P#
```

Chapter 24 DIAGNOSTICS Commands of CLI

Diagnostics

SYNTAX

diagnostics cable interface { * | [GigabitEthernet <port_list>] }

Parameter

cable	cable
interface	Interface status and configuration
GigabitEthernet	GigabitEthernet
*****	All ports
<port_list>	Port List S/X-Y,Z (1/1-26)

EXAMPLE

```
SP6526P# diagnostics cable interface GigabitEthernet 1/6
Cable Diagnostics
======================================
GigabitEthernet 1/6
------------------------------
Pair A   : [Open]
Length A : 0.90 (m)
Pair B   : [Open]
Length B : 0.88 (m)
Pair C   : [Open]
Length C : 0.83 (m)
Pair D   : [Open]
Length D : 0.88 (m)
SP6526P#
```

Chapter 25 DIR Commands of CLI

Directory of all files in flash: file system.

SYNTAX

dir

Parameter

none

EXAMPLE

```
SP6526P# dir
startup-config
SP6526P#
```

Chapter 26 FIND-SWITCH Commands of CLI

Turn on and off all LED light 3 times in 15 seconds

Syntax

find-switch

Parameter

none

EXAMPLE

```
SP6526P# find-switch
SP6526P#
```

Chapter 27 FIRMWARE Commands of CLI

Firmware.

Syntax

firmware swap

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

Parameter

swap	Swap between Active and Alternate firmware image
upgrade	upgrade
<tftp://server/path-and-filename>	TFTP Server IP address, path and file name for the server containing the

new image

EXAMPLE

```
SP6526P# firmware upgrade tftp://192.168.1.1/running-config

Programming image...

SP6526P#
```

Chapter 28 MORE Commands of CLI

Display file

SYNTAX

more String

Parameter

String File in FLASH

EXAMPLE

```
SP6526P# copy running-config startup-config
SP6526P# more startup-config
username admin privilege 15 password none
!
!
interface GigabitEthernet 1/1
!
interface GigabitEthernet 1/2
!
interface GigabitEthernet 1/3
!
interface GigabitEthernet 1/4
!
.
.
.
.
.
.
```

```
.
.
.
interface GigabitEthernet 1/N
!
!
interface vlan 1
 ip address 192.168.1.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
end
SP6526P#
```

Chapter 29 PING Commands of CLI

Send ICMP echo messages.

Syntax

ping ip <ipv4_addr>

ping ip <ipv4_addr> [repeat <Count : 1-60>] [size <Size : 2-1452>]

ping ipv6 <ipv6_addr>

ping ipv6 <ipv6_addr> [repeat <Count : 1-60>] [size <Size : 2-1452>]

Parameter

ip	IP (ICMP) echo
ipv6	IPv6 (ICMPv6) echo
<ipv4_addr>	ICMP destination address (X.X.X.X)
repeat	Specify repeat count
size	Specify datagram size
<Count : 1-60>	1-60; Default is 5 (1..60)
<Size : 2-1452>	2-1452; Default is 56 (excluding MAC, IP and ICMP headers) (2..1452)
<ipv6_addr>	ICMPv6 destination address (X:X:X:X:X:X:X:X)

EXAMPLE

```
SP6526P# ping ip 192.168.1.1 repeat 3 size 3
PING 192.168.1.1 (192.168.1.1): 3 data bytes
11 bytes from 192.168.1.1: seq=0 ttl=64
11 bytes from 192.168.1.1: seq=1 ttl=64
11 bytes from 192.168.1.1: seq=2 ttl=64

--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
SP6526P#
```

Chapter 30 RELOAD Commands of CLI

Reload system.

Syntax

reload cold

reload defaults

reload defaults keep-ip

Parameter

cold	Reload cold
defaults	Reload defaults without rebooting.
keep-ip	Attepmt to keep VLAN1 IP setup

EXAMPLE

```
SP6526P# reload defaults keep-ip
SP6526P#
```

Chapter 31 SHOW Commands of CLI

Show running system information.

Table : SHOW Commands

Command	Function
aaa	Login methods
access	Access management configuration
access-list	Access list
aggregation	Aggregation configuration and Status
clock	Configure time-of-day clock
dms	show dms information
dot1x	IEEE Standard for port-based Network Access Control
event	Show trap event configuration
interface	Interface status and configuration
ip	Internet Protocol
ipv6	IPv6 configuration commands
lldp	show lldp configuraion
logging	Syslog
loop-protect	show Loop protection
mac	Mac Address Table information
mvr	Internet Protocol
ntp	Configure NTP
poe	Power over ethernet
port-security	show port security
privilege	Display privilege level configuration
pvlan	PVLAN status
qos	Quality of Service
radius-server	RADIUS configuration
rmon	RMON statistics
running-config	Current operating configuration
snmp	Display SNMP configurations
spanning-tree	Spanning Tree protocol
System	show system information
tacacs-server	TACACS+ configuration
trap	Trap configuration
upnp	show UPnP configurations
version	System software status
vlan	VLAN status
voice	show voice

31-1 aaa

Login methods.

SYNTAX

show aaa

EXAMPLE

```
SP6526P# show aaa
Automatic Redirect : Disabled

 Client Method1 Method2 Method3 Service Port
------- ------- ------- ------- ------------
 telnet  local                    23
    ssh  local                    22
   http  local                    80
  https                          443

Authorization :
 Client Method Cmd Lvl Cfg Cmd Fallback
------- ------ ------- ------- --------
 telnet  none      0
    ssh  none      0
```

```
Accounting :
 Client Method Cmd Lvl Exec
------- ------ ------- ----
 telnet  none      0
    ssh  none      0

SP6526P#
```

31-2 access

Access management configuration.

SYNTAX

show access management

show access management <1~16>

Parameter

management	Access management configuration
<1~16>	ID of access management entry list (1-16)

EXAMPLE

```
SP6526P# show access management 3
Switch access management mode is : Disable
Idx VID  IP Address          HTTP/HTTPS SNMP TELNET/SSH
--- ---- -------------------- ---------- ---- ----------

SP6526P#
```

31-3 access-list

Access list.

SYNTAX

show access-list ace

show access-list ace <1~384>

Parameter

ace	Access list entry
<1~384>	ACE ID (1-384)

EXAMPLE

```
SP6526P# show access-list ace 3

Switch access-list ace number: 0
SP6526P#
```

31-4 aggregation

Aggregation configuration and status.

SYNTAX

show aggregation aggregators

show aggregation lacp

show aggregation mode

show aggregation status

Parameter

aggregators	aggregator status
lacp	lacp local and neighbor info
mode	Traffic distribution mode
status	aggregation port status

EXAMPLE

```
SP6526P# show aggregation mode
Aggregation Hash Mode : src-dst-mac
LACP System Priority : 32768

SP6526P#
```

31-5 clock

Configure time-of-day clock.

SYNTAX

show clock

EXAMPLE

```
SP6526P# show clock
System Time : 2017-01-01 01:30:50

SP6526P#
```

31-6 dms

Show dms information.

SYNTAX

show dms

show dms upnp [1] [2] [100] [101]

show dms onvif

Parameter

upnp	upnp information
onvif	onvif information
1	upnp information
2	upnp information
100	upnp information
101	upnp information

EXAMPLE

```
SP6526P# show dms upnp 2 1 100 101
Cannot write to the running-config.
The error while request to the config daemon.
SP6526P#
```

31-7 dot1x

IEEE Standard for port-based Network Access Control.

SYNTAX

show dot1x status

show dot1x status interface { * | [Gigbitethernet <port _list>] }

show dot1x statistics [eapol | radius | all] interface { * | [Gigbitethernet <port _list>] }

show dot1x statistics [eapol | radius | all]

Parameter

statistics	Shows statistics for either eapol or radius
Status	Shows dot1x status, such as admin state, port state and last source
interface	Interface
*****	All Ports
Gigbitethernet	1 Gigabit Ethernet Port
<port _list>	Port ID (1/1-26)
all	Show all dot1x statistics
eapol	Show EAPOL statistics
radius	Show Backend Server statistics

EXAMPLE

```
SP6526P# show dot1x statistics radius
                   Rx Access   Rx Other    Rx Auth.    Rx Auth.    Tx          MAC
Interface            Challenges  Requests    Successes   Failures    Responses
Address
--------------------- ---------- ---------- ---------- ---------- ----------
-------
GigabitEthernet 1/1    0          0          0          0          0          -
GigabitEthernet 1/2    0          0          0          0          0          -
GigabitEthernet 1/3    0          0          0          0          0          -
GigabitEthernet 1/4    0          0          0          0          0          -
GigabitEthernet 1/5    0          0          0          0          0          -
.
.
.

GigabitEthernet 1/N   0          0          0          0          0          -
SP6526P#
```

31-8 event

Show trap event configuration.

SYNTAX

show event

EXAMPLE

```
SP6526P# show event
Group Name                    Severity Level    Syslog Mode   Trap Mode
--------------------------------  ----------------  ------------  ------------
ACCESS-MGMT                    Info               Enabled      Disabled
ACL                            Info               Enabled      Disabled
ARP-INSPECTION                 Warning            Enabled      Disabled
AUTH-FAILED                    Warning            Enabled      Disabled
BCS-PROTECTION                 Info               Enabled      Disabled
COLD-START                     Warning            Enabled      Disabled
DHCP                           Info               Enabled      Disabled
DHCP-SNOOPING                  Info               Enabled      Disabled
IP-SOURCE-GUARD                Info               Enabled      Disabled
LACP                           Info               Enabled      Disabled
LINK-UPDOWN                    Warning            Enabled      Disabled
LOGIN                          Info               Enabled      Disabled
LOGOUT                         Info               Enabled      Disabled
LOOP-PROTECTION                Info               Enabled      Disabled
MAC-TABLE                      Info               Enabled      Disabled
MAINTENANCE                    Info               Enabled      Disabled
MGMT-IP-CHANGE                 Info               Enabled      Disabled
NAS                            Info               Enabled      Disabled
PORT                           Info               Enabled      Disabled
PORT-SECURITY                  Info               Enabled      Disabled
RMON                           Info               Enabled      Disabled
SFP                            Info               Enabled      Disabled
SPANNING-TREE                  Info               Enabled      Disabled
SYSTEM                         Info               Enabled      Disabled
USER                           Info               Enabled      Disabled
WARM-START                     Warning            Enabled      Disabled

SP6526P#
```

31-9 interface

Interface status and configuration.

SYNTAX

show interface vlan <vlan_list>

show interface vlan

show interface { * | [GigabitEthernet <port _list>] } green-ethernet

show interface { * | [GigabitEthernet <port _list>] } capabilities

show interface { * | [GigabitEthernet <port _list>] } statistics [bytes | discards | errors | packets] [up |

down]

show interface { * | [GigabitEthernet <port _list>] } statistics [up | down] [bytes | discards | errors | packets]

show interface { * | [GigabitEthernet <port _list>] } status

Parameter

vlan	VLAN status
GigabitEthernet	GigabitEthernet
*****	All switches or All ports
<vlan_list>	List of VLAN interface numbers (1-4095)
<port_list>	Port List S/X-Y,Z (1/1-26)
green-ethernet	Display green-ethernet
status	Display status
statistics	Display statistics
capabilities	Display interface capabilities
bytes	Show byte statistics
discards	Show discard statistics
errors	Show error statistics
packets	Show packet statistics
up	Show ports which are up
down	Show ports which are down

EXAMPLE

```
SP6526P# show interface GigabitEthernet 1/1-3 capabilities

GigabitEthernet 1/1 Capabilities:
SFP Type: None
SFP Vendor name:
SFP Vendor PN:
SFP Vendor revision:

GigabitEthernet 1/2 Capabilities:
SFP Type: None
SFP Vendor name:
SFP Vendor PN:
SFP Vendor revision:

GigabitEthernet 1/3 Capabilities:
SFP Type: None
SFP Vendor name:
SFP Vendor PN:
SFP Vendor revision:
SP6526P#
```

31-10 ip

Internet Protocol.

SYNTAX

show ip arp

show ip arp inspection

show ip arp inspection entry { [dhcp-snooping interface] | [interface] | [static interface] } { * | [GigabitEthernet <port _list>] }

show ip arp inspection interface { * | [GigabitEthernet <port _list>] }

show ip arp inspection vlan <vlan_list>

show ip dhcp pool

show ip dhcp pool <vlan_id>

show ip dhcp relay

show ip dhcp relay statistics

show ip dhcp server

show ip dhcp server status

show ip dhcp snooping

show ip dhcp snooping table

show ip dhcp snooping interface { * | [GigabitEthernet <port _list>] }

show ip dhcp snooping statistics

show ip dhcp snooping statistics interface { * | [GigabitEthernet <port _list>] }

show ip igmp snooping

show ip igmp snooping [detail | group-database | mrouter | vlan]

show ip interface brief

show ip name-server

show ip route

show ip source binding

show ip source binding dhcp-snooping

show ip source binding dhcp-snooping interface { * | [GigabitEthernet <port _list>] }

show ip source binding interface { * | [GigabitEthernet <port _list>] }

show ip source binding static

show ip source binding static interface { * | [GigabitEthernet <port _list>] }

show ip verify source

show ip verify source interface { * | [GigabitEthernet <port _list>] }

Parameter

arp	Address Resolution Protocol
dhcp	Dynamic Host Configuration Protocol
igmp	Internet Protocol
interface	IP interface status and configuration
name-server	Domain Name System
route	Display the current ip routing table
source	source command

verify	verify command
inspection	ARP inspection
entry	arp inspection entries
interface	Select an interface to configure
vlan	VLAN configuration
dhcp-snooping	learn from dhcp snooping
static	setting from static entries
GigabitEthernet	GigabitEthernet
*****	All switches or All ports
<port_list>	Port List S/X-Y,Z (1/1-26)
<vlan_list>	Select a VLAN id to configure (1-4095)
pool	DHCP server pool
relay	DHCP relay
server	DHCP server
snooping	DHCP snooping
<vlan_id>	VLAN id of DHCP server pool (1-4095)
statistics	DHCP option 82
status	DHCP server status
table	show ip dhcp snooping table
statistics	Display DHCP snooping statistics information
snooping	Snooping IGMP
detail	Detail running information/statistics of IGMP snooping
group-database	Multicast group database from IGMP
mrouter	Multicast router port status in IGMP
vlan	Search by VLAN
brief	Brief IP interface status
binding	ip source binding
interface	ip verify source interface config
source	verify source

EXAMPLE

```
SP6526P# show ip interface brief
Interface       Address            Method       Status
---------------- -------------------- ------------- ------
VLAN1          192.168.1.1/24      Manual       UP
SP6526P#
```

31-11 ipv6

IPv6 configuration commands.

SYNTAX

show ipv6 mld snooping [vlan | group-database | detail | mrouter]

show ipv6 mld snooping

show ipv6 interface

show ipv6 interface vlan <vlan_list> brief

show ipv6 neighbor

show ipv6 neighbor interface vlan <vlan_list>

show ipv6 route

show ipv6 route interface vlan <vlan_list>

Parameter

mld	IPv6 configuration commands
interface	IPv6 configuration commands
neighbor	IPv6 neighbors
route	IPv6 routes
snooping	Snooping MLD
detail	Detail running information/statistics of MLD snooping
group-database	Multicast group database from MLD
mrouter	Multicast router port status in MLD
vlan	Search by VLAN
vlan	VLAN of IPv6 interface
<vlan_list>	IPv6 interface VLAN list (1-4095)
brief	Brief summary of IPv6 status and configuration
interface	Select an interface to configure

EXAMPLE

```
SP6526P# show ipv6 mld snooping detail
MLD Snooping is disabled to stop snooping IGMP control plane.
Multicast streams destined to unregistered MLD groups will be flooding.
SP6526P#
```

31-12 lldp

show lldp configuration.

SYNTAX

show lldp

show lldp interface { * | [GigabitEthernet <port _list>] }

show lldp med media-vlan-policy

show lldp med media-vlan-policy <policy_list>

show lldp med remote-device

show lldp med remote-device interface { * | [GigabitEthernet <port _list>] }

show lldp neighbors

show lldp neighbors interface { * | [GigabitEthernet <port _list>] }

show lldp statistics

show lldp statistics [interface <port_type> <port_type_list>] [| {begin | exclude | include } <LINE>]

Parameter

interface	Interface to display
med	Display LLDP-MED neighbors information
neighbors	Display LLDP neighbors information

statistics	Display LLDP statistics information
*****	All Switches or All ports
Gigabitethernet	GigabitEthernet
<port_list>	Port List S/X-Y,Z (1/1-26)
media-vlan-policy	Display media vlan policies
remote-device	Display remote device LLDP-MED neighbors information
<policy_list>	e.g. 0,1,2, (0-31)
Interface	Interface to display

EXAMPLE

```
SP6526P# show lldp interface GigabitEthernet 1/4
LLDP Configuration
======================================
TX Interval : 30 sec
TX Hold : 4 sec
TX Delay : 2 sec
TX Reinit : 2 sec

GigabitEthernet 1/4
------------------------------
TX/RX Mode : Disabled
CDP Aware  : Disable
Port Descr : Enable
Sys Name : Enable
Sys Descr : Enable
Sys Capa : Enable
Mgmt Addr : Enable
SP6526P#
```

31-13 logging

Syslog.

SYNTAX

show logging [<loggin_id : 1-4294967295> | alert | crit | debug | emerg | error | info | notice | warning]

show logging

Parameter

<logging_id: 1-4294967295>	Logging ID (1..4294967295)
alert	Alert
crit	Critical
debug	Debug
emerg	Emergency
error	Error
info	Information

notice	Notice
warning	Warning

EXAMPLE

```
SP6526P# show logging info
Switch logging host mode is disable
Host address 1 :
Host address 2 :
Host address 3 :
Host address 4 :
Host address 5 :
Host address 6 :

Number of entries on Switch:
ID    Level    Time                   Message
----  -------  ---------------------  -----------------------------
3     Info     2017-01-01 00:01:16    LOGIN: Login passed for user 'admin'
4     Info     2017-01-01 00:15:21    LOGOUT: User 'admin' logout
5     Info     2017-01-01 00:15:35    LOGIN: Login passed for user 'admin'
6     Info     2017-01-01 00:25:38    LOGOUT: User 'admin' logout
7     Info     2017-01-01 01:02:02    LOGIN: Login passed for user 'admin'
8     Info     2017-01-01 01:12:03    LOGOUT: User 'admin' logout

SP6526P#
```

31-14 loop-protect

show Loop protection.

SYNTAX

show loop-protect

show loop-protect interface { * | [GigabitEthernet <port _list>] }

Parameter

interface	Interface status and configuration
*****	All Switches or All ports
Gigabitethernet	GigabitEthernet
<port_list>	Port List S/X-Y,Z (1/1-26)

EXAMPLE

```
SP6526P# show loop-protect interface GigabitEthernet 1/3
Loop Protection Configuration
======================================
Loop Protection   : Disable
Transmission Time : 5 sec
Shutdown Time     : 180 sec

GigabitEthernet 1/3
------------------------------
Mode : Enabled
Action : Shutdown
Transmit mode : Disabled
The number of loops : 0
loop : -
Status : Down

SP6526P#
```

31-15 mac

Mac Address Table information.

SYNTAX

show mac address-table

show mac address-table address <mac_ucast>

show mac address-table address <mac_ucast> vlan <vlan_id>

show mac address-table [aging-time| conf |static]

show mac address-table count

show mac address-table count interface { * | [GigabitEthernet <port _list>] }

show mac address-table interface { * | [GigabitEthernet <port _list>] }

show mac address-table learning

show mac address-table learning interface { * | [GigabitEthernet <port _list>] }

show mac address-table vlan <vlan_id>

Parameter

address-table	Mac Address Table
address	MAC address lookup
aging-time	Aging time
conf	User added static mac addresses
count	Total number of mac addresses
interface	Select an interface to configure
learning	Learn/disable/secure state
static	All static mac addresses
vlan	Addresses in this VLAN
<mac_ucast>	48 bit MAC address: xx:xx:xx:xx:xx:xx

vlan	VLAN lookup
<vlan_id>	VLAN IDs 1-4095 (1-4095)
*****	All Switches or All ports
Gigabitethernet	GigabitEthernet
<port_list>	Port List S/X-Y,Z (1/1-26)

EXAMPLE

```
SP6526P# show mac address-table count interface GigabitEthernet 1/4
Port                                Count
-----------------------------------  -----
GigabitEthernet 1/4                   0

Total addresses in table: 1
SP6526P#
```

31-16 mvr

Internet Protocol.

SYNTAX

show mvr

show mvr detail

show mvr group-database

Parameter

detail	Detail running information/statistics of MVR
group-database	Multicast group database from MVR

EXAMPLE

```
SP6526P# show mvr group-database
MVR is currently disabled, please enable MVR to start group registration.

MVR Group Database

Switch-1 MVR Group Count: 0
SP6526P#
```

31-17 ntp

Configure NTP.

SYNTAX

show ntp status

Parameter

status	status

EXAMPLE

```
SP6526P# show ntp status
NTP Mode : Disable
Interval : 1440 min
Idx   Server IP host address (a.b.c.d) or a host name string
---   -------------------------------------------------------
1
2
3
4
5
6

SP6526P#
```

31-18 poe

show poe.

SYNTAX

show poe auto-check

show poe config

show poe config interface { * | [GigabitEthernet <port _list>] }

show poe power-delay

show poe power-delay interface { * | [GigabitEthernet <port _list>] }

show poe profile

show poe profile id <1-16>

show poe status

show poe status interface { * | [GigabitEthernet <port _list>] }

Parameter

status	Display PoE (Power Over Ethernet) status for the switch
config	Display PoE (Power Over Ethernet) config for the switch
auto-check	Display PoE Auto Checking config for the switch
power-delay	Display PoE (Power Over Ethernet) Power Delay config for the switch
profile	poe scheduling profile
interface	Interface status and configuration
*****	All Switches or All ports
Gigabitethernet	GigabitEthernet
<port_list>	Port List S/X-Y,Z (1/1-26)
id	show poe profile
<1-16>	Profile id (1..16)

EXAMPLE

```
SP6526P# show poe status interface GigabitEthernet 1/1-2
                                                Power     Power   Current
Interface                     PD Class  Port Status          Alloc [W] Used[W] Used[mA] Priority
---------------------- --------- ---------------------- ---------- -------- --------
--------
GigabitEthernet 1/1                  -  No PD detected                 0.0      0.0        0  Low
GigabitEthernet 1/2                  -  No PD detected                 0.0      0.0        0  Low
Total                                                            0.0      0.0        0
SP6526P#
```

31-19 port-security

show port security.

SYNTAX

show port-security switch interface { * | [GigabitEthernet <port _list>] }

Parameter

switch	Show Port Security status
interface	Interface status and configuration
*****	All Switches or All ports
Gigabitethernet	GigabitEthernet
<port_list>	Port List S/X-Y,Z (1/1-26)

EXAMPLE

```
SP6526P# show port-security switch interface GigabitEthernet 1/4
Interface                  State        MAC Cnt
----------------------- ------------- -------
GigabitEthernet 1/4      Disabled       -

SP6526P#
```

31-20 privilege

Display privilege level configuration

SYNTAX

show privilege group <group> level

show privilege group level

Parameter

group	Privilege group name
<group>	Privilege group name (access-mgmt / arp-inspection / auth-method / dhcp-relay / dhcp-snooping / diagnostic / dot1x / eee / event / forward-failure / ip / ipmc / ip-source-guard / lacp / lldp / loop-protection / mac-table / mirror / mvr / poe / port / port-security / qos / radius / snmp / stp / system / upnp / vlan)
level	Privilege group level

EXAMPLE

```
SP6526P# show privilege group access-mgmt level
Group Name                  Read-only  Read-write
------------------------------  ---------  ----------
access-mgmt                        5        10

SP6526P#
```

31-21 pvlan

PVLAN status.

SYNTAX

show pvlan

show pvlan <pvlan_list>

show pvlan isolation

show pvlan isolation interface { * | [GigabitEthernet <port _list>] }

Parameter

<pvlan_list>	PVLAN ID to show configuration for (1-10)
isolation	show isolation configuration
interface	Show isolation configuration for specify interface
*****	All Switches or All ports
Gigabitethernet	GigabitEthernet
<port_list>	Port List S/X-Y,Z (1/1-26)

EXAMPLE

```
SP6526P# show pvlan isolation
Port                        Isolation
-------------------------------- ---------
GigabitEthernet 1/1            Disabled
GigabitEthernet 1/2            Disabled
GigabitEthernet 1/3            Disabled
GigabitEthernet 1/4            Disabled
.
.
.
.

GigabitEthernet 1/N          Disabled
SP6526P#
```

31-22 qos

Quality of Service.

SYNTAX

show qos

show qos interface

show qos interface { * | [GigabitEthernet <port _list>] }

show qos map [cos-queue | dscp-queue | precedence-queue | queue-cos | queue-dscp | queue-precedence]

Parameter

interface	QoS Interface status and configuration
map	Display global QoS Maps/Tables
*****	All Switches or All ports
Gigabitethernet	GigabitEthernet
<port_list>	Port List S/X-Y,Z (1/1-26)
cos-queue	Map for CoS to queue
dscp-queue	Map for DSCP to queue
precedence-queue	Map for IP Precedence to queue
queue-cos	Map for queue to CoS
queue-dscp	Map for queue to DSCP
queue-precedence	Map for queue to IP Precedence

EXAMPLE

```
SP6526P# show qos map queue-precedence

Queue to IP Precedence mappings
 Queue          0  1  2  3  4  5  6  7
---------------+-----------------------
 IP Precedence   0  1  2  3  4  5  6  7

SP6526P#
```

31-23 radius-server

RADIUS configuration.

SYNTAX

show radius-server

show radius-server statistics

Parameter

statistics	RADIUS statistics

EXAMPLE

```
SP6526P# show radius-server statistics
Global RADIUS Server Timeout      : 5 seconds
Global RADIUS Server Retransmit   : 3 times
Global RADIUS Server Deadtime     : 0 minutes
Global RADIUS Server Key         :
Global RADIUS Server Attribute 4  :
Global RADIUS Server Attribute 95 :
Global RADIUS Server Attribute 32 :
SP6526P#
```

31-24 rmon

RMON statistics.

SYNTAX

show rmon history

show rmon history <1-65535>

show rmon statistics

show rmon statistics <1-65535>

show rmon alarm

show rmon alarm <1-65535>

show rmon event

show rmon event <1-65535>

Parameter

history	Display the RMON history table
statistics	Display the RMON statistics table
alarm	Display the RMON alarm table
event	Display the RMON event table
<1-65535>	History entry list (1..65535)
<1-65535>	Statistics entry list (1..65535)
<1-65535>	Alarm entry list (1..65535)
<1-65535>	Event entry list (1..65535)

EXAMPLE

```
SP6526P# show rmon statistics 5
SP6526P#
```

31-25 running-config

Current operating configuration.

SYNTAX

show running-config

Parameter

CWORD	Valid words are ‘GVRP’ 'access' 'access-list'

'dhcp' 'dhcp-snooping' 'dns' 'dot1x' 'green-ethernet' 'http' 'icli'

'ip-igmp-snooping' 'ip-igmp-snooping-port'

'ip-igmp-snooping-vlan' 'ipmc-profile'

'ipmc-profile-range' 'ipv4' 'ipv6'

'ipv6-mld-snooping' 'ipv6-mld-snooping-port' 'ipv6-mld-snooping-vlan'

‘lacp’ 'lldp' 'logging' 'loop-protect' 'mac' 'mep'

'monitor' 'mstp' 'mvr' 'mvr-port' 'ntp' ‘phy’ ‘poe’ 'port'

'port-security' 'pvlan' 'qos' 'rmon' ‘sflow’

'snmp' 'source-guard' 'ssh' ‘system’ 'upnp' 'user'

'vlan' 'voice-vlan'

EXAMPLE

```
SP6526P# show running-config
username admin privilege 15 password none
!
!
interface GigabitEthernet 1/1
!
interface GigabitEthernet 1/2
!
interface GigabitEthernet 1/3
!
interface GigabitEthernet 1/4
.
.
.
.
.
.

interface GigabitEthernet 1/N
!
!
interface vlan 1
 ip address 192.168.1.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
end
SP6526P#
```

31-26 snmp

Display SNMP configurations.

SYNTAX

show snmp

show snmp access

show snmp access <GroupName : word32> [v1 | v2c | v3 | any] [auth | noauth | priv]

show snmp community v3

show snmp community v3   <Community : word32>

show snmp security-to-group [v1 | v2c | v3] <SecurityName : word32>

show snmp user

show snmp user <UserName : word32>

show snmp view

show snmp view <ViewName : word32> <OidSubtree : word128>

Parameter

access	access configuration
community	Community
security-to-group	security-to-group configuration
user	User
view	MIB view configuration
<GroupName : word32>	Group name (word32)
v1	v1 security model
v2c	v2c security model
v3	v3 security model
any	any security model
auth	authNoPriv Security Level
noauth	noAuthNoPriv Security Level
priv	authPriv Security Level
v3	SNMPv3
<Community : word32>	Specify community name (word32)
<SecurityName : word32>	security group name (word32)
<UserName : word32>	Security user name (word32)
<ViewName : word32>	MIB view name (word32)
<OidSubtree : word128>	MIB view OID (word128)

EXAMPLE

```
SP6526P# show snmp
SNMP Configuration
Read Community              : public
Write Community             : private
Write Mode                 : enabled

SNMPv3 Communities Table:

SNMPv3 Users Table:

SNMPv3 Groups Table:

SNMPv3 Accesses Table:

SNMPv3 Views Table:

SP6526P#
```

31-27 spanning-tree

Spanning Tree protocol.

SYNTAX

show spanning-tree mst configuration

show spanning-tree mst <0-4094>

show spanning-tree mst <0-4094> port

show spanning-tree mst <0-4094> port configuration

Parameter

mst	STP bridge instance
<0-4094>	MST instance ID , 0 is for CIST (0..4094)
configuration	MST Region Info and MSTI VLAN map
port	MST port status
configuration	MST port configuration

EXAMPLE

```
SP6526P# show spanning-tree mst configuration
Multiple Spanning Tree Protocol : Disable
Force Version : MSTP
Region Name : 00-11-3b-01-03-05
Revision Level : 0

MSTI 0 (CIST) : vlan 1-4094

SP6526P#
```

31-28 system

show system information.

SYNTAX

show system

Parameter

None

EXAMPLE

```
SP6526P# show system
Model Name          : SP6526P
System Description : 24-Port 10/100/1000Mbps PoE and 2-Port Gigabit SFP
Hardware Version   : v1.01
Mechanical Version : v1.01
Firmware Version   : v1.00.981
MAC Address        : 00-11-3b-1F-00-7D
Serial Number      : C020316AR2900005
System Name        : SP6526P
Location           :
Contact            :
System Date        : 2017-01-01 00:23:25 +0000
System Uptime      : 0 days, 0:23:40

SP6526P#
```

31-29 tacacs-server

TACACS+ configuration.

SYNTAX

show tacacs-server

EXAMPLE

```
SP6526P# show tacacs-server
Global TACACS+ Server Timeout      : 5 seconds
Global TACACS+ Server Deadtime     : 0 minutes
Global TACACS+ Server Key          :
SP6526P#
```

31-30 trap

Trap configuration.

SYNTAX

show trap

Parameter

None

EXAMPLE

```
SP6526P# show trap
                   Community            Severity
No Ver Server IP      Name                 Level
-- --- --------------- ----------------------- ---------
1
2
3
4
5
6

SP6526P#
```

31-31 upnp

show UPnP configurations.

SYNTAX

show upnp

EXAMPLE

```
SP6526P# show upnp
UPnP Mode               : Disabled
Interface VLAN           : 1
UPnP TTL                : 4
UPnP Advertising Duration  : 100

SP6526P#
```

31-32 version

System software status.

SYNTAX

show version

EXAMPLE

```
SP6526P# show version
Active Image
------------
Partition       : secondary
Version         : v1.00.844
Date            : 2017-03-06 13:37:35 UTC

Alternate Image
------------
Partition       : primary
Version         : v0.91.422
Date            : 2016-11-18 13:45:16 UTC

SP6526P#
```

31-33 vlan

VLAN status.

SYNTAX

show vlan

show vlan brief

show vlan id <vlan_list>

show vlan ip-subnet

show vlan ip-subnet address

show vlan ip-subnet address< ipv4_addr>

show vlan mac config

show vlan mac config address <mac_ucast>

show vlan mac status

show vlan mac status address <mac_ucast>

show vlan mapping

show vlan protocol

show vlan protocol { [eth2 <ethernet value>] | [llc <dsap value> <ssap value>] | [snap <snap oui> <pid value>] }

show vlan status

show vlan status [admin | all | combined | gvrp | mstp | mvr | nas | vcl | voice-vlan]

show vlan status [admin | all | combined | gvrp | mstp | mvr | nas | vcl | voice-vlan] interface { * | [GigabitEthernet <port _list>] }

show vlan status interface { * | [GigabitEthernet <port _list>] } [admin | all | combined | gvrp | mstp | mvr | nas | vcl | voice-vlan]

Parameter

brief	VLAN summary information
id	VLAN status by VLAN id
ip-subnet	Show VLAN ip-subnet entries
mac	Show VLAN MAC entries

mapping	Show VLAN Selective QinQ entries
protocol	Protocol-based VLAN status
status	Show the VLANs configured for each interface
<vlan_list>	VLAN ID to show configuration for (1-4095)
address	Show a specific ip-subnet entry
<ipv4_addr>	The specific ip-subnet to show. (X.X.X.X)
config	Show VLAN MAC config.
status	Show VLAN MAC status.
address	Show a specific MAC entry
<mac_ucast>	The specific MAC entry to show
eth2	Ethernet protocol based VLAN status
llc	LLC-based VLAN group
snap	SNAP-based VLAN group
<ethernet value>	Ether Type(Range: 0x600 - 0xFFFF)
<dsap value>	DSAP(Range: 0x00 - 0xFF)
<ssap value>	SSAP(Range: 0x00 - 0xFF)
<snap oui>	SNAP OUI(must be 0x000000)
<pid value>	PID(Range: 0x0000 - 0XFFFF)
admin	Show the VLANs configured by administrator
all	Show all VLANs configured
combined	Show the VLANs configured by a combination
gvrp	Show the VLANs configured by GVRP
interface	Show the VLANs configured for a specific interface
mstp	Show the VLANs configured by MSTP
mvr	Show the VLANs configured by MVR
nas	Show the VLANs configured by NAS
vcl	Show the VLANs configured by VCL
voice-vlan	Show the VLANs configured by Voice VLAN
*****	All Switches or All ports
Gigabitethernet	GigabitEthernet
<port_list>	Port List S/X-Y,Z (1/1-26)

EXAMPLE

```
SP6526P# show vlan status all interface GigabitEthernet 1/4
GigabitEthernet 1/4 :
---------------------
VLAN User  PortType      PVID  Frame Type    Ing Filter  Tx Tag
---------  -------------  ----  -------------  ----------  -----------------
Admin     C-Port        1     All           Enabled     None
NAS
GVRP
MVR
Voice VLAN
MSTP
DMS
VCL
Combined   C-Port        1     All           Enabled     None

SP6526P#
```

31-34 voice

show voice.

SYNTAX

show voice vlan

Parameter

vlan	show voice vlan

EXAMPLE

```
SP6526P# show voice vlan
no Switch voice setting

Voice VLAN switchport is configured on following:

GigabitEthernet 1/1 :
---------------------
GigabitEthernet 1/1 switchport voice vlan mode is forced
GigabitEthernet 1/1 switchport voice security is disabled
GigabitEthernet 1/1 switchport voice discovery protocol is oui

GigabitEthernet 1/2 :
---------------------
GigabitEthernet 1/2 switchport voice vlan mode is forced
GigabitEthernet 1/2 switchport voice security is disabled
GigabitEthernet 1/2 switchport voice discovery protocol is oui

GigabitEthernet 1/3 :
---------------------
GigabitEthernet 1/3 switchport voice vlan mode is forced
GigabitEthernet 1/3 switchport voice security is disabled
GigabitEthernet 1/3 switchport voice discovery protocol is oui

GigabitEthernet 1/4 :
---------------------
GigabitEthernet 1/4 switchport voice vlan mode is forced
GigabitEthernet 1/4 switchport voice security is disabled
GigabitEthernet 1/4 switchport voice discovery protocol is oui

GigabitEthernet 1/5 :
---------------------
GigabitEthernet 1/5 switchport voice vlan mode is forced
GigabitEthernet 1/5 switchport voice security is disabled
GigabitEthernet 1/5 switchport voice discovery protocol is oui
GigabitEthernet 1/6 :
---------------------
GigabitEthernet 1/6 switchport voice vlan mode is forced
GigabitEthernet 1/6 switchport voice security is disabled
GigabitEthernet 1/6 switchport voice discovery protocol is oui
.
.
.
.
.
.


GigabitEthernet 1/N :
---------------------
GigabitEthernet 1/N switchport voice vlan mode is forced
GigabitEthernet 1/N switchport voice security is disabled
GigabitEthernet 1/N switchport voice discovery protocol is oui


SP6526P#
```

Chapter 32 SSL Commands of CLI

Setup SSL certificate..

Syntax

ssl

EXAMPLE

```
SP6526P# ssl
Generating a 2048 bit RSA private key
..........................................................................
..........................................................+++
............................................................+++
writing new private key to '/mnt/custfs/ssl/lighttpd.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
```

Chapter 33 TERMINAL Commands of CLI

Set terminal line parameters.

Syntax

terminal exec-timeout <0-1440>

Parameter

exec-timeout	Set the EXEC timeout
<0-1440>	Timeout in minutes

EXAMPLE

```
SP6526P# terminal exec-timeout 3
SP6526P#
```

Chapter 34 TRACEROUTE Commands of CLI

Copy from source to destination.

SYNTAX

traceroute ip <ipv4_addr>

traceroute ip <ipv4_addr> { protocol [icmp | udp] } [wait <1-60>] [ttl <1-255>] [nqueries <1-10>]

traceroute ipv6 <ipv6_addr>

traceroute ipv6 <ipv6_addr> { protocol [icmp | udp] } [wait <1-60>] [ttl <1-255>] [nqueries <1-10>]

Parameter

ip	Internet protocol version 4
ipv6	Internet protocol version 6
<ipv4_addr>	IP destination address (X.X.X.X)
protocol	IP Protocol
wait	Set the number of seconds to wait for response to a probe
ttl	Set the max number of hops
nqueries	Set the number of probes per each hop
Icmp	Use ICMP ECHO for tracerouting (default)
udp	Use UDP Port for tracerouting
tcp	Use TCP Sync for tracerouting (default)
<1-60>	Time in seconds to wait for a response. Default is 3s. (1..60)
<1-255>	Max time-to-live. Default is 30. (1..255)
<1-10>	Max time-to-live. Default is 3. (1..10)
<ipv6_addr>	IPv6 destination address (X:X:X:X:X:X:X:X)

EXAMPLE

```
SP6526P# traceroute ip 192.168.1.1 protocol icmp wait 3 ttl 5 nqueries
6
traceroute to 192.168.1.1 (192.168.1.1), 5 hops max, 38 byte packets
 1  192.168.1.1 (192.168.1.1)  10.000 ms  0.000 ms  0.000 ms  0.000 ms
0.000 ms  0.000 ms
SP6526P#
```

➢

Chapter 35 CLI COMMAND REFERENCEs

This chapter introduces the CLI privilege level and command modes.

- The privilege level determines whether or not the user could run the particular commands
- If the user could run the particular command, then the user has to run the command in the correct mode.

35-1 Privilege level

Every command has a privilege level (0-15). Users can run a command if the session's privilege level is greater than or equal to the command's privilege level. The session's privilege level initially comes from the login account's privilege level, though it is possible to change the session's privilege level after logging in.

PRIVILEGE LEVEL	TYPES OF COMMANDS AT THIS PRIVILEGE LEVEL
0	Display basic system information
13	Configure features except for login accounts, the authentication method sequence, multiple logins, and administrator and enable passwords.
15	Configure login accounts, the authentication method sequence, multiple logins, and administrator and enable passwords.

35-2 Command modes

The CLI is divided into several modes. If a user has enough privilege to run a particular command, the user has to run the command in the correct mode. The modes that are available depend on the session's privilege level.

COMMAND	MODE

Command Summary

COMMAND	DESCRIPTION	P	M
show access management	Use the show access management user EXEC command without keywords to display the access management configuration, or use the statistics keyword to display statistics, or use the <AccessId> keyword to display the specific access management entry.	15	EXEC
clear access management statistics	Use the clear access management statistics privileged EXEC command to clear the statistics maintained by access management.	15	EXEC
access management	Use the access management global configuration command to enable the access management. Use the no form of this command to disable the access management.	15	GLOBAL_CONFIG
access management <1-16> <1-4094> <ipv4_addr> [to <ipv4_addr>] { [web] [snmp] [telnet] | all }	Use the access management <AccessId> global configuration command to set the access management entry for IPv4 address.	15	GLOBAL_CONFIG
access management <1-16> <1-4094>	Use the access management	15	GLOBAL_CONFIG

<ipv6_addr> [to <ipv6_addr>] { [web] [snmp] [telnet] | all }	<AccessId> global configuration command to set the access management entry for IPv6 address.		
no access management <1~16>	Use the no access management <AccessIdList> global configuration command to delete the specific access management entry.	15	GLOBAL_CONFIG
access-list action { permit | deny }	Use the access-list action interface configuration command to configure access-list action. The access-list interface configuration will affect the received frames if it doesn't match any ACE.	15	INTERFACE_PORT_LIST
access-list rate-limiter <1-16>	Use the access-list rate-limiter interface configuration command to configure the access-list rate-limiter ID . The access-list interface configuration will affect the received frames if it doesn't match any ACE.	15	INTERFACE_PORT_LIST
no access-list rate-limiter	Use the no access-list rate-limiter interface configuration command to disable the access-list rate-limiter. The access-list interface configuration will affect the received frames if it doesn't match any ACE.	15	INTERFACE_PORT_LIST
access-list { redirect | port-copy } interface { <port_type_id> | <port_type_list> }	Use the no access-list redirect interface configuration command to configure the access-list redirect interface.	15	INTERFACE_PORT_LIST
no access-list { redirect | port-copy }	Use the no access-list redirect interface configuration command to disable the access-list redirect. The access-list interface configuration will affect the received frames if it doesn't match any ACE.	15	INTERFACE_PORT_LIST
access-list mirror	Use the access-list mirror interface configuration command to enable access-list mirror. Use the no form of this command to disable access-list mirror. The access-list interface configuration will affect the received frames if it doesn't match any ACE.	15	INTERFACE_PORT_LIST
access-list logging	Use the access-list logging interface configuration command to enable access-list logging. Use the no form of this command to disable access-list logging. The access-list interface configuration will affect the received frames if it doesn't match any ACE.	15	INTERFACE_PORT_LIST
access-list shutdown	Use the access-list shutdown interface configuration command to enable access-list shutdown. Use the no form of this command to disable access-list shutdown. The access-list interface configuration will affect the received frames if it doesn't match any ACE.	15	INTERFACE_PORT_LIST
access-list evc-policer <1-256>	Use the access-list evc-policer interface configuration command to configure the access-list evc-policer ID. The access-list interface configuration will affect the received frames if it doesn't match any ACE.	15	INTERFACE_PORT_LIST
no access-list evc-policer	Use the no access-list evc-policer interface configuration command to configure the access-list evc-policer ID. The access-list interface configuration will affect the received frames if it doesn't match any ACE.	15	INTERFACE_PORT_LIST
access-list policy <0-255>	Use the access-list policy interface configuration command to configure the access-list policy value. The access-list interface configuration will affect the received frames if it doesn't match any ACE.	15	INTERFACE_PORT_LIST
no access-list policy	Use the no access-list policy interface configuration command to restore the default access-list policy ID. The access-list interface configuration will affect the received frames if it doesn't match any ACE.	15	INTERFACE_PORT_LIST

access-list port-state	Use the access-list port-state interface configuration command to enable access-list port state. Use the no form of this command to disable access-list port state.	15	INTERFACE_PORT_LIST
access-list rate-limiter [<1~16>] { pps <1,2,4,8,16,32,64,128,256,512>| 100pps <1-32767> | kpps <1,2,4,8,16,32,64,128,256,512,1024> | 100kbps <0-10000> }	Use the access-list rate-limiter global configuration command to configure the access-list rate-limiter.	15	INTERFACE_PORT_LIST
default access-list rate-limiter [<1~16>]	Use the default access-list rate-limiter global configuration command to restore the default setting of access-list rate-limiter.	15	GLOBAL_CONFIG
access-list ace [update] <1-256> [next {<1-256>|last}] [ingress {switch <switch_id>|switchport {<1-53>|<1~53>}|interface {<port_type_id>|<port_type_list>}|any}] [policy <0-255> [policy-bitmask <0x0-0xFF>]] [tag {tagged|untagged|any}] [vid {<1-4095>|any}] [tag-priority {<0-7>|0-1|2-3|4-5|6-7|0-3|4-7|any}] [dmac-type {unicast|multicast|broadcast|any}] [frametype { any| etype [etype-value {<0x600-0x7ff,0x801-0x805,0x807-0x86dc,0x86de-0xffff>|any}] [smac {<mac_addr>|any}] [dmac {<mac_addr>|any}]| arp [sip {<ipv4_subnet>|any}] [dip {<ipv4_subnet>|any}] [smac {<mac_addr>|any}] [arp-opcode {arp|rarp|other|any}] [arp-flag [arp-request {<0-1>|any}] [arp-smac {<0-1>|any}] [arp-tmac {<0-1>|any}] [arp-len {<0-1>|any}] [arp-ip {<0-1>|any}] [arp-ether {<0-1>|any}]]| ipv4 [sip {<ipv4_subnet>|any}] [dip {<ipv4_subnet>|any}] [ip-protocol {<0,2-5,7-16,18-255>|any}] [ip-flag [ip-ttl {<0-1>|any}] [ip-options {<0-1>|any}] [ip-fragment {<0-1>|any}]]| ipv4-icmp [sip {<ipv4_subnet>|any}] [dip {<ipv4_subnet>|any}] [icmp-type {<0-255>|any}] [icmp-code {<0-255>|any}] [ip-flag [ip-ttl {<0-1>|any}] [ip-options {<0-1>|any}] [ip-fragment {<0-1>|any}]]| ipv4-udp [sip {<ipv4_subnet>|any}] [dip {<ipv4_subnet>|any}] [sport {<0-65535> [to <0-65535>]|any}] [dport {<0-65535> [to <0-65535>]|any}] [ip-flag [ip-ttl {<0-1>|any}] [ip-options {<0-1>|any}] [ip-fragment {<0-1>|any}]]| ipv4-tcp [sip {<ipv4_subnet>|any}] [dip {<ipv4_subnet>|any}] [sport {<0-65535> [to <0-65535>]|any}] [dport {<0-65535> [to <0-65535>]|any}] [ip-flag [ip-ttl {<0-1>|any}] [ip-options {<0-1>|any}] [ip-fragment {<0-1>|any}]] [tcp-flag [tcp-fin {<0-1>|any}] [tcp-syn {<0-1>|any}] [tcp-rst {<0-1>|any}] [tcp-psh {<0-1>|any}] [tcp-ack {<0-1>|any}] [tcp-urg {<0-1>|any}]]| ipv6 [next-header {<0-5,7-16,18-57,59-255>|any}] [sip {<ipv6_addr> [sip-bitmask <uint>]|any}] [hop-limit {<0-1>|any}]| ipv6-icmp [sip {<ipv6_addr> [sip-bitmask <uint>]|any}] [icmp-type {<0-255>|any}] [icmp-code {<0-255>|any}] [hop-limit {<0-1>|any}]| ipv6-udp [sip {<ipv6_addr> [sip-bitmask <uint>]|any}] [sport {<0-65535> [to <0-65535>]|any}] [dport {<0-65535> [to <0-65535>]|any}] [hop-limit {<0-1>|any}]| ipv6-tcp [sip {<ipv6_addr> [sip-bitmask <uint>]|any}] [sport {<0-65535> [to <0-65535>]|any}] [dport {<0-65535> [to <0-65535>]|any}] [hop-limit {<0-1>|any}] [tcp-flag [tcp-fin {<0-1>|any}] [tcp-syn {<0-1>|any}] [tcp-rst {<0-1>|any}] [tcp-psh {<0-1>|any}] [tcp-ack {<0-1>|any}] [tcp-urg {<0-1>|any}]]}] [action {permit|deny|filter {switchport <1~53>|interface <port_type_list>}}] [rate-limiter {<1-16>|disable}] [evc-policer {<1-256>|disable}] [{redirect|port-copy} {switchport {<1-53>|<1~53>}|interface {<port_type_id>|<port_type_list>}|disable}] [mirror [disable]] [logging [disable]] [shutdown [disable]] [lookup [disable]]	Use the access-list ace global configuration command to set the access-list ace. The command without the update keywrod will creates or overwrites an existing ACE, any unspecified parameter will be set to its default value. Use the update keyword to update an existing ACE and only specified parameter are modified. The ACE must ordered by an appropriate sequence, the received frame will only be hit on the first matched ACE. Use the next or last keyword to adjust the ACE's sequence order.	15	GLOBAL_CONFIG
no access-list ace <1~256>	Use the no access-list ace global configuration command to delete the access-list ace.	15	GLOBAL_CONFIG
show access-list [interface [<port_type_list>]]	Use the show access-list privilege	15	EXEC

[rate-limiter [<1~16>]] [ace statistics [<1~256>]]	EXEC command without keywords to display the access-list configuration, or particularly the show access-list interface for the access-list interface configuration, or use the rate-limiter keyword to display access-list rate-limiter configuration, or use the ace keyword to display access-list ace configuration.		
clear access-list ace statistics	Use the clear access-list ace statistics privileged EXEC command to clear the statistics maintained by access-list, including access-list interface statistics and ACE's statistics.	15	EXEC
show access-list ace-status [static] [link-oam] [loop-protect] [dhcp] [ptp] [upnp] [arp-inspection] [mep] [ipmc] [ip-source-guard] [ip-mgmt] [conflicts] [switch <switch_list>]	Use the show access-list ace-status privilege EXEC command without keywords to display the access-list ace status for all access-list users, or particularly the access-list user for the access-list ace status. Use conflicts keyword to display the access-list ace that doesn't apply on on the hardware. In other word, it means the specific ACE is not applied to the hardware due to hardware limitations.	15	EXEC
show aggregation [mode]		15	EXEC
aggregation mode { [smac] [dmac] [ip] [port] }		15	GLOBAL_CONFIG
no aggregation mode		15	GLOBAL_CONFIG
aggregation group <uint>		15	INTERFACE_PORT_LIST
no aggregation group		15	INTERFACE_PORT_LIST
ip arp inspection	Use the ip arp inspection global configuration command to globally enable ARP inspection. Use the no form of this command to globally disable ARP inspection.	13	GLOBAL_CONFIG
ip arp inspection vlan <vlan_list>	Use the ip arp inspection global configuration command to globally enable ARP inspection. Use the no form of this command to globally disable ARP inspection.	13	GLOBAL_CONFIG
ip arp inspection vlan <vlan_list> logging { deny | permit | all }		13	GLOBAL_CONFIG
no ip arp inspection vlan <vlan_list> logging		13	GLOBAL_CONFIG
ip arp inspection entry interface <port_type_id> <vlan_id> <mac_ucast> <ipv4_ucast>		13	GLOBAL_CONFIG
arp_inspection_translate		13	GLOBAL_CONFIG
arp_inspection_port_mode	Use the ip arp inspection trust interface configuration command to configure a port as trusted for ARP inspection purposes. Use the no form of this command to configure a port as untrusted.	13	INTERFACE_PORT_LIST
arp_inspection_port_check_vlan	Use the ip arp inspection check-vlan interface configuration command to configure a port as VLAN mode for ARP inspection purposes. Use the no form of this command to configure a port as default.	13	INTERFACE_PORT_LIST
ip arp inspection logging { deny | permit | all }	Use the ip arp inspection logging interface configuration command to configure a port as some logging mode for ARP inspection purposes. Use the no form of this command to configure a port as logging none.	13	INTERFACE_PORT_LIST
no ip arp inspection logging	Use the no ip arp inspection logging interface configuration command to configure a port as default logging mode for ARP inspection purposes.	13	INTERFACE_PORT_LIST
show ip arp inspection [interface <port_type_list> | vlan <vlan_list>]		0	EXEC
show ip arp inspection entry [dhcp-snooping | static] [interface <port_type_list>]		13	EXEC
aaa authentication login { telnet | ssh | http } { [local | radius | tacacs] ... }	Use the aaa authentication login command to configure the authentication methods.	15	GLOBAL_CONFIG
no aaa authentication login { telnet | ssh | http }		15	GLOBAL_CONFIG
radius-server timeout <1-1000>	Use the radius-server timeout command to configure the global RADIUS timeout value.	15	GLOBAL_CONFIG

no radius-server timeout	Use the no radius-server timeout command to reset the global RADIUS timeout value to default.	15	GLOBAL_CONFIG
radius-server retransmit <1-1000>	Use the radius-server retransmit command to configure the global RADIUS retransmit value.	15	GLOBAL_CONFIG
no radius-server retransmit	Use the no radius-server retransmit command to reset the global RADIUS retransmit value to default.	15	GLOBAL_CONFIG
radius-server deadtime <1-1440>	Use the radius-server deadtime command to configure the global RADIUS deadtime value.	15	GLOBAL_CONFIG
no radius-server deadtime	Use the no radius-server deadtime command to reset the global RADIUS deadtime value to default.	15	GLOBAL_CONFIG
radius-server key <line1-63>	Use the radius-server key command to configure the global RADIUS key.	15	GLOBAL_CONFIG
no radius-server key	Use the no radius-server key command to remove the global RADIUS key.	15	GLOBAL_CONFIG
radius-server attribute 4 <ipv4_ucast>		15	GLOBAL_CONFIG
no radius-server attribute 4		15	GLOBAL_CONFIG
radius-server attribute 95 <ipv6_ucast>		15	GLOBAL_CONFIG
no radius-server attribute 95		15	GLOBAL_CONFIG
radius-server attribute 32 <line1-253>		15	GLOBAL_CONFIG
no radius-server attribute 32		15	GLOBAL_CONFIG
radius-server host <word1-255> [auth-port <0-65535>] [acct-port <0-65535>] [timeout <1-1000>] [retransmit <1-1000>] [key <line1-63>]	Use the radius-server host command to add a new RADIUS host.	15	GLOBAL_CONFIG
no radius-server host <word1-255> [auth-port <0-65535>] [acct-port <0-65535>]	Use the no radius-server host command to delete an existing RADIUS host.	15	GLOBAL_CONFIG
tacacs-server timeout <1-1000>	Use the tacacs-server timeout command to configure the global TACACS+ timeout value.	15	GLOBAL_CONFIG
no tacacs-server timeout	Use the no tacacs-server timeout command to reset the global TACACS+ timeout value to default.	15	GLOBAL_CONFIG
tacacs-server deadtime <1-1440>	Use the tacacs-server deadtime command to configure the global TACACS+ deadtime value.	15	GLOBAL_CONFIG
no tacacs-server deadtime	Use the no tacacs-server deadtime command to reset the global TACACS+ deadtime value to default.	15	GLOBAL_CONFIG
tacacs-server key <line1-63>	Use the tacacs-server key command to configure the global TACACS+ key.	15	GLOBAL_CONFIG
no tacacs-server key	Use the no tacacs-server key command to remove the global TACACS+ key.	15	GLOBAL_CONFIG
tacacs-server host <word1-255> [port <0-65535>] [timeout <1-1000>] [key <line1-63>]	Use the tacacs-server host command to add a new TACACS+ host.	15	GLOBAL_CONFIG
no tacacs-server host <word1-255> [port <0-65535>]	Use the no tacacs-server host command to delete an existing TACACS+ host.	15	GLOBAL_CONFIG
show aaa	Use the show aaa command to view the currently active authentication login methods.	15	GLOBAL_CONFIG
show radius-server [statistics]	Use the show radius-server command to view the current RADIUS configuration and statistics.	15	EXEC
show tacacs-server	Use the show tacacs-server command to view the current TACACS+ configuration.	15	EXEC
debug auth { telnet | ssh | http } <word31> [<word31>]		debug	EXEC
clock summer-time <word16> recurring [<1-5> <1-7> <1-12> <hhmm> <1-5> <1-7> <1-12> <hhmm> [<1-1440>]]		13	GLOBAL_CONFIG
clock summer-time <word16> date [<1-12> <1-31> <2000-2097> <hhmm> <1-12> <1-31> <2000-2097> <hhmm> [<1-1440>]]		13	GLOBAL_CONFIG
no clock summer-time		13	GLOBAL_CONFIG
clock timezone <word16> <-23-23> [<0-59>]		13	GLOBAL_CONFIG
no clock timezone		13	GLOBAL_CONFIG
show clock detail		0	EXEC
clock summer-time <word16> recurring [<1-5> <1-7> <1-12> <hhmm> <1-5> <1-7> <1-12> <hhmm> [<1-1440>]]		13	GLOBAL_CONFIG
clock summer-time <word16> date [<1-12> <1-31> <2000-2097> <hhmm> <1-12> <1-31> <2000-2097> <hhmm> [<1-1440>]]		13	GLOBAL_CONFIG

no clock summer-time		13	GLOBAL_CONFIG
clock timezone <word16> <-23-23> [<0-59>]		13	GLOBAL_CONFIG
no clock timezone		13	GLOBAL_CONFIG
show clock detail		0	EXEC
show ip dhcp detailed statistics { server | client | snooping | relay | normal-forward | combined } [interface <port_type_list>]	Use the show ip dhcp detailed statistics user EXEC command to display statistics. Notice that the normal forward per-port TX statistics isn't increased if the incoming DHCP packet is done by L3 forwarding mechanism. Notice that the normal forward per-port TX statistics isn't increased if the incoming DHCP packet is done by L3 forwarding mechanism.	0	EXEC
clear ip dhcp detailed statistics { server | client | snooping | relay | helper | all } [interface <port_type_list>]	Use the clear ip dhcp detailed statistics privileged EXEC command to clear the statistics, or particularly the IP DHCP statistics for the interface. Notice that except for clear statistics on all interfaces, clear the statistics on specific port may not take effect on global statistics since it gathers the different layer overview.	15	EXEC
clear ip dhcp relay statistics	Use the clear ip dhcp relay statistics privileged EXEC command to clear the statistics maintained by IP DHCP realy.	15	EXEC
show ip dhcp relay [statistics]	Use the show ip dhcp relay user EXEC command without keywords to display the DHCP relay configuration, or use the statistics keyword to display statistics.	0	EXEC
ip dhcp relay	Use the ip dhcp relay global configuration command to enable the DHCP relay server. Use the no form of thiscommand to disable the DHCP relay server.	15	GLOBAL_CONFIG
ip helper-address <ipv4_ucast>	Use the ip helper-address global configuration command to configure the host address of DHCP relay server.	15	GLOBAL_CONFIG
no ip helper-address	Use the no ip helper-address global configuration command to clear the host address of DHCP relay server.	15	GLOBAL_CONFIG
ip dhcp relay information option	Use the ip dhcp relay information option global configuration command to enable the DHCP relay information option. Use the no form of this command to disable the DHCP relay information option. The option 82 circuit ID format as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID(in standalone device it always equal 0, in stackable device it means switch ID), and the last two characters are the port number. For example, "00030108" means the DHCP message receive form VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal the switch MAC address.	15	GLOBAL_CONFIG
ip dhcp relay information policy { drop | keep | replace }	Use the ip dhcp relay information policy global configuration command to configure the DHCP relay information policy. When DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' policy is invalid when relay information mode is disabled.	15	GLOBAL_CONFIG
no ip dhcp relay information policy	Use the ip dhcp relay information policy global configuration command to restore the default DHCP relay information policy.	15	GLOBAL_CONFIG
show ip dhcp pool [<word32>]		0	EXEC
show ip dhcp pool counter [<word32>]		debug	EXEC
show ip dhcp excluded-address		0	EXEC
show ip dhcp server binding [state {allocated | committed | expired}] [type {automatic | manual | expired}]		0	EXEC

show ip dhcp server binding <ipv4_ucast>		0	EXEC
show ip dhcp server		0	EXEC
show ip dhcp server statistics		0	EXEC
show ip dhcp server declined-ip		0	EXEC
show ip dhcp server declined-ip <ipv4_addr>		0	EXEC
clear ip dhcp server binding <ipv4_ucast>		13	EXEC
clear ip dhcp server binding { automatic | manual | expired }		13	EXEC
clear ip dhcp server statistics		13	EXEC
ip dhcp server		13	GLOBAL_CONFIG
ip dhcp excluded-address <ipv4_addr> [<ipv4_addr>]		13	GLOBAL_CONFIG
no ip dhcp pool <word32>		13	GLOBAL_CONFIG
ip dhcp server		13	INTERFACE_VLAN
network <ipv4_addr> <ipv4_netmask>		13	DHCP_POOL
no network		13	DHCP_POOL
broadcast <ipv4_addr>		13	DHCP_POOL
no broadcast		13	DHCP_POOL
default-router <ipv4_ucast> [<ipv4_ucast> [<ipv4_ucast> [<ipv4_ucast>]]]		13	DHCP_POOL
no default-router		13	DHCP_POOL
lease { <0-365> [<0-23> [<uint>]] | infinite }		13	DHCP_POOL
no lease		13	DHCP_POOL
domain-name <word128>		13	DHCP_POOL
no domain-name		13	DHCP_POOL
dns-server <ipv4_ucast> [<ipv4_ucast> [<ipv4_ucast> [<ipv4_ucast>]]]		13	DHCP_POOL
no dns-server		13	DHCP_POOL
ntp-server <ipv4_ucast> [<ipv4_ucast> [<ipv4_ucast> [<ipv4_ucast>]]]		13	DHCP_POOL
no ntp-server		13	DHCP_POOL
netbios-name-server <ipv4_ucast> [<ipv4_ucast> [<ipv4_ucast> [<ipv4_ucast>]]]		13	DHCP_POOL
no netbios-name-server		13	DHCP_POOL
netbios-node-type { b-node | h-node | m-node | p-node }		13	DHCP_POOL
no netbios-node-type		13	DHCP_POOL
netbios-scope <line128>		13	DHCP_POOL
no netbios-scope		13	DHCP_POOL
nis-domain-name <word128>		13	DHCP_POOL
no nis-domain-name		13	DHCP_POOL
nis-server <ipv4_ucast> [<ipv4_ucast> [<ipv4_ucast> [<ipv4_ucast>]]]		13	DHCP_POOL
no nis-server		13	DHCP_POOL
host <ipv4_ucast> <ipv4_netmask>		13	DHCP_POOL
no host		13	DHCP_POOL
client-identifier { fqdn <line128> | mac-address <mac_addr> }		13	DHCP_POOL
no client-identifier		13	DHCP_POOL
hardware-address <mac_ucast>		13	DHCP_POOL
no hardware-address		13	DHCP_POOL
client-name <word32>		13	DHCP_POOL
no client-name		13	DHCP_POOL
vendor class-identifier <string64> specific-info <hexval32>		13	DHCP_POOL
no vendor class-identifier <string64>		13	DHCP_POOL
debug dhcp server memsize		debug	EXEC
debug dhcp server declined add <ipv4_addr>		debug	EXEC
debug dhcp server declined delete <ipv4_addr>		debug	EXEC
show ip dhcp snooping [interface <port_type_list>]	Use the show ip dhcp snooping user EXEC command to display the DHCP snooping configuration.	0	EXEC
show ip dhcp snooping [statistics] [interface <port_type_list>]	Use the show ip dhcp snooping user EXEC command without keywords to display the DHCP snooping configuration, or particularly the ip dhcp snooping statistics for the interface, or use the statistics keyword to display statistics.	0	EXEC
clear ip dhcp snooping statistics [interface <port_type_list>]	Use the clear ip dhcp snooping statistics privileged EXEC command to clear the statistics maintained by IP DHCP snooping, or particularly the IP DHCP snooping statistics for the interface.	15	EXEC
ip dhcp snooping	Use the ip dhcp snooping global configuration command to globally enable DHCP snooping. Use the no	15	GLOBAL_CONFIG

	form of this command to globally disable DHCP snooping.		
dhcp_snooping_port_mode	Use the ip dhcp snooping trust interface configuration command to configure a port as trusted for DHCP snooping purposes. Use the no form of this command to configure a port as untrusted.	15	INTERFACE_PORT_LIST
show ip dhcp snooping table	Use the show ip dhcp snooping table user EXEC command to display the IP assigned information that is obtained from DHCP server except for local VLAN interface IP addresses.	15	EXEC
ip name-server { <ipv4_ucast> | dhcp [interface vlan <vlan_id>] }	Set the DNS server for resolving domain names	15	GLOBAL_CONFIG
no ip name-server	Stop resolving domain names by accessing DNS server	15	GLOBAL_CONFIG
show ip name-server	Display the active domain name server information	0	EXEC
ip dns proxy	Enable DNS proxy service	15	GLOBAL_CONFIG
show version	Use show version to display firmware information.	0	EXEC
firmware upgrade <word>	Use firmware upgrade to load new firmware image to the switch.	15	EXEC
firmware swap	Use firmware swap to swap the active and alternative firmware images.	15	EXEC
show green-ethernet fan	Shows Fan status (chip Temperature and fan speed).	15	GLOBAL_CONFIG
green-ethernet fan temp-on <-127-127>	Sets temperature at which to turn fan on to the lowest speed.	15	GLOBAL_CONFIG
no green-ethernet fan temp-on	Sets temperature at which to turn fan on to the lowest speed to default.	15	GLOBAL_CONFIG
green-ethernet fan temp-max <-127-127>	Sets temperature where the fan must be running at full speed.	15	GLOBAL_CONFIG
no green-ethernet fan temp-max	Sets temperature at which the fan shall be running at full speed to default.	15	GLOBAL_CONFIG
green-ethernet led interval <0~24> intensity <0-100>	Use green-ethernet led interval to configure the LED intensity at specific interval of the day.	15	GLOBAL_CONFIG
no green-ethernet led interval <0~24>		15	GLOBAL_CONFIG
green-ethernet led on-event { [link-change <0-65535>] [error] }*1	Use green-ethernet led on-event to configure when to turn LEDs intensity to 100%%.	15	GLOBAL_CONFIG
no green-ethernet led on-event [link-change] [error]		15	GLOBAL_CONFIG
show green-ethernet eee [interface <port_type_list>]	Shows Green Ethernet EEE status.	15	EXEC
show green-ethernet short-reach [interface <port_type_list>]	Shows Green Ethernet short-reach status.	15	EXEC
show green-ethernet energy-detect [interface <port_type_list>]	Shows Green Ethernet energy-detect status.	15	EXEC
show green-ethernet [interface <port_type_list>]	Shows Green Ethernet status.	15	EXEC
green-ethernet eee	Sets EEE mode.	15	INTERFACE_PORT_LIST
green-ethernet eee urgent-queues [<range_list>]	Sets EEE urgeent queues.	15	INTERFACE_PORT_LIST
green-ethernet eee optimize-for-power	Sets if EEE should be optimized for least traffic latency or least power comsumption	15	GLOBAL_CONFIG
green-ethernet energy-detect	Enables energy-detect power savings.	15	INTERFACE_PORT_LIST
green-ethernet short-reach	Enables short-reach power savings.	15	INTERFACE_PORT_LIST
show ip http server secure status	Use the show ip http server secure status privileged EXEC command to display the secure HTTP web server status.	15	EXEC
ip http secure-server	Use the ip http secure-server global configuration command to enable the secure HTTP web server. Use the no form of this command to disable the secure HTTP web server.	15	GLOBAL_CONFIG
ip http secure-redirect	Use the http secure-redirect global configuration command to enable the secure HTTP web redirection. When the secure HTTP web server is enabled, the feature automatic redirect the none secure HTTP web connection to the secure HTTP web connection. Use the no form of this command to disable the secure HTTP web redirection.	15	GLOBAL_CONFIG
reload { { { cold | warm } [sid <1-16>] } | { defaults	Reload system, either cold (reboot) or	15	EXEC

[keep-ip] } }	restore defaults without reboot.		
show running-config [all-defaults]		15	EXEC
show running-config feature <cword> [all-defaults]		15	EXEC
show running-config interface <port_type_list> [all-defaults]		15	EXEC
show running-config interface vlan <vlan_list> [all-defaults]		15	EXEC
show running-config vlan <vlan_list> [all-defaults]		15	EXEC
show running-config line vty <range_list> [all-defaults]		15	EXEC
copy { startup-config | running-config | <word> } { startup-config | running-config | <word> } [syntax-check]		15	EXEC
dir		15	EXEC
more <word>		15	EXEC
delete <word>		debug	EXEC
debug icfg wipe-flash-fs-conf-block		debug	EXEC
debug icfg wipe-specific-block {local|global} <uint>		debug	EXEC
debug icfg silent-upgrade status		debug	EXEC
debug icfg dir		debug	EXEC
debug icfg error-trace <line>		debug	EXEC
ip routing	Enable routing for IPv4 and IPv6	15	GLOBAL_CONFIG
no ip routing	Disable routing for IPv4 and IPv6	15	GLOBAL_CONFIG
ip address {{<ipv4_addr> <ipv4_netmask>} | {dhcp [fallback <ipv4_addr> <ipv4_netmask> [timeout <uint>]]}}	IP address configuration	15	INTERFACE_VLAN
ip dhcp retry interface vlan <vlan_id>	Restart the dhcp client	15	EXEC
no ip address	IP address configuration	15	INTERFACE_VLAN
ip route <ipv4_addr> <ipv4_netmask> <ipv4_addr>	Add new IP route	15	GLOBAL_CONFIG
no ip route <ipv4_addr> <ipv4_netmask> <ipv4_addr>	Delete an existing IP route	15	GLOBAL_CONFIG
show interface vlan [<vlan_list>]	Vlan interface status	15	EXEC
show ip interface brief	Brief IP interface status	0	EXEC
show ip arp	Print ARP table	0	EXEC
clear ip arp	Clear ARP cache	0	EXEC
show ip route	Routing table status	0	EXEC
ping ip <word1-255> [repeat <1-60>] [size <2-1452>] [interval <0-30>]		0	EXEC
clear ip statistics [system] [interface vlan <vlan_list>] [icmp] [icmp-msg <0~255>]		0	EXEC
show ip statistics [system] [interface vlan <vlan_list>] [icmp] [icmp-msg <0~255>]		0	EXEC
debug ipstack log [ERR|NOERR] [WARNING|NOWARNING] [NOTICE|NONOTICE] [INFO|NOINFO] [DEBUG|NODEBUG] [MDEBUG|NOMDEBUG] [IOCTL|NOIOCTL] [INIT|NOINIT] [ADDR|NOADDR] [FAIL|NOFAIL] [EMERG|NOEMERG] [CRIT|NOCRIT]		debug	EXEC
debug ip kmem		debug	EXEC
debug ip route		debug	EXEC
debug ip sockets		debug	EXEC
debug ip lpm stat ip <vlan_list>		debug	EXEC
debug ip lpm stat ipv6 <vlan_list>		debug	EXEC
debug ip lpm stat clear <vlan_list>		debug	EXEC
debug ip lpm sticky clear		debug	EXEC
debug ip lpm usage		debug	EXEC
debug ip global interface table change		debug	EXEC
debug ip vlan ipv4 created <vlan_list>		debug	EXEC
debug ip vlan ipv4 changed <vlan_list>		debug	EXEC
debug ip vlan ipv6 created <vlan_list>		debug	EXEC
debug ip vlan ipv6 changed <vlan_list>		debug	EXEC
show ip igmp snooping mrouter [detail]		0	EXEC
clear ip igmp snooping [vlan <vlan_list>] statistics		15	EXEC
show ip igmp snooping [vlan <vlan_list>] [group-database [interface <port_type_list>] [sfm-information]] [detail]		0	EXEC
ip igmp snooping		15	GLOBAL_CONFIG
ip igmp unknown-flooding		15	GLOBAL_CONFIG
ip igmp host-proxy [leave-proxy]		15	GLOBAL_CONFIG
ip igmp ssm-range <ipv4_mcast> <4-32>		15	GLOBAL_CONFIG
no ip igmp ssm-range		15	GLOBAL_CONFIG
ip igmp snooping vlan <vlan_list>		15	GLOBAL_CONFIG
no ip igmp snooping vlan [<vlan_list>]		15	GLOBAL_CONFIG
ip igmp snooping		15	INTERFACE_VLAN
ip igmp snooping querier { election | address		15	INTERFACE_VLAN

<ipv4_ucast> }			
no ip igmp snooping querier { election | address }		15	INTERFACE_VLAN
ip igmp snooping compatibility { auto | v1 | v2 | v3 }		15	INTERFACE_VLAN
no ip igmp snooping compatibility		15	INTERFACE_VLAN
ip igmp snooping priority <0-7>		15	INTERFACE_VLAN
no ip igmp snooping priority		15	INTERFACE_VLAN
ip igmp snooping robustness-variable <1-255>		15	INTERFACE_VLAN
no ip igmp snooping robustness-variable		15	INTERFACE_VLAN
ip igmp snooping query-interval <1-31744>		15	INTERFACE_VLAN
no ip igmp snooping query-interval		15	INTERFACE_VLAN
ip igmp snooping query-max-response-time <0-31744>		15	INTERFACE_VLAN
no ip igmp snooping query-max-response-time		15	INTERFACE_VLAN
ip igmp snooping last-member-query-interval <0-31744>		15	INTERFACE_VLAN
no ip igmp snooping last-member-query-interval		15	INTERFACE_VLAN
ip igmp snooping unsolicited-report-interval <0-31744>		15	INTERFACE_VLAN
no ip igmp snooping unsolicited-report-interval		15	INTERFACE_VLAN
ip igmp snooping immediate-leave		15	INTERFACE_VLAN
ip igmp snooping mrouter		15	INTERFACE_PORT_LIST
ip igmp snooping max-groups <1-10>		15	INTERFACE_PORT_LIST
no ip igmp snooping max-groups		15	INTERFACE_PORT_LIST
ip igmp snooping filter <word16>		15	INTERFACE_PORT_LIST
no ip igmp snooping filter		15	INTERFACE_PORT_LIST
ipv6 mld snooping		15	GLOBAL_CONFIG
ipv6 mld unknown-flooding		15	GLOBAL_CONFIG
ipv6 mld host-proxy [leave-proxy]		15	GLOBAL_CONFIG
ipv6 mld ssm-range <ipv6_mcast> <8-128>		15	GLOBAL_CONFIG
no ipv6 mld ssm-range		15	GLOBAL_CONFIG
ipv6 mld snooping vlan <vlan_list>		15	GLOBAL_CONFIG
no ipv6 mld snooping vlan [<vlan_list>]		15	GLOBAL_CONFIG
ipv6 mld snooping immediate-leave		15	INTERFACE_PORT_LIST
ipv6 mld snooping mrouter		15	INTERFACE_PORT_LIST
ipv6 mld snooping max-groups <1-10>		15	INTERFACE_PORT_LIST
no ipv6 mld snooping max-groups		15	INTERFACE_PORT_LIST
ipv6 mld snooping filter <word16>		15	INTERFACE_PORT_LIST
no ipv6 mld snooping filter		15	INTERFACE_PORT_LIST
show ipv6 mld snooping mrouter [detail]		0	EXEC
clear ipv6 mld snooping [vlan <vlan_list>] statistics		15	EXEC
show ipv6 mld snooping [vlan <vlan_list>] [group-database [interface <port_type_list>] [sfm-information]] [detail]		0	EXEC
ipv6 mld snooping		15	INTERFACE_VLAN
ipv6 mld snooping querier election		15	INTERFACE_VLAN
ipv6 mld snooping compatibility { auto | v1 | v2 }		15	INTERFACE_VLAN
no ipv6 mld snooping compatibility		15	INTERFACE_VLAN
ipv6 mld snooping priority <0-7>		15	INTERFACE_VLAN
no ipv6 mld snooping priority		15	INTERFACE_VLAN
ipv6 mld snooping robustness-variable <1-255>		15	INTERFACE_VLAN
no ipv6 mld snooping robustness-variable		15	INTERFACE_VLAN
ipv6 mld snooping query-interval <1-31744>		15	INTERFACE_VLAN
no ipv6 mld snooping query-interval		15	INTERFACE_VLAN
ipv6 mld snooping query-max-response-time <0-31744>		15	INTERFACE_VLAN
no ipv6 mld snooping query-max-response-time		15	INTERFACE_VLAN
ipv6 mld snooping last-member-query-interval <0-31744>		15	INTERFACE_VLAN
no ipv6 mld snooping last-member-query-interval		15	INTERFACE_VLAN
ipv6 mld snooping unsolicited-report-interval <0-31744>		15	INTERFACE_VLAN
no ipv6 mld snooping unsolicited-report-interval		15	INTERFACE_VLAN
ip verify source		13	GLOBAL_CONFIG
i ip verify source		13	INTERFACE_PORT_LIST
ip verify source limit <0-2>		13	INTERFACE_PORT_LIST
no ip verify source limit		13	INTERFACE_PORT_LIST
ip verify source translate		13	GLOBAL_CONFIG
show ip verify source [interface <port_type_list>]		0	EXEC
show ip source binding [dhcp-snooping | static] [interface <port_type_list>]		13	EXEC
ip source binding interface <port_type_id> <vlan_id> <ipv4_ucast> <mac_ucast>		13	GLOBAL_CONFIG
ip source binding interface <port_type_id> <vlan_id> <ipv4_ucast> <ipv4_netmask>		13	GLOBAL_CONFIG
show lacp { internal | statistics | system-id | neighbour }	Show LACP configuration and status	15	EXEC

clear lacp statistics	Clear all LACP statistics	15	EXEC
lacp system-priority <1-65535>	Set the LACP system priority	15	GLOBAL_CONFIG
lacp	Enable LACP on an interface	15	INTERFACE_PORT_LIST
lacp key { <1-65535> | auto }	Set the LACP key	15	INTERFACE_PORT_LIST
lacp role { active | passive }	Set the LACP role, active or passive in transmitting BPDUs	15	INTERFACE_PORT_LIST
lacp timeout { fast | slow }	Set the LACP timeout, i.e. how fast to transmit BPDUs, once a sec or once each 30 sec.	15	INTERFACE_PORT_LIST
lacp port-priority <1-65535>	Set the lacp port priority,	15	INTERFACE_PORT_LIST
lldp holdtime <2-10>	Sets LLDP hold time (The neighbor switch will discarded the LLDP information after \"hold time\" multiplied with \"timer\" seconds)	15	GLOBAL_CONFIG
no lldp holdtime		15	GLOBAL_CONFIG
lldp timer <5-32768>	Sets LLDP TX interval (The time between each LLDP frame transmitted in seconds).	15	GLOBAL_CONFIG
no lldp timer		15	GLOBAL_CONFIG
lldp reinit <1-10>	Sets LLDP reinitialization delay.	15	GLOBAL_CONFIG
no lldp reinit	Sets LLDP reinitialization delay.	15	GLOBAL_CONFIG
lldp tlv-select {management-address | port-description | system-capabilities | system-description | system-name}	Enables/disables LLDP optional TLVs.	15	INTERFACE_PORT_LIST
lldp transmit	Sets if switch shall transmit LLDP frames.	15	INTERFACE_PORT_LIST
lldp receive	Sets if switch shall update LLDP entry table with incoming LLDP information.	15	INTERFACE_PORT_LIST
show lldp neighbors [interface <port_type_list>]	Shows the LLDP neighbors information.	0	EXEC
show lldp statistics [interface <port_type_list>]	Shows the LLDP statistics information.	0	EXEC
clear lldp statistics	Clears the LLDP statistics.	0	EXEC
lldp transmission-delay <1-8192>	Sets LLDP transmision-delay. LLDP transmission delay (the amount of time that the transmission of LLDP frames will delayed after LLDP configuration has changed) in seconds.)	15	GLOBAL_CONFIG
no lldp transmission-delay		15	GLOBAL_CONFIG
lldp cdp-aware	Configures if the interface shall be CDP aware (CDP discovery information is added to the LLDP neighbor table)	15	INTERFACE_PORT_LIST
show lldp med remote-device [interface <port_type_list>]	Show LLDP-MED neighbor device information.	0	EXEC
show lldp med media-vlan-policy [<0~31>]	Show media vlan policy(ies)	0	EXEC
lldp med location-tlv latitude { north | south } <word8>	Use the lldp med location-tlv latitude to configure the location latitude.	15	GLOBAL_CONFIG
no lldp med location-tlv latitude	Use no lldp med location-tlv latitude to configure the latitude location to north 0 degrees.	15	GLOBAL_CONFIG
lldp med location-tlv longitude { west | east } <word9>	Use the lldp med location-tlv longitude to configure the location longitude.	15	GLOBAL_CONFIG
no lldp med location-tlv longitude	Use no lldp med location-tlv longitude to configure the longitude location to north 0 degrees.	15	GLOBAL_CONFIG
lldp med location-tlv altitude { meters | floors } <word11>	Use the lldp med location-tlv altitude to configure the location altitude.	15	GLOBAL_CONFIG
no lldp med location-tlv altitude	Use the lldp med location-tlv altitude to configure the location altitude.	15	GLOBAL_CONFIG
lldp med location-tlv civic-addr { country | state | county | city | district | block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark | additional-info | name | zip-code | building | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code } <string250>	Use lldp med location-tlv civic-addr to configure the civic address.	15	GLOBAL_CONFIG
no lldp med location-tlv civic-addr { country | state | county | city | district | block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark | additional-info | name | zip-code | building | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code }		15	GLOBAL_CONFIG
lldp med location-tlv elin-addr <dword25>	Use the lldp med location-tlv elin-addr to configure value for the Emergency Call Service	15	GLOBAL_CONFIG
no lldp med location-tlv elin-addr	Use the no lldp med location-tlv elin-addr to configure value for the	15	GLOBAL_CONFIG

	Emergency Call Service to default value.		
lldp med transmit-tlv [capabilities] [location] [network-policy]	Use the lldp med transmit-tlv to configure which TLVs to transmit to link partner.	15	INTERFACE_PORT_LIST
no lldp med transmit-tlv [capabilities] [location] [network-policy]		15	INTERFACE_PORT_LIST
lldp med datum { wgs84 | nad83-navd88 | nad83-mllw }	Use the lldp med datum to configure the datum (geodetic system) to use.	15	GLOBAL_CONFIG
no lldp med datum		15	GLOBAL_CONFIG
lldp med fast <1-10>	Use the lldp med fast to configure the number of times the fast start LLDPDU are being sent during the activation of the fast start mechanism defined by LLDP-MED (1-10).	15	GLOBAL_CONFIG
no lldp med fast		15	GLOBAL_CONFIG
lldp med media-vlan-policy <0-31> { voice | voice-signaling | guest-voice-signaling | guest-voice | softphone-voice | video-conferencing | streaming-video | video-signaling } { tagged <vlan_id> | untagged } [l2-priority <0-7>] [dscp <0-63>]	Use the media-vlan-policy to create a policy, which can be assigned to an interface.	15	GLOBAL_CONFIG
no lldp med media-vlan-policy <0~31>		15	GLOBAL_CONFIG
lldp med media-vlan policy-list <range_list>	Use the media-vlan policy-list to assign policy to the interface.	15	INTERFACE_PORT_LIST
loop-protect	Loop protection configuration	15	GLOBAL_CONFIG
loop-protect transmit-time <1-10>	Loop protection transmit time interval	15	GLOBAL_CONFIG
no loop-protect transmit-time		15	GLOBAL_CONFIG
loop-protect shutdown-time <0-604800>	Loop protection shutdown time interval	15	GLOBAL_CONFIG
no loop-protect shutdown-time		15	GLOBAL_CONFIG
loop-protect	Loop protection configuration	15	INTERFACE_PORT_LIST
loop-protect action { [shutdown] [log] }*1		15	INTERFACE_PORT_LIST
no loop-protect action		15	INTERFACE_PORT_LIST
loop-protect tx-mode		15	INTERFACE_PORT_LIST
show loop-protect [interface <port_type_list>]		13	EXEC
mac address-table learning [secure]	Enable learning on port	15	INTERFACE_PORT_LIST
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>]		0	EXEC
clear mac address-table		15	EXEC
mac address-table static <mac_addr> vlan <vlan_id> interface <port_type_list>	Assign a static mac address to this port	15	GLOBAL_CONFIG
mac address-table aging-time <0,10-1000000>	Set switch aging time, 0 to disable.	15	GLOBAL_CONFIG
no mac address-table aging-time	Default aging time.	15	GLOBAL_CONFIG
monitor destination interface <port_type_id>	Sets monitor destination port.	15	GLOBAL_CONFIG
no monitor destination	Sets monitor destination port.	15	GLOBAL_CONFIG
monitor source { { interface <port_type_list> } | { cpu [<range_list>] } } { both | rx | tx }	Sets monitor source port(s).	15	GLOBAL_CONFIG
no monitor source { { interface <port_type_list> } | { cpu [<range_list>] } }	Sets monitor source port(s).	15	GLOBAL_CONFIG
debug chip [{ 0 | 1 | all }]		debug	EXEC
debug api [interface <port_type_list>] [{ ail | cil }] [{ init | misc | port | counters | phy | vlan | pvlan | mac-table | acl | qos | aggr | stp | mirror | evc | erps | eps | packet | fdma | ts | pts | wm | ipmc | stack | cmef | mplscore | mplsoam | vxlat | oam | sgpio | l3 | afi | macsec }] [full] [clear]		debug	EXEC
debug suspend		debug	EXEC
debug resume		debug	EXEC
debug kr-conf [cm1 <-32-31>] [c0 <-32-31>] [cp1 <-32-31>] [ampl <300-1275>] [{ ps25 | ps35 | ps55 | ps70 | ps120 }] [en-ob | dis-ob] [ser-inv | ser-no-inv]		debug	INTERFACE_PORT_LIST
show spanning-tree [summary | active | { interface <port_type_list> } | { detailed [interface <port_type_list>] } | { mst [configuration | { <0-7> [interface <port_type_list>] }] }]		15	EXEC
clear spanning-tree { { statistics [interface <port_type_list>] } | { detected-protocols [interface <port_type_list>] } }		15	EXEC
spanning-tree mode { stp | rstp | mstp }		15	GLOBAL_CONFIG
no spanning-tree mode		15	GLOBAL_CONFIG
spanning-tree transmit hold-count <1-10>		15	GLOBAL_CONFIG
no spanning-tree transmit hold-count		15	GLOBAL_CONFIG
spanning-tree mst max-hops <6-40>		15	GLOBAL_CONFIG
no spanning-tree mst max-hops		15	GLOBAL_CONFIG
spanning-tree mst max-age <6-40> [forward-time		15	GLOBAL_CONFIG

<4-30>]			
no spanning-tree mst max-age		15	GLOBAL_CONFIG
spanning-tree mst forward-time <4-30>		15	GLOBAL_CONFIG
no spanning-tree mst forward-time		15	GLOBAL_CONFIG
spanning-tree edge bpdu-filter		15	GLOBAL_CONFIG
spanning-tree edge bpdu-guard		15	GLOBAL_CONFIG
spanning-tree recovery interval <30-86400>		15	GLOBAL_CONFIG
no spanning-tree recovery interval		15	GLOBAL_CONFIG
spanning-tree mst <0-7> priority <0-61440>		15	GLOBAL_CONFIG
no spanning-tree mst <0-7> priority		15	GLOBAL_CONFIG
spanning-tree mst <0-7> vlan <vlan_list>		15	GLOBAL_CONFIG
no spanning-tree mst <0-7> vlan		15	GLOBAL_CONFIG
spanning-tree mst name <word32> revision <0-65535>		15	GLOBAL_CONFIG
no spanning-tree mst name		15	GLOBAL_CONFIG
spanning-tree		15	INTERFACE_PORT_LIST
spanning-tree edge		15	INTERFACE_PORT_LIST
spanning-tree auto-edge		15	INTERFACE_PORT_LIST
spanning-tree link-type { point-to-point | shared | auto }		15	INTERFACE_PORT_LIST
no spanning-tree link-type		15	INTERFACE_PORT_LIST
spanning-tree restricted-role		15	INTERFACE_PORT_LIST
spanning-tree restricted-tcn		15	INTERFACE_PORT_LIST
spanning-tree bpdu-guard		15	INTERFACE_PORT_LIST
spanning-tree mst <0-7> cost { <1-200000000> | auto }		15	INTERFACE_PORT_LIST
no spanning-tree mst <0-7> cost		15	INTERFACE_PORT_LIST
spanning-tree mst <0-7> port-priority <0-240>		15	INTERFACE_PORT_LIST
no spanning-tree mst <0-7> port-priority		15	INTERFACE_PORT_LIST
spanning-tree		15	STP_AGGR
spanning-tree edge		15	STP_AGGR
spanning-tree auto-edge		15	STP_AGGR
spanning-tree link-type { point-to-point | shared | auto }		15	STP_AGGR
no spanning-tree link-type		15	STP_AGGR
spanning-tree restricted-role		15	STP_AGGR
spanning-tree restricted-tcn		15	STP_AGGR
spanning-tree bpdu-guard		15	STP_AGGR
spanning-tree mst <0-7> cost { <1-200000000> | auto }		15	STP_AGGR
no spanning-tree mst <0-7> cost		15	STP_AGGR
spanning-tree mst <0-7> port-priority <0-240>		15	STP_AGGR
no spanning-tree mst <0-7> port-priority		15	STP_AGGR
mvr vlan <vlan_list> type { source | receiver }		15	INTERFACE_PORT_LIST
mvr name <word16> type { source | receiver }		15	INTERFACE_PORT_LIST
no mvr vlan <vlan_list> type		15	INTERFACE_PORT_LIST
no mvr name <word16> type		15	INTERFACE_PORT_LIST
mvr immediate-leave		15	INTERFACE_PORT_LIST
clear mvr [vlan <vlan_list> | name <word16>] statistics		15	EXEC
show mvr [vlan <vlan_list> | name <word16>] [group-database [interface <port_type_list>] [sfm-information]] [detail]		0	EXEC
mvr		15	GLOBAL_CONFIG
mvr vlan <vlan_list> [name <word16>]		15	GLOBAL_CONFIG
no mvr vlan <vlan_list>		15	GLOBAL_CONFIG
mvr vlan <vlan_list> mode { dynamic | compatible }		15	GLOBAL_CONFIG
mvr name <word16> mode { dynamic | compatible }		15	GLOBAL_CONFIG
no mvr vlan <vlan_list> mode		15	GLOBAL_CONFIG
no mvr name <word16> mode		15	GLOBAL_CONFIG
mvr vlan <vlan_list> igmp-address <ipv4_ucast>		15	GLOBAL_CONFIG
mvr name <word16> igmp-address <ipv4_ucast>		15	GLOBAL_CONFIG
no mvr vlan <vlan_list> igmp-address		15	GLOBAL_CONFIG
no mvr name <word16> igmp-address		15	GLOBAL_CONFIG
mvr vlan <vlan_list> frame priority <0-7>		15	GLOBAL_CONFIG
mvr vlan <vlan_list> frame tagged		15	GLOBAL_CONFIG
mvr name <word16> frame priority <0-7>		15	GLOBAL_CONFIG
mvr name <word16> frame tagged		15	GLOBAL_CONFIG
no mvr vlan <vlan_list> frame priority		15	GLOBAL_CONFIG
no mvr name <word16> frame priority		15	GLOBAL_CONFIG
mvr vlan <vlan_list> last-member-query-interval <0-31744>		15	GLOBAL_CONFIG
mvr name <word16> last-member-query-interval <0-31744>		15	GLOBAL_CONFIG
no mvr vlan <vlan_list> last-member-query-interval		15	GLOBAL_CONFIG

no mvr name <word16> last-member-query-interval		15	GLOBAL_CONFIG
mvr vlan <vlan_list> channel <word16>		15	GLOBAL_CONFIG
no mvr vlan <vlan_list> channel		15	GLOBAL_CONFIG
no mvr name <word16> channel		15	GLOBAL_CONFIG
show dot1x statistics { eapol | radius | all} [interface <port_type_list>]	Shows statistics for either eapol or radius.	0	EXEC
show dot1x status [interface <port_type_list>] [brief]	Shows dot1x status, such as admin state, port state and last source.	0	EXEC
clear dot1x statistics [interface <port_type_list>]	Clears the statistics counters	15	EXEC
dot1x re-authentication	Set Re-authentication state	15	GLOBAL_CONFIG
dot1x authentication timer re-authenticate <1-3600>	The period between re-authentication attempts in seconds	15	GLOBAL_CONFIG
no dot1x authentication timer re-authenticate		15	GLOBAL_CONFIG
dot1x timeout tx-period <1-65535>	the time between EAPOL retransmissions.	15	GLOBAL_CONFIG
no dot1x timeout tx-period		15	GLOBAL_CONFIG
dot1x authentication timer inactivity <10-1000000>	Time in seconds between check for activity on successfully authenticated MAC addresses.	15	GLOBAL_CONFIG
no dot1x authentication timer inactivity		15	GLOBAL_CONFIG
dot1x timeout quiet-period <10-1000000>	Time in seconds before a MAC-address that failed authentication gets a new authentication chance.	15	GLOBAL_CONFIG
no dot1x timeout quiet-period		15	GLOBAL_CONFIG
dot1x re-authenticate	Refresh (restart) 802.1X authentication process.	15	INTERFACE_PORT_LIST
dot1x initialize [interface <port_type_list>]	Force re-authentication immediately	15	EXEC
dot1x system-auth-control	Set the global NAS state	15	GLOBAL_CONFIG
dot1x port-control { force-authorized | force-unauthorized | auto | single | multi | mac-based }	Sets the port security state.	15	INTERFACE_PORT_LIST
no dot1x port-control	Sets the port security state.	15	INTERFACE_PORT_LIST
dot1x guest-vlan	Enables/disables guest VLAN	15	INTERFACE_PORT_LIST
dot1x max-reauth-req <1-255>	The number of times a Request Identity EAPOL frame is sent without response before considering entering the Guest VLAN	15	GLOBAL_CONFIG
no dot1x max-reauth-req	The number of times a Request Identity EAPOL frame is sent without response before considering entering the Guest VLAN	15	GLOBAL_CONFIG
dot1x guest-vlan <1-4095>	Guest VLAN ID used when entering the Guest VLAN.	15	GLOBAL_CONFIG
no dot1x guest-vlan	Guest VLAN ID used when entering the Guest VLAN.	15	GLOBAL_CONFIG
dot1x guest-vlan supplicant	The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port.	15	GLOBAL_CONFIG
dot1x radius-qos	Enables/disables per-port state of RADIUS-assigned QoS.	15	INTERFACE_PORT_LIST
dot1x radius-vlan	Enables/disables per-port state of RADIUS-assigned VLAN.	15	INTERFACE_PORT_LIST
dot1x feature { [guest-vlan] [radius-qos] [radius-vlan] }*1	Globally enables/disables a dot1x feature functionality	15	GLOBAL_CONFIG
show dot1x statistics { eapol | radius | all} [interface <port_type_list>]	Shows statistics for either eapol or radius.	0	EXEC
ntp	Enable NTP	13	GLOBAL_CONFIG
ntp server <1-5> ip-address {<ipv4_ucast>|<ipv6_ucast>|<hostname>}		13	GLOBAL_CONFIG
ntp server <1-5> ip-address {<ipv4_ucast>|<hostname>}		13	GLOBAL_CONFIG
no_ntp_server_ip_address		13	GLOBAL_CONFIG
show ntp status		13	EXEC
show platform phy [interface <port_type_list>]	Show PHY module's information for all or a given interface	15	EXEC
show platform phy id [interface <port_type_list>]	Platform PHY's IDs	15	EXEC

show platform phy instance		15	EXEC
show platform phy failover		15	EXEC
platform phy instance restart { cool | warm }		15	EXEC
platform phy instance default-activate		15	EXEC
show platform phy status [interface <port_type_list>]		15	EXEC
no platform phy instance		15	GLOBAL_CONFIG
platform phy failover		15	INTERFACE_PORT_LIST
debug phy read [<0~31>] [<0-0xffff>] [addr-sort]		debug	INTERFACE_PORT_LIST
debug phy write [<0~31>] <0-0xffff> [<0-0xffff>]		debug	INTERFACE_PORT_LIST
debug phy do-page-chk [enable|disable]		debug	EXEC
debug phy force-pass-through-speed {1G | 100M | 10M}		debug	INTERFACE_PORT_LIST
debug phy reset		debug	INTERFACE_PORT_LIST
debug phy gpio <0-13> mode {output|input|alternative}		debug	INTERFACE_PORT_LIST
debug phy gpio <0-13> get		debug	INTERFACE_PORT_LIST
show poe [interface <port_type_list>]	Use the show poe to show PoE status.	0	EXEC
poe mode { standard | plus }	Use poe mode to configure of PoE mode.	15	INTERFACE_PORT_LIST
no poe mode	Use poe mode to configure of PoE mode.	15	INTERFACE_PORT_LIST
poe priority { low | high | critical }	Use poe priority to configure PoE priority.	15	INTERFACE_PORT_LIST
no poe priority	Use poe priority to configure PoE priority.	15	INTERFACE_PORT_LIST
poe management mode { class-consumption | class-reserved-power | allocation-consumption | allocation-reserved-power | lldp-consumption | lldp-reserved-power }	Use management mode to configure PoE power management method.	15	GLOBAL_CONFIG
no poe management mode		15	GLOBAL_CONFIG
poe power limit { <fword2.1> }	Use poe power limit to configure the maximum allowed power for the interface when power management is in allocation mode.	15	INTERFACE_PORT_LIST
no poe power limit	Use poe power limit to configure the maximum allowed power for the interface when power management is in allocation mode.	15	INTERFACE_PORT_LIST
poe supply sid <1~16> <1-2000>	Use poe supply to specify the maximum power the power supply can deliver.	15	GLOBAL_CONFIG
no poe supply [sid <1~16>]		15	GLOBAL_CONFIG
poe schedule-mode	Configure PoE Schedule mode.	15	INTERFACE_PORT_LIST
no poe schedule-mode	disable PoE power management method.	15	INTERFACE_PORT_LIST
poe select-all <range_list>	Configure PoE Schedule mode.	15	GLOBAL_CONFIG
no poe schedule-all <range_list>	disable PoE power management method.	15	GLOBAL_CONFIG
poe delay-mode <range_list>	Configure PoE Power Delay mode.	15	GLOBAL_CONFIG
no poe delay-mode <range_list>		15	GLOBAL_CONFIG
poe delay-time <range_list> <0-300>	Configure PoE Power Delay time.	15	GLOBAL_CONFIG
poe hour <0-23>	This command is used to set hour time per week to enable PoE.	15	INTERFACE_PORT_LIST
no poe hour <0-23>	This command is used to set hour time per week to disable PoE.	15	INTERFACE_PORT_LIST
poe Sun	This command is used to set hour time on Sunday to enable PoE.	15	INTERFACE_PORT_LIST
no poe Sun	This command is used to set hour time on Sunday to disble PoE.	15	INTERFACE_PORT_LIST
poe Mon	This command is used to set hour time on Monday to enable PoE.	15	INTERFACE_PORT_LIST
no poe Mon	This command is used to set hour time on Monday to disable PoE.	15	INTERFACE_PORT_LIST
poe Tue	This command is used to set hour time on Tuesday to enable PoE.	15	INTERFACE_PORT_LIST
no poe Tue	This command is used to set hour time on Tuesday to disable PoE.	15	INTERFACE_PORT_LIST
poe Wed	This command is used to set hour time on Wednesday to enable PoE.	15	INTERFACE_PORT_LIST
no poe Wed	This command is used to set hour time on Wednesday to disable PoE.	15	INTERFACE_PORT_LIST
poe Thr	This command is used to set hour time on Thursday to enable PoE.	15	INTERFACE_PORT_LIST
no poe Thr	This command is used to set hour time on Thursday to enable PoE.	15	INTERFACE_PORT_LIST
poe Fri	This command is used to set hour time on Friday to enable PoE.	15	INTERFACE_PORT_LIST

no poe Fri	This command is used to set hour time on Friday to disable PoE.	15	INTERFACE_PORT_LIST
poe Sat	This command is used to set hour time on Saturday to enable PoE.	15	INTERFACE_PORT_LIST
no poe Sat	This command is used to set hour time on Saturday to disable PoE.	15	INTERFACE_PORT_LIST
show interface <port_type_list> statistics [{ packets | bytes | errors | discards | filtered | { priority [<0~7>] } }] [{ up | down }]	Shows the statistics for the interface.	0	EXEC
show interface <port_type_list> veriphy	Run and display cable diagnostics.	0	EXEC
clear statistics [interface] <port_type_list>	Clears the statistics for the interface.	0	EXEC
show interface <port_type_list> capabilities		0	EXEC
show interface <port_type_list> status	Display status for the interface.	0	EXEC
mtu <'VTSS_MAX_FRAME_LENGTH_STANDARD'-'VTSS_MAX_FRAME_LENGTH_MAX'>	Use mtu to specify maximum frame size (1518-9600 bytes).	15	INTERFACE_PORT_LIST
no mtu	Use no mtu to set maximum frame size to default.	15	INTERFACE_PORT_LIST
shutdown	Use shutdown to shutdown the interface.	15	INTERFACE_PORT_LIST
speed {2500 | 1000 | 100 | 10 | auto {[10] [100] [1000]} }	Configures interface speed. If you use 10, 100, or 1000 keywords with the auto keyword the port will only advertise the specified speeds.	15	INTERFACE_PORT_LIST
no speed	Use "no speed" to configure interface to default speed.	15	INTERFACE_PORT_LIST
duplex { half | full | auto [half | full] }	Use duplex to configure interface duplex mode.	15	INTERFACE_PORT_LIST
no duplex	Use "no duplex" to set duplex to default.	15	INTERFACE_PORT_LIST
media-type { rj45 | sfp | dual }	Use media-type to configure the interface media type.	15	INTERFACE_PORT_LIST
no media-type	Use to configure the interface media-type type to default.	15	INTERFACE_PORT_LIST
flowcontrol { on | off }	Use flowcontrol to configure flow control for the interface.	15	INTERFACE_PORT_LIST
no flowcontrol	Use no flowcontrol to set flow control to default.	15	INTERFACE_PORT_LIST
excessive-restart	Use excessive-restart to configure backoff algorithm in half duplex mode.	15	INTERFACE_PORT_LIST
show web privilege group [<cword>] level		0	EXEC
web privilege group <cword> level { [cro <0-15>] [crw <0-15>] [sro <0-15>] [srw <0-15>] }*1		15	GLOBAL_CONFIG
no web privilege group [<cword>] level		15	GLOBAL_CONFIG
show port-security port [interface <port_type_list>]	Show MAC Addresses learned by Port Security	0	EXEC
show port-security switch [interface <port_type_list>]	Show Port Security status.	0	EXEC
no port-security shutdown [interface <port_type_list>]	Reopen one or more ports whose limit is exceeded and shut down.	15	EXEC
port-security	Enable/disable port security globally.	15	GLOBAL_CONFIG
port-security aging	Enable/disable port security aging.	15	GLOBAL_CONFIG
port-security aging time <10-10000000>	Time in seconds between check for activity on learned MAC addresses.	15	GLOBAL_CONFIG
no port-security aging time		15	GLOBAL_CONFIG
port-security	Enable/disable port security per interface.	15	INTERFACE_PORT_LIST
port-security maximum [<1-1024>]	Maximum number of MAC addresses that can be learned on this set of interfaces.	15	INTERFACE_PORT_LIST
no port-security maximum		15	INTERFACE_PORT_LIST
port-security violation { protect | trap | trap-shutdown | shutdown }	The action involved with exceeding the limit.	15	INTERFACE_PORT_LIST
no port-security violation	The action involved with exceeding the limit.	15	INTERFACE_PORT_LIST
pvlan <range_list>	Use the pvlan add or remove command to add or remove a port from a PVLAN.	13	INTERFACE_PORT_LIST
pvlan isolation	Use the pvlan isolation command to add the port into an isolation group.	13	INTERFACE_PORT_LIST
show pvlan [<range_list>]	Use the show pvlan command to view the PVLAN configuration.	13	EXEC
show pvlan isolation [interface <port_type_list>]	Use the show pvlan isolation command to view the PVLAN isolation configuration.	13	EXEC
show qos [{ interface [<port_type_list>] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<1-256>] }]		15	EXEC

qos map dscp-cos { <0~63> | <dscp> } cos <0-7> dpl <dpl>		15	GLOBAL_CONFIG
no qos map dscp-cos { <0~63> | <dscp> }		15	GLOBAL_CONFIG
qos map dscp-ingress-translation { <0~63> | <dscp> } to { <0-63> | <dscp> }		15	GLOBAL_CONFIG
no qos map dscp-ingress-translation { <0~63> | <dscp> }		15	GLOBAL_CONFIG
qos map dscp-classify { <0~63> | <dscp> }		15	GLOBAL_CONFIG
qos map cos-dscp <0~7> dpl <0~1> dscp { <0-63> | <dscp> }		15	GLOBAL_CONFIG
no qos map cos-dscp <0~7> dpl <0~1>		15	GLOBAL_CONFIG
qos map dscp-egress-translation { <0~63> | <dscp> } <0~1> to { <0-63> | <dscp> }		15	GLOBAL_CONFIG
no qos map dscp-egress-translation { <0~63> | <dscp> } <0~1>		15	GLOBAL_CONFIG
qos wred queue <0~5> min-th <0-100> mdp-1 <0-100> mdp-2 <0-100> mdp-3 <0-100>		15	GLOBAL_CONFIG
qos wred queue <0~5> min-fl <0-100> max <1-100> [fill-level]		15	GLOBAL_CONFIG
no qos wred queue <0~5>		15	GLOBAL_CONFIG
qos storm { unicast | multicast | broadcast } { { <1,2,4,8,16,32,64,128,256,512> [kfps] } | { 1024 kfps } }		15	GLOBAL_CONFIG
no qos storm { unicast | multicast | broadcast }		15	GLOBAL_CONFIG
qos qce { [update] } <uint> [{ next <uint> } | last] [interface <port_type_list>] [smac { <mac_addr> | <oui> | any }] [dmac { <mac_addr> | unicast | multicast | broadcast | any }] [tag { [type { untagged | tagged | c-tagged | s-tagged | any }] [vid { <vcap_vr> | any }] [pcp { <pcp> | any }] [dei { <0-1> | any }] }*1] [inner-tag { [type { untagged | tagged | c-tagged | s-tagged | any }] [vid { <vcap_vr> | any }] [pcp { <pcp> | any }] [dei { <0-1> | any }] }*1] [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 }] } | { ipv4 [proto { <0-255> | tcp | udp | any }] [sip { <ipv4_subnet> | any }] [dip { <ipv4_subnet> | any }] [dscp { <vcap_vr> | <dscp> | any }] [fragment { yes | no | any }] [sport { <vcap_vr> | any }] [dport { <vcap_vr> | any }] } | { ipv6 [proto { <0-255> | tcp | udp | any }] [sip { <ipv4_subnet> | any }] [dip { <ipv4_subnet> | any }] [dscp { <vcap_vr> | <dscp> | any }] [sport { <vcap_vr> | any }] [dport { <vcap_vr> | any }] } }] [action { [cos { <0-7> | default }] [dpl { <0-1> | default }] [pcp-dei { <0-7> <0-1> | default }] [dscp { <0-63> | <dscp> | default }] [policy { <uint> | default }] }*1]		15	GLOBAL_CONFIG
no qos qce <'QCE_ID_START'~'QCE_ID_END'>		15	GLOBAL_CONFIG
qos qce refresh		15	GLOBAL_CONFIG
qos cos <0-7>		15	GLOBAL_CONFIG
no qos cos		15	INTERFACE_PORT_LIST
qos dpl <dpl>		15	INTERFACE_PORT_LIST
no qos dpl		15	INTERFACE_PORT_LIST
qos pcp <0-7>		15	INTERFACE_PORT_LIST
no qos pcp		15	INTERFACE_PORT_LIST
qos dei <0-1>		15	INTERFACE_PORT_LIST
no qos dei		15	INTERFACE_PORT_LIST
qos trust tag		15	INTERFACE_PORT_LIST
qos trust dscp		15	INTERFACE_PORT_LIST
qos map tag-cos pcp <0~7> dei <0~1> cos <0-7> dpl <dpl>		15	INTERFACE_PORT_LIST
no qos map tag-cos pcp <0~7> dei <0~1>		15	INTERFACE_PORT_LIST
qos policer <uint> [fps] [flowcontrol]		15	INTERFACE_PORT_LIST
no qos policer		15	INTERFACE_PORT_LIST
qos queue-policer queue <0~7> <uint>		15	INTERFACE_PORT_LIST
qos queue-policer queue <0~7> <uint>		15	INTERFACE_PORT_LIST
no qos queue-policer queue <0~7>		15	INTERFACE_PORT_LIST
qos wrr <1-100> <1-100> <1-100> <1-100> <1-100> <1-100>		15	INTERFACE_PORT_LIST
no qos wrr		15	INTERFACE_PORT_LIST
qos shaper <uint>		15	INTERFACE_PORT_LIST
no qos shaper		15	INTERFACE_PORT_LIST
qos queue-shaper queue <0~7> <uint> [excess]		15	INTERFACE_PORT_LIST
no qos queue-shaper queue <0~7>		15	INTERFACE_PORT_LIST

qos tag-remark { pcp <0-7> dei <0-1> | mapped }		15	INTERFACE_PORT_LIST
no qos tag-remark		15	INTERFACE_PORT_LIST
qos map cos-tag cos <0~7> dpl <0~1> pcp <0-7> dei <0-1>		15	INTERFACE_PORT_LIST
no qos map cos-tag cos <0~7> dpl <0~1>		15	INTERFACE_PORT_LIST
qos dscp-translate		15	INTERFACE_PORT_LIST
qos dscp-classify { zero | selected | any }		15	INTERFACE_PORT_LIST
no qos dscp-classify		15	INTERFACE_PORT_LIST
qos dscp-remark { rewrite | remap | remap-dp }		15	INTERFACE_PORT_LIST
no qos dscp-remark		15	INTERFACE_PORT_LIST
qos storm { unicast | broadcast | unknown } <100-13200000> [fps]		15	INTERFACE_PORT_LIST
no qos storm { unicast | broadcast | unknown }		15	INTERFACE_PORT_LIST
qos qce { [addr { source | destination }] [key { double-tag | normal | ip-addr | mac-ip-addr }] }*1		15	INTERFACE_PORT_LIST
no qos qce { [addr] [key] }*1		15	INTERFACE_PORT_LIST
debug qos shaper cir { <100-3300000> [cbs <4096-258048>] } { [eir <100-3300000> [ebs <4096-258048>]] }		debug	INTERFACE_PORT_LIST
no debug qos shaper		debug	INTERFACE_PORT_LIST
debug qos queue-shaper queue <0~7> { cir <100-3300000> [cbs <4096-258048>] } { [eir <100-3300000> [ebs <4096-258048>]] } [excess]		debug	INTERFACE_PORT_LIST
no debug qos queue-shaper queue <0~7>		debug	INTERFACE_PORT_LIST
debug show qos shapers		debug	EXEC
debug qos cmef [{ enable | disable }]		debug	EXEC
show rmon statistics [<1~65535>]		15	EXEC
show rmon history [<1~65535>]		15	EXEC
show rmon alarm [<1~65535>]		15	EXEC
show rmon event [<1~65535>]		15	EXEC
rmon alarm <1-65535> <word255> <1-2147483647> {absolute | delta} rising-threshold <-2147483648-2147483647> [<0-65535>] falling-threshold <-2147483648-2147483647> [<0-65535>] {[rising | falling | both]}		15	GLOBAL_CONFIG
no rmon alarm <1-65535>		15	GLOBAL_CONFIG
rmon event <1-65535> [log] [trap <word127>] {[description <line127>]}		15	GLOBAL_CONFIG
no rmon event <1-65535>		15	GLOBAL_CONFIG
rmon collection stats <1-65535>		15	INTERFACE_PORT_LIST
no rmon collection stats <1-65535>		15	INTERFACE_PORT_LIST
rmon collection history <1-65535> [buckets <1-65535>] [interval <1-3600>]		15	INTERFACE_PORT_LIST
no rmon collection history <1-65535>		15	INTERFACE_PORT_LIST
show sflow statistics { receiver [<range_list>] | samplers [interface [<range_list>] <port_type_list>]}	Use sflow statistics to show statistics for either receiver or sample interface.	0	EXEC
show sflow	Use show sflow to display the current sFlow configuration.	0	EXEC
clear sflow statistics { receiver [<range_list>] | samplers [interface [<range_list>] <port_type_list>] }	Clearing statistics.	15	EXEC
sflow agent-ip {ipv4 <ipv4_addr> | ipv6 <ipv6_addr>}	The agent IP address used as agent-address in UDP datagrams. Defaults to IPv4 loopback address.	15	GLOBAL_CONFIG
no sflow agent-ip	Sets the agent IP address used as agent-address in UDP datagrams to 127.0.0.1.	15	GLOBAL_CONFIG
sflow timeout [receiver <range_list>] <0-2147483647>	Receiver timeout measured in seconds. The switch decrements the timeout once per second, and as long as it is non-zero, the receiver receives samples. Once the timeout reaches 0, the receiver and all its configuration is reset to defaults.	15	GLOBAL_CONFIG
no sflow timeout [receiver <range_list>]	Receiver timeout measured in seconds. The switch decrements the timeout once per second, and as long as it is non-zero, the receiver receives samples. Once the timeout reaches 0, the receiver and all its configuration is reset to defaults.	15	GLOBAL_CONFIG
sflow collector-address [receiver <range_list>] [<word>]	Collector address	15	GLOBAL_CONFIG
no sflow collector-address [receiver <range_list>]		15	GLOBAL_CONFIG
sflow collector-port [receiver <range_list>] <1-65535>	Collector UDP port. Valid range is 0-65536.	15	GLOBAL_CONFIG

no sflow collector-port [receiver <range_list>]	Collector UDP port. Valid range is 0-65536.	15	GLOBAL_CONFIG
sflow max-datagram-size [receiver <range_list>] <200-1468>	Maximum datagram size.	15	GLOBAL_CONFIG
no sflow max-datagram-size [receiver <range_list>]	Maximum datagram size.	15	GLOBAL_CONFIG
sflow sampling-rate [sampler <range_list>] [<1-4294967295>]	Specifies the statistical sampling rate. The sample rate is specified as N to sample 1/Nth of the packets n the monitored flows. There are no restrictions on the value, but the switch will adjust it to the closest possible sampling rate.	15	INTERFACE_PORT_LIST
sflow max-sampling-size [sampler <range_list>] [<14-200>]	Specifies the maximum number of bytes to transmit per flow sample.	15	INTERFACE_PORT_LIST
no sflow max-sampling-size [sampler <range_list>]	Specifies the maximum number of bytes to transmit per flow sample.	15	INTERFACE_PORT_LIST
sflow counter-poll-interval [sampler <range_list>] [<1-3600>]	The interval - in seconds - between counter poller samples.	15	INTERFACE_PORT_LIST
no sflow counter-poll-interval [<range_list>]	The interval - in seconds - between counter poller samples.	15	INTERFACE_PORT_LIST
sflow [<range_list>]	Enables/disables flow sampling on this port.	15	INTERFACE_PORT_LIST
show smtp	Email information	0	EXEC
smtp delete { server | username | sender | returnpath | mailaddress <1-6> }	Delete email server	15	GLOBAL_CONFIG
smtp mailaddress <1-6> <word47>	Set email server	15	GLOBAL_CONFIG
smtp returnpath <word47>		15	GLOBAL_CONFIG
smtp returnpath <word47>		15	GLOBAL_CONFIG
smtp sender <word47>		15	GLOBAL_CONFIG
smtp username <word31> <word31>		15	GLOBAL_CONFIG
smtp server <word47>		15	GLOBAL_CONFIG
smtp level <0-7>		15	GLOBAL_CONFIG
show snmp		15	EXEC
show snmp community v3 [<word127>]		15	EXEC
show snmp user [<word32> <word10-32>]			
show snmp security-to-group [{ v1 | v2c | v3 } <word32>]			
show snmp access [<word32> { v1 | v2c | v3 | any } { auth | noauth | priv }]			
show snmp view [<word32> <word255>]			
snmp-server	Enable SNMP server.	13	GLOBAL_CONFIG
snmp-server engine-id local <word10-32>	To specify SNMP server's engine ID.	13	GLOBAL_CONFIG
no snmp-server engined-id local	To set SNMP server's engine ID to default value.	15	GLOBAL_CONFIG
snmp-server version { v1 | v2c | v3 }	Set the SNMP server version to SNMPv1, SNMPv2c or SNMPv3.	15	GLOBAL_CONFIG
no snmp-server version	Set SNMP server's version to default setting.	15	GLOBAL_CONFIG
snmp-server community v2c <word127> [ro | rw]		15	GLOBAL_CONFIG
snmp-server community v3 <word127> [<ipv4_addr> <ipv4_netmask>]		15	GLOBAL_CONFIG
no snmp-server community v2c		15	GLOBAL_CONFIG
no snmp-server community v3 <word127>		15	GLOBAL_CONFIG
snmp-server user <word32> engine-id <word10-32> [{md5 <word8-32> | sha <word8-40> } [priv { des | aes } <word8-32>]]		15	GLOBAL_CONFIG
no snmp-server user <word32> engine-id <word10-32>		15	GLOBAL_CONFIG
snmp-server security-to-group model { v1 | v2c | v3 } name <word32> group <word32>		15	GLOBAL_CONFIG
no snmp-server security-to-group model { v1 | v2c | v3 } name <word32>		15	GLOBAL_CONFIG
snmp-server access <word32> model { v1 | v2c | v3 | any } level { auth | noauth | priv } [read <word255>] [write <word255>]		15	GLOBAL_CONFIG
no snmp-server access <word32> model { v1 | v2c | v3 | any } level { auth | noauth | priv }		15	GLOBAL_CONFIG
snmp-server view <word32> <word255> { include | exclude }		15	GLOBAL_CONFIG
no snmp-server view <word32> <word255>		15	GLOBAL_CONFIG
snmp-server contact <line255>	To specify the system contact string.	15	GLOBAL_CONFIG
no snmp-server contact	To clear the system contact string.	15	GLOBAL_CONFIG
snmp-server location <line255>	To specify the system location string.	15	GLOBAL_CONFIG
no snmp-server location	To specify the system location string.	15	GLOBAL_CONFIG
show snmp mib context	Use the show snmp mib context user EXEC command to display \ the supported MIBs	15	EXEC

	in the switch.		
show snmp mib ifmib ifIndex	Use the show snmp mib ifmib ifIndex user EXEC command to \ display the SNMP ifIndex(defined in IF-MIB) mapping \ information in the switch.	15	EXEC
show snmp mib redefine	Use the show snmp mib redefine user EXEC command to display \ the redefined MIBs in the switch, that are different \ definitions from the standard MIBs.	15	EXEC
snmp-server trap		15	GLOBAL_CONFIG
no snmp-server host <word32>		15	GLOBAL_CONFIG
shutdown		15	SNMPS_HOST
host { <ipv4_ucast> | <hostname> } [<1-65535>] [traps | informs]		15	SNMPS_HOST
host <ipv6_ucast> [<1-65535>] [traps | informs]		15	SNMPS_HOST
no host		15	SNMPS_HOST
version { v1 [<word127>] | v2 [<word127>] | v3 [probe | engineID <word10-32>] [<word32>] }		15	SNMPS_HOST
no version		15	SNMPS_HOST
informs retries <0-255> timeout <0-2147>		15	SNMPS_HOST
no informs		15	SNMPS_HOST
traps [aaa authentication] [system [coldstart] [warmstart]] [switch [stp] [rmon]]		15	SNMPS_HOST
no traps		15	SNMPS_HOST
snmp-server host <word32> traps [linkup] [linkdown] [lldp]		15	INTERFACE_PORT_LIST
no snmp-server host <word32> traps		15	INTERFACE_PORT_LIST
show snmp host [<word32>] [system] [switch] [interface] [aaa]		15	EXEC
switch stack re-elect	Config commands for the switches in the stack	13	EXEC
switch stack priority {local | <1-16>} <1-4>	Configure master election priority	13	GLOBAL_CONFIG
switch stack swap <1-16> <1-16>	Swap switch ID	13	GLOBAL_CONFIG
no switch stack <1-16>		13	GLOBAL_CONFIG
switch stack <1-16> mac <mac_ucast>	MAC address of the switch	13	GLOBAL_CONFIG
switch stack { enable | disable }	Enable/disable stacking	13	GLOBAL_CONFIG
switch stack interface <port_type_list>	Configure stacking interface	13	GLOBAL_CONFIG
show switch stack [details]	Show switch Detail information	0	EXEC
show switch stack debug	Show switch Debug information	debug	EXEC
show ip ssh	Use the show ip ssh privileged EXEC \ command to display the SSH status.	15	EXEC
ip ssh	Use the ip ssh global configuration command to \ enable the SSH. Use the no form of this \ command to disable the SSH.	15	GLOBAL_CONFIG
show network-clock	Show selector state.	0	EXEC
clear network-clock clk-source <range_list>	Clear active WTR timer.	15	EXEC
network-clock clk-source <range_list> nominate { clk-in | {interface <port_type_id>} }	Nominate a clk input to become a selectable clock source.	15	GLOBAL_CONFIG
no network-clock clk-source <range_list> nominate		15	GLOBAL_CONFIG
network-clock input-source { 1544khz | 2048khz | 10mhz }	Sets the station clock input frequency	15	GLOBAL_CONFIG
no network-clock input-source		15	GLOBAL_CONFIG
network-clock output-source { 1544khz | 2048khz | 10mhz }	Sets the station clock output frequency	15	GLOBAL_CONFIG
no network-clock output-source		15	GLOBAL_CONFIG
network-clock clk-source <range_list> aneg-mode { master | slave | forced}	Sets the preferred negotiation.	15	GLOBAL_CONFIG
no network-clock clk-source <range_list> aneg-mode		15	GLOBAL_CONFIG
network-clock clk-source <range_list> hold-timeout <3-18>	The hold off timer value in 100 ms.Valid values are range 3-18.	15	GLOBAL_CONFIG
no network-clock clk-source <range_list> hold-timeout		15	GLOBAL_CONFIG
network-clock selector { { manual clk-source <uint> } | selected | nonrevertive | revertive | holdover | freerun }	Selection mode of nominated clock sources	15	GLOBAL_CONFIG
no network-clock selector		15	GLOBAL_CONFIG
network-clock clk-source <range_list> priority <0-1>	Priority of nominated clock sources.	15	GLOBAL_CONFIG

no network-clock clk-source <range_list> priority		15	GLOBAL_CONFIG
network-clock wait-to-restore <0-12>	WTR time (0-12 min) '0' is disable	15	GLOBAL_CONFIG
no network-clock wait-to-restore		15	GLOBAL_CONFIG
network-clock ssm-holdover { prc | ssua | ssub | eec2 | eec1 | dnu | inv }	Hold Over SSM overwrite	15	GLOBAL_CONFIG
no network-clock ssm-holdover		15	GLOBAL_CONFIG
network-clock ssm-freerun { prc | ssua | ssub | eec2 | eec1 | dnu | inv }	Free Running SSM overwrite	15	GLOBAL_CONFIG
no network-clock ssm-freerun		15	GLOBAL_CONFIG
network-clock clk-source <range_list> ssm-overwrite { prc | ssua | ssub | eec2 | eec1 | dnu }	Clock source SSM overwrite	15	GLOBAL_CONFIG
no network-clock clk-source <range_list> ssm-overwrite		15	GLOBAL_CONFIG
network-clock option { eec1 | eec2 }	EEC options	15	GLOBAL_CONFIG
no network-clock option		15	GLOBAL_CONFIG
network-clock synchronization ssm	SSM enable/disable.	15	INTERFACE_PORT_LIST
show logging [info] [warning] [error] [switch <switch_list>]	Use the show logging privileged EXEC command without keywords to display the logging configuration, or particularly the logging message summary for the logging level.	15	EXEC
show logging <1-4294967295> [switch <switch_list>]	Use the show logging privileged EXEC command with logging ID to display the detail logging message. OC_CMD_DEFAULT =	15	EXEC
clear logging [info] [warning] [error] [switch <switch_list>]	Use the clear logging privileged EXEC command to clear the logging message.	15	EXEC
logging on	Use the logging on global configuration command to enable the logging server. Use the no form of this command to disable the logging server.	15	GLOBAL_CONFIG
logging host { <ipv4_ucast> | <hostname> }	Use the logging host global configuration command to configure the host address of logging server.	15	GLOBAL_CONFIG
no logging host	Use the no logging host global configuration command to clear the host address of logging server.	15	GLOBAL_CONFIG
logging level { info | warning | error }	Use the logging level global configuration command to configure what level of message will send to logging server.	15	GLOBAL_CONFIG
show clock	Show running system information	0	EXEC
show version	System hardware and software status	0	EXEC
password unencrypted <line31>	Use the password encrypted <password> global configuration command to configure administrator password with unencrypted password for the local switch access.	15	GLOBAL_CONFIG
password encrypted <word4-44>	Use the password encrypted <password> global configuration command to configure administrator password with encrypted password for the local switch access.	15	GLOBAL_CONFIG
password none	Use the password none global configuration command to remove the administrator password.	15	GLOBAL_CONFIG
show system	Show system information	0	EXEC
system contact <line255>	To specify the system contact string.	15	GLOBAL_CONFIG
no system contact	To clear the system contact string.	15	GLOBAL_CONFIG
system location <line255>	To specify the system location string.	15	GLOBAL_CONFIG
no system location	To specify the system location string.	15	GLOBAL_CONFIG
system name <line255>	To specify the system mode name string.	15	GLOBAL_CONFIG
no system name	To specify the system model name string.	15	GLOBAL_CONFIG
show thermal-protect [interface <port_type_list>]	Shows thermal protection status (chip temperature and port status).	15	EXEC
thermal-protect prio <0~3> temperature <0-255>	Thermal protection configuirations.	15	GLOBAL_CONFIG
no thermal-protect prio <0~3>	Sets temperature at which to turn ports with the corresponding priority off.	15	GLOBAL_CONFIG
thermal-protect port-prio <0-3>	Sets temperature at which to turn ports with the corresponding priority off.	15	INTERFACE_PORT_LIST
no thermal-protect port-prio	Sets temperature at which to turn ports with the corresponding priority off.	15	INTERFACE_PORT_LIST
show upnp		15	EXEC
upnp		15	GLOBAL_CONFIG
upnp ttl <1-255>		15	GLOBAL_CONFIG

no upnp ttl		15	GLOBAL_CONFIG
upnp advertising-duration <100-86400>		15	GLOBAL_CONFIG
no upnp advertising-duration		15	GLOBAL_CONFIG
username <word31> privilege <0-15> password unencrypted <line31>	Use the username <username> privilege <level> password encrypted <password> global configuration command to add a user with unencrypted password for the local switch access.	15	GLOBAL_CONFIG
username <word31> privilege <0-15> password encrypted <word4-44>	Use the username <username> privilege <level> password encrypted <password> global configuration command to add a user with encrypted password for the local switch access.	15	GLOBAL_CONFIG
username <word31> privilege <0-15> password none	Use the username <username> privilege <level> password none global configuration command to remove the password for specific username.	15	GLOBAL_CONFIG
no username <word31>	Use the no username <username> global configuration command to delete a local user.	15	GLOBAL_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>		13	GLOBAL_CONFIG
switchport vlan mac <mac_ucast> vlan <vlan_id>	Use the switchport vlan mac command to associate a MAC address to VLAN ID.	13	INTERFACE_PORT_LIST
switchport vlan protocol group <word16> vlan <vlan_id>	Use the no form of this command to remove the group to vlan mapping.	13	INTERFACE_PORT_LIST
show vlan protocol [eth2 {<0x600-0xffff>|arp|ip|ipx|at}] [snap {<0x0-0xffffff>|rfc-1042|snap-8021h} <0x0-0xffff>] [llc <0x0-0xff> <0x0-0xff>]	Use the switchport vlan protocol group command to add group to vlan mapping.	13	EXEC
show vlan mac [address <mac_ucast>]		13	EXEC
show vlan ip-subnet [id <1-128>]		13	EXEC
switchport vlan ip-subnet id <1-128> <ipv4_subnet> vlan <vlan_id>		13	INTERFACE_PORT_LIST
no switchport vlan ip-subnet id <1~128>		13	INTERFACE_PORT_LIST
debug vcl policy <uint>		debug	INTERFACE_PORT_LIST
no debug vcl policy		debug	GLOBAL_CONFIG
debug show vcl policy		debug	EXEC
switchport mode {access | trunk | hybrid}	Use the switchport mode command to define the type of the port.	13	INTERFACE_PORT_LIST
no switchport mode		13	INTERFACE_PORT_LIST
switchport access vlan <vlan_id>	Use the switchport access vlan command to configure a port to a VLAN. Valid VLAN IDs are 1 to 4095.	13	INTERFACE_PORT_LIST
no switchport access vlan		13	INTERFACE_PORT_LIST
switchport trunk native vlan <vlan_id>	Use the switchport native vlan command to configure a port VLAN ID for a trunk port.	13	INTERFACE_PORT_LIST
no switchport trunk native vlan	Set trunk mode characteristics of the interface	13	INTERFACE_PORT_LIST
switchport hybrid native vlan <vlan_id>	Use the switchport native vlan command to configure a port VLAN ID for a hybrid port.	13	INTERFACE_PORT_LIST
no switchport hybrid native vlan	Set hybrid mode characteristics of the interface	13	INTERFACE_PORT_LIST
switchport hybrid port-type { unaware | c-port | s-port | s-custom-port }	Set hybrid characteristics of the interface	13	INTERFACE_PORT_LIST
no switchport hybrid port-type	Set hybrid characteristics of the interface	13	INTERFACE_PORT_LIST
switchport hybrid ingress-filtering	Set hybrid characteristics of the interface	13	INTERFACE_PORT_LIST
switchport hybrid acceptable-frame-type { all | tagged | untagged }	Set hybrid characteristics of the interface	13	INTERFACE_PORT_LIST
no switchport hybrid acceptable-frame-type	Set hybrid characteristics of the interface	13	INTERFACE_PORT_LIST
switchport hybrid egress-tag {none | all [except-native]}	Set hybrid characteristics of the interface	13	INTERFACE_PORT_LIST
no switchport hybrid egress-tag	Set hybrid characteristics of the interface	13	INTERFACE_PORT_LIST
switchport trunk vlan tag native	Set trunk characteristics of the interface	13	INTERFACE_PORT_LIST
switchport trunk allowed vlan {all | none | [add | remove | except] <vlan_list>}	Set trunk mode characteristics of the interface	13	INTERFACE_PORT_LIST
no switchport trunk allowed vlan	Set trunk characteristics of the interface,	13	INTERFACE_PORT_LIST

switchport hybrid allowed vlan {all | none | [add | remove | except] <vlan_list>}	Set hybrid characteristics of the interface	13	INTERFACE_PORT_LIST
no switchport hybrid allowed vlan	Set hybrid characteristics of the interface	13	INTERFACE_PORT_LIST
vlan ethertype s-custom-port <0x0600-0xffff>		13	GLOBAL_CONFIG
no vlan {{ethertype s-custom-port} | <vlan_list>}		15	GLOBAL_CONFIG
show interface <port_type_list> switchport [access | trunk | hybrid]	Use the how interfaces command to display the administrative and operational status of all interfaces or a specified interface.	0	EXEC
show vlan [id <vlan_list> | name <vword32> | brief]	Use the show vlan command to view the VLAN configuration.	13	EXEC
show vlan status [interface <port_type_list>] [combined|admin|nas|mvr|voice-vlan|mstp|erps|vcl|evc|gvrp|all|conflicts]	Use the show VLAN status command to view the VLANs configured for each interface.	13	EXEC
name <vword32>	Use the name <vword32> command to configure VLAN name.	13	CONFIG_VLAN
no name	The no form of this command will restore the VLAN name to its default.	13	CONFIG_VLAN
switchport forbidden vlan {add|remove} <vlan_list>	Adds or removes forbidden VLANs from the current list of forbidden VLANs	15	INTERFACE_PORT_LIST
no switchport forbidden vlan	Allows for adding VLANs to an interface	15	INTERFACE_PORT_LIST
show switchport forbidden [{vlan <vlan_id>} | {name <word>}]	Lookup VLAN Forbidden port entry.	0	EXEC
voice vlan	Use the voice vlan global configuration command to enable voice vlan. Use the no form of this command to globally disable voice vlan.	15	GLOBAL_CONFIG
voice vlan vid <vlan_id>	Use the voice vlan vid global configuration command to configure voice vlan vid.	15	GLOBAL_CONFIG
no voice vlan vid	Use the no voice vlan vid global configuration command to restore the default voice vlan vid.	15	GLOBAL_CONFIG
voice vlan aging-time <10-10000000>	Use the voice vlan aging-time global configuration command to configure default voice vlan aging-time.	15	GLOBAL_CONFIG
no voice vlan aging-time	Use the no voice vlan aging-time global configuration command to restore the default voice vlan aging-time.	15	GLOBAL_CONFIG
voice vlan class { <0-7> | low | normal | medium | high }	Use the voice vlan class global configuration command to configure voice vlan class.	15	GLOBAL_CONFIG
no voice vlan class	Use the no voice vlan class global configuration command to restore the default voice vlan class.	15	GLOBAL_CONFIG
voice vlan oui <oui> [description <line32>]	Use the voice vlan oui global configuration command to set the oui entry for voice vlan.	15	GLOBAL_CONFIG
no voice vlan oui <oui>	Use the no voice vlan oui global configuration command to delete the oui entry.	15	GLOBAL_CONFIG
switchport voice vlan mode { auto | force | disable }	Use the switchport voice vlan mode interface configuration command to configure to switchport voice vlan mode.	15	INTERFACE_PORT_LIST
no switchport voice vlan mode	Use the no switchport voice vlan mode interface configuration command to restore the default switchport voice vlan mode.	15	INTERFACE_PORT_LIST
switchport voice vlan security	Use the switchport voice vlan security interface configuration command to configure switchport voice vlan security mode. Use the no form of this command to globally disable switchport voice vlan security mode.	15	INTERFACE_PORT_LIST
switchport voice vlan discovery-protocol {oui | lldp | both}	Use the switchport voice vlan discovery-protocol interface configuration command to configure to switchport voice vlan discovery-protocol.	15	INTERFACE_PORT_LIST
no switchport voice vlan discovery-protocol	Use the no switchport voice vlan discovery-protocol interface configuration command to restore the default switchport voice vlan discovery-protocol.	15	INTERFACE_PORT_LIST
show voice vlan [oui <oui> | interface <port_type_list>]	Use the show voice vlan privilege EXEC command without keywords to display the voice vlan configuration, or particularly switchport configuration for the interface, or use the oui keyword to	15	EXEC

	display oui table.		
debug gvrp protocol-state interface <port_type_list> vlan <vlan_list>		debug	EXEC
debug gvrp msti		debug	EXEC
debug gvrp statistic		debug	EXEC
gvrp		15	GLOBAL_CONFIG
gvrp time { [join-time <1-20>] [leave-time <60-300>] [leave-all-time <1000-5000>] }*1		15	GLOBAL_CONFIG
gvrp max-vlans <1-4095>		15	GLOBAL_CONFIG
gvrp		15	INTERFACE_PORT_LIST
gvrp join-request vlan <vlan_list>		15	INTERFACE_PORT_LIST
gvrp leave-request vlan <vlan_list>		15	INTERFACE_PORT_LIST