antaira®

making connectivity simple...

Software Manual

Version 1.1
(August 2024)

Firmware 6.2

Table of Contents

** = Feature only supported on PoE Switches

1 Access with Web Browser 1
1.1 Web GUI Login 1
2 Dashboard 2
2.1 System Information 2
2.2 CPU Load 3
2.3 PoE Load** 3
2.4 Startup-Config 4
3 Quick Setup 5
3.1 ERPS - Ethernet Ring Protection Switching 5
4 Configuration 7
4.1 System 7
4.1.1 Information 7
4.1.2 CPU Load 8
4.1.3 IP 8
4.1.4 NTP 13
4.1.5 Time 14
4.1.6 Log 17
4.1.7 Event Warning 18
4.1.7.1 Relay Warning Events Settings 18
4.1.7.2 Email Warning Event Settings 20
4.2 Green Ethernet 21
4.2.1 Port Power Savings 21
4.3 Port 23
4.3.1 Port Configuration 23
4.4 DHCP 26
4.4.1 Server 26
4.4.1.1 Mode - DHCP Server Mode Configuration 26
4.4.1.2 Excluded IP 26
4.4.1.3 Pool 27
4.4.1.4 Port Address 29
4.4.2 Snooping 31
4.4.3 Relay 32
4.5 Security 34
4.5.1 Switch 34
4.5.1.1 Users 34
4.5.1.2 Privilege level 36
4.5.1.3 Auth Method 37
4.5.1.4 SSH 39

4.5.1.5 Telnet....39
4.5.1.6 HTTPS....40
4.5.1.7 Access Management....42
4.5.2 SNMP....43
4.5.2.1 System....43
4.5.2.2 Trap....43
4.5.2.3 Communities....48
4.5.2.4 Users....49
4.5.2.5 Groups....50
4.5.2.6 Views....51
4.5.2.7 Access....52
4.5.3 RMON....53
4.5.3.1 Statistics....53
4.5.3.2 History....53
4.5.3.3 Alarm....54
4.5.3.4 Event....55
4.6 Network....56
4.6.1 Port Security....56
4.6.2 NAS....58
4.6.3 ACL....68
4.6.3.1 Ports....68
4.6.3.2 Rate Limiters....70
4.6.3.3 Access Control List....71
4.6.4 IP Source Guard....75
4.6.4.1 Configuration....75
4.6.4.2 Static Table....76
4.6.5 ARP Inspection....77
4.6.5.1 Port Configuration....77
4.6.5.2 VLAN Mode Configuration....79
4.6.5.3 Static Table....80
4.6.5.4 Dynamic Table....81
4.7 AAA....82
4.7.1 RADIUS....82
4.7.2 TACAS+....84
4.8 Aggregation....85
4.8.1 Common....85
4.8.2 Groups....86
4.8.3 LACP....87
4.9 Loop Protection....88
4.10 Spanning Tree....90
4.10.1 Bridge Settings....90

4.10.2 MSTI Mapping....92
4.10.3 MSTI Priorities....93
4.10.4 CIST Ports....93
4.10.5 MSTI Ports....96
4.11 IPMC Profile....97
4.11.1 Profile Table....97
4.11.2 Address Entry....98
4.12 MVR....99
4.13 IPMC....102
4.13.1 IGMP Snooping....102
4.13.1.1 Basic Configuration....102
4.13.1.2 VLAN Configuration....104
4.13.1.3 Port Filtering Profile....106
4.13.2 MLD Snooping....107
4.13.2.1 Basic Configuration....107
4.13.2.2 VLAN Configuration....109
4.13.2.3 Port Filtering Profile....110
4.14 LLDP....111
4.14.1 LLDP Configuration....111
4.14.2 LLDP-MED....114
4.15 PoE (Supported on PoE Switches only)....121
4.15.1 Power Budget....121
4.15.2 Ping Alive....123
4.15.3 Schedule....124
Add New Schedule....125
4.16 MEP....125
4.17 ERPS....127
4.18 MAC Table....128
4.19 VLANs....130
4.20 Private VLANs....135
4.20.1 Membership....135
4.20.2 Port Isolation....136
4.21 VCL....136
4.21.1 MAC-based VLAN....136
4.21.2 Protocol-based VLAN....137
4.21.2.1 Protocol to Group....137
4.21.2.2 Group to VLAN....138
4.21.3 IP Subnet-based VLAN....139
4.22 Voice VLAN....140
4.22.1 Voice VLAN Configuration....140
4.22.2 Voice VLAN OUI....142

4.23 QoS ... 143
4.23.1 Port Classification ... 143
4.23.2 Port Policing ... 145
4.23.3 Queue Policing ... 146
4.23.4 Port Scheduler ... 147
4.23.5 Port Shaping ... 148
4.23.6 Port Tag Remarking ... 149
4.23.7 Port DSCP ... 150
4.23.8 DSCP-Based QoS ... 151
4.23.9 DSCP Translation ... 153
4.23.10 DSCP Classification ... 154
4.23.11 QoS Control List ... 154
4.23.12 Storm Policing ... 158
4.24 Mirroring ... 159
4.25 MRP ... 160
4.25.1 Ports ... 160
4.25.2 MVRP ... 161
4.26 GVRP ... 162
4.26.1 Global Config ... 162
4.26.2 Port Config ... 163
4.27 sFLOW ... 164
sFLOW Configuration ... 164
4.28 DDMI ... 167
4.29 Modbus TCP ... 167
4.30 NAT ... 169
4.30.1 Global Config ... 169
4.30.2 Rules Config ... 171
4.31 SMTP ... 172
5 Monitor ... 175
5.1 System ... 175
5.1.1 Information ... 175
6 Diagnostics ... 177
6.1 Ping (IPv4) ... 177
6.2 Ping (IPv6) ... 179
6.3 Traceroute (IPv4) ... 181
6.4 Traceroute (IPv6) ... 183
6.5 Server Report ... 185
6.6 Relay ... 186
6.7 LED Blinking ... 186
7 Maintenance ... 187
7.1 USB ... 187

7.2 Reset Button.....188
7.3 Restart Device.....188
7.4 Factory Defaults.....189
7.5 Reboot Schedule.....190
7.6 Software.....191
7.6.1 Upload.....191
7.6.2 Image Select.....192
7.7 Configuration.....193
7.7.1 Save Start-up Config.....193
7.7.2 Download.....194
7.7.3 Upload.....195
7.7.4 Activate.....196
7.7.5 Delete.....197
Appendix A - Routing and VLANs.....198
Static Routing/VLANs.....198
Configuration via CLI.....200
Appendix B - ERPS.....201
Setting up ERPS in Quick Setup.....201
Appendix C - DHCP.....202
DHCP per Port.....202
Appendix - Supported CLI Commands.....207
Command Line Interface.....207
Partial Command.....207
Command History.....207
General Maintenance Commands.....208
Configure terminal.....208
Interface.....208
exit.....208
End.....209
show running-config.....209
show running-config all-default.....209
dir.....210
copy running-config startup-config.....210
copy running-config flash:<file-name>.....210
del flash:<file-name>.....211
reload cold.....211
reload defaults.....211
reload defaults keep-ip.....212
show version.....212
Network.....213
Ethernet ports - configuration commands.....213

shutdown....213
speed....213
duplex....214
Flowcontrol....214
MTU....215
Ethernet ports - view commands....215
show interface status....216
IPv4, IPv6....216
ip name-server - DNS Server....216
ip (ipv6) address - IPv4,IPv6 interface....217
IP Routes (Default gateway)....217
Show interface vlan....218
NTP (Network Time Protocol)....218
ntp server - Configure NTP server....218
show ntp status - view NTP status....219
Time Zone....219
clock timezone - time zone configuration....219
clock summer-time - Daylight Savings Time configuration....219
Time zone - view commands....220
show clock detail....220
SysLog report....221
logging - Enable and configure SysLog....221
show logging....221
MAC Table Learning – configuration commands....222
mac address-table aging-time....222
mac address-table learning....222
mac address-table static....223
show mac address-table....224
Routing....224
show ip route....224
ACCESS CONTROL....226
Local Users - configuration commands....226
username - Add local user or change password....226
Local Users....227
show user-privilege....227
show users....227
Web Server....228
ip http secure-server....228
ip http secure-certificate....228
show ip http....229
Telnet/SSH/Web....229

aaa authentication login....230
aaa accounting....231
show aaa....231
Access Control List....232
access management....232
show access management....232
VLAN....233
VLAN configuration commands and port types....233
vlan - create VLAN....234
vlan ethertype s-custom-port....235
switchport mode....235
switchport trunk native vlan....236
switchport trunk vlan tag native....236
switchport trunk allowed vlan....237
switchport forbidden vlan....237
switchport hybrid native vlan....238
switchport hybrid port-type....238
switchport hybrid ingress-filtering....239
switchport hybrid acceptable-frame-type....239
switchport hybrid egress-tag....240
switchport trunk allowed vlan....240
show vlan....241
show vlan status....241
POE **(Feature Supported on PoE switches only)....242
PoE-BT Power (Only supported on PoE BT switches)....242
poe extended-bt-power-mode....242
poe uninterruptible-power....242
poe power....243
poe mode....243
poe priority....243
poe terminal-description....244
show poe....244
Spanning tree Protocol....245
STP Bridge Configuration commands....245
spanning-tree mode....245
spanning-tree system settings....245
spanning-tree port settings....247
show spanning-tree....248
SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)....248
Enable/Disable SNMP and configure MIB-II system OiDs....249
snmp-server....249

snmp-server contact, System-Name (host) and location 249
snmp-server view 249
snmp-server community 250
snmp-server user 250
snmp-server security-to-group model 251
snmp-server access 252
snmp-server trap 252
snmp-server host 253
show snmp 254
RADIUS TACACS+ 254
RADIUS Server configuration commands 254
Global configuration commands 254
Radius server configuration 255
show radius-server 256
tacacs Global configuration commands 256
TACACS+ Server configuration 257
show tacacs-server 257
AGGREGATION/LACP 258
Aggregation Group Configuration commands 258
aggregation mode 258
aggregation group 258
lacp failover 259
lacp max-bundle 259
show aggregation 259
lacp system-priority 260
lacp port-priority 260
lacp timeout 261
show lacp system-id 261
show lacp internal details 261
show lacp neighbor details 262
show lacp statistics details 262
LLDP (LINK LAYER DISCOVERY PROTOCOL) 262
LLDP Configuration commands 262
LLDP parameters 262
LLDP Interface configuration 263
show lldp neighbors 264
show lldp statistics 264
PRIVATE VLAN / PORT ISOLATION 265
Private VLAN 265
pvlan 265
show pvlan 265

Port Isolation....265
pvlan isolation....265
show pvlan isolation....266
LOOP PROTECTION....266
Loop protection configuration commands....266
loop-protect (general settings)....266
loop-protect (port settings)....267
show loop-protect....268
IGMP (INTERNET GROUP MANAGEMENT PROTOCOL)....268
IGMP Snooping Configuration commands....268
ip igmp (global parameters)....268
ip igmp snooping (port parameters)....269
ip igmp snooping (vlan parameters)....270
show ip igmp snooping group-database....271
show ip igmp snooping mrouter....272
PORT MIRRORING....272
Port mirroring configuration....272
monitor session....272
Port configuration....272
Unit Configuration....273
Software update....273
Upload new version....273
Select active Image....274
DIAGNOSTICS....274
View log file....274
Ping....275
View CPU Load....275

© Copyright 2024 Antaira Technologies, LLC
All Rights Reserved
This document contains information, which is protected by copyright. Reproduction, adaptation or translation without prior permission is prohibited, except as allowed under the copyright laws.

Trademark Information
Antaira is a registered trademark of Antaira Technologies, LLC., Microsoft Windows and the Windows logo are the trademarks of Microsoft Corp. All other brand and product names are trademarks or registered trademarks of their respective owners.

Disclaimer
Antaira Technologies, LLC provides this manual without warranty of any kind, expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Antaira Technologies, LLC may make improvements and/or changes to the product and/or specifications of the product described in this manual, without prior notice. Antaira Technologies, LLC will not be liable for any technical inaccuracies or typographical errors found in this guide. Changes are periodically made to the information contained herein and will be incorporated into later versions of the manual. The information contained is subject to change without prior notice.

Software Manual
Version 1.1 (August 2024)

The manual supports the following models:

- LMP-xxxx
- LMX-xxxx

Please check our website (www.antaira.com) for any updated manual or contact us by e-mail (support@antaira.com).

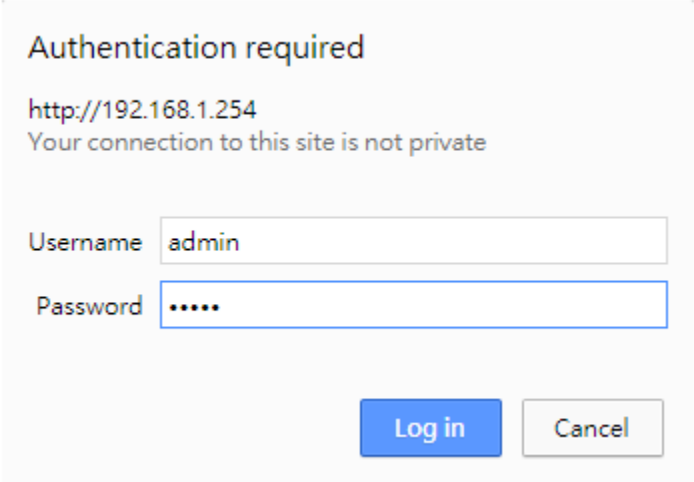
1 Access with Web Browser

1.1 Web GUI Login

All of Antaira's industrial managed devices are embedded with HTML web GUI interfaces. They provide user-friendly management features through its design and allow users to manage the devices from anywhere on the network through a web browser.

Step 1: To access the WEB GUI, open a web browser and type the following IP address: http://192.168.1.254

Step 2: The default WEB GUI login:
Username: admin
Password: admin

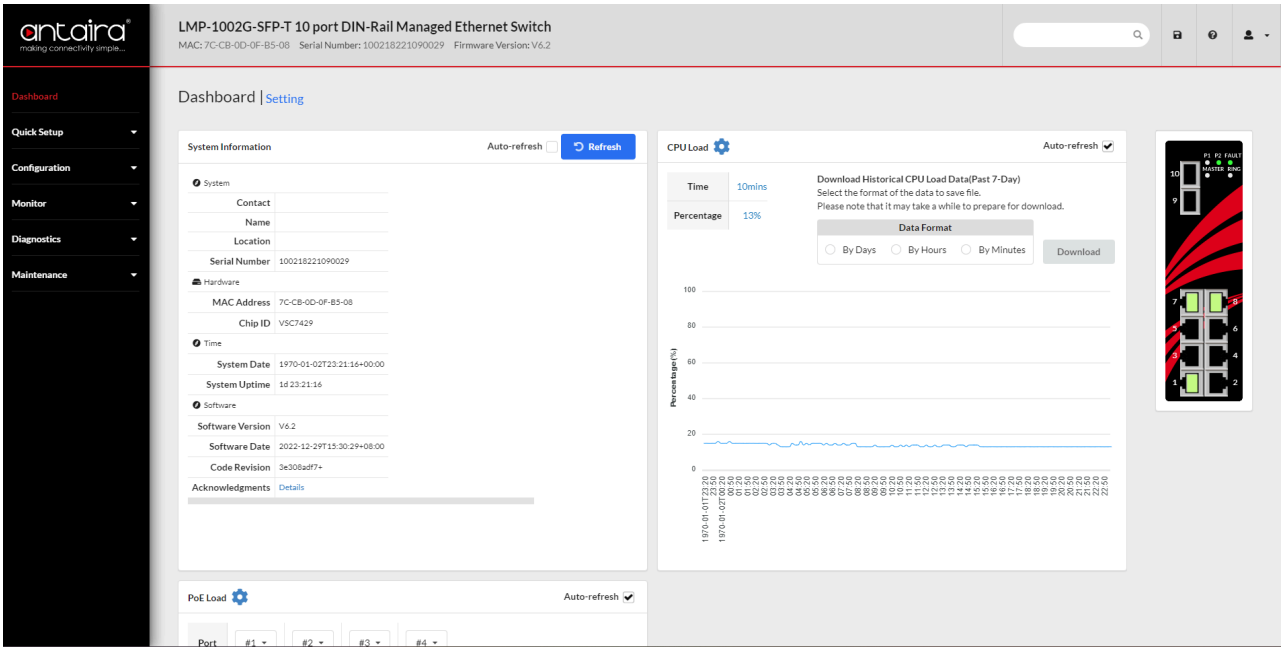


NOTE: Make sure that the PC and Switches are on the same logical subnetwork

2 Dashboard

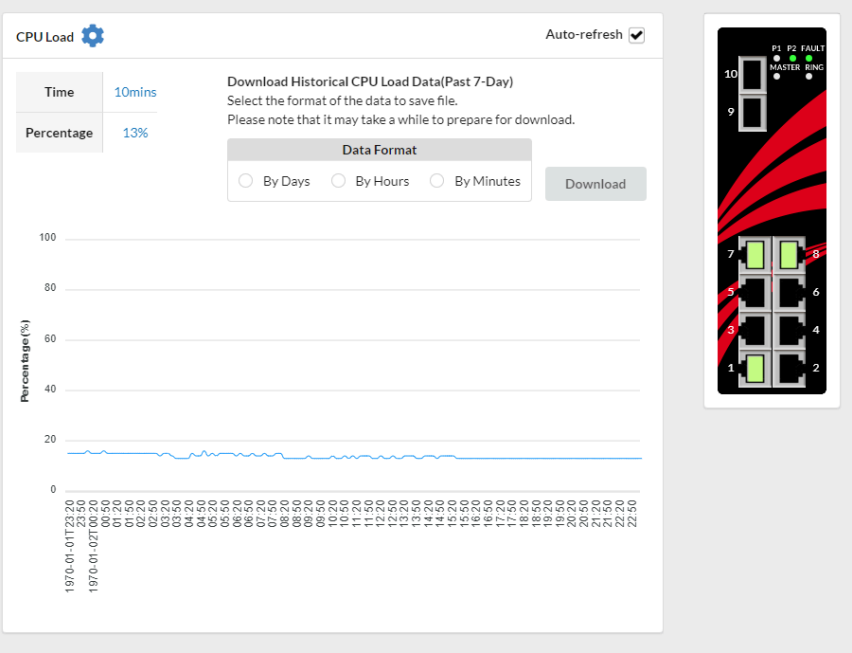
2.1 System Information

Once logging in, the Web GUI Interface's "Dashboard" page shows your switch system's status. Additionally, a visual representation of each port's condition is available, which remains consistent across the Web GUI. The dashboard offers an overview of system-related information, hardware details, current time, and software status. Furthermore, it indicates whether ports are active or inactive.



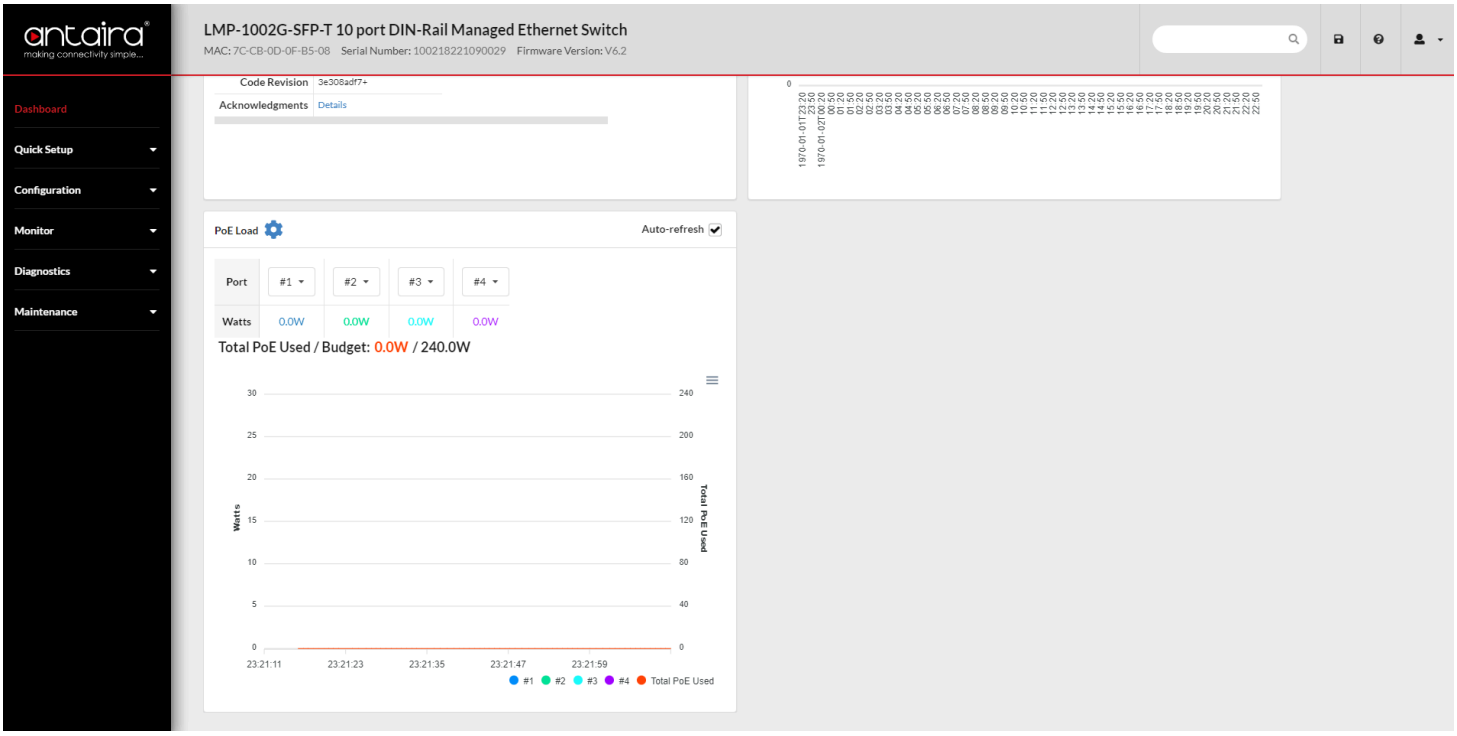
2.2 CPU Load

Simple viewing of CPU load graph, facilitating performance over time. Downloadable CPU data.



2.3 PoE Load**

Feature only supports PoE switches.
Quick overview of PoE load of 4 ports at a time, with a graph of Watts over time.



2.4 Startup-Config

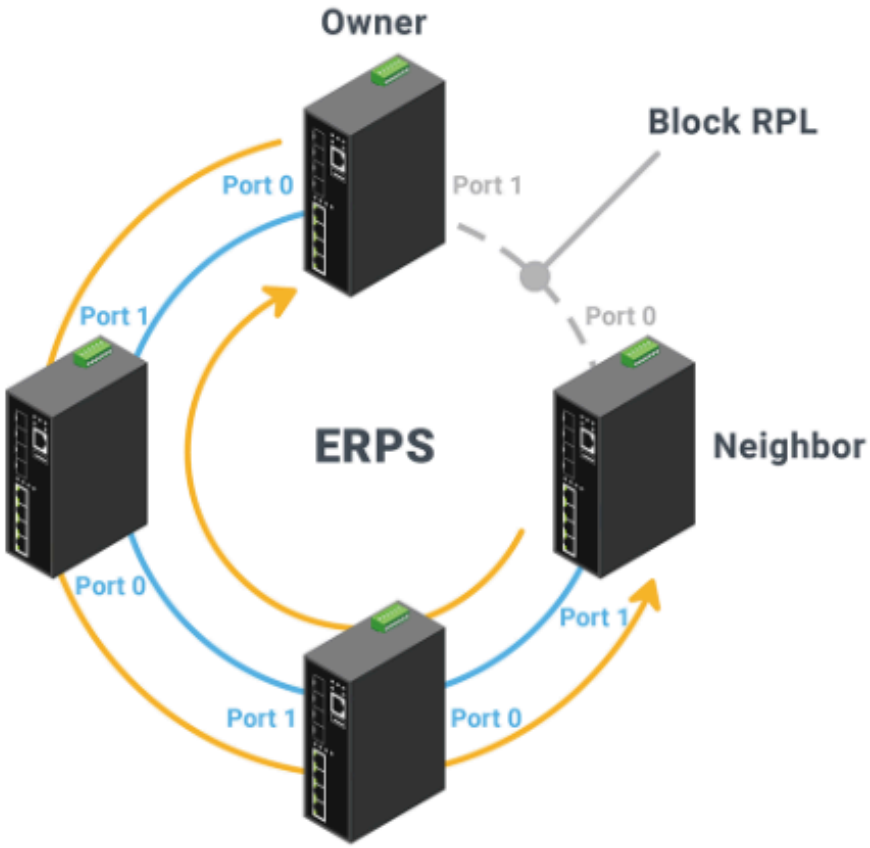
Save disk icon copies running-config to start-config, thereby ensuring that the currently active configuration will be used at the next reboot.
The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch.



3 Quick Setup

3.1 ERPS - Ethernet Ring Protection Switching

This Quick Setup of ERPS is only for **Single Ring Setting**

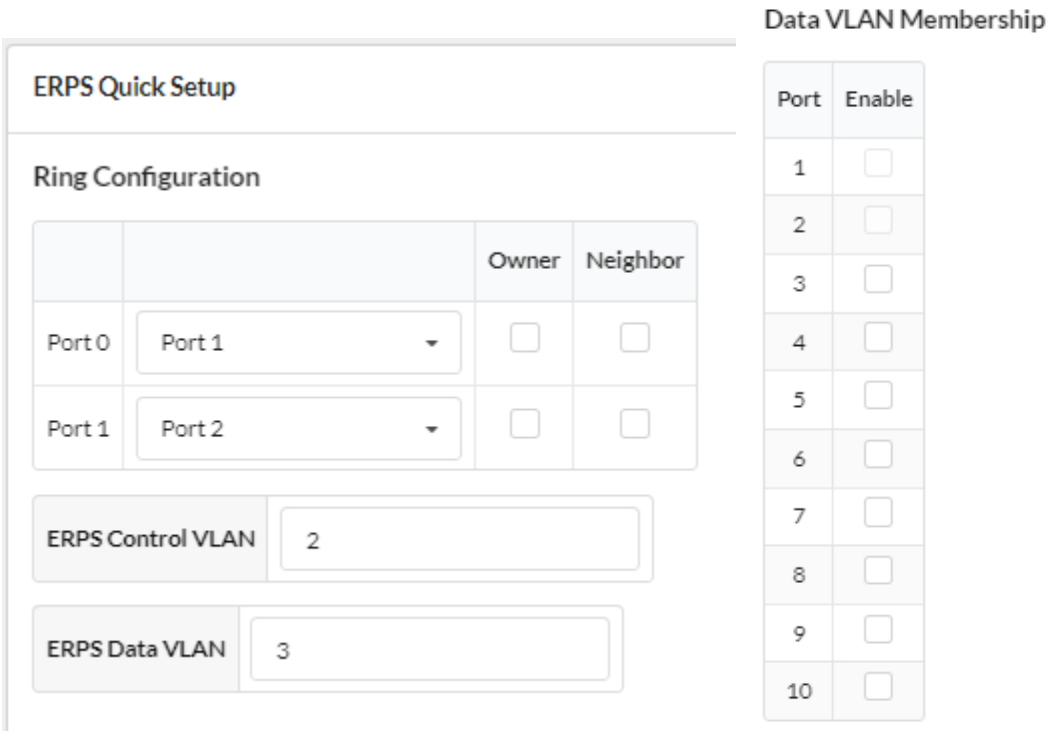


CONTINUE

NOTE: This Quick Setup of ERPS is only for Single Ring Setting

Ring Configuration

Must first create a VLAN with IP address per Switch before setting up ERPS Quick Setup. Control and Data VLAN need ip addresses which will correspond to their VLAN ID.



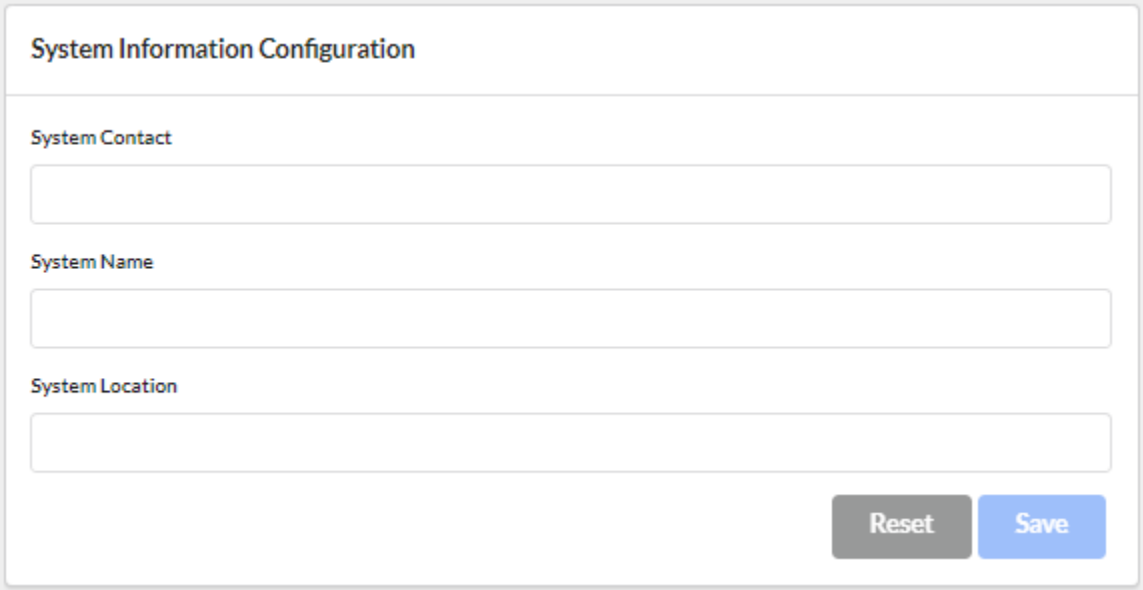
Setting	Description
Port 0	Selecting a switch port to be used for the first ERPS ring member port.
Port 1	Selecting a switch port to be used for the second ERPS ring member port.
ERPS Control VLAN	Setting the VLAN ID for transfer/receive R-APS messages.
ERPS Data VLAN	Setting the Protection VLAN ID.
Data VLAN Membership	Setting which port can access Data VLAN.

4 Configuration

4.1 System

4.1.1 Information

To change the system configuration information.



System Contact

Setting	Description	Factory Default
Max. 255 Characters	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 255, and the allowed content is the ASCII characters from 32 to 126.	None

System Name

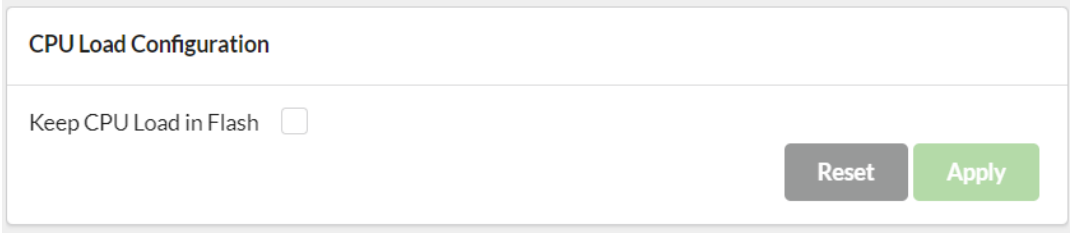
Setting	Description	Factory Default
Max. 255 Characters	An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Z, a-z), digits (0-9), minus sign (-). No space characters are permitted 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 255.	None

System Location

Setting	Description	Factory Default
Max. 255 Characters	The physical location of this node(e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.	None

4.1.2 CPU Load

To enable/disable system log in Flash



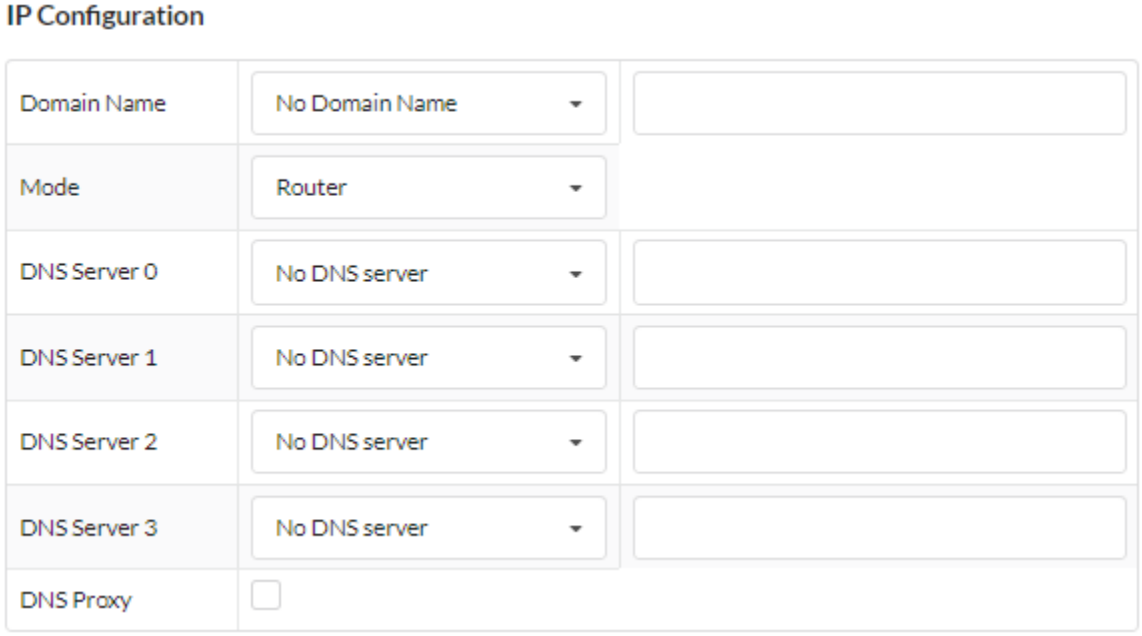
Keep CPU Load in Flash

The CPU Load will be stored in the switch DRAM by default. Check if you want to keep all the CPU Load in the flash memory. You could get all the CPU Load if these logs are stored in the Flash. Otherwise, it will disappear when the switch reboots. The log file will write into the flash memory every 30 mins.

4.1.3 IP

IP Configuration

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 32.



Domain Name

The name string of the local domain where the device belongs.
Most queries for names within this domain can use short names relative to the local domain. The system then appends the domain name as a suffix to unqualified names.
For example, if the domain name is set as 'example.com' and you specify the PING destination by the unqualified name as 'test', then the system will qualify the name to be 'test.example.com'.

Here is the following drop-down list:

Setting	Description	Factory Default
No Domain Name	No domain name will be used.	No Domain Name
Configured Domain Name	Explicitly specify the name of the local domain. Make sure the configured domain name meets your organization's given domain.	
From any DHCPv6 interfaces	The first domain name offered from a DHCPv6 lease to a DHCPv6-enabled interface will be used.	
From this DHCPv6 interface	Specify from which DHCPv6-enabled interface a provided domain name should be preferred.	

Mode

Configure whether the IP stack should act as a Hostor a Router.

Setting	Description	Factory Default
Host	IP traffic between interfaces will not be routed.	Host
Router	IP traffic is routed between all interfaces.	

DNS Server

This setting controls the DNS name resolution done by the switch. There are four servers available for configuration, and the index of the server presents the preference (less index has higher priority) in doing DNS name resolution. The system selects the active DNS server from the configuration. If the preferred server does not respond in five attempts.

Setting	Description	Factory Default
No DNS server	No DNS server will be used.	
From any DHCPv4 interfaces	The first DNS server offered from a DHCPv4 lease to a DHCPv4-enabled interface will be used.	No DNS server

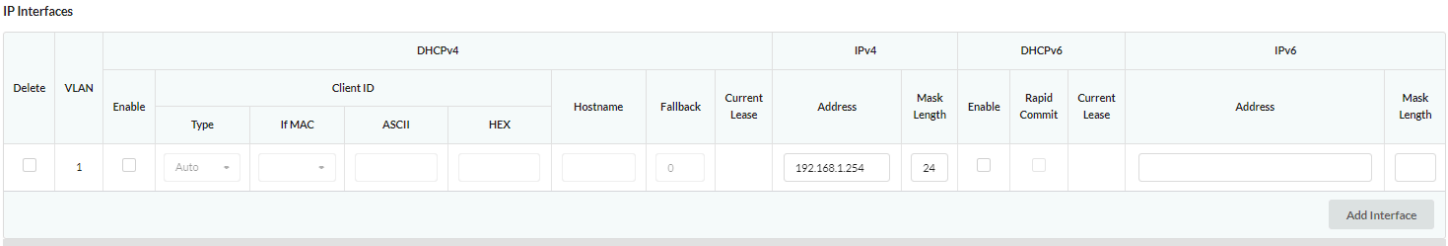
Configured IPv4	Explicitly provide the valid IPv4 unicast address of the DNS Server in dotted decimal notation. Make sure the configured DNS server could be reachable (e.g. via PING) for activating DNS service.
From this DHCPv4 interface	Specify from which DHCPv4-enabled interface a provided DNS server should be preferred.
Configured IPv6	Explicitly provide the valid IPv6 unicast (except link local) address of the DNS Server. Make sure the configured DNS server could be reachable (e.g. via PING6) for activating DNS service.
From this DHCPv6 interface	Specify from which DHCPv6-enabled interface a provided DNS server should be preferred.
From any DHCPv6 interfaces	The first DNS server offered from a DHCPv6 lease to a DHCPv6-enabled interface will be used.

DNS Proxy

When DNS proxy is enabled, the system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network. Only IPv4 DNS proxy is now supported.

IP Interfaces

Click the **Add Interface** button to add a new IP interface. A maximum of 8 interfaces is supported.



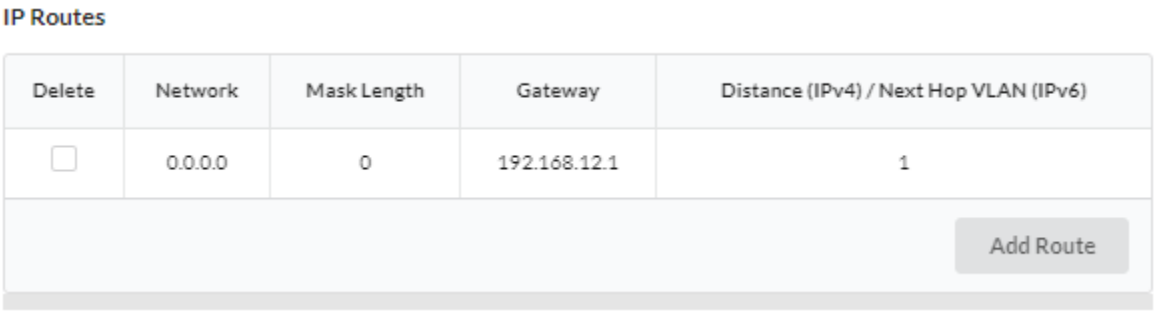
Setting	Description
Delete	Select this option to delete an existing IP interface.
VLAN	The VLAN is associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface.
IPv4 DHCP Enabled	Enable the DHCPv4 client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCPv4 protocol. The DHCPv4 client will announce the configured System Name as the hostname to provide DNS lookup.
IPv4 DHCP Client Identifier Type	The type of DHCP client identifier. Users can choose Auto, ifmac, ASCII, and HEX.

IPv4 DHCP Client Identifier IfMac	The interface name of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type is 'ifmac', the configured interface's hardware MAC address will be used in the DHCP option 61 field.
IPv4 DHCP Client Identifier ASCII	The ASCII string of DHCP client identifiers. When the DHCPv4 client is enabled and the client identifier type is 'ascii', the ASCII string will be used in the DHCP option 61 field.
IPv4 DHCP Client Identifier HEX	The hexadecimal string of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type 'hex', the hexadecimal value will be used in the DHCP option 61 field.
IPv4 DHCP Hostname	The hostname of DHCP client. If DHCPv4 client is enabled, the configured hostname will be used in the DHCP option 12 field. When this value is an empty string, the field uses the configured system name plus the latest three bytes of system MAC addresses as the hostname.
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 shows the current interface address, as provided by the DHCP server.
IPv4 Address	The IPv4 address of the interface is in dotted decimal notation. If DHCP is enabled, this field configures the fallback address. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.
IPv4 Mask	The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for an IPv4 address. If DHCP is enabled, this field configures the fallback address network mask. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.
DHCPv6 Enable	Enable the DHCPv6 client by checking this box. If this option is enabled, the system will configure the IPv6 address of the interface using the DHCPv6 protocol.
DHCPv6 Rapid Commit	Enable the DHCPv6 Rapid-Commit option by checking this box. If this option is enabled, the DHCPv6 client terminates the waiting process as soon as a Reply message with a Rapid Commit option is received. This option is only manageable when the DHCPv6 client is enabled.
DHCPv6 Current Lease	For DHCPv6 interface with an active lease, this column shows the interface address provided by the DHCPv6 server.

IPv6 Address	The IPv6 address of the interface. An 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. The system accepts the valid IPv6 unicast address only, except IPv4-Compatible address and IPv4-Mapped address. 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 an IPv6 address. The field may be left blank if IPv6 operation on the interface is not desired.

IP Routes

Click the **Add Route** button to add a new IP route. A maximum of 32 routes is supported.



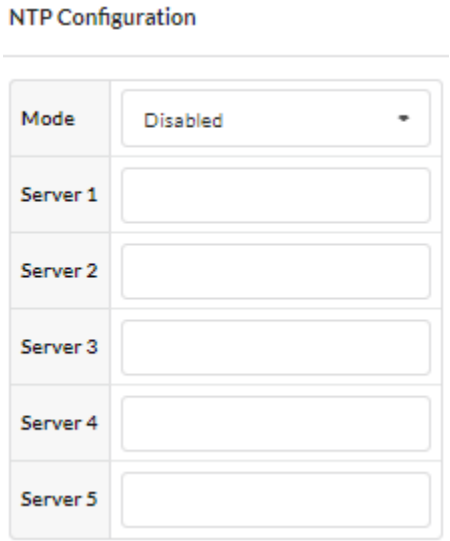
Setting	Description
Delete	Select this option to delete an existing IP route.
Network	The destination IP network or host address of this route. Valid format is dotted decimal notation for a valid IPv6 notation. A default route can use the value **0.0.0.0** or IPv6 **::** notation.
Mask Length	The destination IP network or hostmask, 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.
Distance (Only for IPv4)	The distance value of route entry is used to provide the priority information of the routing protocols to routers. When two or more different routing protocols are involved and have the same destination, the distance value can be used to select the best path.

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 4095 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, the system ignores the next hop VLAN for the gateway.

4.1.4 NTP

Network Time Protocol Configuration

Configure NTP on this page.



Mode

Setting	Description	Factory Default
Enabled	Enable NTP client mode operation.	Disabled
Disabled	Disable NTP client mode operation.	

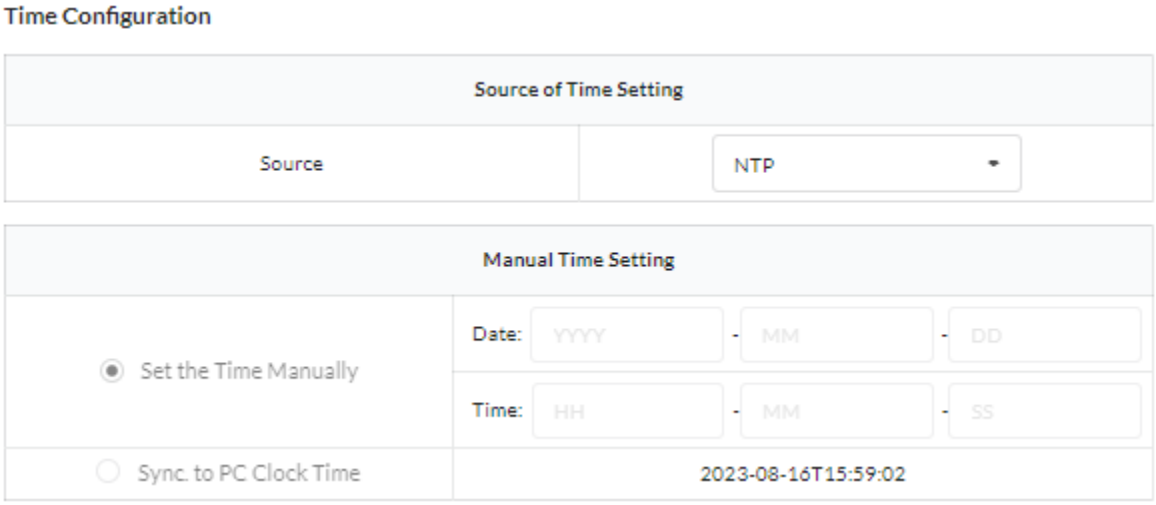
Server

Setting	Description	Factory Default
IPv4 or IPv6 address of a NTP server	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. In addition, it can also accept a domain name address.	None

4.1.5 Time

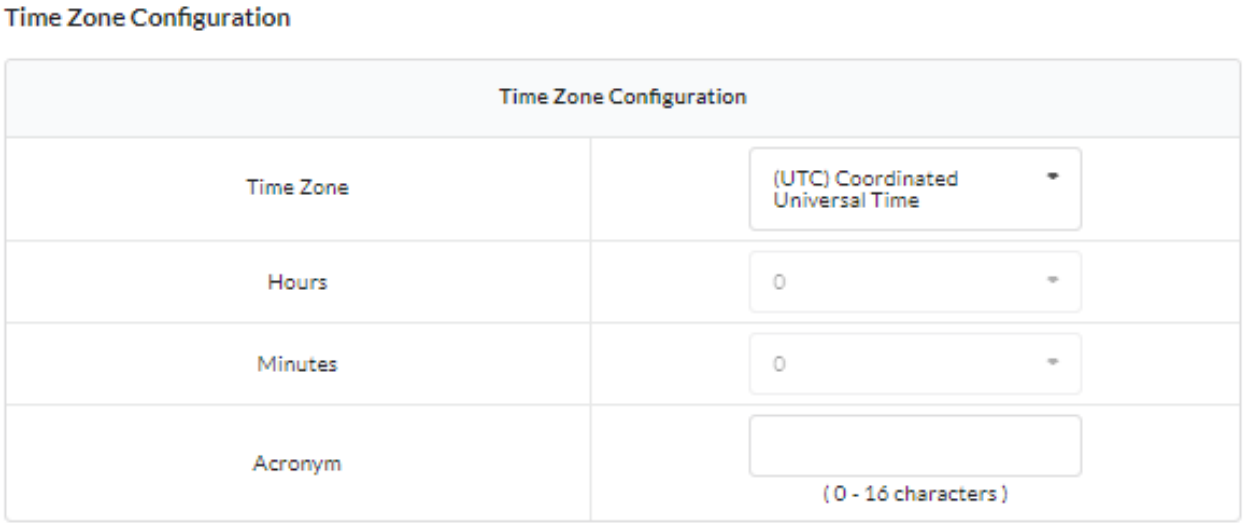
Time Configuration

Setting the system time



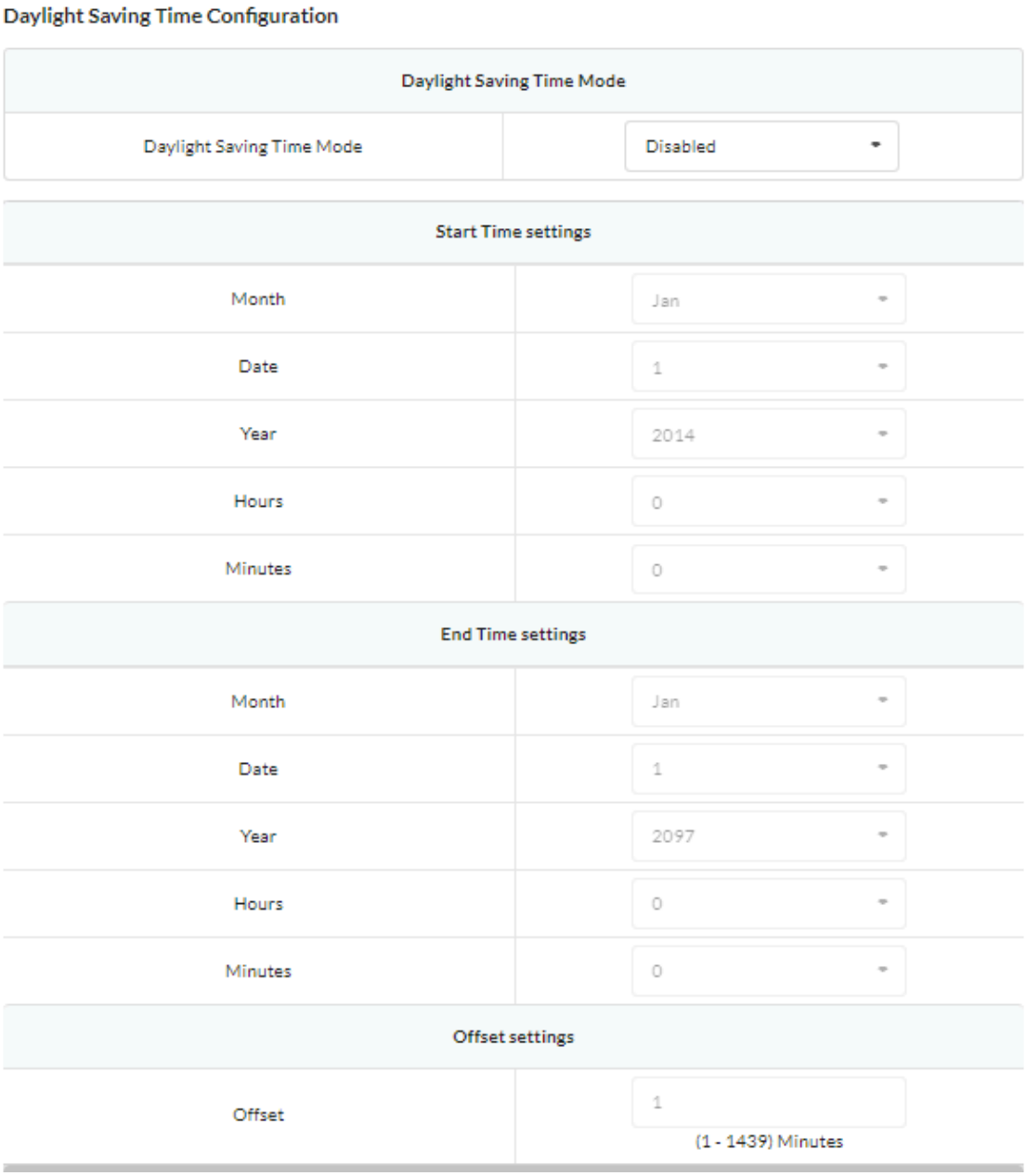
Setting	Description	Factory Default
Source	Choose NTP or manual time for the system time setting	NTP
Manual	**Set the Time Manually** - Manual keying time setting for date and time. **Sync to PC Clock Time** - Synchronizing to clock time of the PC/local device.	none

Time Zone Configuration



Setting	Description	Factory Default
Time Zone	Lists various Time Zones world wide. Select the appropriate Time Zone from the drop down and click Save to set. The 'Manual Setting' option is used for the specific time zone which is excluded from the options list.	UTC
Hours	Number of hours offset from UTC. The field is only available when time zone manual setting.	0
Minutes	Number of minutes offset from UTC. The field is only available when time zone manual setting.	0
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) Notice the string " is a special syntax that is reserved for null input.	None

Daylight Saving Time Configuration



Daylight Saving Time Mode

Setting	Description	Factory Default
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.	Disabled

Start time settings

Select the starting Month, Date, Year, Hours and Minutes.

End time settings

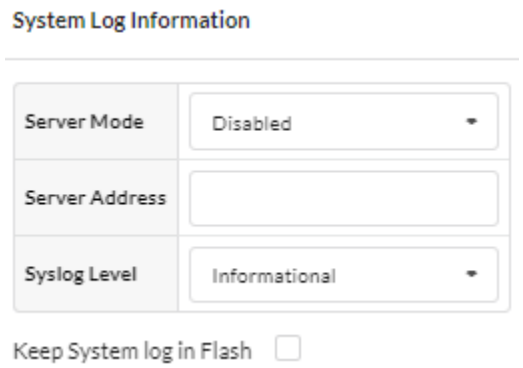
Select the ending Month, Date, Year, Hours and Minutes.

Offset settings

Setting	Description	Factory Default
Offset	Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1439)	1

4.1.6 Log

System log Information



Server Mode

Indicates the server mode operation. When the mode operation is enabled, the syslog message will be sent out to the 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.

Setting	Description	Factory Default
Enabled	Enable server mode operation.	Disabled
Disabled	Disable server mode operation.	

Server Address

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

Syslog Level

Indicates what kind of message will be sent to the syslog server.

Setting	Description	Factory Default
Error	Send the specific messages whose severity code is less or equal to Error(3).	Informational
Warning	Send the specific messages whose severity code is less or equal to Warning(4).	
Notice	Send the specific messages whose severity code is less or equal to Notice(5).	
Informational	Send the specific messages in which the severity code is less or equal to Informational(6).	

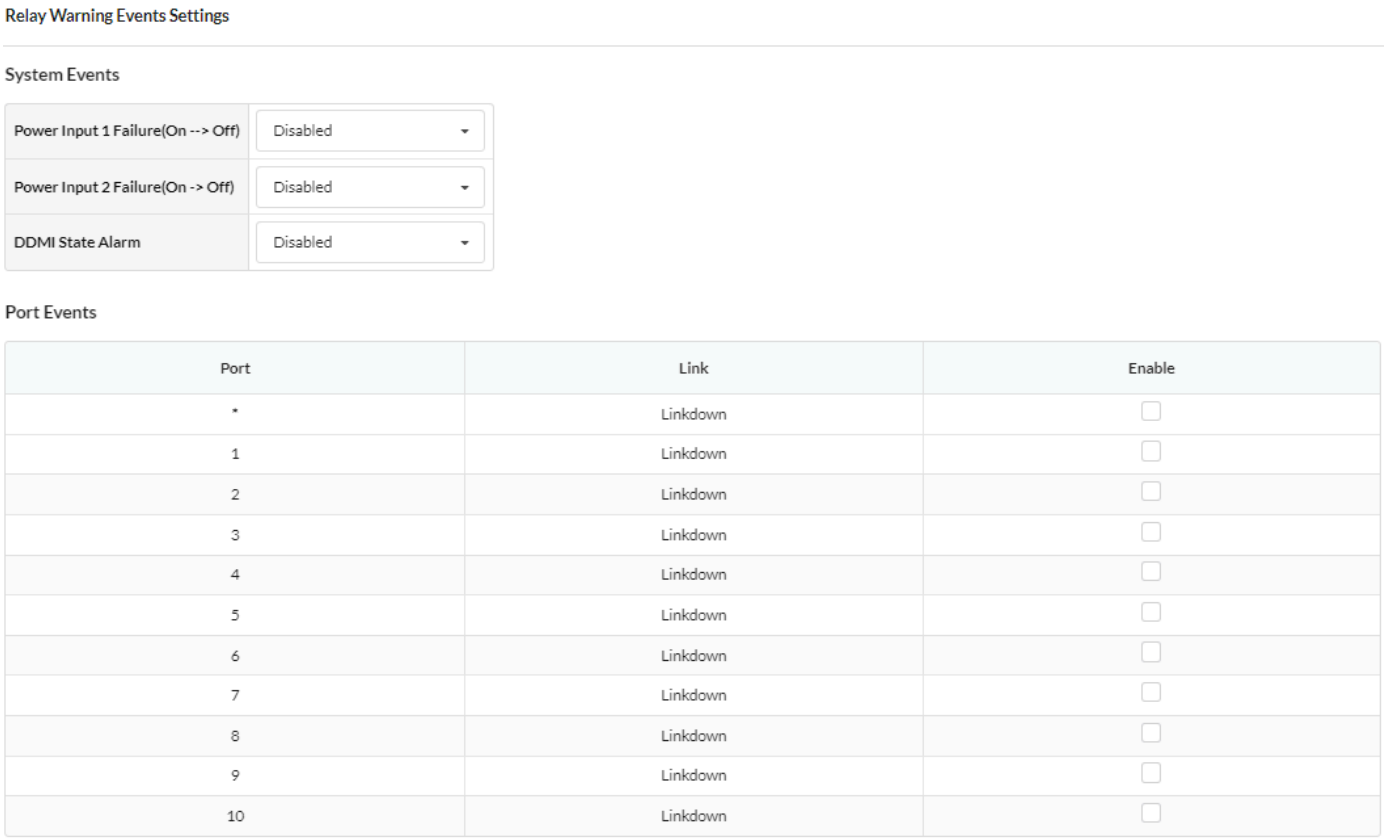
Keep System log in Flash

The system log will be stored in the switch DRAM by default. Check if you want to keep all the system logs in the flash memory. You could get all the system logs if these logs are stored in the Flash. Otherwise, it will disappear when the switch reboots. The log file will write into the flash memory every 30 mins.

4.1.7 Event Warning

4.1.7.1 Relay Warning Events Settings

The Relay Warning function uses relay output to alert the user when certain user-configured events take place.



System Events

Power Failure Events

Indicates power down mode operation. Warning: Relay output is triggered when the switch is powered down.

Setting	Description	Factory Default
Enabled	Enable system event mode operation.	Disabled
Disabled	Disable system event mode operation.	

DDMI State Alarm

Indicates the SFP DDMI information alarm operation. The warning Relay output is triggered when the switch SFP DDMI current value exceeds the alarm threshold.
* DDMI function is only supported by the SFP model.

Setting	Description	Factory Default
Enabled	Enable DDMI information alerts.	Disabled
Disabled	Disable DDMI information alerts.	

Port Events

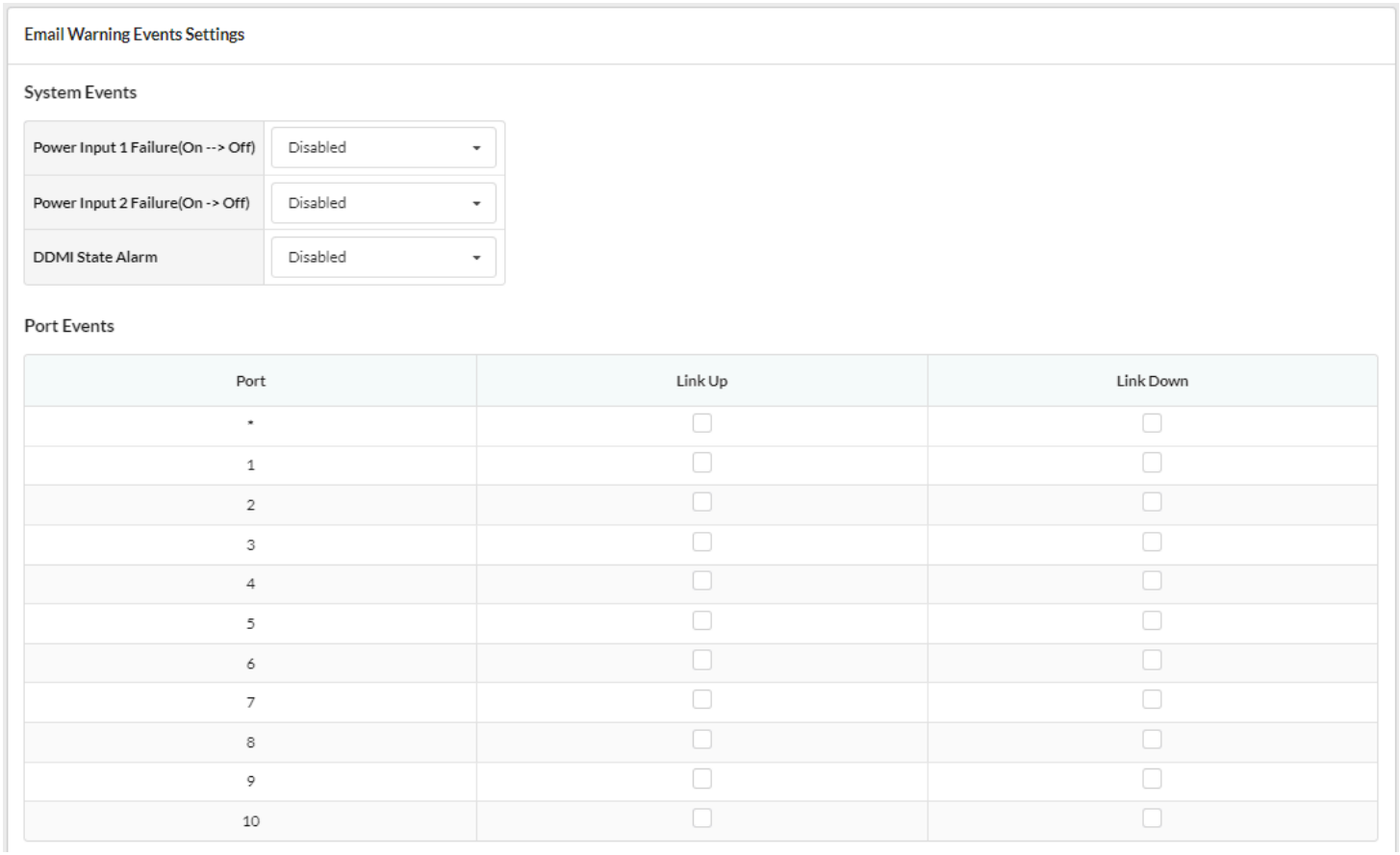
Port Link Status Events

Indicates the port link status operation. Warning: Relay output is triggered when the port is linkdown .

Setting	Description
Link Down	Controls whether port link down event warning is enabled on this switch port.

4.1.7.2 Email Warning Event Settings

The Email Warning function uses SMTP to send Email when certain user-configured events take place.



System Events

Power Failure Events

Indicates power down mode operation. Warning: Relay output is triggered when the switch is powered down.

Setting	Description	Factory Default
Enabled	Enable system event mode operation.	Disabled
Disabled	Disable system event mode operation.	

DDMI State Alarm

Indicates the SFP DDMI information alarm operation. Warning Relay output is triggered when the switch SFP DDMI current value exceeds the alarm threshold.
* DDMI function is only supported by the SFP model.

Setting	Description	Factory Default
Enabled	Enable DDMI information alerts.	Disabled
Disabled	Disable DDMI information alerts.	

Port Events

Port Status Events

Indicate the port link status operation. Warning: Relay output is triggered when the port is link-down

Setting	Description
Port	The switch port number of the port
Link Up	Indicate whether the event warning via Email for Port Link-up is enabled or not
Link Down	Indicate whether the event warning via Email for Port Link-down is enabled or not.

4.2 Green Ethernet

4.2.1 Port Power Savings



What is EEE

EEE is a power-saving option that reduces power usage when there is low or no traffic utilization.
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 wake-up 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 wake-up time information using the LLDP protocol.
EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100 Mbit full duplex mode.
For ports that are not EEE-capable the corresponding EEE checkboxes are grayed out and thus impossible to enable EEE for.
When a port is powered down for saving power, outgoing traffic is stored in a buffer until the port is powered up again. Because there is some overhead in turning the port down and up, more power can be saved if the traffic can be buffered up until a large burst of traffic can be transmitted. Buffering traffic will give some latency in the traffic.

Optimize EEE

The switch can be set to optimize EEE for either best power saving or least traffic latency.

Setting	Description	Factory Default
Power	Best power saving	Latency
Latency	Least traffic latency	

Port Configuration

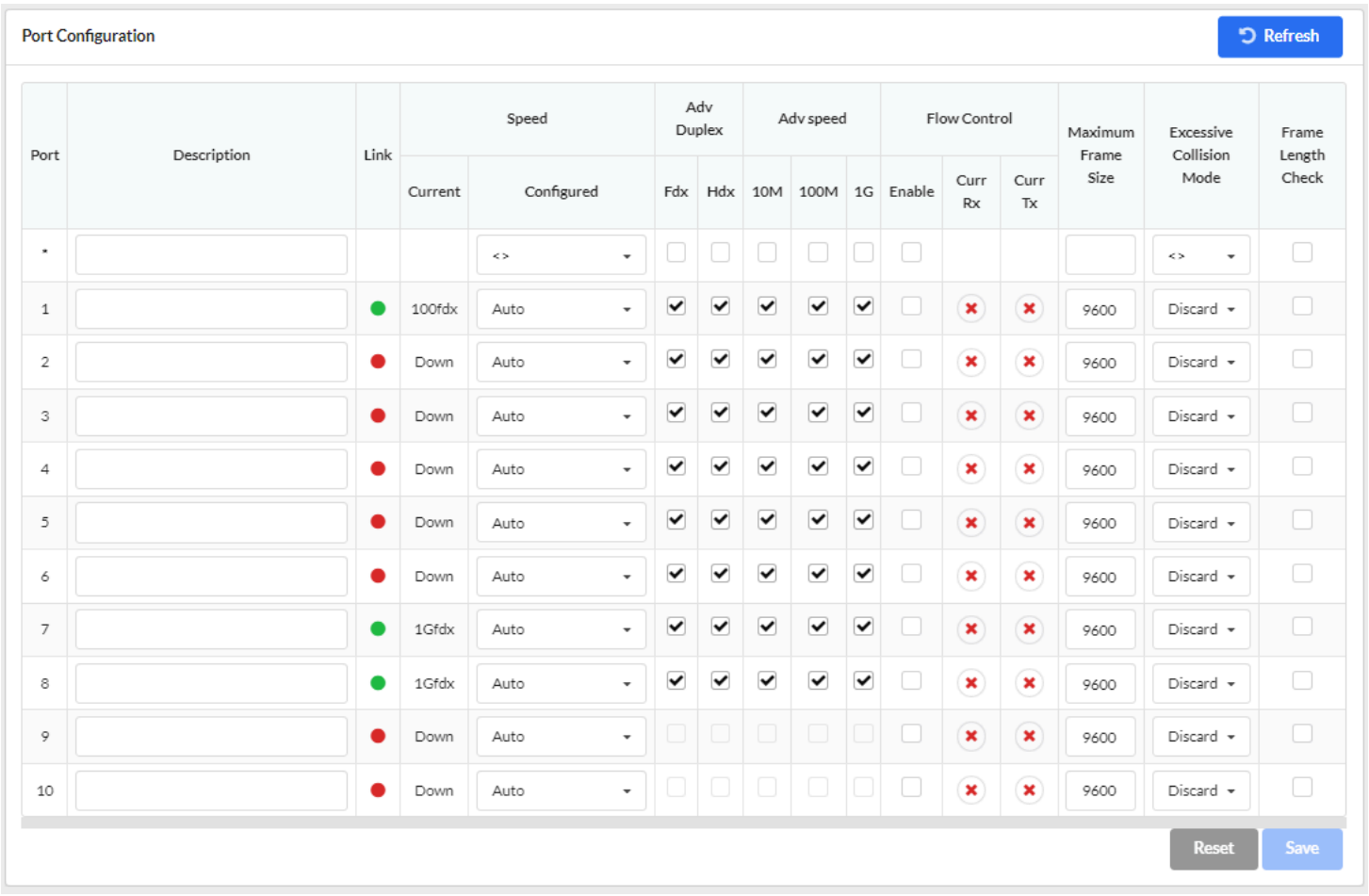
				EEE Urgent Queues							
Port	ActiPHY	PerfectReach	EEE	1	2	3	4	5	6	7	8
*	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
9	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
10	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Setting	Description
Port	The switch port number of the logical port.
ActiPHY	Link down power savings enabled. ActiPHY works by lowering the power for a port when there is no link. The port is powered up for a short moment in order to determine if cable is inserted.
PerfectReach	Cable length power savings enabled. PerfectReach works by determining the cable length and lowering the power for ports with short cables.
EEE	Controls whether EEE is enabled for this switch port. For maximizing power savings, the circuit isn't started at once transmit data is ready for a port, but is instead queued until a burst of data is ready to be transmitted. This will give some traffic latency. If desired it is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then marking the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.
EEE Urgent Queues	Queues set will activate the transmission of frames as soon as data is available. Otherwise, the queue will postpone transmission until a burst of frames can be transmitted.

4.3 Port

4.3.1 Port Configuration

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



Port

This is the logical port number for this row.

Link

The current link state is displayed graphically.

Color	Description
Green	Link is up.
Red	Link 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 are shown.

Setting	Description	Factory Default
Disabled	Disables the switch port operation.	Auto
Auto	Port auto-negotiation 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.	
5Gbps FDX	Forces the Serdes port in 5 Gbps full duplex mode.	
10Gbps FDX	Forces the Serdes port in 10 Gbps full duplex mode.	
SFP_Auto	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.	
100-FX	SFP port at 100-FX speed.	
1000-X	SFP port at 1000-X speed.	

Advertise Duplex

When duplex is set as auto i.e auto-negotiation, the port will only advertise the specified duplex as either **Fdx** or **Hdx** to the link partner. By default port will advertise all the supported duplexes if the Duplex is Auto.

Advertise Speed

When Speed is set as auto i.e auto-negotiation, the port will only advertise the specified speeds (**10M 100M 1G 2.5G 5G 10G**) to the link partner. By default port will advertise all the supported speeds if speed is set as Auto.

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.

NOTE: The 100FX standard doesn't support Auto Negotiation, so when in 100FX mode the flow control capabilities will always be shown as **disabled**.

Maximum Frame Size

Setting	Description	Factory Default

1518-9600	Enter the maximum frame size allowed for the switch port, including FCS. The range is 1518-9600 bytes.	9600

Excessive Collision Mode

Configure port transmit collision behavior.

Setting	Description	Factory Default
Discard	Discard frame after 16 collisions.	Discard
Restart	Restart backoff algorithm after 16 collisions.	

Frame Length Check

Configures if frames with incorrect frame length in the EtherType/Length field shall be dropped. An Ethernet frame contains a field EtherType which can be used to indicate the frame payload size (in bytes) for values of 1535 and below. If the EtherType/Length field is above 1535, it indicates that the field is used as an EtherType (indicating which protocol is encapsulated in the payload of the frame).

Setting	Description	Factory Default
Checked	Frames with payload size less than 1536 bytes are dropped, if the EtherType/Length field doesn't match the actual payload length.	Unchecked
Unchecked	Frames are not dropped due to frame length mismatch.	

NOTE: No drop counters count frames dropped due to frame length mismatch.

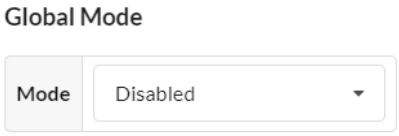
4.4 DHCP

4.4.1 Server

4.4.1.1 Mode - DHCP Server Mode Configuration

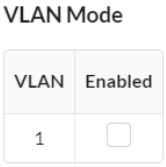
This page configures global mode and VLAN mode to enable/disable DHCP server per system and per VLAN.

Global Mode



Setting	Description	Factory Default
Enabled	Enable DHCP server per system.	Disabled
Disabled	Disable DHCP server per system.	

VLAN Mode



Mode

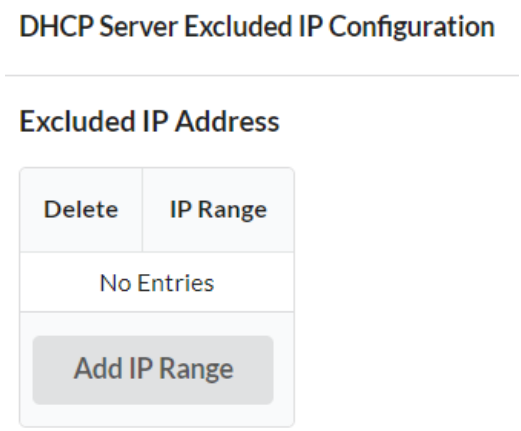
Setting	Description	Factory Default
Checked	Enable DHCP server per VLAN n.	Unchecked
Unchecked	Disable DHCP server per VLAN n.	

4.4.1.2 Excluded IP

This page configures excluded IP addresses. The DHCP server will not allocate these excluded IP addresses to the DHCP client.

Excluded IP Address

Configure excluded IP addresses.



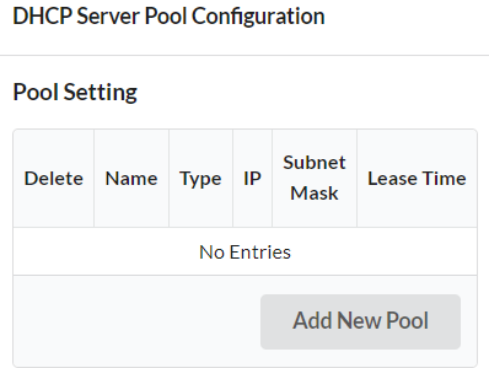
IP Range

Define the IP range to be excluded IP addresses. The first excluded IP must be smaller than or equal to the second excluded IP. BUT, if the IP range contains only 1 excluded IP, then you can just input it to either one of the first and second excluded IP or both.



4.4.1.3 Pool

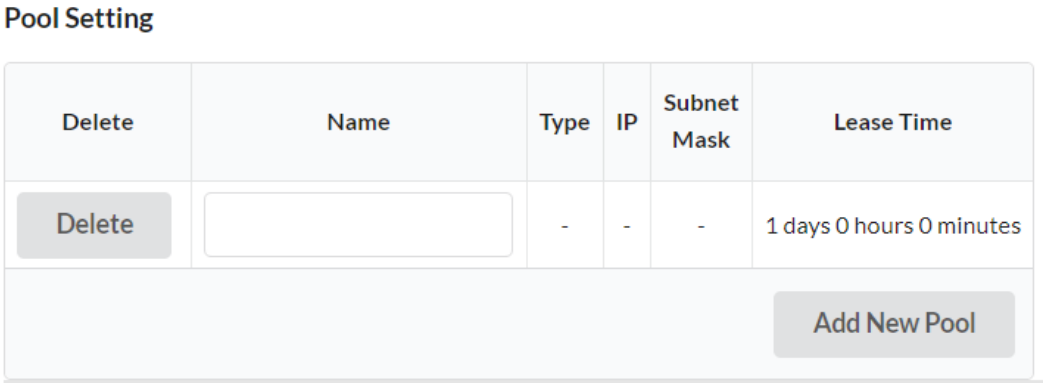
This page manages DHCP pools. According to the DHCP pool, DHCP server will allocate IP address and deliver configuration parameters to DHCP client.



Pool Setting

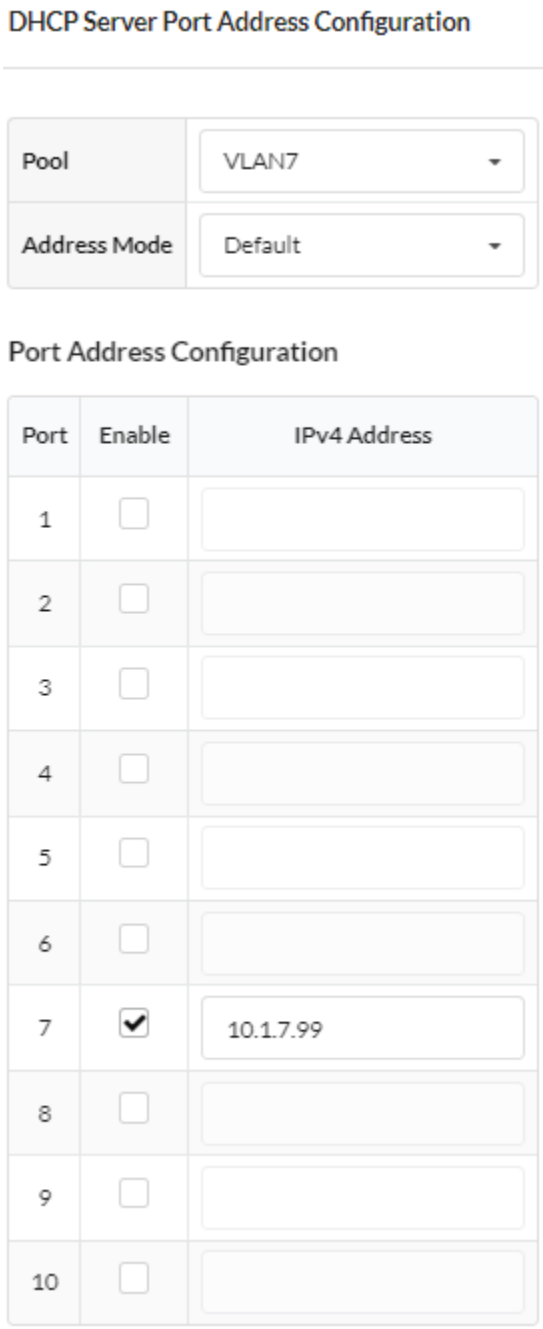
Add or delete pools.

Adding a pool and giving a name is to create a new pool with "default" configuration. If you want to configure all settings including type, IP subnet mask, and lease time, you can click the pool name to go to the configuration page.



Setting	Description
Name	Display the selected pool name.
Type	Specify which type of the pool is. **Network:** the pool defines a pool of IP addresses to service more than one DHCP client. **Host:** the pool services for a specific DHCP client identified by client identifier or hardware address.
IP	Specify network number of the DHCP address pool.
Subnet Mask	Specify subnet mask of the DHCP address pool.
Lease Time	Specify lease time that allows the client to request a lease time for the IP address. If all are 0's, then it means the lease time is infinite.
Domain Name	Specify domain name that client should use when resolving hostname via DNS.
Broadcast Address	Specify the broadcast address in use on the client's subnet.
Default Router	Specify a list of IP addresses for routers on the client's subnet.
DNS Server	Specify a list of Domain Name System name servers available to the client.
NTP Server	Specify a list of IP addresses indicating NTP servers available to the client.
NetBIOS Node Type	Specify NetBIOS node type option to allow Netbios over TCP/IP clients which are configurable to be configured as described in RFC 1001/1002.
NetBIOS Scope	Specify the NetBIOS over TCP/IP scope parameter for the client as specified in RFC 1001/1002.
NetBIOS Name Server	Specify a list of NBNS name servers listed in order of preference.
NIS Domain Name	Specify the name of the client's NIS domain.
NIS Server	Specify a list of IP addresses indicating NIS servers available to the client.
Client Identifier	Specify client's unique identifier to be used when the pool is the type of host.
Hardware Address	Specify client's hardware (MAC) address to be used when the pool is the type of host.
Client Name	Specify the name of the client to be used when the pool is the type of host.
Vendor # Class Identifier	Specify to be used by a DHCP client to optionally identify the vendor type and configuration of a DHCP client. DHCP server will deliver the corresponding option 43 specific information to the client that sends option 60 vendor class identifier.
Vendor # Specific Information	Specify vendor specific information according to option 60 vendor class identifier.

4.4.1.4 Port Address



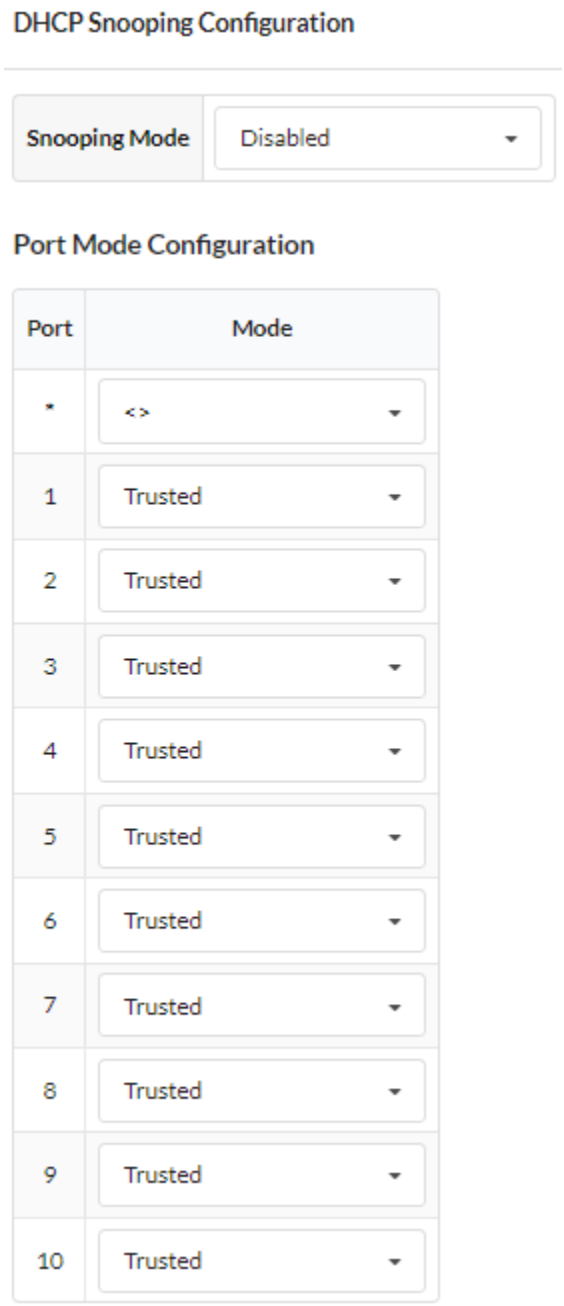
Pool Port Address Configuration

Setting	Description
Pool	Select pool by pool name to configure the settings.
Address mode	For the ports which have no reserved address configured. **Default**: the DHCP server assigns addresses from the pool network as normal behavior. **Port Address Only**: the DHCP server wouldn't assign addresses for these ports.

Port Based Address Assignment

Setting	Description
Port	This is the logical port number of this ro.
Enable	Enable or clear the address configuration
IPv4 Address	Assign the IP address to the client on a specific interface. • Can't conflict with other interfaces. • Can't conflict with DHCP Server Address. • Must be included in the Pool subnet.

4.4.2 Snooping



Snooping mode

Setting	Description	Factory Default
Enabled	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.	Disabled
Disabled	Disable DHCP snooping mode operation	

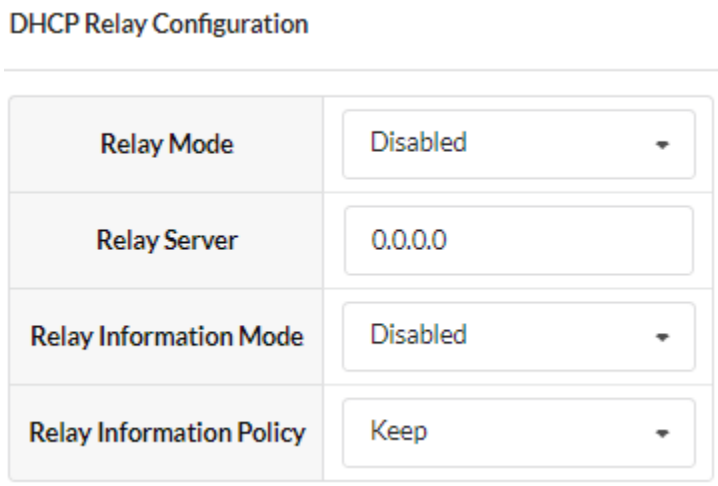
Port Mode Configuration

Setting	Description	Factory Default
Trusted	Configures the port as a trusted source of the DHCP messages.	Trusted
Untrusted	Configures the port as an untrusted source of the DHCP messages.	

4.4.3 Relay

Relay 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 the GIADDR field to determine the assigned subnet. For such conditions, please make sure the switch configuration of VLAN interface IP address and PVID(Port VLAN ID) correctly.



Relay Mode

Setting	Description	Factory Default
Enabled	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.	Disabled
Disabled	Disable DHCP relay mode operation.	

Relay Server

Setting	Description

IP address.	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 equals 0, in stackable device it means switch ID), and the last two characters are the port number. For example, "00030108" means the DHCP message received from VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal to the switch MAC address.

Setting	Description	Factory Default
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
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.

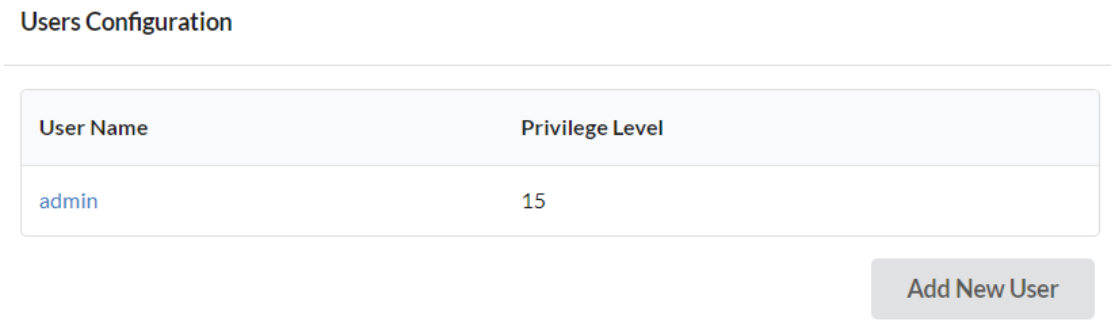
Setting	Description	Factory Default
Replace	Replace the original relay information when a DHCP message that already contains it is received.	Keep
Keep	Keep the original relay information when a DHCP message that already contains it is received.	
Drop	Drop the package when a DHCP message that already contains relay information is received.	

4.5 Security

4.5.1 Switch

4.5.1.1 Users

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.

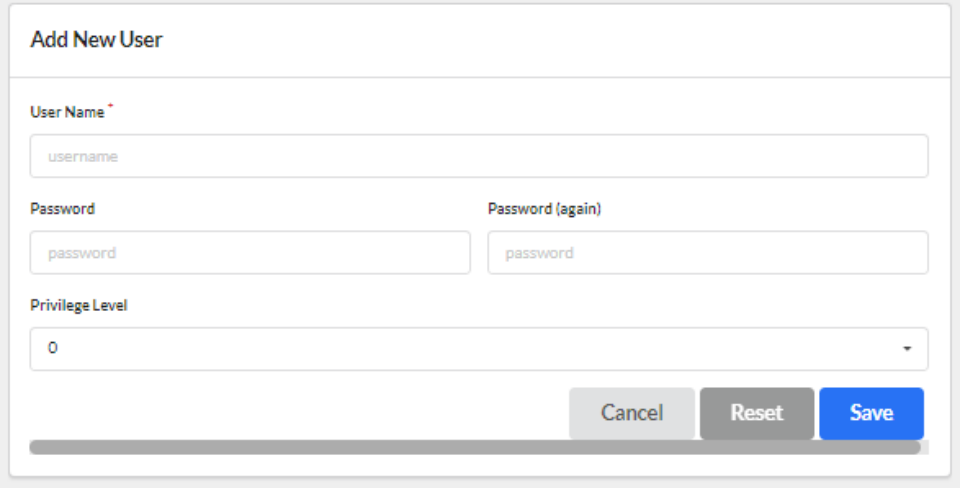


User Configuration

Setting	Description	Factory Default
User Name	The name identifying the user.	None
Privilege Level 0~15	The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the full control of the device. But others' values need to refer to each group privilege level. User's privilege should be the same or greater than the group privilege level to have the access of that group. By default setting, most group's 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 etc.) need user privilege level 15. Generally, 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.	0

Add/Edit User

Click the **Add New User** button to add a new user. Also you can click User Name to edit a user.



User Name

Setting	Description	Factory Default
Max. 31 Characters	A string identifying the user name that this entry should belong to. The allowed string length is **1 to 31**. The valid user name allows letters, numbers and underscores.	None

Password

Setting	Description	Factory Default
Max. 31 Characters	The password of the user. The allowed string length is **0 to 31**. Any printable characters including space are accepted.	None

Privilege Level

Setting	Description	Factory Default
0~15	The privilege level of the user. The allowed range is **0 to 15**. If the privilege level value is 15, it can access all groups, i.e. that is granted the full control of the device. But others' values need to refer to each group privilege level. User's privilege should be the same or greater than the group privilege level to have the access of that group. By default setting, most group's 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 etc.) need user privilege level 15. Generally, 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.	0

4.5.1.2 Privilege level

This page provides an overview of the privilege levels.

Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/Write	Status/Statistics Read-only	Status/Statistics Read/Write
Aggregation	5	10	5	10
Alarm	5	10	5	10
CLI_Client	5	10	5	10

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 contain 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.
- **Debug**: Only present in CLI.

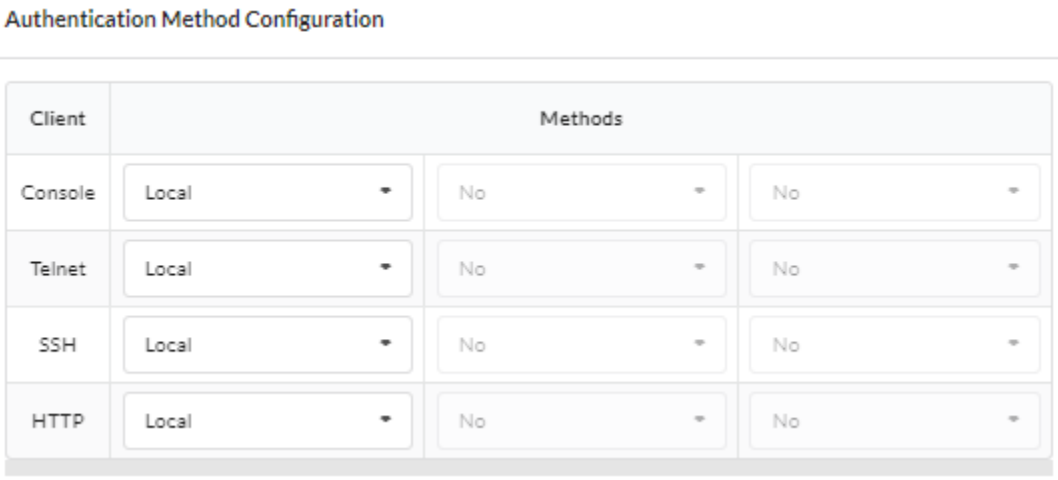
Privilege Levels

The Privilege Levels can be configured between **0** to **15** (where 0 is lowest level and 15 is highest level) Every group has an authorization Privilege level for the following sub groups: configuration read-only, configuration/execute read-write, status/statistics read-only, status/statistics read-write (e.g. for clearing of statistics). User Privilege should be the same or greater than the authorization Privilege level to have the access to that group.

4.5.1.3 Auth Method

Authentication Method Configuration

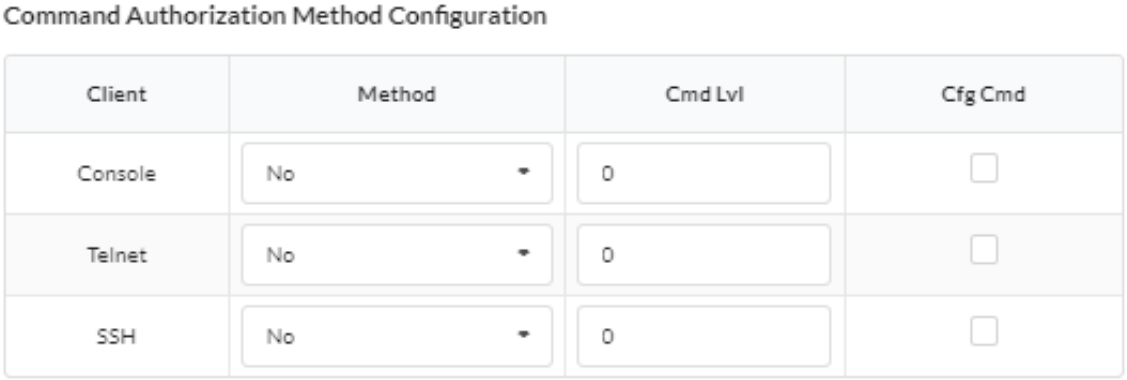
The authentication section allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces.



Setting	Description
Client	The management client for which the configuration below applies.
Methods	Method can be set to one of the following values: • **No:** Authentication is disabled and login is not possible. • **Local:** Use the local user database on the switch for authentication. • **RADIUS:** Use remote RADIUS server(s) for authentication. • **ACACS:** Use remote TACACS+ server(s) for authentication. Methods that involve 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.

Command Authorization Method Configuration

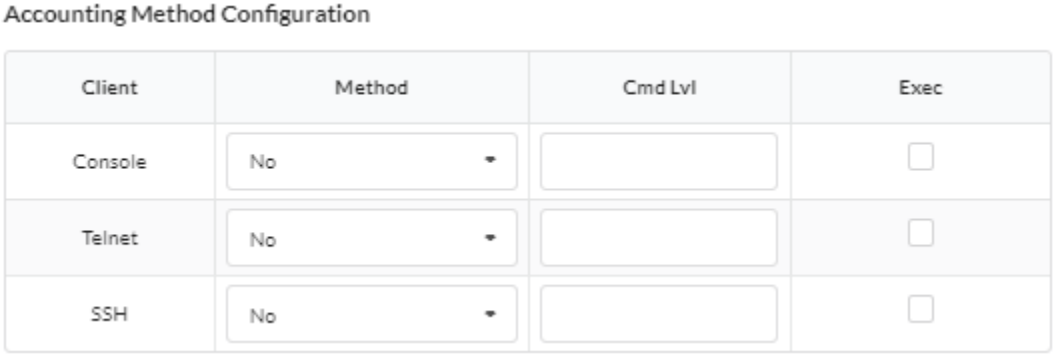
The command authorization section allows you to limit the CLI commands available to a user.



Setting	Description
Client	The management client for which the configuration below applies.
Methods	Method can be set to one of the following values: • **No:** Command authorization is disabled. User is granted access to CLI commands according to his privilege level. • **TACACS:** Use remote TACACS+ server(s) for command authorization. If all remote servers are offline, the user is granted access to CLI commands according to his privilege level.
Cmd Lvl (0~15)	Authorize all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15.
Cfg Cmd	Also authorize configuration commands.

Accounting Method Configuration

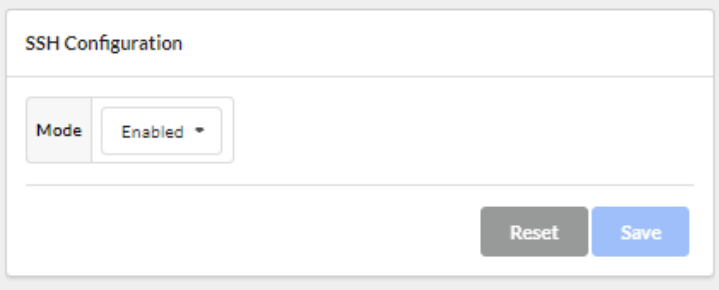
The accounting section allows you to configure command and exec (login) accounting.



Setting	Description
Client	The management client for which the configuration below applies.
Methods	Method can be set to one of the following values: • **No:** Accounting is disabled. • **TACACS:** Use remote TACACS+ server(s) for accounting.
Cmd Lvl (0~15)	Enable accounting of all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15. Leave the field empty to disable command accounting.
Exec	Enable exec (login) accounting.

4.5.1.4 SSH

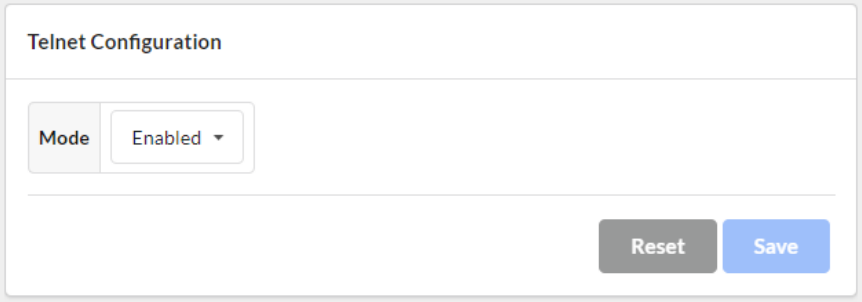
SSH Configuration



Mode	Description	Factory Default
Enabled	Enable SSH mode operation.	Enabled
Disabled	Disable SSH mode operation.	

4.5.1.5 Telnet

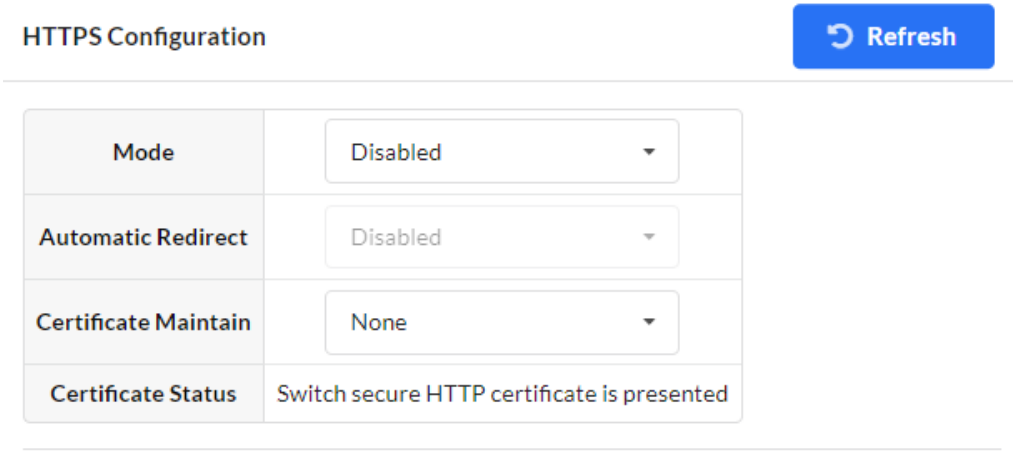
Telnet Configuration



Mode	Description	Factory Default
Enabled	Enable Telnet mode operation.	Enabled
Disabled	Disable Telnet mode operation.	

4.5.1.6 HTTPS

HTTPS Configuration



Mode

Setting	Description	Factory Default
Enabled	Enable HTTPS mode operation.	Disabled
Disabled	Disable HTTPS mode operation.	

Automatic Redirect

Indicate the HTTPS redirect mode operation. It is only significant when "HTTPS Mode Enabled" is selected. When the redirect mode is enabled, the HTTP connection will be redirected to HTTPS connection automatically. Notice that the browser may not allow the redirect operation due to the security consideration unless the switch certificate is trusted to the browser. You need to initialize the HTTPS connection manually for this case.

Setting	Description	Factory Default
Enabled	Enable HTTPS redirect mode operation.	Disabled
Disabled	Disable HTTPS redirect mode operation.	

Certificate Maintain

Setting	Description	Factory Default
None	No operation.	None
Delete	Delete the current certificate.	
Upload	Upload a certificate PEM file. Possible methods are: **Web Browser** or **URL**.	
Generate	Generate a new self-signed RSA certificate.	

Certificate Passphrase

Setting	Description	Factory Default
Pass phrase	Enter the passphrase in this field if your uploading certificate is protected by a specific passphrase.	None

Certificate Upload

Upload a certificate PEM file into the switch. The file should contain the certificate and private key together. If you have two separated files for saving certificate and private key. Use the Linux cat command to combine them into a single PEM file. For example, *cat my.cert my.key > my.pem*
Notice that the RSA certificate is recommended since most of the new version of browsers has removed support for DSA in certificates, e.g. Firefox v37 and Chrome v39.

Setting	Description	Factory Default
Web Browser	Upload a certificate via Web browser.	Web Browser
URL	Upload a certificate via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP. The URL format is <protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>]/<file_name>. For example, tftp://10.10.10.10/new_image_path/new_image.dat, http:// username:password@10.10.10.10:80/new_image_path/new_image.dat. A valid file name is a text string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under score(_). The maximum length is 63 and the hyphen must not be the first character. The file name content that only contains '.' is not allowed.	

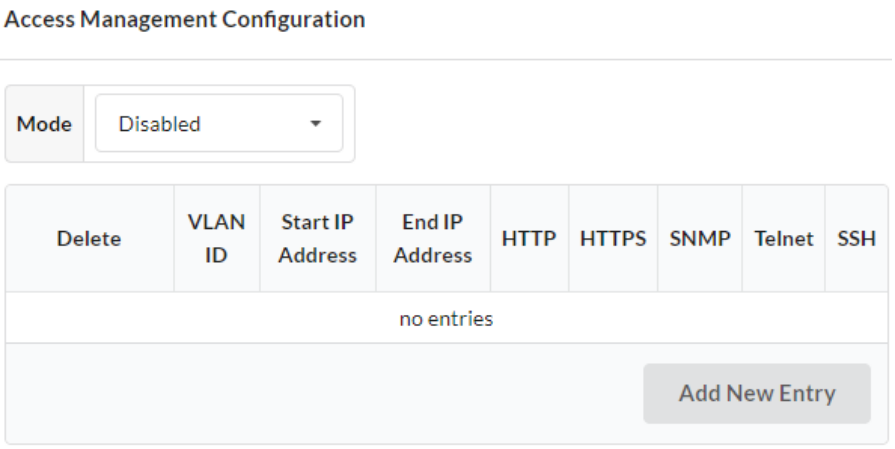
Certificate Status

Display the current status of the certificate on the switch.

- Switch secure HTTP certificate is presented.
- Switch secure HTTP certificate is not presented.
- Switch secure HTTP certificate is generated ...

4.5.1.7 Access Management

Access Management Configuration



Mode

Indicates the access management mode operation.

Setting	Description	Factory Default
Enabled	Enable access management mode operation.	Disabled
Disabled	Disable access management mode operation.	

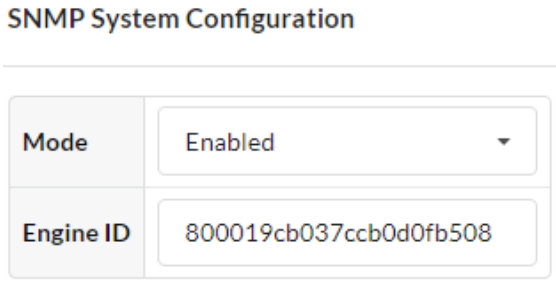
Add New Entry

Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	Indicates the VLAN ID for the access management entry.
Start IP address	Indicates the start IP address for the access management entry.
End IP address	Indicates the end IP address for the access management entry.
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.

4.5.2 SNMP

4.5.2.1 System

SNMP System Configuration



Mode

Setting	Description	Factory Default
Enabled	Enable SNMP mode operation.	Enabled
Disabled	Disable SNMP mode operation.	

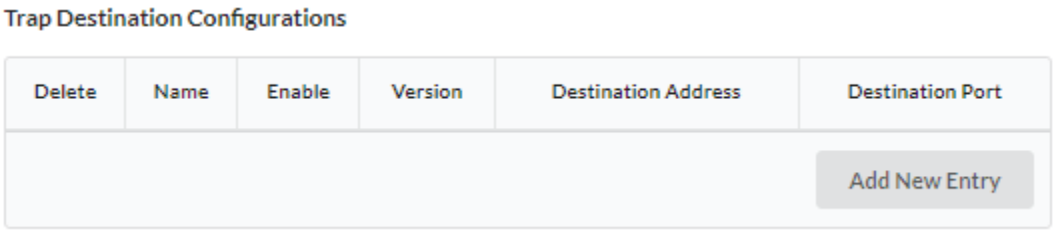
Engine ID

Indicates the SNMPv3 engine ID. The string must contain an even number (in hexadecimal format) with a number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Only users on this Engine ID can access the device (local users), so changing the Engine ID will revoke access for all current local users.

4.5.2.2 Trap

Destinations

Trap Destination Configurations



Name

Indicates the trap Configuration's name. Indicates the trap destination's name.

Enable

Indicates the trap destination mode operation.

Setting	Description	Factory Default
Enabled	Enable SNMP trap mode operation.	Disabled
Disabled	Disable SNMP trap mode operation.	

Version

Setting	Description	Factory Default
SNMP v1	Set SNMP supported version 1.	SNMP v2c
SNMP v2c	Set SNMP supported version 2c.	
SNMP v3	Set SNMP supported version 3.	

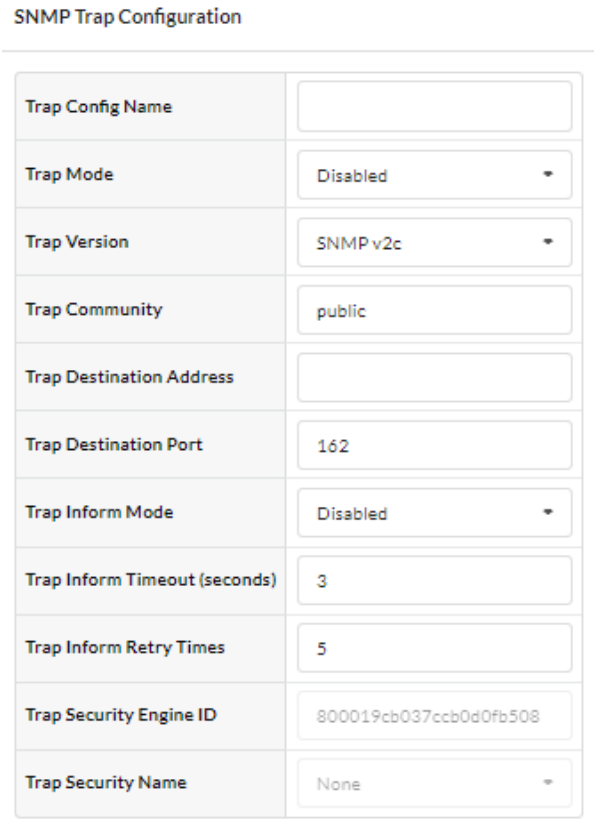
Destination Address

Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). And it also allows a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash.
Indicates the SNMP trap destination IPv6 address. 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**.

Destination port

Indicates the SNMP trap destination port. SNMP Agent will send SNMP messages via this port, the port range is 1~65535.

SNMP Trap Configuration



Trap Config Name

Setting	Description	Factory Default
1~32 characters	Indicates which trap Configuration's name for configuring. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.	None

Trap Mode

Setting	Description	Factory Default
Enabled	Enable SNMP trap mode operation.	Disabled
Disabled	Disable SNMP trap mode operation.	

Trap Version

Setting	Description	Factory Default
SNMP v1	Set SNMP supported version 1.	SNMP v2c
SNMP v2c	Set SNMP supported version 2c.	
SNMP v3	Set SNMP supported version 3.	

Trap Community

Setting	Description	Factory Default
0 ~ 63 characters	Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 63, and the allowed content is ASCII characters from 33 to 126.	Public

Trap Destination Address

Setting	Description	Factory Default
IP address	Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). And it also allows a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0- 9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash. Indicates the SNMP trap destination IPv6 address. 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**.	None

Trap Destination port

Setting	Description	Factory Default
1~65535	Indicates the SNMP trap destination port. SNMP Agent will send SNMP messages via this port, the port range is 1~65535.	162

Trap Inform Mode

Setting	Description	Factory Default
Enabled	Enable SNMP trap inform mode operation.	Disabled
Disabled	Disable SNMP trap inform mode operation.	

Trap Inform Timeout (seconds)

Setting	Description	Factory Default
0~2147	Indicates the SNMP trap informs timeout. The allowed range is 0 to 2147.	3

Trap Inform Retry Times

Setting	Description	Factory Default
0~255	Indicates the SNMP trap informs retry times. The allowed range is 0 to 255.	5

Trap Security Engine ID

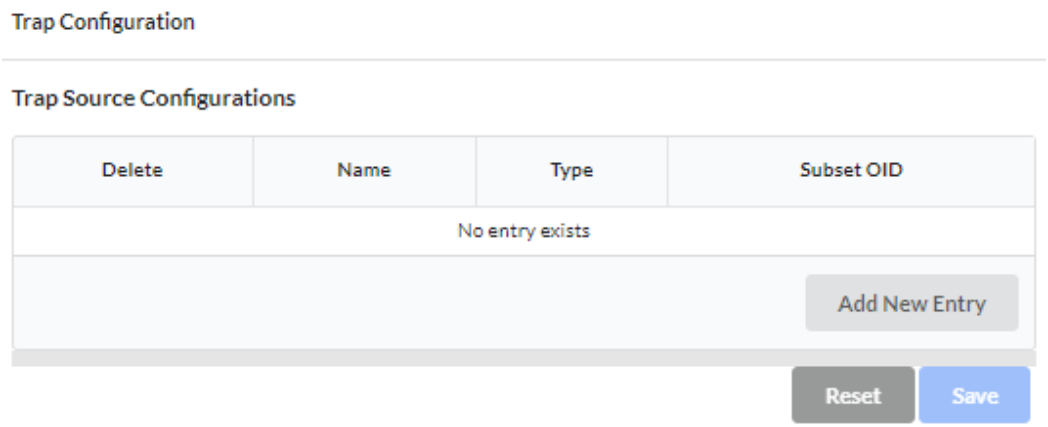
Indicates the SNMP trap security engine ID. SNMPv3 sends traps and information using USM for authentication and privacy. A unique engine ID for these traps and information is needed. When Trap Probe Security Engine ID is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number(in hexadecimal format) with a number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.

Trap Security Name

Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and information are enabled.

Sources

Trap Source Configuration



Delete

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

Name

Indicates the name for the entry.

Type

The filter type for the entry.

Setting	Description	Factory Default
included	An optional flag to indicate a trap is sent for the given trap source, is matched.	included
excluded	An optional flag to indicate a trap is not sent for the given trap source, is matched.	

Subset OID

The subset OID for the entry. The value should depend on what kind of trap name. For example, the ifIdex is the subset OID of linkUp and linkDown. A valid subset OID is one or more digital number(0-4294967295) or asterisk(*) which are separated by dots(.). The first character must not begin with asterisk(*) and the maximum OID count must not exceed 128.

4.5.2.3 Communities

SNMPv3 Community Configuration

Configure SNMPv3 community table on this page. The entry index key is Community.



Add New Entry

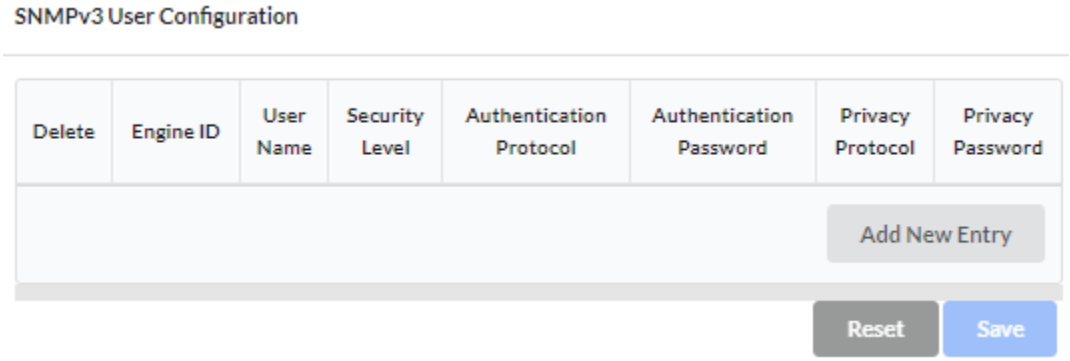
Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Community Name	Indicates the security name to map the community to the SNMP Groups configuration. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Community Secret	Indicates the community secret (access string) to permit access using SNMPv1 and SNMPv2c to the SNMP agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

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 prefix.
Source Prefix	Indicates the SNMP access source address prefix.

4.5.2.4 Users

User Configuration

Configure SNMPv3 user table on this page. The entry index keys are Engine ID and User Name.



Add New Entry

Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Engine ID	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number(in hexadecimal format) with a number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if the user engine ID equals system engine ID then it is a local user; otherwise it's a remote user.
User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
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: • **None:** No authentication protocol. • **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 you 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 32. For SHA authentication protocol, the allowed string length is 8 to 40. 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: • **None:** No privacy protocol. • **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 32, and the allowed content is ASCII characters from 33 to 126.

4.5.2.5 Groups

Group Configuration

Configure SNMPv3 group table on this page. The entry index keys are Security Model and Security Name.

SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
☐	v1	public	default_ro_group
☐	v1	private	default_rw_group
☐	v2c	public	default_ro_group
☐	v2c	private	default_rw_group

Add New Entry

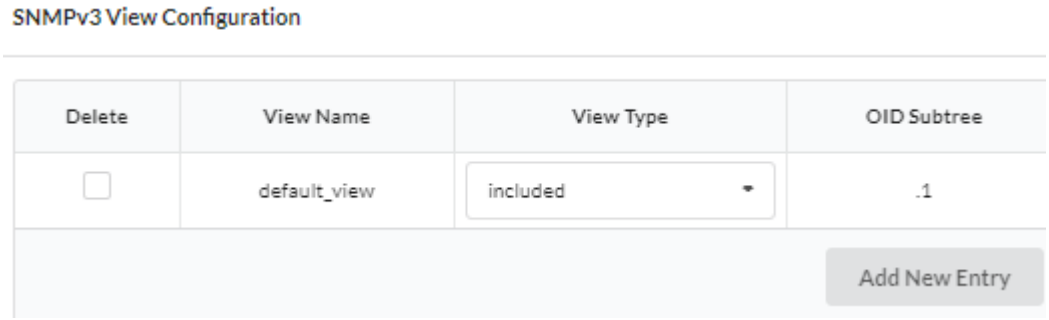
Add New Entry

Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
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 32, 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.

4.5.2.6 Views

View Configuration

Configure SNMPv3 view table on this page. The entry index keys are View Name and OID Subtree.



Add New Entry

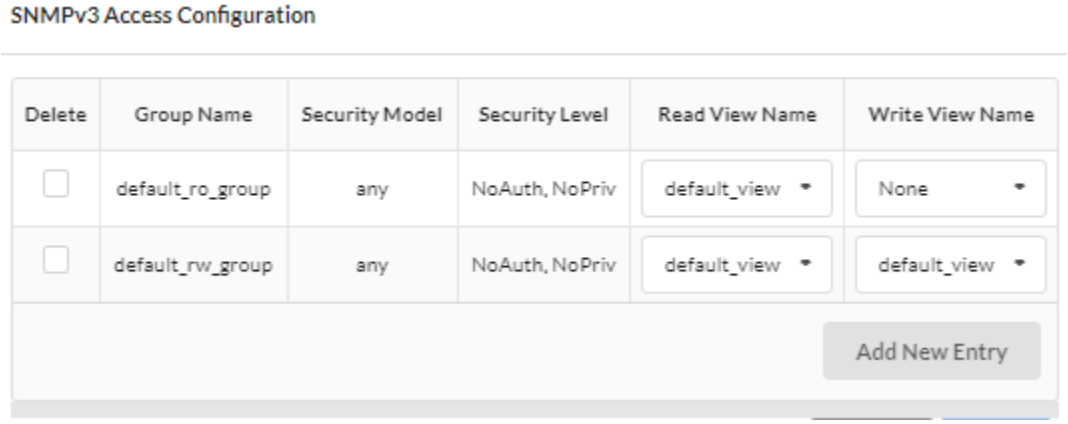
Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
View Name	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
View Type	Indicates the view 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 its OID subtree should overstep the **excluded** view entry.

OID Subtree	The OID defines 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(*).

4.5.2.7 Access

Access Configuration

Configure SNMPv3 access table on this page. The entry index keys are Group Name, Security Model and Security Level.



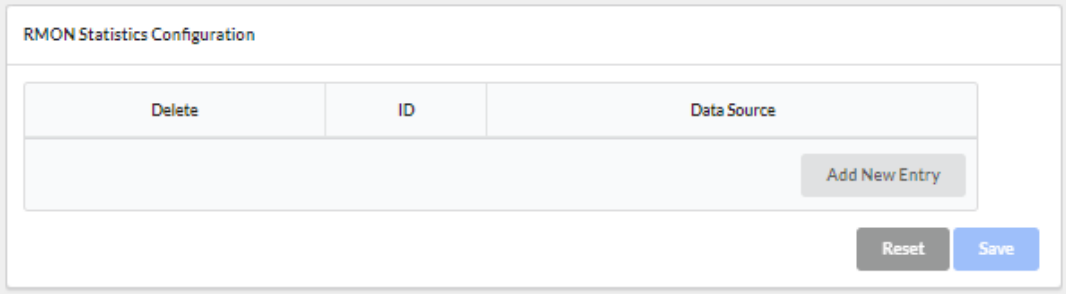
Add New Entry

Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
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.
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 32, 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 32, and the allowed content is ASCII characters from 33 to 126.

4.5.3 RMON

4.5.3.1 Statistics

Configure RMON Statistics table on this page. The entry index key is **ID**.

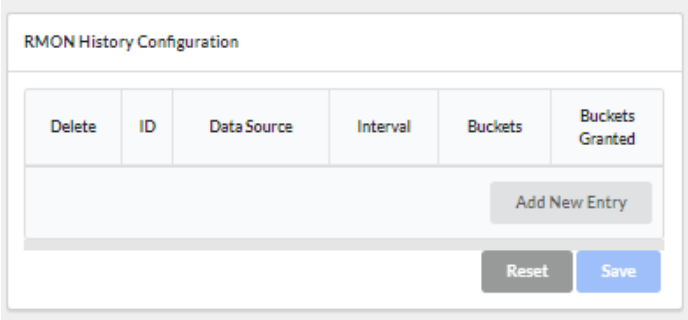


Add New Entry

Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
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 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005.

4.5.3.2 History

RMON History Table. The entry index key is **ID**.

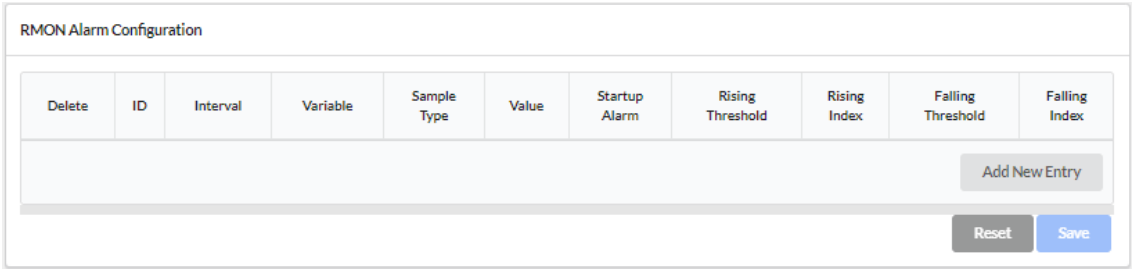


Add New Entry

Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
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 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005.
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 with 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.

4.5.3.3 Alarm

Configure RMON Alarm table on this page. The entry index key is **ID**.



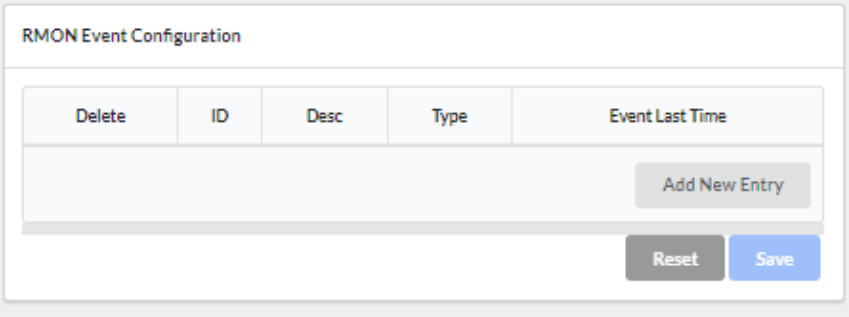
Add New Entry

Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
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 unicast packets delivered to a higher-layer protocol. • **InNUcastPkts:** The number of broad-cast and multicast packets delivered to a higher-layer protocol. • **InDiscards:** The number of inbound packets that are discarded even if 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 unicast packets that request to transmit. • **OutNUcastPkts:** The number of broad-cast and multicast packets that request to transmit. • **OutDiscards:** The number of outbound packets that are discarded even if the packets are normal. • **OutErrors:** 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: • **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. • **RisingOrFalling:** Trigger 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).

4.5.3.4 Event

Configure RMON Event table on this page. The entry index key is **ID**.



Add New Entry

Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
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. **snmptrap:** Send SNMP trap when the event is triggered. **logandtrap:** Create SNMP log entry and send SNMP trap when the event is triggered.

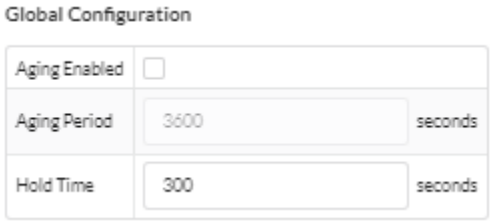
Event Last Time	Indicates the value of sysUpTime at the time this event entry last generated an event.

4.6 Network

4.6.1 Port Security

Port Security configuration of global and per-port.

Port Security allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Port Security is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken depending on violation mode. The violation mode can be one of the four differences described below.

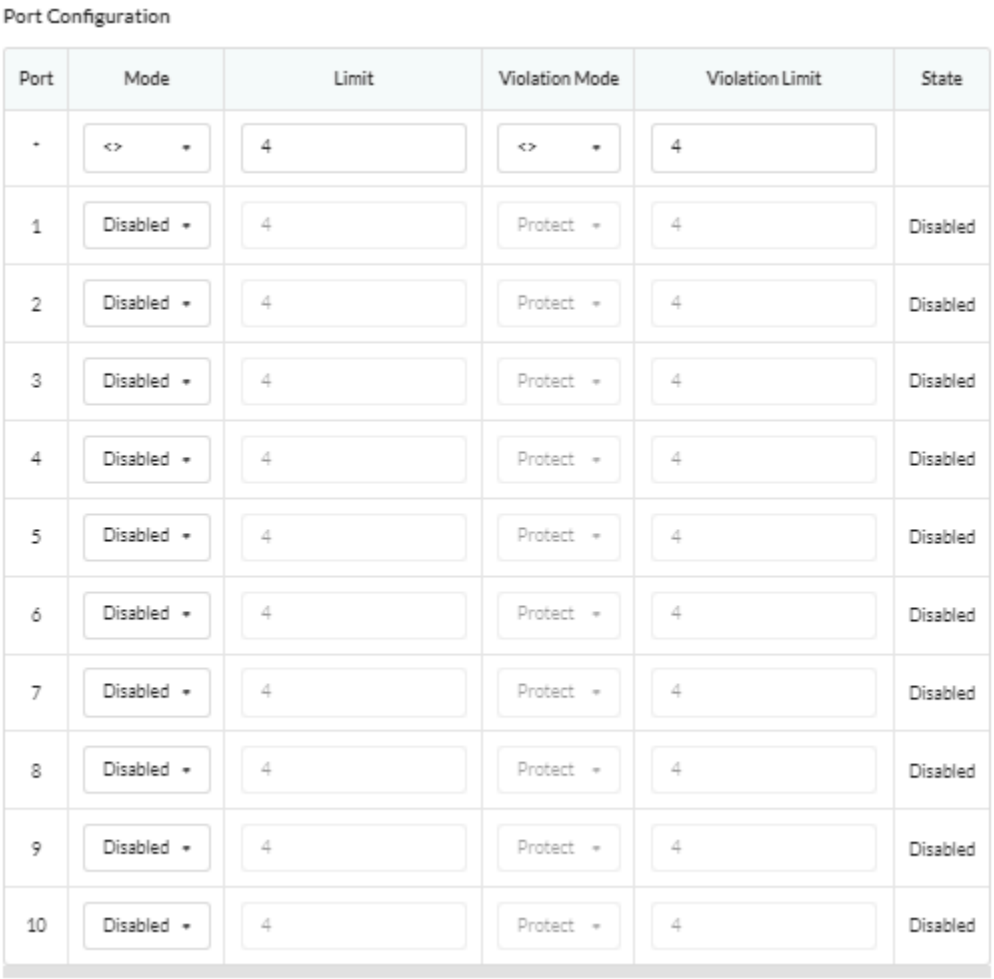


Global Configuration

Setting	Description
Aging Enabled	If checked, secured MAC addresses are subject to aging as discussed under Aging Period.
Aging Period	If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying functionality for securing MAC addresses, they may have other requirements to the aging period. The underlying functionality will use the shorter requested aging period of all modules that have aging enabled. The Aging Period can be set to a number between 10 and 10000000 seconds with a default of 3600 seconds. To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Port Security is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Hold Time	The hold time - measured in seconds - is used to determine how long a MAC address is held in the MAC table if it has been found to violate the limit. Valid range is between 10 and 10000000 seconds with a default of 300 seconds. The reason for holding a violating MAC address in the MAC table is primarily to ensure that the same MAC address doesn't give rise to continuous notifications (if notifications on violation count is enabled).

Port Configuration



Setting	Description
Port	The port number to which the configuration below applies.
Mode	Controls whether Port Security is enabled on this port. Notice that other modules may still use the underlying port security features without enabling Port Security on a given port.
Limit	The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1023. Default is 4. If the limit is exceeded, an action is taken corresponding to the violation mode.

	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.
Violation Mode	If Limit is reached, the switch can take one of the following actions: **Protect**: Do not allow more than Limit MAC addresses on the port, but take no further action. **Restrict**: If Limit is reached, subsequent MAC addresses on the port will be counted and marked as violating. Such MAC addresses are removed from the MAC table when the hold time expires. At most Violation Limit MAC addresses can be marked as violating at any given time. **Shutdown**: If Limit is reached, one additional MAC address will cause the port to be shut down. This implies that all secured MAC addresses be removed from the port, and no new addresses be learned. There are three ways to re-open the port: 1) In the "Configuration→Ports" page's "Configured" column, first disable the port, then restore the original mode. 2) Make a Port Security configuration change on the port. 3) Boot the switch.
Violation Limit	The maximum number of MAC addresses that can be marked as violating this port. This number cannot exceed 1023. Default is 4. It is only used when Violation Mode is **Restricted**.
State	This column shows the current Port Security state of the port. The state takes one of four values: **Disabled**: Port Security is disabled on the port. **Ready**: The limit is not yet reached. This can be shown for all violation modes. **Limit Reached**: Indicates that the limit is reached on this port. This can be shown for all violation modes. **Shutdown**: Indicates that the port is shut down by Port Security. This state can only be shown if violation mode is set to **Shutdown**.

4.6.2 NAS

Network Access Server Configuration

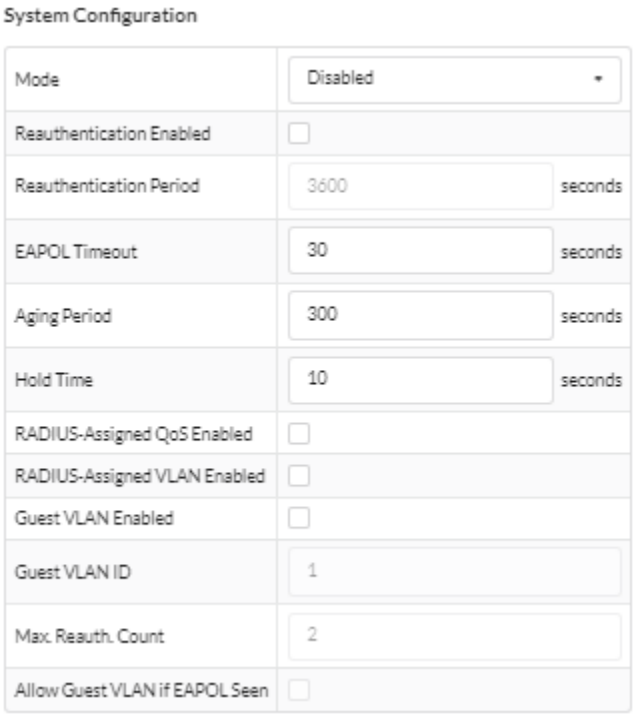
This page allows you to configure the IEEE 802.1X and MAC-based authentication system and port settings.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the "Configuration→Security→AAA" page. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.

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

The NAS configuration consists of two sections, a system- and a port-wide

System Configuration



Setting	Description
Mode	Indicates if NAS 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 re-authenticated 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 re-authenticated. This is only active if the Re-authentication 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.
Aging Period	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: • **Single 802.1X** • **Multi 802.1X** • **MAC-Based Auth.** When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds. If re-authentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries. For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.
Hold Time	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: • **Single 802.1X** • **Multi 802.1X** • **MAC-Based Auth.** If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request timed out (according to the timeout specified on the **Configuration > Security > AAA** page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication. In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time. The Hold Time can be set to a number between 10 and 1000000 seconds
RADIUS-Assigned QoS Enabled	RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this

	feature (see RADIUS-Assigned QoS Enabled below for a detailed description). The RADIUS-Assigned QoS Enabled checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto settings determine whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.
RADIUS-Assigned VLAN Enabled	RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see **RADIUS-Assigned VLAN Enabled** below for a detailed description). The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto settings determine whether RADIUS-assigned VLAN is enabled on that port. When unchecked, the RADIUS-server assigned VLAN is disabled on all 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; 4095].
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 is globally enabled.

Port Configuration

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart
*	<>	☐	☐	☐		
1	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate Reinitialize
2	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate Reinitialize
3	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate Reinitialize
4	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate Reinitialize
5	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate Reinitialize
6	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate Reinitialize
7	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate Reinitialize
8	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate Reinitialize
9	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate Reinitialize
10	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate Reinitialize

Admin State

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

	Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.
Multi 802.1X	Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module. In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port. The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.
MAC-based Auth.	Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as a separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly. When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

	The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

RADIUS-Assigned QoS Enabled

When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).
This option is only available for single-client modes, i.e.

- **Port-based 802.1X**
- **Single 802.1X**

RADIUS attributes used in identifying a QoS Class:
The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet.
Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:

- All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '7', which translates into the desired QoS Class in the range [0; 7].

RADIUS-Assigned VLAN Enabled

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

- **Port-based 802.1X**
- **Single 802.1X**

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.

RADIUS attributes used in identifying a VLAN ID:
RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:

- The **Tunnel-Medium-Type, Tunnel-Type**, and **Tunnel-Private-Group-ID** attributes must all be present at least once in the Access-Accept packet.
- The switch looks for the first set of these attributes that have the same **Tag** value and fulfill the following requirements (if Tag == 0 is used, the **Tunnel-Private-Group-ID** does not need to include a Tag):
    - Value of **Tunnel-Medium-Type** must be set to IEEE-802.
    - Value of **Tunnel-Type** must be set to **VLAN**.
    - Value of **Tunnel-Private-Group-ID** must be a string of ASCII chars in the range **0 ~ 9**, which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].

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:** NAS is globally disabled.
- **Link Down:** NAS 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.

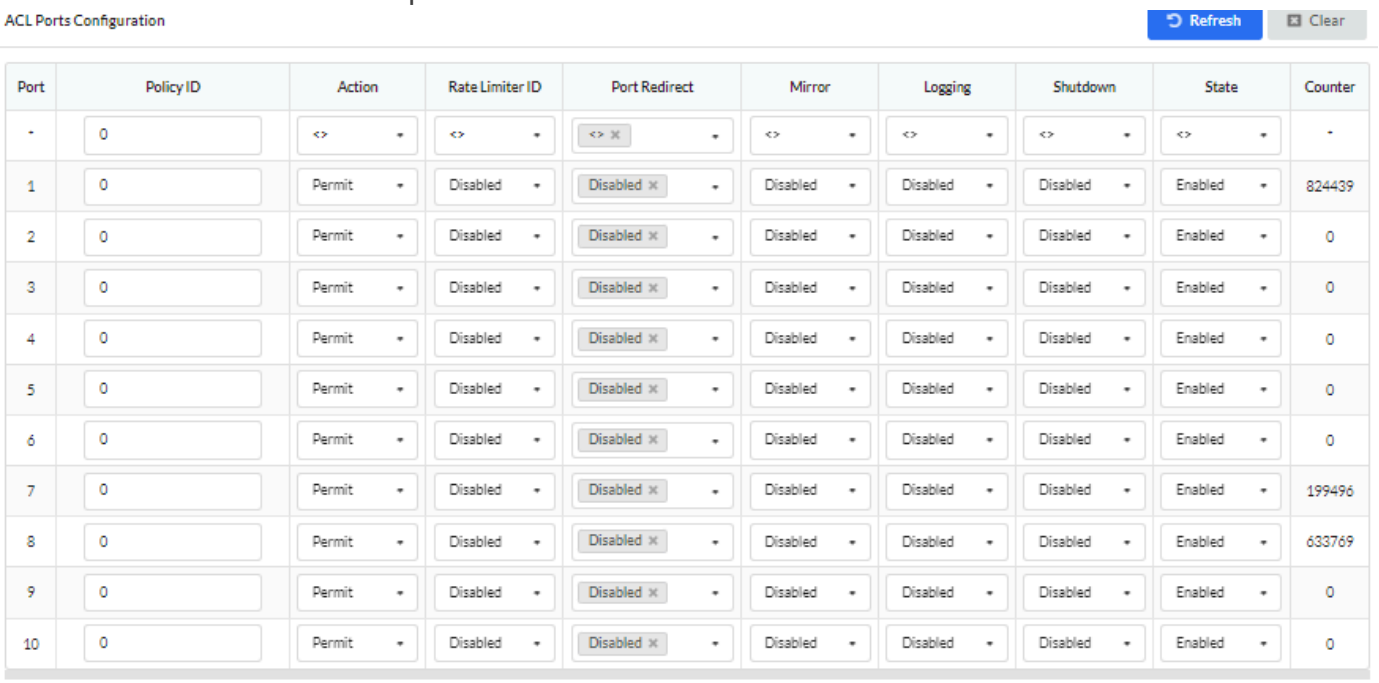
- **Reauthenticate:** Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.
- **Reinitialize:** Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

4.6.3 ACL

4.6.3.1 Ports

ACL Port Configuration

Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.



Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	<>	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	824439
2	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	199496
8	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	633769
9	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
10	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0

Port

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

Policy ID

Setting	Description	Factory Default
0~255	Select the policy to apply to this port. The allowed values are **0** through **255**.	0

Action

Setting	Description	Factory Default
Permit	Forwarding is permitted.	Permit
Deny	Forwarding is denied.	

Rate Limiter ID

Setting	Description	Factory Default
Disabled	Rate Limiter is disabled.	Disabled
1~16	Select which rate limiter to apply on this port.	

Port Redirect

Setting	Description	Factory Default
Disabled	Port Redirect is disabled.	Disabled
Port X	Select which port frames are redirected on.	

Mirror

Setting	Description	Factory Default
Disabled	Frames received on the port are not mirrored.	Disabled
Enabled	Frames received on the port are mirrored.	

Logging

Specify the logging operation of this port. Notice that the logging message doesn't include the 4 bytes CRC.

Setting	Description	Factory Default
Disabled	Frames received on the port are not logged.	Disabled
Enabled	Frames received on the port are stored in the System Log.	

NOTE: The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited.

Shutdown

Setting	Description	Factory Default
Disabled	Port shutdown is disabled.	Disabled
Enabled	If a frame is received on the port, the port will be disabled.	

NOTE: The shutdown feature only works when the packet length is less than 1518(without VLAN tags).

State

Setting	Description	Factory Default
Disabled	To close ports by changing the volatile port configuration of the ACL user module.	Enabled
Enabled	To reopen ports by changing the volatile port configuration of the ACL user module.	

Counter

Counts the number of frames that match this ACE.

4.6.3.2 Rate Limiters

ACL Rate Limiter Configuration

ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
*		<>
1	1	pps
2	1	pps
3	1	pps
4	1	pps
5	1	pps
6	1	pps
7	1	pps
8	1	pps
9	1	pps
10	1	pps
11	1	pps
12	1	pps
13	1	pps
14	1	pps
15	1	pps
16	1	pps

Rate

Setting	Description	Factory Default
0-3276700	The valid rate is 0-3276700in pps. or 0, 100, 200, 300, ..., 1000000 in kbps	1

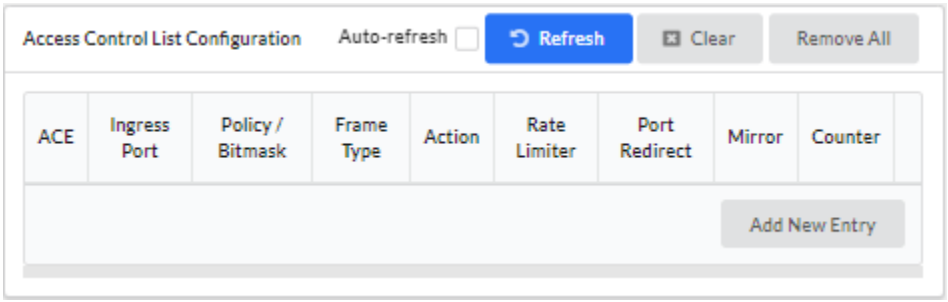
Unit

Setting	Description	Factory Default
pps	packets per second	pps
kbps	Kbits per second.	

4.6.3.3 Access Control List

Access Control List Configuration

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 and the priority is highest.



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

Setting	Description	Factory Default
All	The ACE applies to all ports.	All
Port n	The ACE applies to this port number, where n is the number of the switch port.	

Policy Filter

Setting	Description	Factory Default
Any	No policy filter is specified.	Any
Specific	If you want to filter a specific policy with this ACE, choose this value. Two fields for entering a policy value and bitmask appear.	

Policy Value

Setting	Description	Factory Default

0~255	When **Specific** is selected for the policy filter, you can enter a specific policy value. The allowed range is 0 to 255.	0

Policy Bitmask

Setting	Description	Factory Default
0x0 ~ 0xff	When **Specific** is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is 0x0 to 0xff. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [policy_value & policy_bitmask]. For example, if the policy value is 3 and the policy bitmask is 0x10(bit 0 is "don't-care" bit), then policy 2 and 3 are applied to this rule.	0xff

Frame Type

Select the frame type for this ACE. These frame types are mutually exclusive.

Setting	Description	Factory Default
Any	Any frame can match this ACE.	Any
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) and the value should not be equal to 0x800(IPv4), 0x806(ARP) or 0x86DD(IPv6).	
ARP	Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type.	
IPv4	Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type.	
IPv6	Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with Ethernet type.	

Action

Specify the action to take with a frame that hits this ACE.

Setting	Description	Factory Default
Permit	The frame that hits this ACE is granted permission for the ACE operation.	Permit
Deny	The frame that hits this ACE is dropped.	
Filter	Frames matching the ACE are filtered.	

Rate Limiter

Specify the rate limiter in the number of base units.

Setting	Description	Factory Default
Disabled	Rate limiter operation is disabled.	Disabled
1~16	Specify the rate limiter in the number of base units. The allowed range is 1 to 16.	

Port Redirect

Frames that hit the ACE are redirected to the port number specified here. The rate limiter will affect these ports. The allowed range is the same as the switch port number range. **Disabled** indicates that the port redirect operation is disabled and the specific port number of 'Port Redirect' can't be set when action is permitted.

Setting	Description	Factory Default
Disabled	Port redirect operation is disabled	Disabled
Enabled	Port redirect operation is enabled	

Mirror

Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The rate limiter will not affect frames on the mirror port.

Setting	Description	Factory Default
Enabled	Frames received on the port are mirrored.	Disabled
Disabled	Frames received on the port are not mirrored.	

Logging

Specify the logging operation of the ACE. Notice that the logging message doesn't include the 4 bytes CRC information.

Setting	Description	Factory Default
Enabled	Frames matching the ACE are stored in the System Log.	Disabled
Disabled	Frames matching the ACE are not logged.	

NOTE: The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited.

Shutdown

Setting	Description	Factory Default
Enabled	If a frame matches the ACE, the ingress port will be disabled.	Disabled
Disabled	Port shutdown is disabled for the ACE.	

NOTE: The shutdown feature only works when the packet length is less than 1518(without VLAN tags).

Counter

The counter indicates the number of times the ACE was hit by a frame.

VLAN Parameters

802.1Q Tagged

Setting	Description	Factory Default
Any	Any value is allowed.	Any
Enabled	Tagged frame only.	
Disabled	Untagged frame only.	

VLAN ID Filter

Setting	Description	Factory Default
Any	No VLAN ID filter is specified.	Any
Specific	If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.	

VLAN ID

Setting	Description	Factory Default
1~4095	When **Specific** is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.	1

Tag Priority

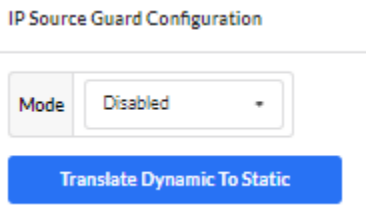
Setting	Description	Factory Default
Any	No tag priority is specified	Any
0~7, 0-1, 2-3, 4-5, 6-7,	Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority.	

0-3, 4-7		

4.6.4 IP Source Guard

4.6.4.1 Configuration

IP Source Guard Configuration

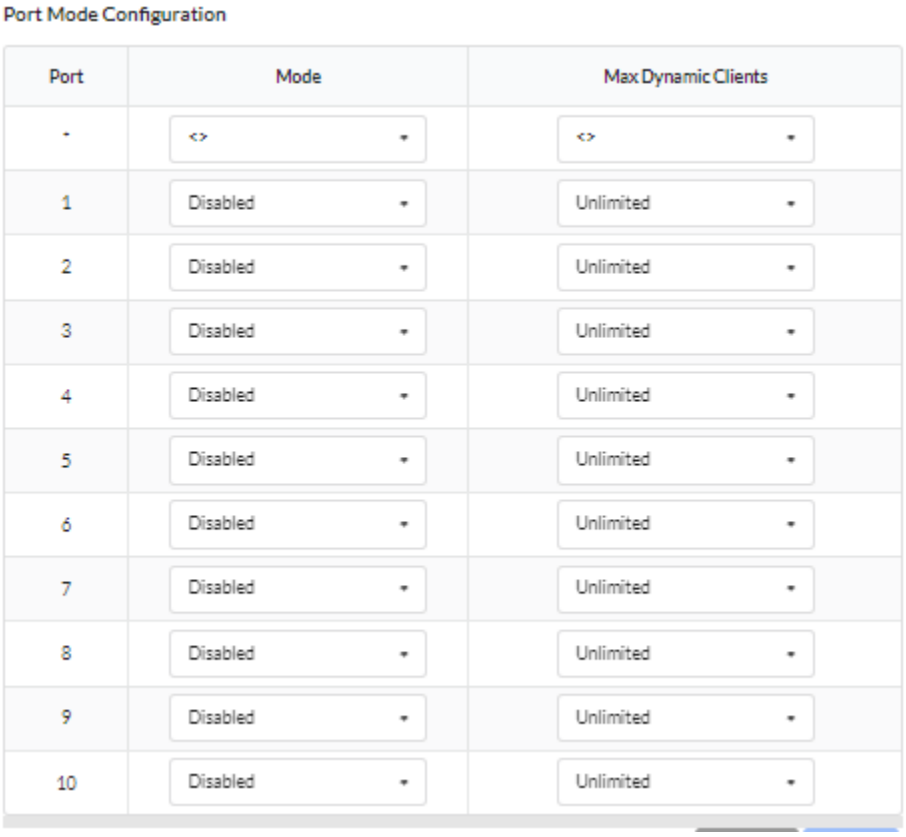


Mode

Setting	Description	Factory Default
Enabled	Enable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.	Disabled
Disabled	Disable the Global IP Source Guard.	

Translate dynamic to static button
Click to translate all dynamic entries to static entries.

Port Mode Configuration



Mode

Setting	Description	Factory Default
Enabled	Port Mode is enabled	Disabled
Disabled	Port Mode is disabled	

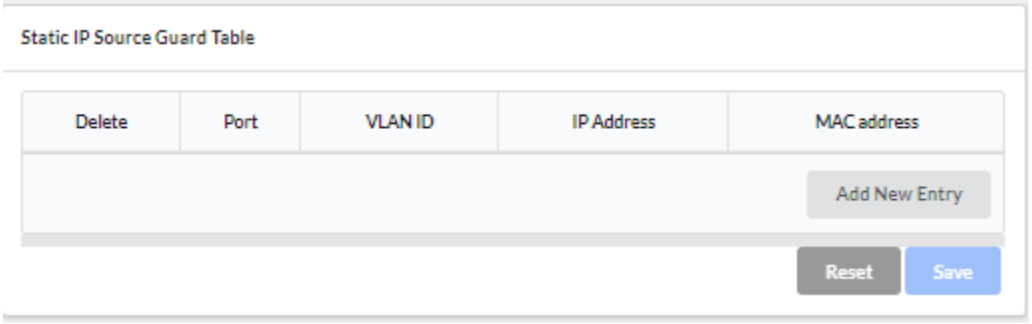
Max Dynamic Clients

Setting	Description	Factory Default
0,1,2,Unlimited	Specify the maximum number of dynamic clients that can be learned on a 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.	Unlimited

4.6.4.2 Static Table

Static IP Source Guard Table

Shows and adds the static IP Source Guard rules. The maximum number of rules is 112 on the switch.



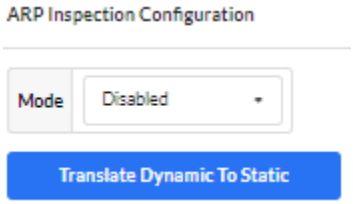
Add New Entry

Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Port	The logical port for the settings.
VLAN ID	The VLAN id for the settings.
IP Address	Allowed Source IP address.
MAC address	Allowed Source MAC address.

4.6.5 ARP Inspection

4.6.5.1 Port Configuration

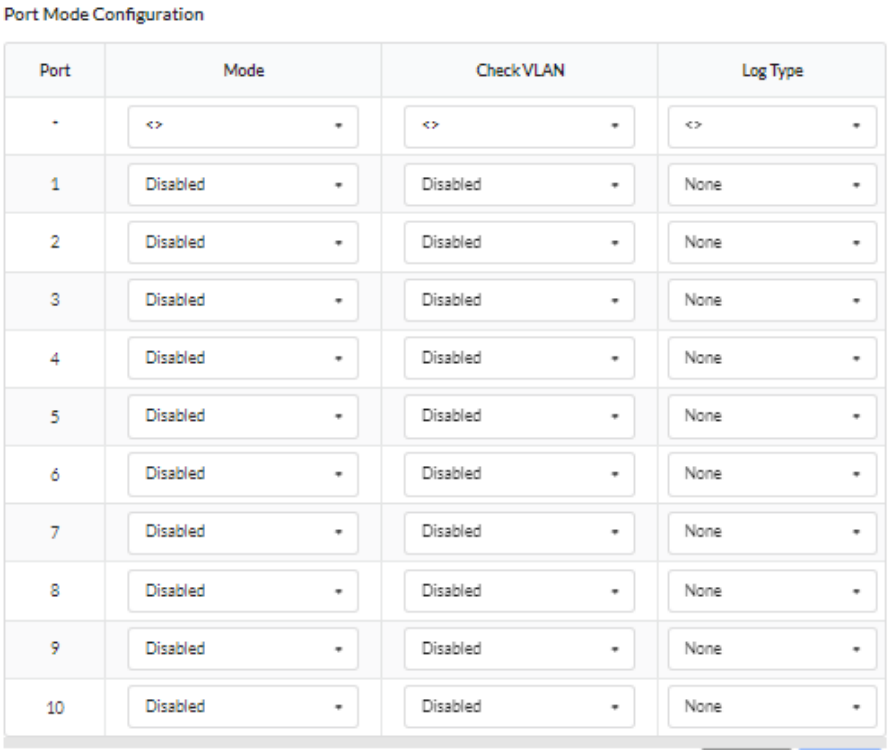
Mode of ARP Inspection Configuration



Setting	Description	Factory Default
Enabled	Enable the Global ARP Inspection	Disabled
Disable	Disable the Global ARP Inspection	

Translate dynamic to static button
Click to translate all dynamic entries to static entries.

Port Mode Configuration



Mode

Setting	Description	Factory Default
Enabled	Enable ARP Inspection operation.	Disabled
Disabled	Disable ARP Inspection operation.	

Check VLAN

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.

Setting	Description	Factory Default
Enabled	Enable check VLAN operation.	Disabled
Disabled	Disable check VLAN operation.	

Log Type

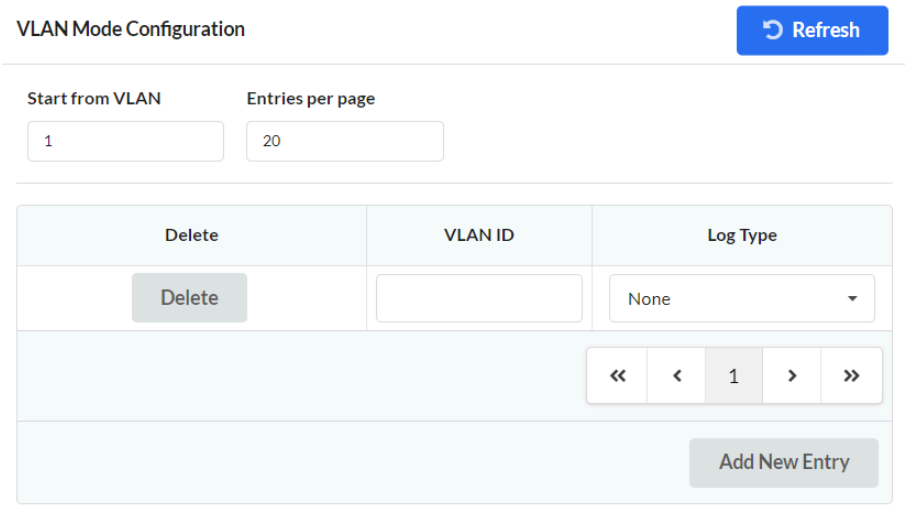
Only the Global Mode and Port Mode on a given port are enabled, and the setting of Check VLAN is disabled, the log type of ARP Inspection will refer to the port setting, the log type of ARP Inspection will refer to the port setting.

Setting	Description	Factory Default
None	Log nothing.	None
Deny	Log denied entries.	
Permit	Log permitted entries.	
ALL	Log all entries.	

4.6.5.2 VLAN Mode Configuration

Navigating the VLAN Configuration

Each 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.



VLAN Mode Configuration

Specify ARP Inspection is enabled on which VLANs. First, you have to enable the port setting on the 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.

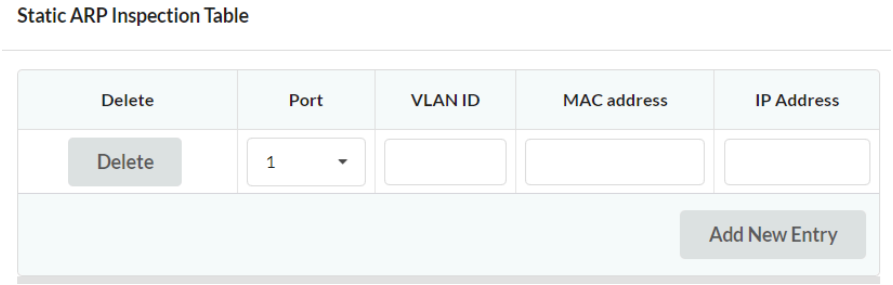
ADD New Entry

Setting	Description	Factory Default
None	Log nothing	None
Deny	Log denied entries	
Permit	Log permitted entries	
ALL	Log all entries	

4.6.5.3 Static Table

Static ARP Inspection Table

This page shows the static ARP Inspection rules. The maximum number of rules is 256 on the switch.



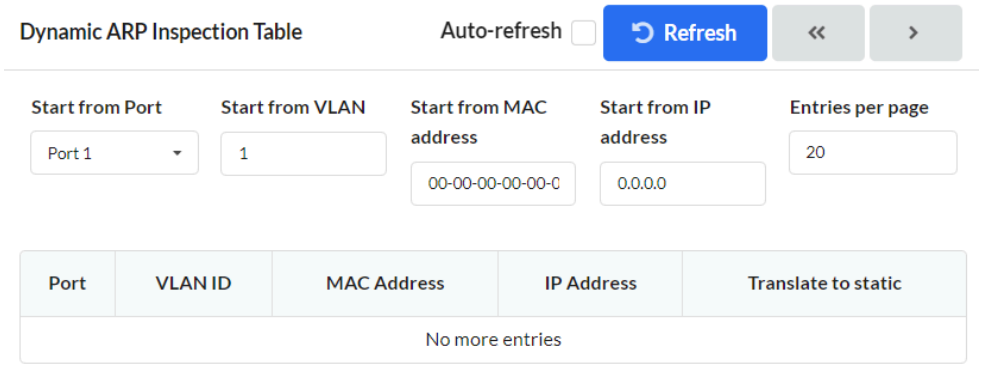
ADD New Entry

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

4.6.5.4 Dynamic Table

Dynamic ARP Inspection Table

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 256 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. All dynamic entries are learning from DHCP Snooping.



Navigating the ARP Inspection Table

Each page shows up to 99 entries from the Dynamic ARP Inspection 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 Dynamic ARP Inspection Table.
The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table.

ARP Inspection Table Columns

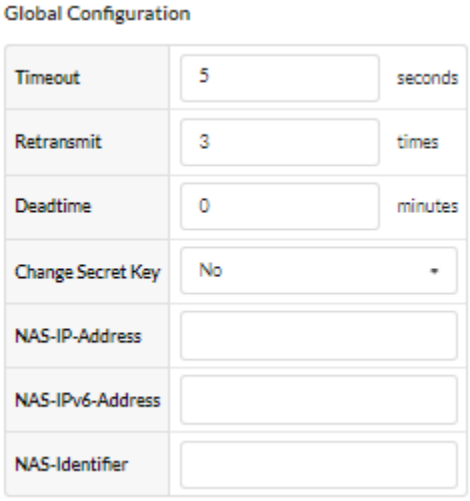
Setting	Description
Port	Switch Port Number for which the entries are displayed.
VLAN ID	VLAN-ID in which the ARP traffic is permitted.
IP Address	User IP address of the entry
Translated to static	Select the checkbox to translate the entry to static entry.

4.7 AAA

4.7.1 RADIUS

Global Configuration

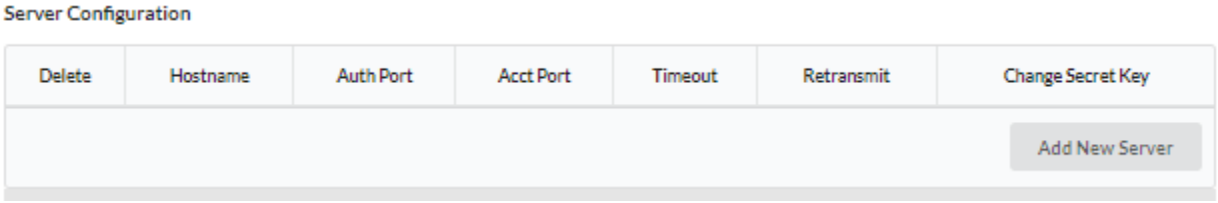
Allows you to configure up to 5 RADIUS servers.



Setting	Description	Factory Default
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.	5
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.	3
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.	0
Change Secret Key	Specify to change the secret key or not. When “Yes” is selected for the option, you can change the secret key - up to 63 characters long – shared between the RADIUS server and the switch.	No
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.	None
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.	None

NAS-Identifier	The identifier - up to 253 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.	None

Server Configuration



Add New Server Button

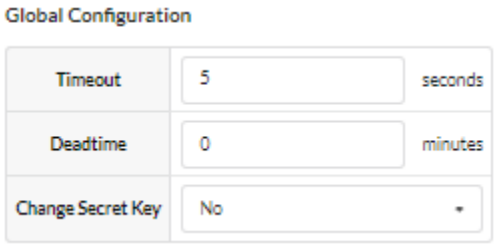
Click “Add New Server” button to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported.
The “Delete” button can be used to undo the addition of the new server.

Setting	Description
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. Set to 0 to disable authentication.
Acct Port	The UDP port to use on the RADIUS server for accounting. Set to 0 to disable 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.
Change Secret Key	Specify to change the secret key or not. When the checkbox is checked, you can change the setting overrides the global key. Leaving it blank will use the global key.

4.7.2 TACAS+

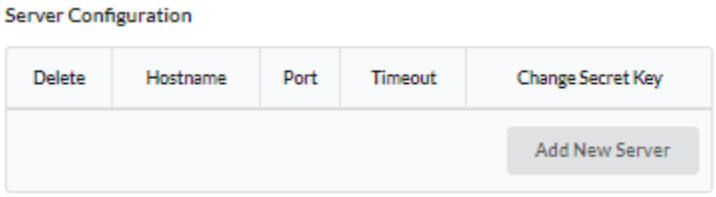
Allows to configure up to 5 TACAS servers

Global Configuration



Setting	Description
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.
Change Secret Key	Specify to change the secret key or not. When "Yes" is selected for the option, you can change the secret key - up to 63 characters long - shared between the TACACS+ server and the switch.

Server Configuration



Add New Server Button

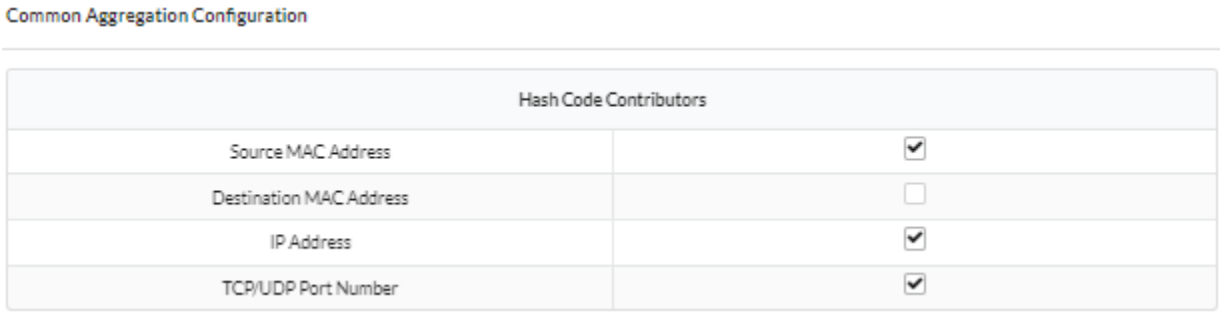
Click “Add New Server” button to add a new TACACS+ server. An empty row is added to the table, and the TACACS+ server can be configured as needed. Up to 5 servers are supported.
The “Delete” button can be used to undo the addition of the new server.

Setting	Description
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.

Change Secret Key	Specify to change the secret key or not. When the checkbox is checked, you can change the setting overrides the global key. Leaving it blank will use the global key.

4.8 Aggregation

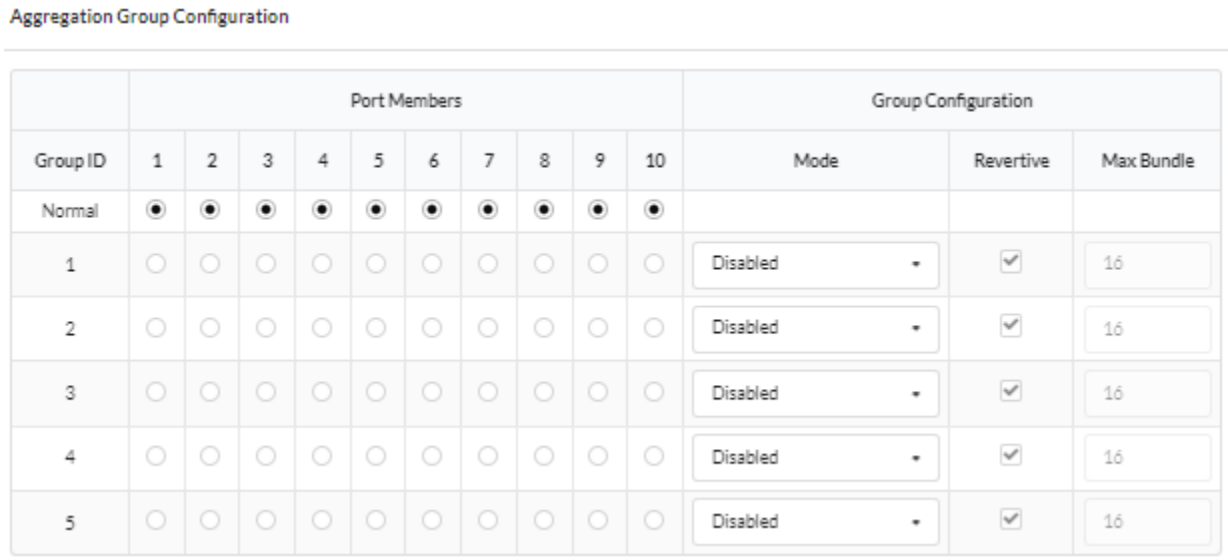
4.8.1 Common



Hash Code Contributors

Setting	Description	Factory Default
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	Enabled
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.	Disabled
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.	Enabled
TCP/UDP Port Number	The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable.	Enabled

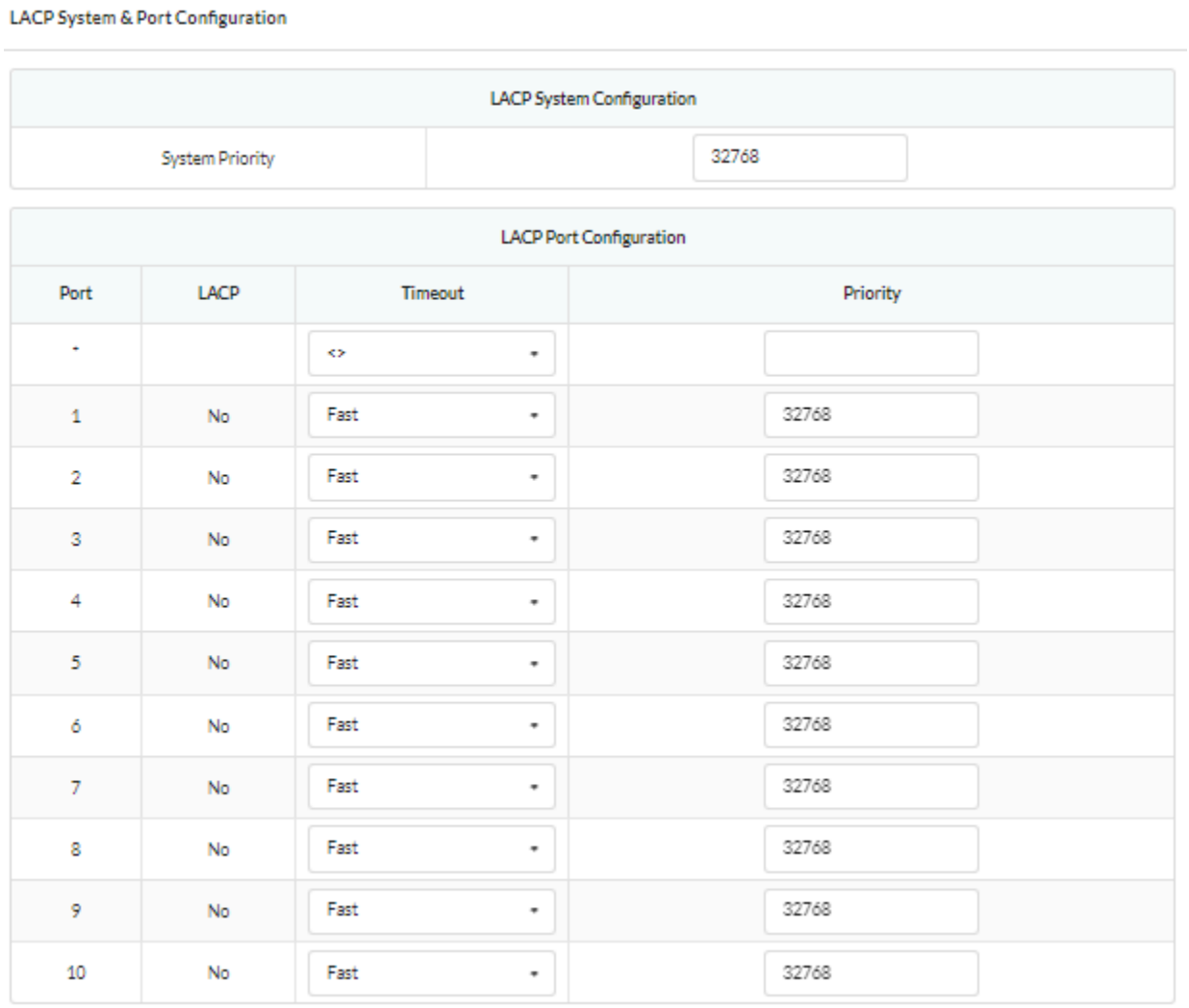
4.8.2 Groups



Setting	Description
Group ID	Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.
Port Members	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.
Mode	This parameter determines the mode for the aggregation group. ● **Disabled**: The group is disabled. ● **Static**: The group operates in static aggregation mode. ● **LACP (Active)**: The group operates in LACP active aggregation mode. See IEEE 801.AX-2014, section 6.4.1 for details. ● **LACP (Passive)**: The group operates in LACP passive aggregation mode. See IEEE 801.AX-2014, section 6.4.1 for details.
Revertive	This parameter only applies to LACP-enabled groups. It determines if the group will perform automatic link (re-)calculation when links with higher priority become available.
Max Bundle	This parameter only applies to LACP-enabled groups. It determines the maximum number of active bundled LACP ports allowed in an aggregation.

4.8.3 LACP

Inspect the current LACP port configurations, and change them as well.



Setting	Description
Port	The switch port number.
LACP	Show whether LACP is currently enabled on this switch port.
Timeout	The **Timeout** controls the period between BPDU transmissions. **Fast** will transmit LACP packets each second, while **Slow** will wait for 30 seconds before sending a LACP packet.
Priority	The **Priority** controls the priority of the port, range 1-65535. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.

4.9 Loop Protection

Loop Protection Configuration

Allows to inspect the current Loop Protection Configurations, and change them as well.

Loop Protection Configuration

General Settings

Global Configuration	
Enable Loop Protection	Disable
Transmission Time	5 seconds
Shutdown Time	180 seconds

Port Configuration

Port	Enable	Action	Tx Mode
*	☐	<>	<>
1	☑	Shutdown Port	Enable
2	☑	Shutdown Port	Enable
3	☑	Shutdown Port	Enable
4	☑	Shutdown Port	Enable
5	☑	Shutdown Port	Enable
6	☑	Shutdown Port	Enable
7	☑	Shutdown Port	Enable
8	☑	Shutdown Port	Enable
9	☑	Shutdown Port	Enable
10	☑	Shutdown Port	Enable

General Settings

Setting	Description	Factory Default
Enable Loop Protection	Controls whether loop protections are enabled (as a whole).	Disabled
Transmission Time	The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds.	5
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 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until the next device restart).	180

Port Configuration

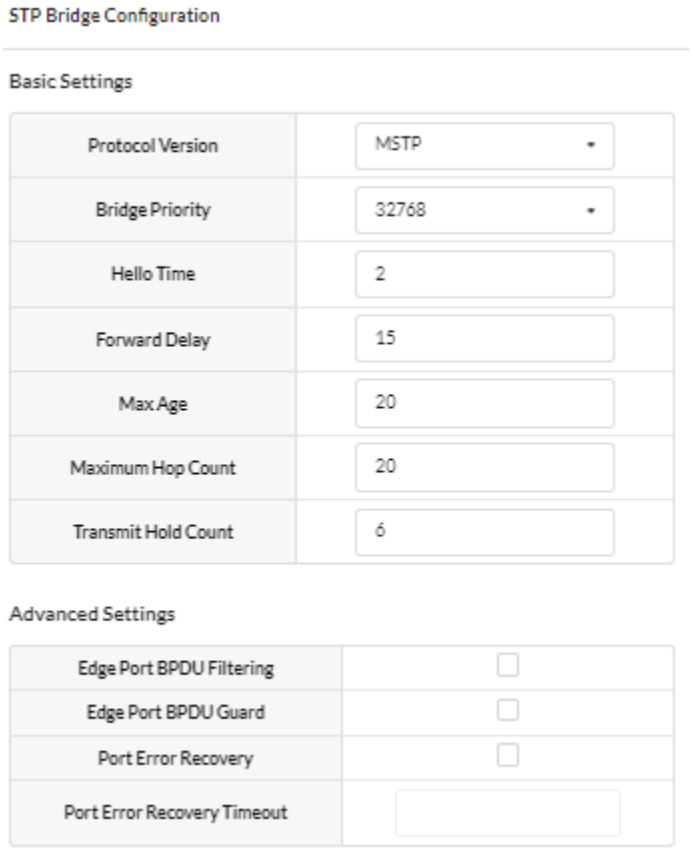
Setting	Description	Factory Default
Port	The switch port number of the port.	-
Enable	Controls whether loop protection is enabled on this switch port.	Enable
Action	Configures the action performed when a loop is detected on a port. Valid values are **Shutdown Port**, **Shutdown Port and Log** or **Log Only**.	Shutdown Port
Tx Mode	Controls whether the port is actively generating loop protection PDUs, or whether it is just passively looking for looped PDUs.	Enable

4.10 Spanning Tree

4.10.1 Bridge Settings

STP Bridge Configuration

Allows you to configure STP system settings. The settings are used by all STP Bridge instances in the Switch .



Basic Settings

Setting	Description	Factory Default
Protocol Version	The MSTP / RSTP / STP protocol version setting. Valid values are **STP**, **RSTP** and **MSTP**.	MSTP
Bridge Priority	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For **MSTP** operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.	32768
Hello Time	The interval between sending STP BPDU's. Valid values are in the range 1 to 10 seconds. **NOTE:** Changing this parameter from the default value is not recommended, and may have adverse effects on your network.	2

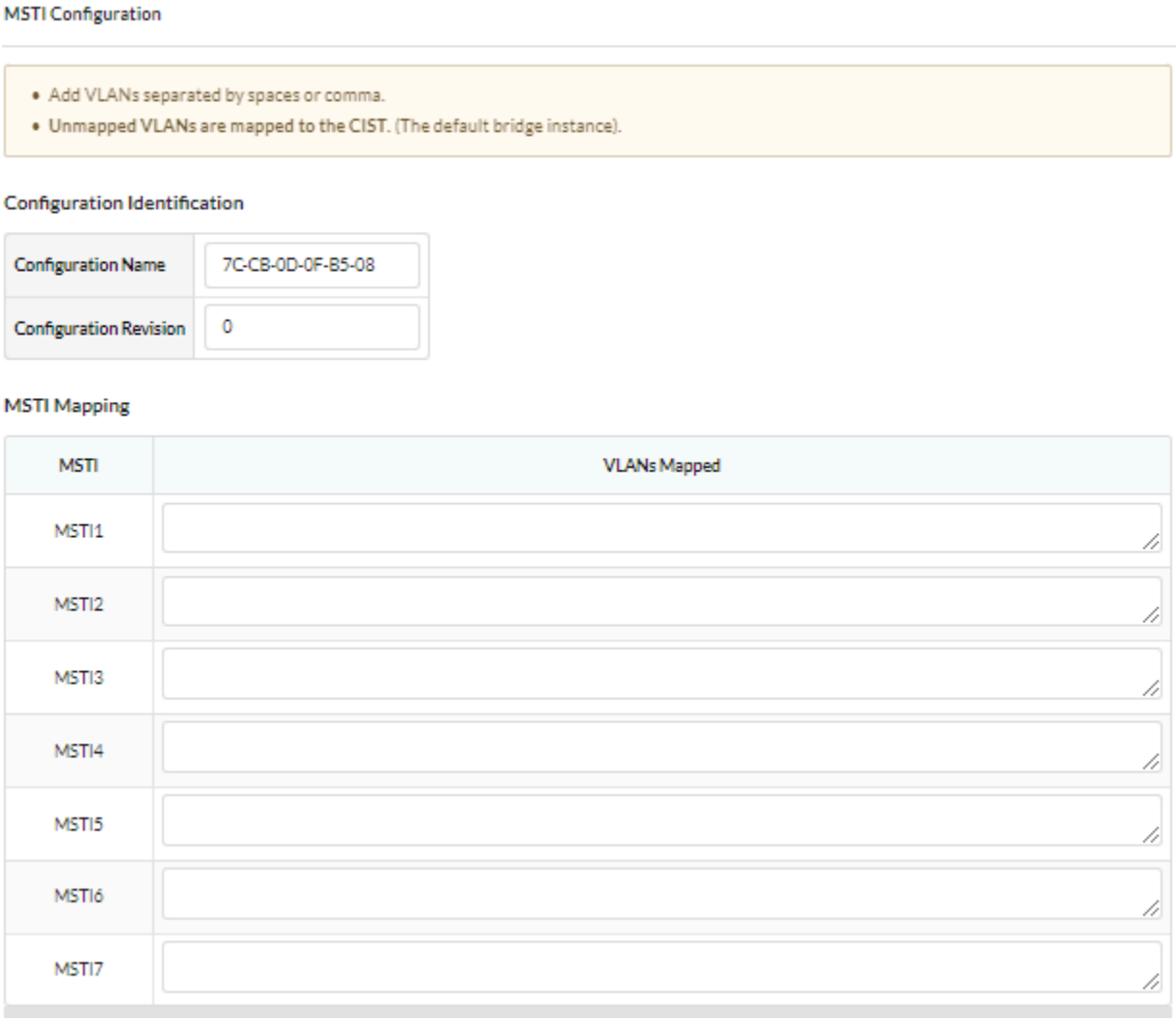
Forward Delay	The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.	15
Max Age	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.	20
Maximum Hop Count	This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.	20
Transmit Hold Count	The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.	6

Advanced Settings

Setting	Description
Edge Port BPDU Filtering	Control whether a port explicitly configured as **Edge** will transmit and receive BPDUs.
Edge Port BPDU Guard	Control whether a port explicitly configured as **Edge** will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.
Port Error Recovery	Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.
Port Error Recovery Timeout	The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

4.10.2 MSTI Mapping

MSTI Configuration



Configuration Identification

Setting	Description
Configuration Name	The name identifies 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 MISTI'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.

MSTI Mapping

Setting	Description
MSTI	The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.

VLANs Mapped	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**.

4.10.3 MSTI Priorities

Inspect the current STP MSTI bridge instance priority configurations, change them as well.

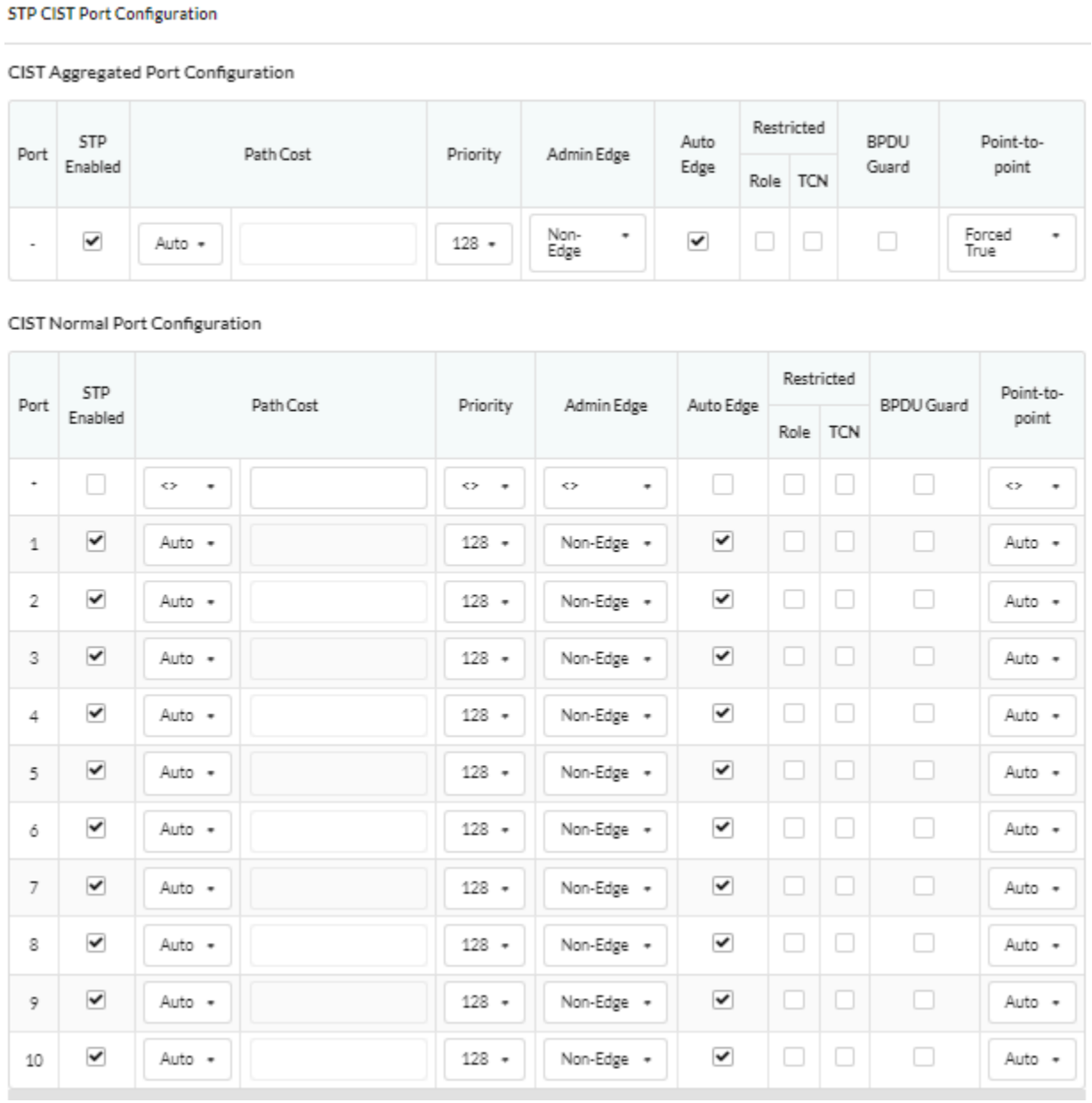


MSTI Priority Configuration

Setting	Description
MSTI	The bridge instance. The CIST is the default instance, which is always active.
Priority	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

4.10.4 CIST Ports

Inspect the current STP CIST port configurations, and change them as well.



CIST Aggregated/ Normal Port Configuration

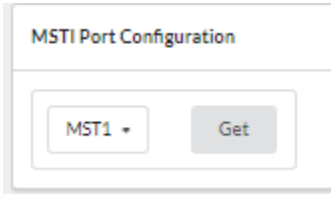
Setting	Description
Port	The switch port number of the logical STP port.
STP Enabled	Controls whether STP is enabled on this switch port.
Path Cost	Controls the path cost incurred by the port. The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the **Specific** setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost.

operEdge (state flag)	Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having operEdge true) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor > Spanning Tree > STP Detailed Bridge Status.
AdminEdge	Controls whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized).
AutoEdge	Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.
Restricted Role	If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause a lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.
Restricted TCN	If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.
BPDU Guard	If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port **Edge** status does not affect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.
Point-to-Point	Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

4.10.5 MSTI Ports

Inspect the current STP MSTI port configurations, and change them as well.

MSTI Port Configuration

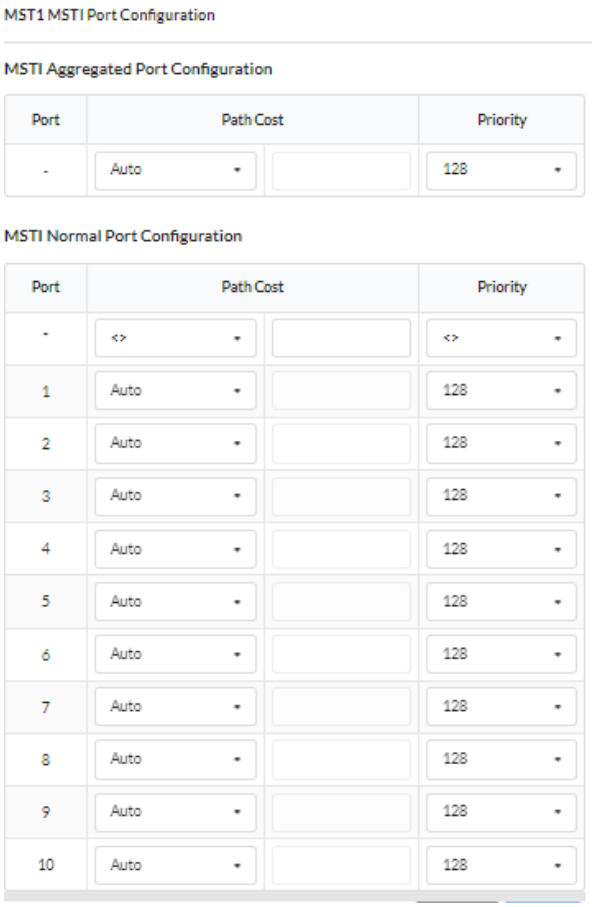


Select MSTI

Select **MSTI port number** and Click **"Get"** Button to configure.

(MSTn) MSTI Port Configuration

An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.



MSTI Aggregated/Normal Port Configuration

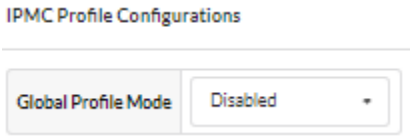
Setting	Description
Port	The switch port number of the corresponding STP CIST (and MSTI) port.
Path Cost	Controls the path cost incurred by the port. The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the **Specific** setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost.

4.11 IPMC Profile

4.11.1 Profile Table

IPMC Profile Configurations

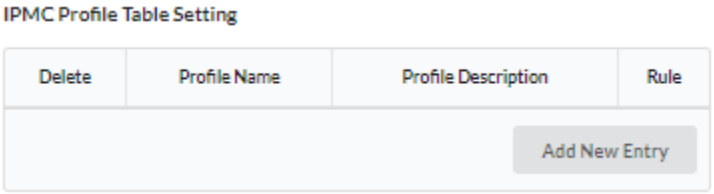
This page provides IPMC Profile related configurations.
The IPMC profile is used to deploy the access control on IP multicast streams. It is allowed to create at maximum 64 Profiles with at maximum 128 corresponding rules for each.



Global Profile Mode

Enable/Disable the Global IPMC Profile.

IPMC Profile Table Setting



Add New IPMC Profile button

Click to add a new IPMC profile. Specify the name and configure the new entry.

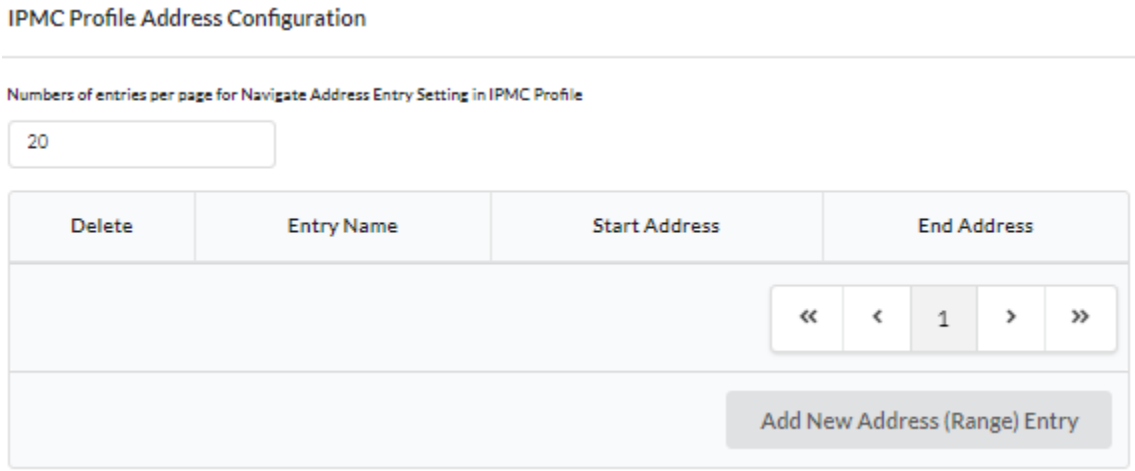
Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Profile Name	The name used for indexing the profile table. Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.

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 separate 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.

4.11.2 Address Entry

IPMC Profile Address Configuration

This page provides address range settings used in IPMC profiles.
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.



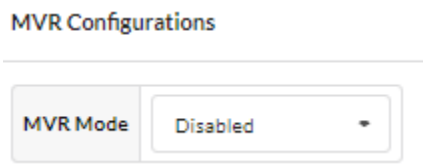
Add New Address (Range) Entry button

Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
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. At least one alphabet must be present.
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.

4.12 MVR

MVR Configurations

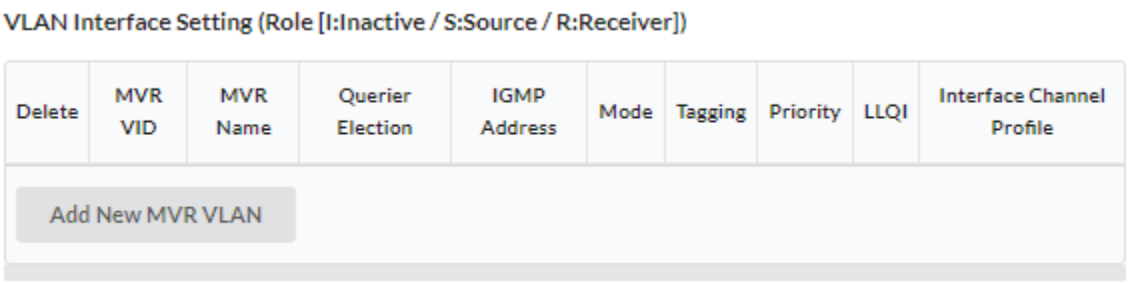
The MVR feature enables multicast traffic forwarding on the Multicast VLANs. In a multicast television application, a PC or a network television or a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP/MLD report message to Switch A to join the appropriate multicast group address. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.
The Querier should connect to the source port. By giving the static membership of MVR VLAN, the device only forwards the IGMP reports from downstream(receiver ports) to upstream(source ports) and the Query packet which comes from the downstream will be ignored silently.



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.

VLAN Interface Setting



Add New MVR VLAN button

Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
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 16. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.
Querier Election	Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.
IGMP Address	Define the IPv4 address as the 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, the system uses the IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, the system uses the first available IPv4 management address. Otherwise, the system uses a predefined 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 IPMC Profile as the channel filtering condition for the specific MVR VLAN. Summary about the Interface Channel Profiling (of the MVR VLAN) will be shown by clicking the view button. Profiles selected for designated interface channels are not allowed to have overlapped permit group addresses.
 **Profile Management Button**	List the rules associated with the designated profile.
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 in 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 Setting



Setting	Description	Factory Default

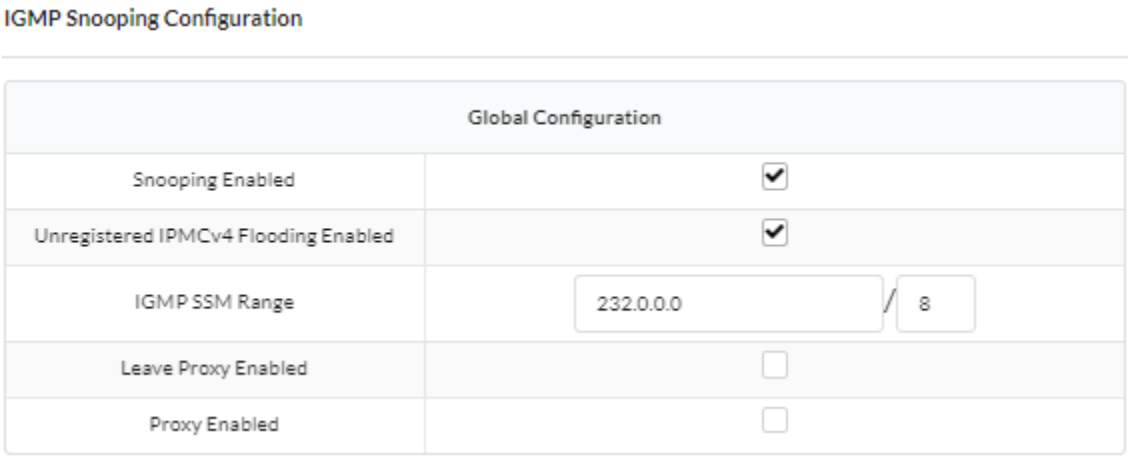
Enabled	Enable the fast leave on the port. System will remove group records and stop forwarding data upon receiving the IGMPc2/MLDv1 leave message without sending last member query messages. It is recommended to enable this feature only when a single IGMPv2/MLDv1 host is connected to the specific port.	Disabled
Disabled	Disable the fast leave on the port.	

4.13 IPMC

4.13.1 IGMP Snooping

4.13.1.1 Basic Configuration

IGMP Snooping Configuration



Global Configuration

Setting	Description
Snooping Enabled	Enable the Global IGMP Snooping.
Unregistered IPMCv4 Flooding Enabled	Enable unregistered IPMCv4 traffic flooding. The flooding control takes effect only when IGMP Snooping is enabled. When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting.
IGMP SSM Range	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers to run the SSM service model for the groups in the address range. Assign valid IPv4 multicast address as prefix with a prefix length (from 4 to 32) for the range.
Leave Proxy Enabled	Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
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

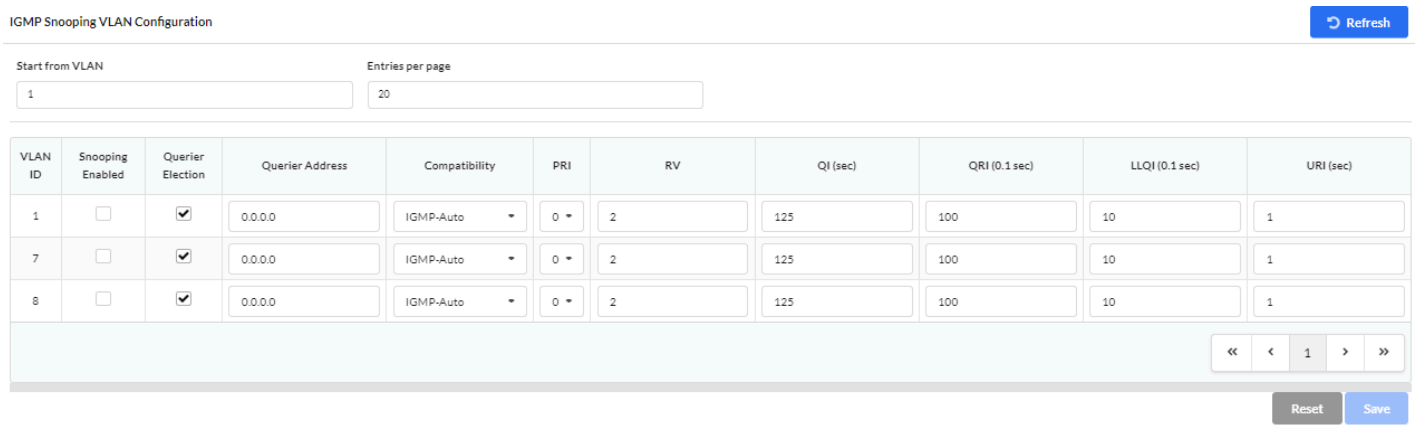
Port Related Configuration

Port	Router Port	Fast Leave	Throttling
-	☐	☐	<>
1	☐	☐	Unlimited
2	☐	☐	Unlimited
3	☐	☐	Unlimited
4	☐	☐	Unlimited
5	☐	☐	Unlimited
6	☐	☐	Unlimited
7	☐	☐	Unlimited
8	☐	☐	Unlimited
9	☐	☐	Unlimited
10	☐	☐	Unlimited

Setting	Description
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. System will remove group records and stop forwarding data upon receiving the IGMPv2 leave message without sending last member query messages. It is recommended to enable this feature only when a single IGMPv2 host is connected to the specific port.
Throttling	Enable to limit the number of multicast groups to which a switch port can belong.

4.13.1.2 VLAN Configuration

IGMP Snooping VLAN Configuration



Each 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.

Setting	Description
VLAN ID	The VLAN ID of the entry.
IGMP Snooping Enabled	Enable the per-VLAN IGMP Snooping. Up to 8 VLANs can be selected for IGMP Snooping.
Querier Election	Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non- Querier.
Querier Address	Define the IPv4 address as the source address used in IP header for IGMP Querier election. When the Querier address is not set, the system uses the IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, the system uses the first available IPv4 management address. Otherwise, the system uses a predefined value. By default, this value will be 192.0.2.1.
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.
PRI	Priority of Interface. It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is **0** (best effort) to **7** (highest), default interface priority value is 0.

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	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	Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response 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	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.

4.13.1.3 Port Filtering Profile

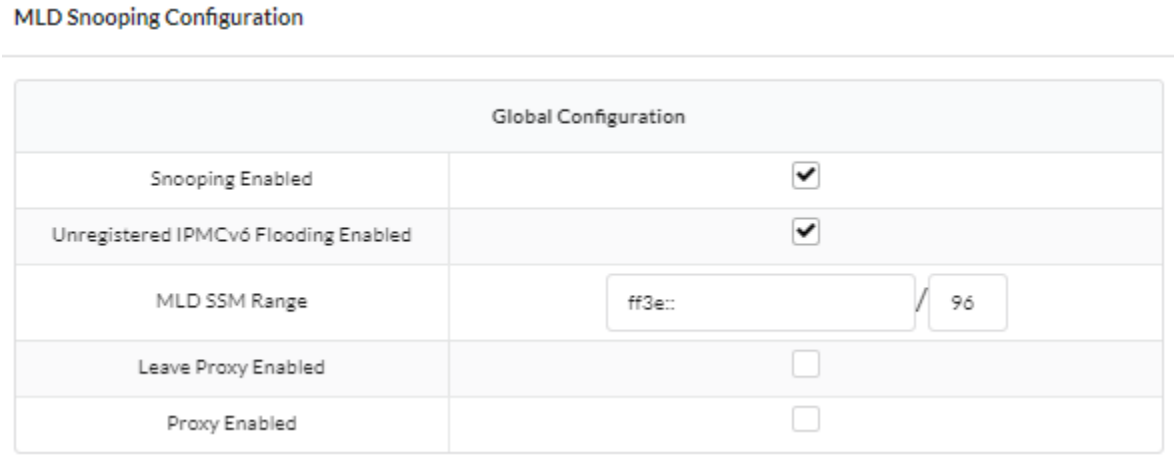
IGMP Snooping Port Filtering Profile Configuration



Setting	Description
Port	The logical port for the settings.
Filtering Profile	Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.
Profile Management Button	List the rules associated with the designated profile.

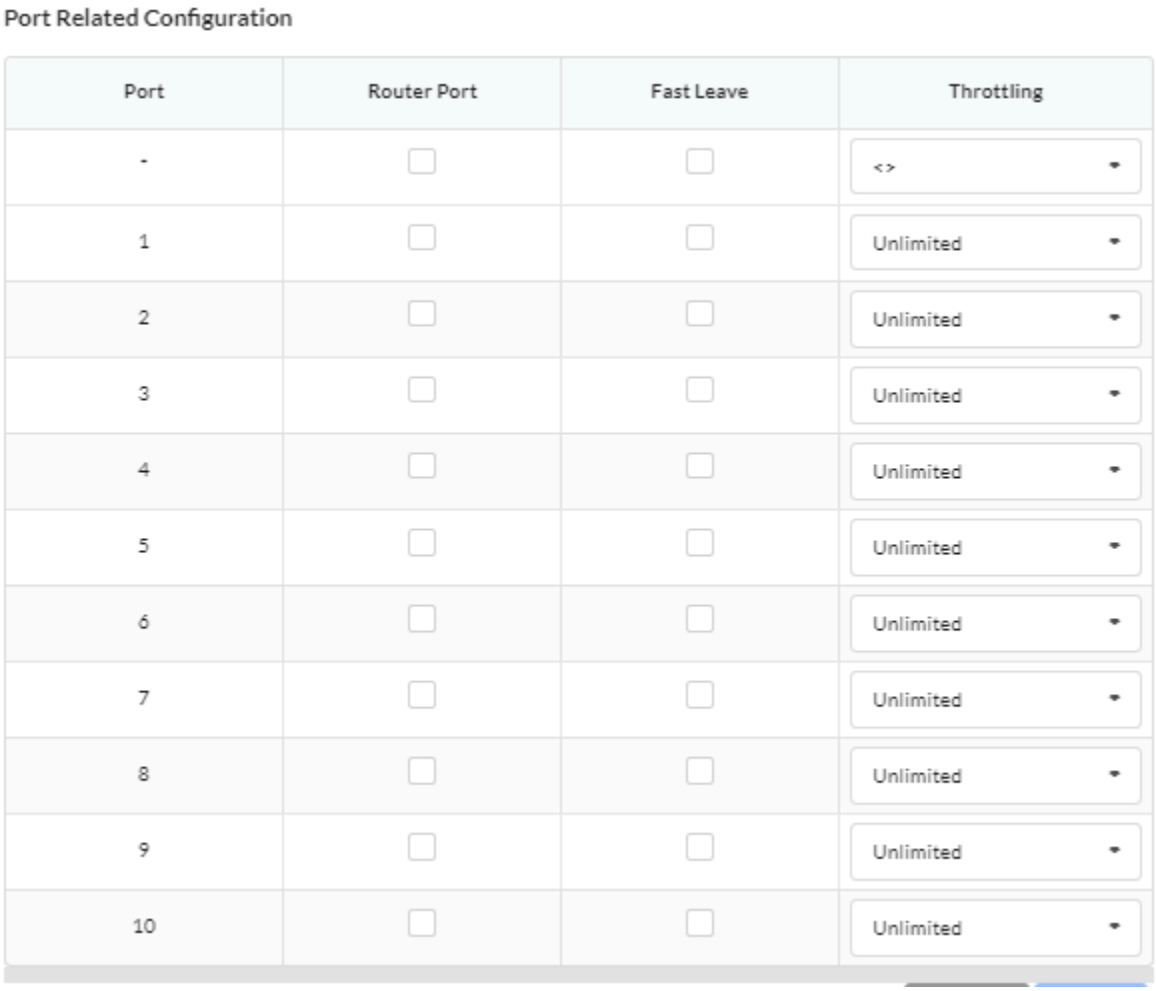
4.13.2 MLD Snooping

4.13.2.1 Basic Configuration



Global Configuration

Setting	Description
Snooping Enabled	Enable 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 to run the SSM service model for the groups in the address range. Assign valid IPv6 multicast address as prefix with a prefix length (from 8 to 128) for the range.
Leave Proxy Enabled	Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
Proxy Enabled	Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

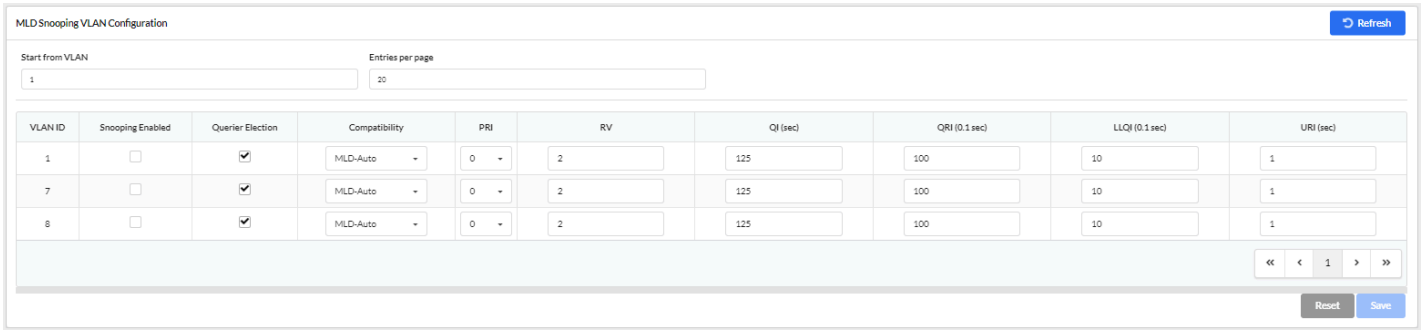


Port Related Configuration

Setting	Description
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	Enable the fast leave on the port. System will remove group records and stop forwarding data upon receiving the MLDv1 leave message without sending last member query messages. It is recommended to enable this feature only when a single MLDv1 host is connected to the specific port.
Throttling	Enable to limit the number of multicast groups to which a switch port can belong.

4.13.2.2 VLAN Configuration

Each 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.



Setting	Description
VLAN ID	The VLAN ID of the entry.
Snooping Enabled	Enable the per-VLAN MLD Snooping. Up to 8 VLANs can be selected for MLD Snooping.
Querier Election	Enable to join the MLD Querier election in the VLAN. Disable to act as a MLD Non- Querier.
Compatibility	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selection is **MLD-Auto**, **Forced MLDv1**, **Forced MLDv2**, default compatibility value is MLD-Auto.
PRI	Priority of Interface. It indicates the MLD control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is **0** (best effort) to **7** (highest), default interface priority value is 0.
RV	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a link. The allowed range is **1** to **255**, default robustness variable value is 2.
QI	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	Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response 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	Last Listener Query Interval. The Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done

	messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages. The allowed range is **0** to **31744** in tenths of seconds, default last listener query interval is 10 in tenths of seconds (1 second).
URI	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address. The allowed range is **0** to **31744** seconds, default unsolicited report interval is 1 second.

4.13.2.3 Port Filtering Profile



Setting	Description
Port	The logical port for the settings.
Filtering Profile	Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.
Profile Management Button	List the rules associated with the designated profile.

4.14 LLDP

4.14.1 LLDP Configuration

LLDP Parameters



Tx Interval

Setting	Description	Factory Default
5 ~ 32768	The switch periodically transmits LLDP frames to its neighbors 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.	30

Tx Hold

Setting	Description	Factory Default
2 ~ 10	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 **Texas Hold** multiplied by **Tx Interval** seconds. Valid values are restricted to 2 - 10 times.	4

Tx Delay

Setting	Description	Factory Default
1 ~ 8192	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.	2

Tx Reinit

Setting	Description	Factory Default

1 ~ 10	When an interface is disabled, LLDP is disabled or the switch is rebooted, a 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.	2

LLDP Interface Configuration

LLDP Interface Configuration

				Optional TLVs				
Interface	Mode	CDP aware	Trap	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☐	☐	☐	☐	☐	☐	☐
GigabitEthernet 1/1	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/2	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/3	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/4	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/5	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/6	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/7	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/8	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/9	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/10	Enabled	☐	☐	☑	☑	☑	☑	☑

Setting	Description
Interface	The switch interface name of the logical LLDP interface.
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 decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the interface 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' tables 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 interfaces have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one interface has CDP awareness enabled all CDP frames are terminated by the switch. **NOTE:** When CDP awareness on an interface is disabled the CDP information isn't removed immediately, but gets removed 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.

4.14.2 LLDP-MED

LLDP- MED Configuration

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

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 interface. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected in order to share LLDP-MED information as fast as possible to new neighbors.

Because there is a risk of an LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbors 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.

LLDP-MED Interface Configuration

It is possible to select which LLDP-MED information that shall be transmitted to the neighbors. When the checkbox is checked the information is included in the frame transmitted to the neighbor.

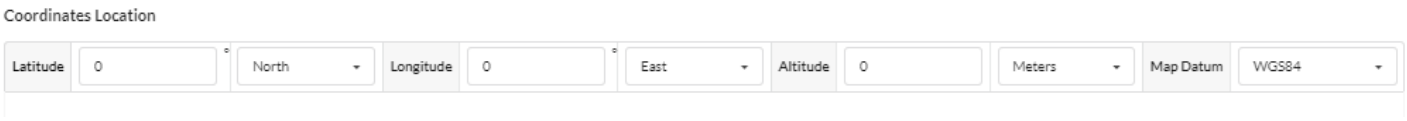
LLDP-MED Interface Configuration

	Transmit TLVs				
Interface	Capabilities	Policies	Location	PoE	Device Type
-	☐	☐	☐	☐	<>
GigabitEthernet 1/1	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/2	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/3	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/4	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/5	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/6	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/7	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/8	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/9	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/10	☑	☑	☑	☑	Connectivity

Setting	Description
Interface	The interface name to which the configuration applies.
Transmit TLVs - Capabilities	When checked the switch's capabilities are included in LLDP-MED information transmitted.
Transmit TLVs - Policies	When checked the configured policies for the interface are included in LLDP-MED information transmitted.
Transmit TLVs - Location	When checked the configured location information for the switch is included in LLDP-MED information transmitted.
Transmit TLVs - PoE	When checked the configured PoE (Power Over Ethernet) information for the interface is included in LLDP-MED information transmitted.
Device Type	Any LLDP-MED Device is operating as a specific type of LLDP-MED Device, which may be either a Network Connectivity Device or a specific Class of Endpoint Device, as defined below. A Network Connectivity Device is a LLDP-MED Device that provides 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 that can relay IEEE 802 frames via any method.

	An Endpoint Device is a LLDP-MED Device that sits at the network edge and provides some aspect of IP communications service, based on IEEE 802 LAN technology. The main difference between a Network Connectivity Device and an Endpoint Device is that only an Endpoint Device can start the LLDP-MED information exchange. Even though a switch always should be a Network Connectivity Device, it is possible to configure it to act as an Endpoint Device, and thereby start the LLDP-MED information exchange (In the case where two Network Connectivity Devices are connected together)

Coordinates Location



Setting	Description
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 4 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 -2097151.9 to 2097151.9 with a maximum of 1 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 Geodetic System 1984, CRS Code 4327, 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.

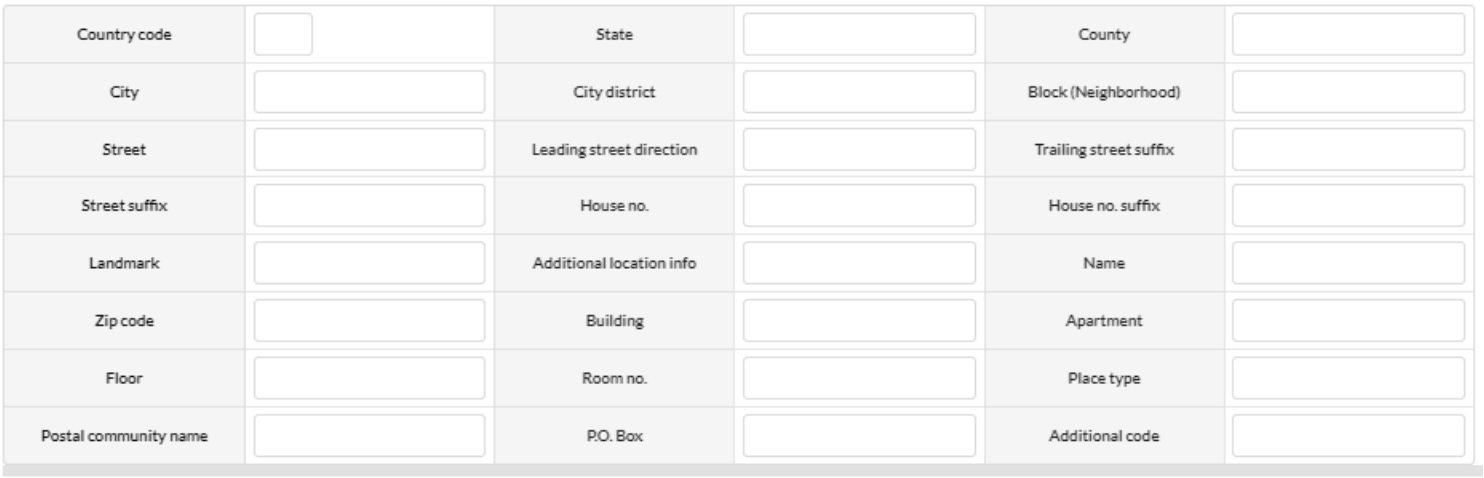
Civic Address Location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI). The total number of characters for the combined civic address information must not exceed 250 characters.

A couple of notes to the limitation of 250 characters.

1. A non-empty civic address location will use 2 extra characters in addition to the civic address location text.
2. The 2 letter country code is not part of the 250 characters limitation.

Civic Address Location

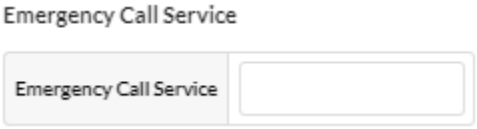


Setting	Description
Country code	The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.
State	National subdivisions (state, canton, region, province, prefecture).
County	County, parish, gun (Japan), district.
City	City, township, shi (Japan) - Example: Copenhagen.
City district	City division, borough, city district, ward, chou (Japan).
Block (Neighborhood)	Neighborhood, block.
Street	Street - Example: Poppelvej.
Leading street direction	Leading street direction - Example: N.
Trailing street suffix	Trailing street suffix - Example: SW.
Street suffix	Street suffix - Example: Ave, Platz.
House no.	House number - Example: 21.
House no. suffix	House number suffix - Example: A, 1/2.
Landmark	Landmark or vanity address - Example: Columbia University.
Additional 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	(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 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

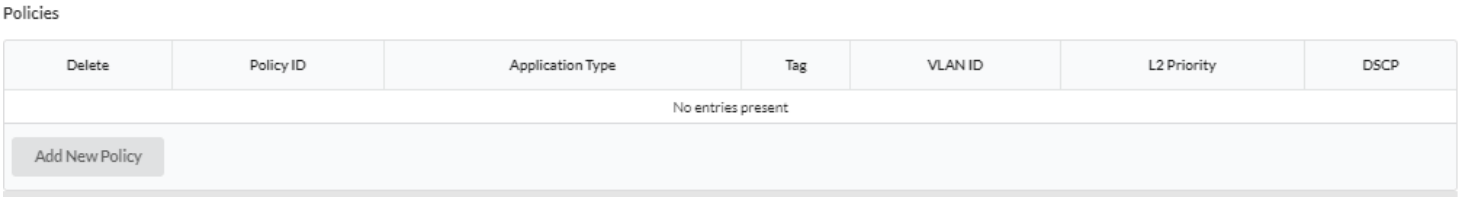
Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant 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 / Signaling (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.



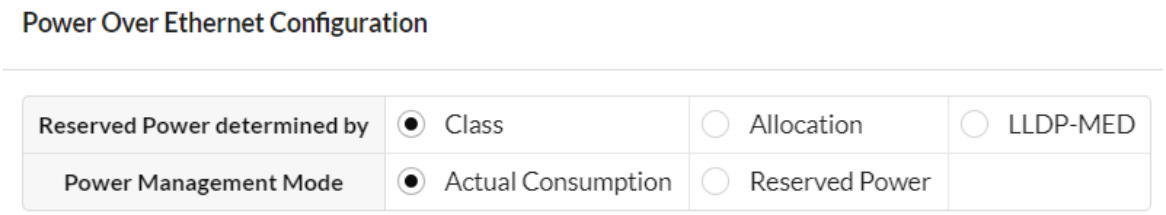
Setting	Description
Delete	Check to delete the policy. It will be deleted during the next save.
Policy ID	ID for the policy. This is auto generated and shall be used when selecting the policies that shall be mapped to the specific interfaces.
Application Type	Intended use of the application types: 1. **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 Signaling (conditional)** - for use in network topologies that require a different policy for the voice signaling 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 Signaling (conditional)** - for use in network topologies that require a different policy for the guest voice signaling 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 Signaling (conditional)** - for use in network topologies that require a separate policy for the video signaling 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 interface 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 behavior 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.
Adding a new policy	Click "**Add New Policy**" button to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click "Save". The number of policies supported is 32

4.15 PoE (Supported on PoE Switches only)

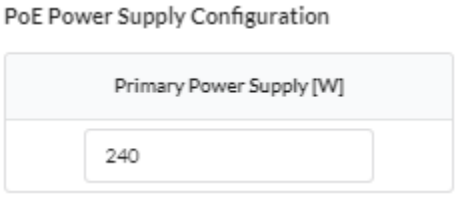
4.15.1 Power Budget

Power Over Ethernet Configuration



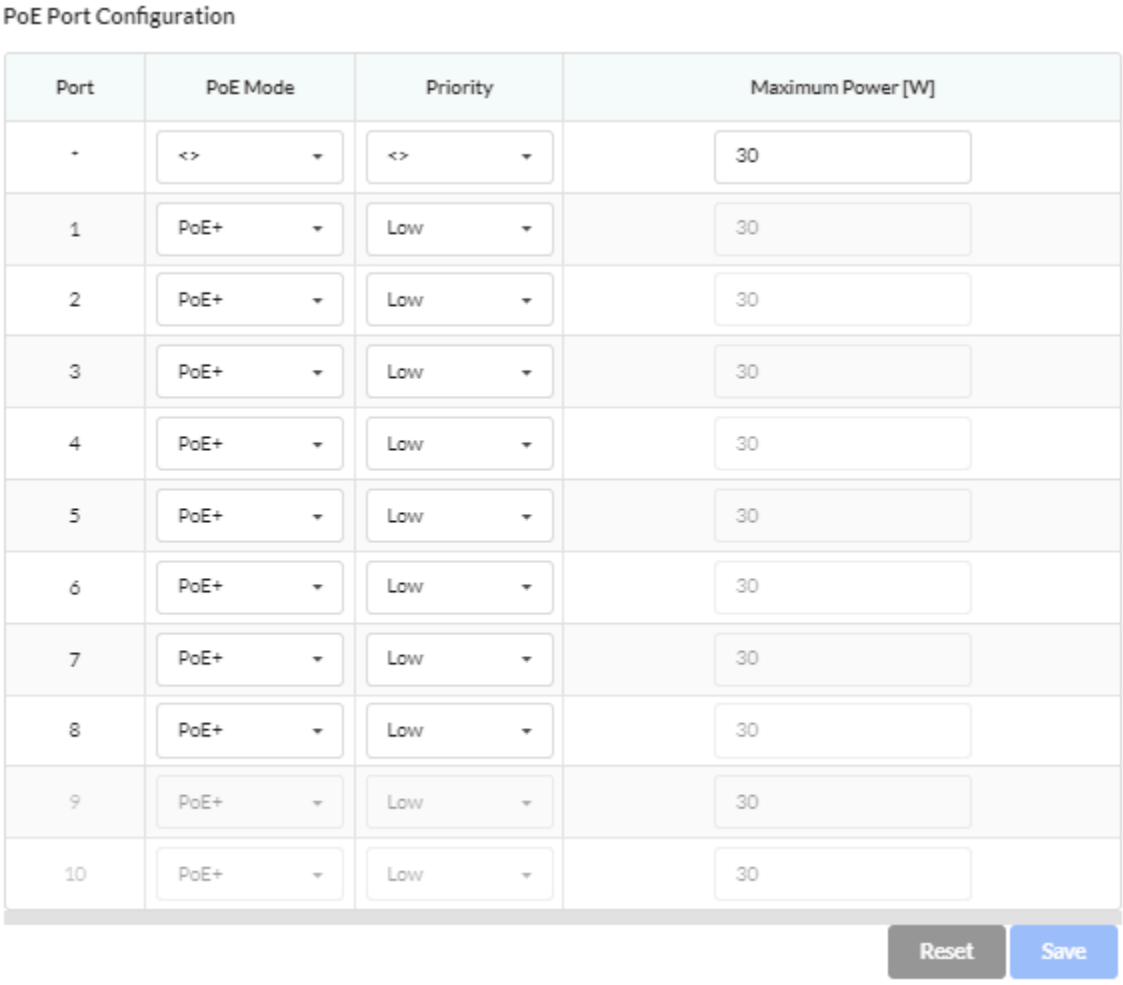
Setting	Description
Reserved Power determined by	There are three modes for configuring how the ports/PDsmay reserve power. 1. **Allocated mode:** In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields. 2. **Class mode:** In this mode each port automatically determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Eight different port classes exist and one for 4, 7, 15.4, 30, 45, 60, 75 or 90 Watts. 3. **LLDP-MED mode:** This mode is similar to the Class mode expect that each port determine the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the class mode. In this mode the Maximum Power fields have no effect **For all modes:** If a port uses more power than the reserved power for the port, the port is shut down.
Power Management Mode	There are 2 modes for configuring when to shut down the ports: 1. **Actual Consumption:** In this mode the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shut down. 2. **Reserved Power:** In this mode the ports are shut down when total reserved power exceeds the amount of power that the power supply can deliver. In this mode the port power is not turned on if the PD requests more power than available from the power supply.

PoE Supply Configure



Setting	Description
Primary Power Supply [W]	For being able to determine the amount of power the PD may use, it must be defined what amount of power a power source can deliver. Valid values are in the range 1 to 240 Watts.

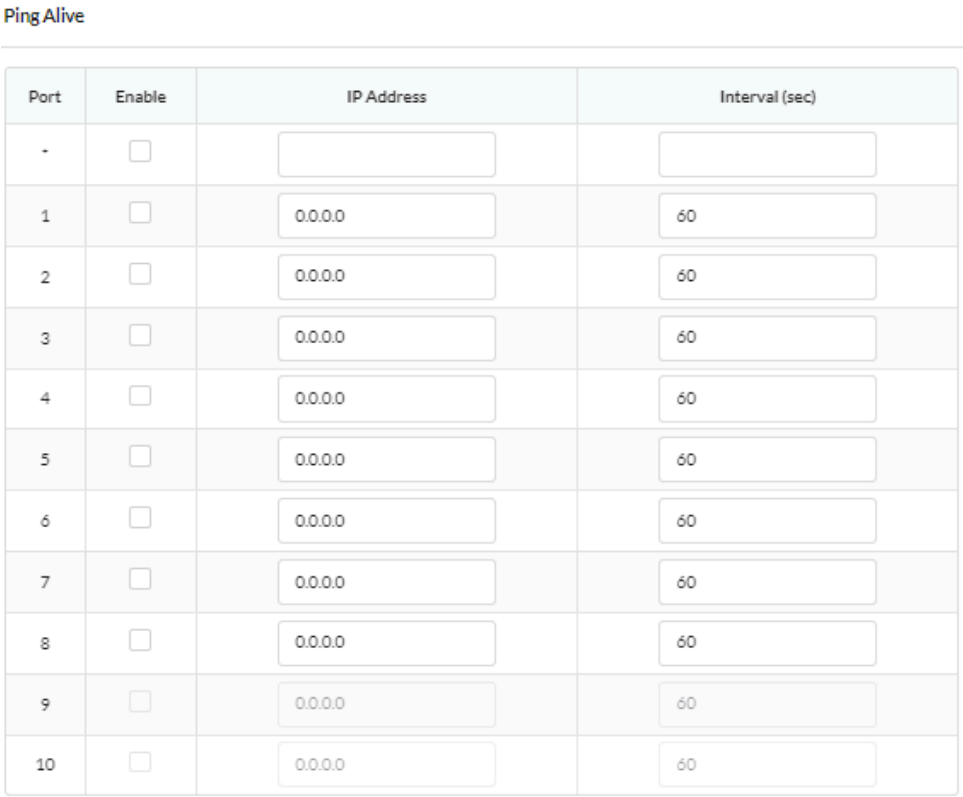
PoE Port Configuration



Setting	Description
PoE Mode	The PoE Mode represents the PoE operating mode for the port. • **Disabled:** PoE disabled for the port. • **PoE :** Enables PoE IEEE 802.3af (Class 4 PDs limited to 15.4W) • **PoE+ :** Enables PoE+ IEEE 802.3at (Class 4 PDs limited to 30W)
Priority	The Priority represents the port's priority. There are three levels of power priority named **Low, High** and **Critical**. The priority is used in the case where the remote devices require more power than the power supply can deliver. In this case the port with the lowest priority will be turned off starting from the port with the highest port number.
Maximum Power	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.

4.15.2 Ping Alive

Allows to give the user control over the system's Powered Device failure check.



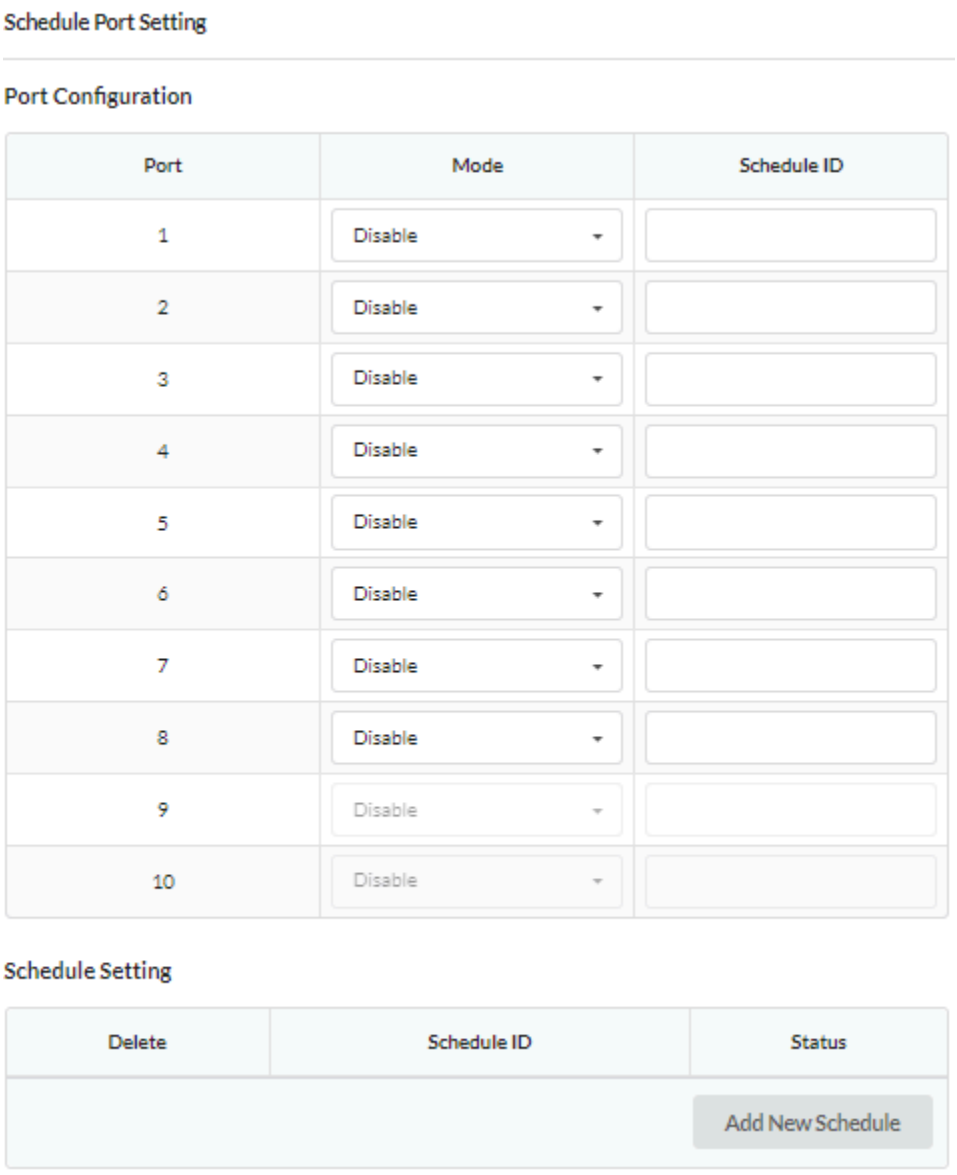
Ping Alive Port Configuration

Setting	Description
Port	The switch port number of the port.
Enable	Controls whether poe ping alive is enabled on this switch port.
IP Address	The IP for the Powered Device.
Interval	The time for IP checking period.

4.15.3 Schedule

Schedule Port Setting

This page is divided into Port Configuration and Schedule Setting parts. Port Configuration allows the user to set PoE schedule identifier and PoE schedule mode for each PoE port. Schedule Setting allows the user to add new schedule timetabling.



Port Configuration

Setting	Description
Port	The switch port number of the port.
Mode	**Disable:** Disable schedule operation. **Schedule On:** If current time is within the range of schedule limitation, PSE will provide PD with power.

	Schedule Off: If current time is within the range of schedule limitation, PSE will not provide PD with power.
Schedule ID	Controls whether schedules need to be executed. Schedule id ranges from 1 to 32.

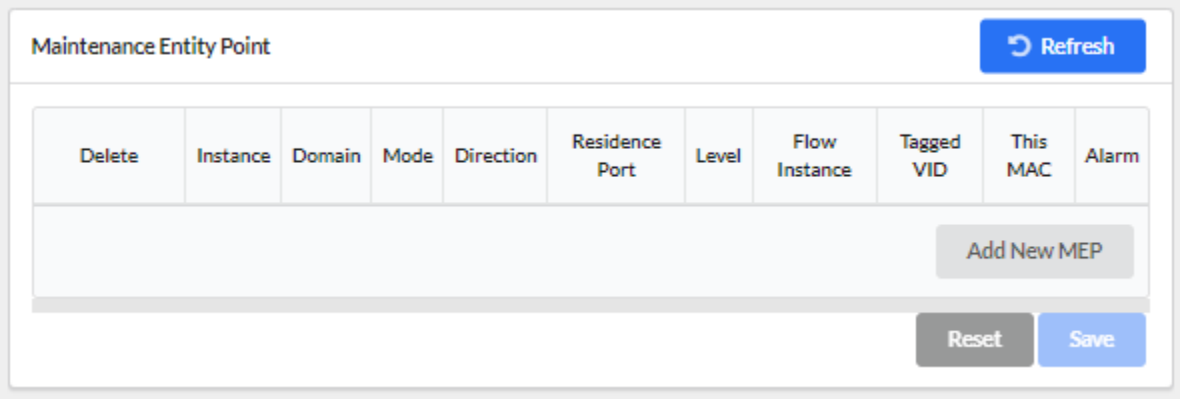
Schedule Setting

Setting	Description
Schedule ID	PoE schedule id. Schedule id ranges from 1 to 32.
Status	PoE schedule status.

Add New Schedule
Click “Add New Schedule” schedule ID number to edit PoE schedule time configuration

4.16 MEP

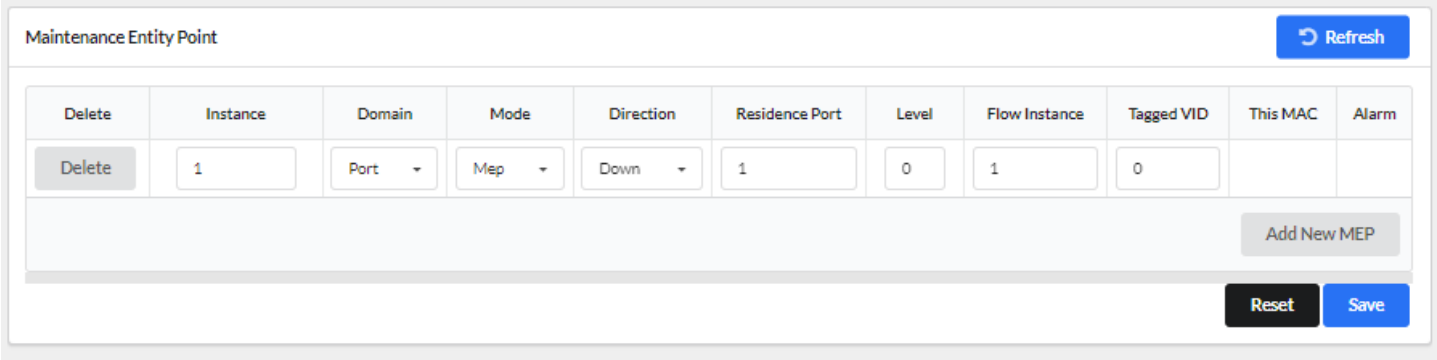
Maintenance Entity Point



Setting	Description
Delete	This box is used to mark a MEP for deletion in the next Save operation.
Instance	The ID of the MEP. Click on the ID of a MEP to enter the configuration page. The range is from **1** through **100**.
Domain	**Port:** This is a MEP in the Port Domain.
Mode	**MEP:** This is a Maintenance Entity End Point. **MIP:** This is a Maintenance Entity Intermediate Point.
Direction	**Down:** This is a Down MEP - monitoring ingress OAM and traffic on Residence Port. **Up:** This is a Up MEP – monitoring OAM and traffic on Residence Port.
Residence Port	The port where MEP is monitoring - see 'Direction'. For an EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member.
Level	The MEG level of this MEP.
Flow Instance	The MEP is related to this flow - See 'Domain'. This is not relevant and not shown in case of Port MEP.

Tagged VID	**Port MEP:** An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added. **EVC MEP:** This is not used. **VLAN MEP:** This is not used. **EVC MIP:** On Serval, this is the Subscriber VID that identifies the subscriber flow in this EVC where the MIP is active.
This MAC	The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).
Alarm	There is an active alarm on the MEP.

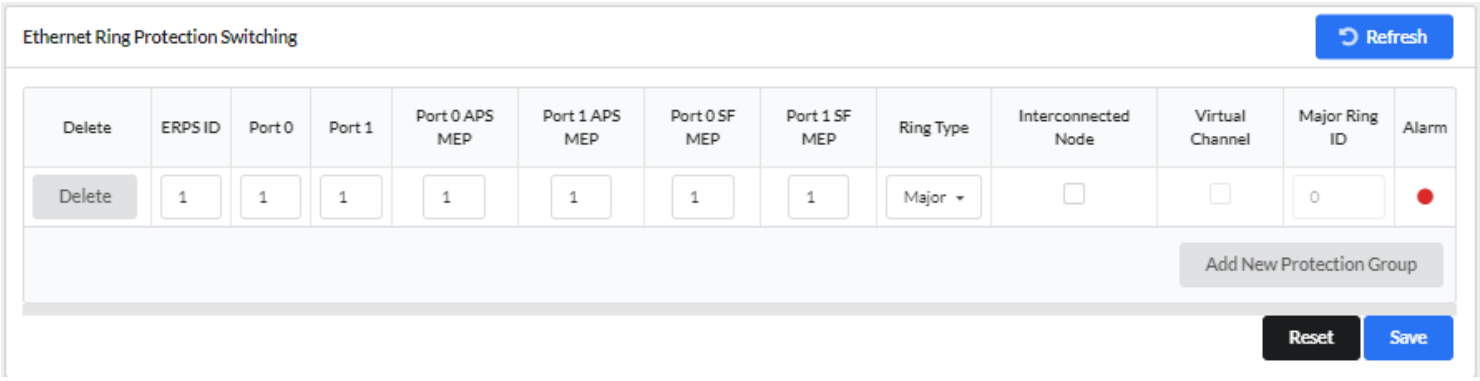
Add New MEP



Setting	Description
Instance	The ID of the MEP.
Domain	**Port:** This is a MEP in the Port Domain.
Mode	**MEP:** This is a Maintenance Entity End Point. **MIP:** This is a Maintenance Entity Intermediate Point.
Direction	**Down:** This is a Down MEP - monitoring ingress OAM and traffic on Residence Port. **Up:** This is a Up MEP
Residence Port	The port where MEP is monitoring - see 'Direction'. For an EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member.
Flow Instance	The MEP is related to this flow - See 'Domain'. This is not relevant and not shown in case of Port MEP.
Tagged VID	**Port MEP:** An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added. **EVC MEP:** This is not used. **VLAN MEP:** This is not used. **EVC MIP:** On Serval, this is the Subscriber VID that identifies the subscriber flow in this EVC where the MIP is active.

4.17 ERPS

Ethernet Ring Protection Switching



Setting	Description
Delete	This box is used to mark an ERPS for deletion in the next Save operation.
ERPS ID	The ID of the created Protection group, It must be an integer value between 1 and 64. The maximum number of ERPS Protection Groups that can be created are 64. Click on the ID of a Protection group to enter the configuration page.
Port 0	This will create a Port 0 of the switch in the ring.
Port 1	This will create Port 1 of the switch in the Ring. As interconnected sub-ring will have only one ring port, Port 1 is configured as 0 for interconnected sub-ring. 0 in this field indicates that no Port 1 is associated with this instance
Port 0 APS MEP	The Port 0 APS PDU handling MEP.
Port 1 APS MEP	The Port 1 APS PDU handling MEP. As only one APS MEP is associated with an interconnected sub-ring without a virtual channel, it is configured as 0 for such ring instances. 0 in this field indicates that no Port 1 APS MEP is associated with this instance.
Port 0 SF MEP	The Port 0 Signal Fail reporting MEP.
Port 1 SF MEP	The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with an interconnected sub-ring without a virtual channel, it is configured as 0 for such ring instances. 0 in this field indicates that no Port 1 SF MEP is associated with this instance.
Ring Type	Type of Protecting ring. It can be either a major ring or sub-ring.
Interconnected Node	Interconnected Node indicates that the ring instance is interconnected. Click on the checkbox to configure this. Yes indicates it is an interconnected node for this instance. No indicates that the configured instance is not interconnected.
Virtual Channel	Sub-rings can either have a virtual channel or not on the interconnected node. This is configured using the Virtual Channel checkbox. Yes indicates it is a sub-ring with a virtual channel. No indicates, sub-ring doesn't have a virtual channel.

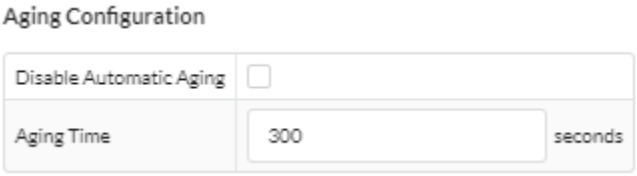
Major Ring ID	Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If the ring is major, this value is the same as the protection group ID of this ring.
Alarm	There is an active alarm on the ERPS.

4.18 MAC Table

MAC Address Table Configuration

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.

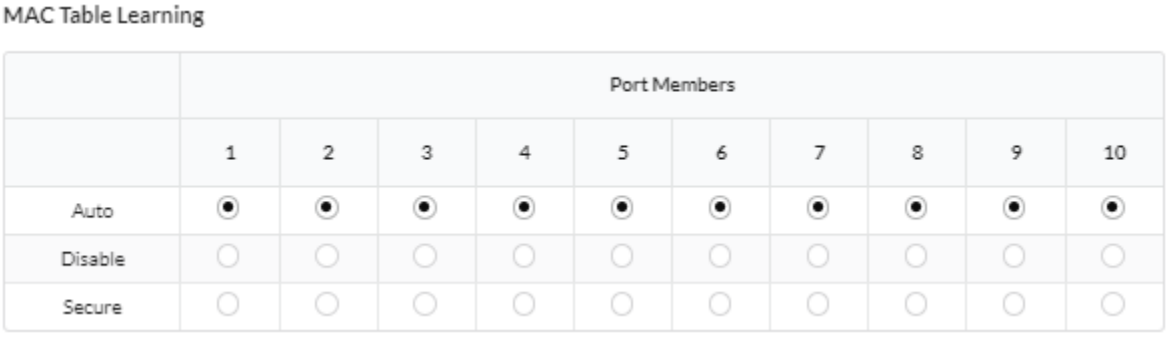
Aging Configuration



Setting	Description
Disable Automatic Aging	Disable the automatic aging of dynamic entries by checking Disable automatic aging.
Aging Time	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. The allowed range is 10 to 1000000 seconds.

MAC Table Learning

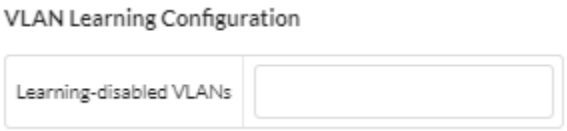
If the learning mode for a given port is grayed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X.



Setting	Description
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.

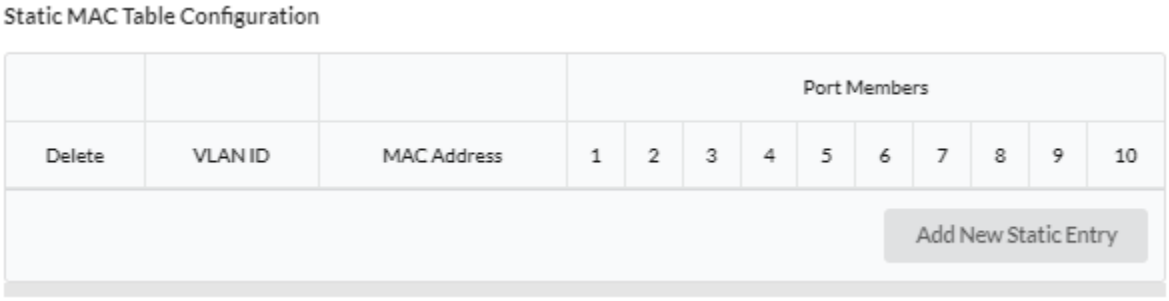
VLAN Learning Configuration



Setting	Description
Learning-disabled VLANs	This field shows the Learning-disabled VLANs. When a NEW MAC arrives into a learning-disabled VLAN, the MAC won't be learnt. By default, the field is empty. 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.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.

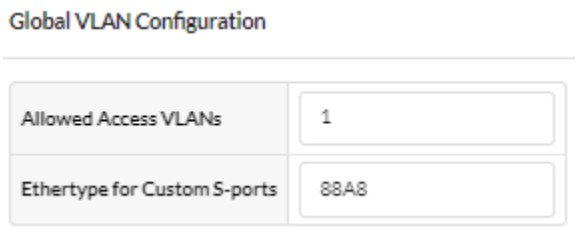


Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID of the entry.
MAC Address	The MAC address of the entry.
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

4.19 VLANs

This page allows for controlling VLAN configuration on the switch.
The page is divided into a global section and a per-port configuration section.

Global VLAN Configuration



Setting	Description
Allowed Access VLANs	This field shows the allowed Access VLANs, i.e. it only affects ports configured as Access ports. Ports in other modes are members of the VLANs specified in the Allowed VLANs field. By default, only VLAN 1 is enabled. 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 VLAN Configuration

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

Setting	Description
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 and C-tagged frames • Discards all frames 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 VLANs (1-4095) • The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs • Frames classified to a VLAN that the port is not a member of are 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 **Hybrid:** Hybrid ports resemble trunk ports in many ways, but add 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 ports 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 frames 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 egress, if frames must be tagged, they will be tagged with an S-tag. On ingress, frames with a VLAN tag with TPID = 0x88A8 get classified to the VLAN ID embedded in the tag. Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept ***Tagged Only*** frames (see Ingress Acceptance below), frames without this TPID are dropped. ***Notice:*** If the S-port is configured to accept ***Tagged and Untagged*** frames (see Ingress Acceptance below), frames with a C-tag are treated like frames with an S-tag. If the S-port is configured to accept ***Untagged Only*** frames, S-tagged frames will be discarded (except for priority S-tagged frames). C-tagged frames are initially considered untagged and will therefore not be discarded. Later on in the ingress classification process, they will get classified to the VLAN embedded in the tag instead of the port VLAN ID. **S-Custom-Port:** On egress, if frames must be tagged, they will be tagged with the custom S-tag. On ingress, frames with a VLAN tag with a TPID equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag.

	Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept ***Tagged Only*** frames (see Ingress Acceptance below), frames without this TPID are dropped. ***Notice:*** If the custom S-port is configured to accept ***Tagged and Untagged*** frames (see Ingress Acceptance below), frames with a C-tag are treated like frames with a custom S-tag. If the Custom S-port is configured to accept ***Untagged Only*** frames, custom S-tagged frames will be discarded (except for priority custom S-tagged frames). C-tagged frames are initially considered untagged and will therefore not be discarded. Later on in the ingress classification process, they will get classified to the VLAN embedded in the tag instead of the port VLAN ID.
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.
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. See Port Type for a description of when a frame is considered tagged. **Tagged Only:** Only frames tagged with the corresponding Port Type tag are accepted on ingress. **Untagged Only:** Only untagged frames are accepted on ingress. See Port Type for a description of when a frame is considered untagged.
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 members of one VLAN, the Access VLAN. The field's syntax is identical to the syntax used in the Enabled VLANs field. By default, a Trunk or Hybrid port will become a member of all VLANs, and is therefore set to **1-4095**. The field may be left empty, which means that the port will not become a member of any VLANs.
Forbidden VLANs	A port may be configured to never become a member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs.

	The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Enabled VLANs field. By default, the field is left blank, which means that the port may become a member of all possible VLANs.

4.20 Private VLANs

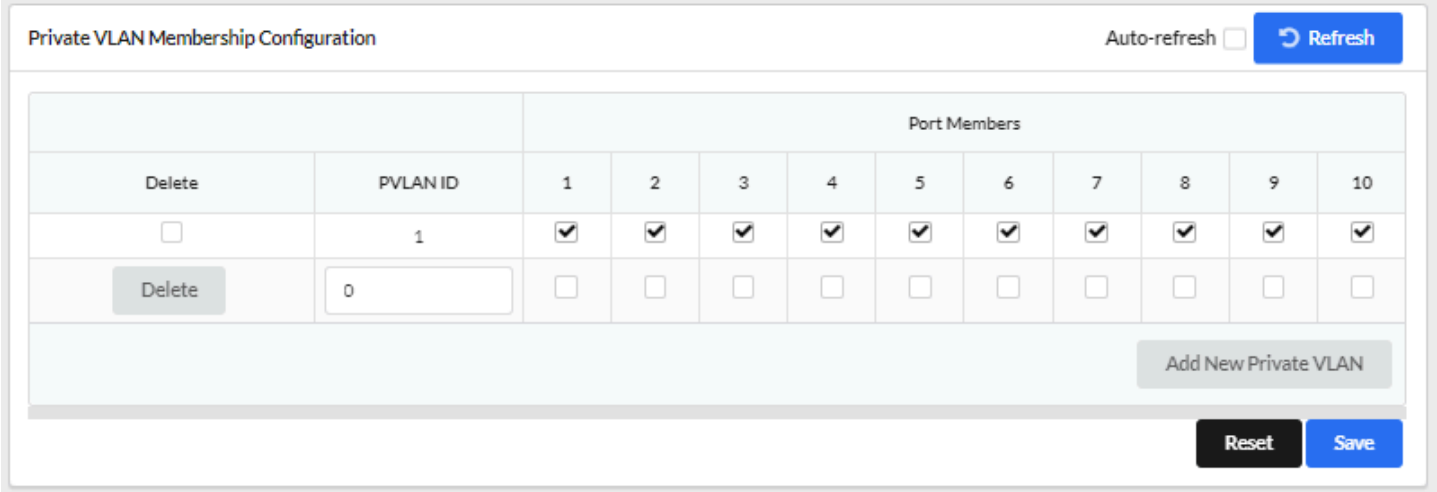
4.20.1 Membership

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

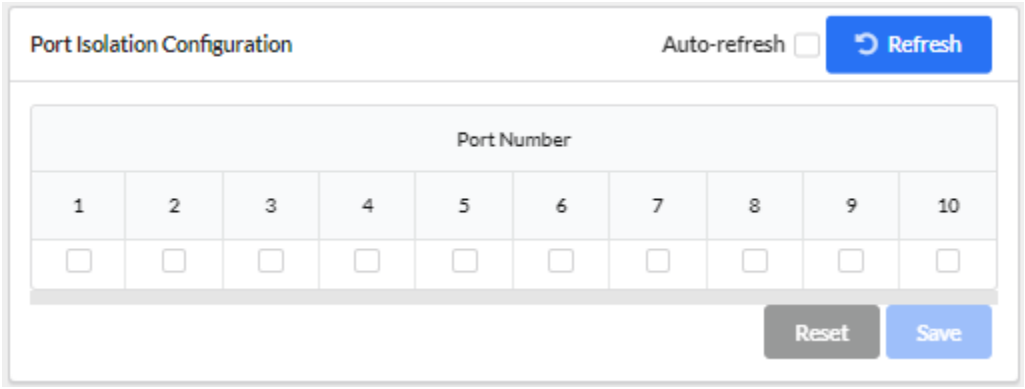


Setting	Description
Delete	To delete a private VLAN entry, check this box. The entry will be deleted during the next save.
Private VLAN ID	Indicates the ID of this particular private VLAN.
Port Members	A row of checkboxes for each port is displayed for each private VLAN ID. To include a port in a Private 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.

4.20.2 Port Isolation

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.



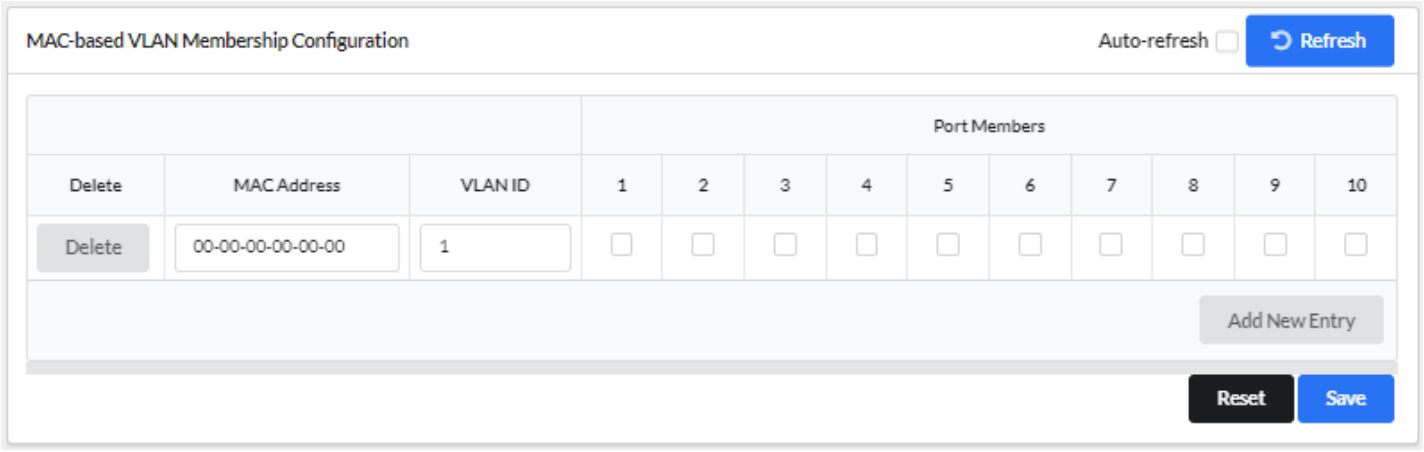
Port Number

Setting	Description	Factory Default
Checked	Port isolation is enabled on that port.	Unchecked
Unchecked	Port isolation is disabled on that port.	

4.21 VCL

4.21.1 MAC-based VLAN

The MAC address to VLAN ID mappings can be configured here. This page allows adding and deleting MAC-based VLAN Classification List entries and assigning the entries to different ports.



Setting	Description
Delete	To delete a MAC to VLAN ID mapping entry, check this box and press save. The entry will be deleted in the stack.
MAC Address	Indicates the MAC address of the mapping.
VLAN ID	Indicates the VLAN ID the above MAC will be mapped to.

Port Members	A row of checkboxes for each port is displayed for each MAC to VLAN ID mapping entry. To include a port in the 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.

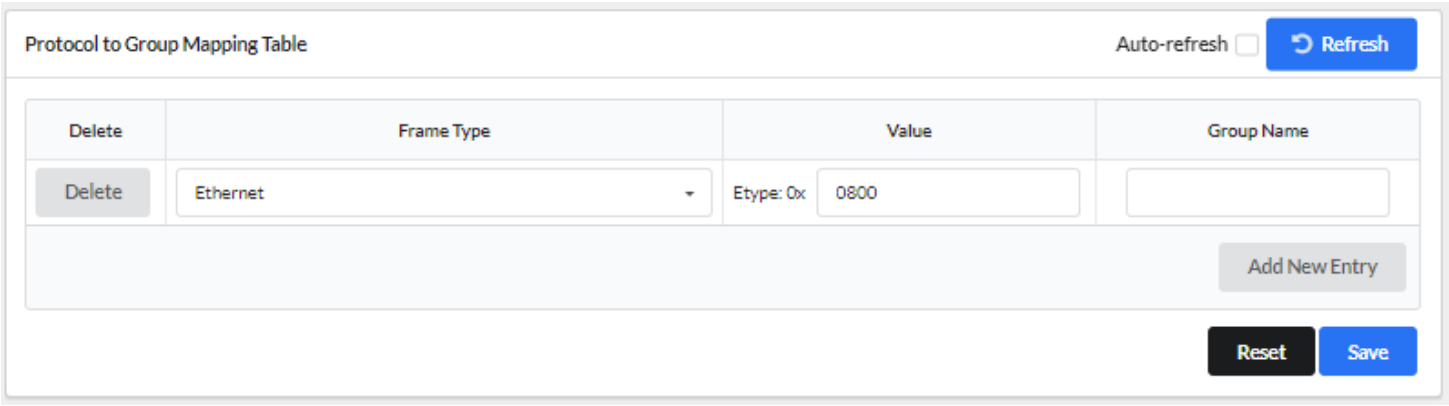
Add New Entry button

Click “Add New Entry” button to add a new MAC to VLAN ID mapping entry. An empty row is added to the table, and the mapping can be configured as needed. Any unicast MAC address can be used to configure the mapping. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 through 4095.
The MAC to VLAN ID entry is enabled when you click on "Save". A mapping without any port members will not be added when you click "Save". The maximum possible MAC to VLAN ID mapping entries are limited to 256.

4.21.2 Protocol-based VLAN

4.21.2.1 Protocol to Group

This page allows you to add a new Protocol to Group Name (each protocol can be part of only one Group) mapping entries as well as allow you to see and delete already mapped entries for the switch.



Setting	Description
Delete	To delete a Protocol to Group Name map entry, check this box. The entry will be deleted from the switch during the next Save.
Frame Type	Frame Type can have one of the following values: • **Ethernet** • **LLC** • **SNAP** **NOTE:** When changing the Frame type field, the 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 preceding Frame Type selection menu. Below are the criteria for the three different Frame Types: • **Ethernet:** Value in the text field when Ethernet is selected as a Frame Type is called e type. Valid values for e type range between 0x0600 and 0xffff

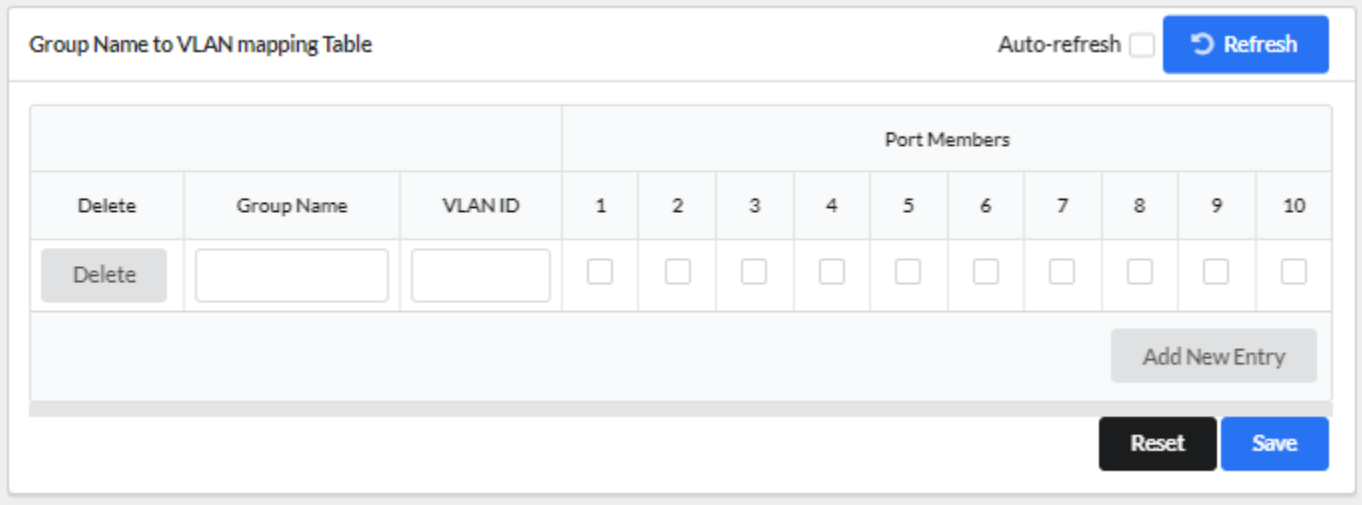
	• **LLC:** Valid value in this case is composed of two different sub-values. a. ***DSAP:*** 1-byte long string (0x00-0xff) b. ***SSAP:*** 1-byte long string (0x00-0xff) • **SNAP:** Valid value in this case is also composed of two different sub-values. a. ***OUI:*** OUI (Organizationally Unique Identifier) is a parameter in the format of xx-xx-xx where each pair (xx) in the string is a hexadecimal value ranging between 0x00 and 0xff. b. ***PID:*** PID (Protocol ID). If OUI is hexadecimal 000000, then the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if 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 the value of OUI field is 00-00-00 then the value of PID will be e type (0x0600-0xffff) and if the value of OUI is other than 00-00-00 then valid values of PID will be any value between 0x0000 and 0xffff.
Group Name	A valid Group Name is a 16-character long string, unique for every entry, which consists of a combination of alphabets (a-z or A-Z) and integers (0-9). **NOTE:** Special characters and underscores (_) are not allowed.

Add New Entry button

Click "Add New Entry" to add a new entry in the mapping table. An empty row is added to the table, where Frame Type, Value and the Group Name can be configured as needed. The maximum possible Protocol to Group mappings are limited to 128.

4.21.2.2 Group to VLAN

This page allows you to map a Group Name (already configured or to be configured in the future) to a VLAN for the switch.



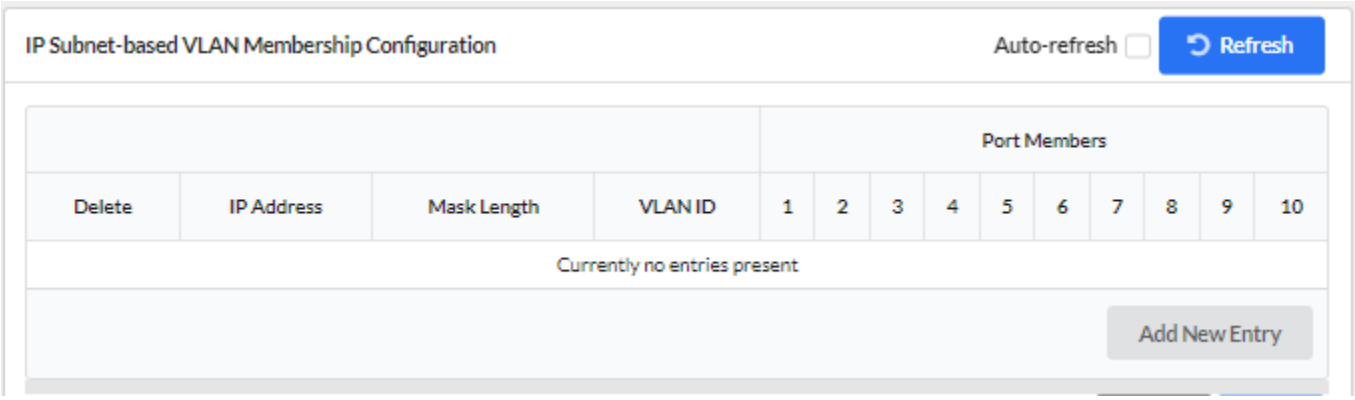
Setting	Description
Delete	To delete a Group Name to VLAN mapping, check this box. The entry will be deleted from the switch during the next Save.
Group Name	A valid Group Name is a string, at most 16 characters long, which consists of a combination of alphabets (a-z or A-Z) and integers(0-9) with no special characters allowed. You may either use a Group that already includes one or more protocols (see Protocol to Group mappings), or create a Group to VLAN ID mapping that will become active the moment you add one or more protocols inside that Group. Furthermore, the Group to VLAN ID mapping is not unique, as long as the port lists of these mappings are mutually exclusive (e.g. Group1 can be mapped to VID 1 on port#1 and to VID 2 on port#2).
VLAN ID	Indicates the VLAN ID to which the Group Name will be mapped. A valid VLAN ID ranges from 1 to 4095.
Port Members	A row of checkboxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in the 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.

Add New Entry button

Click "Add New Entry" button to add a new entry in the mapping table. An empty row is added to the table and the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The maximum possible Group to VLAN mappings are limited to 256.

4.21.3 IP Subnet-based VLAN

The IP subnet to VLAN ID mappings can be configured here. This page allows adding, updating and deleting IP subnets to VLAN ID mapping entries and assigning them to different ports.



Setting	Description
Delete	To delete a mapping, check this box and press save. The entry will be deleted in the stack.
IP Address	Indicates the subnet's IP address (Any of the subnet's host addresses can be also provided here, the application will convert it automatically).
Mask Length	Indicates the subnet's mask length.
VLAN ID	Indicates the VLAN ID the subnet will be mapped to. IP Subnet to VLAN ID is a unique matching.

Port Members	A row of checkboxes for each port is displayed for each IP subnet to VLAN ID mapping entry. To include a port in a mapping, simply 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.

Add New Entry button

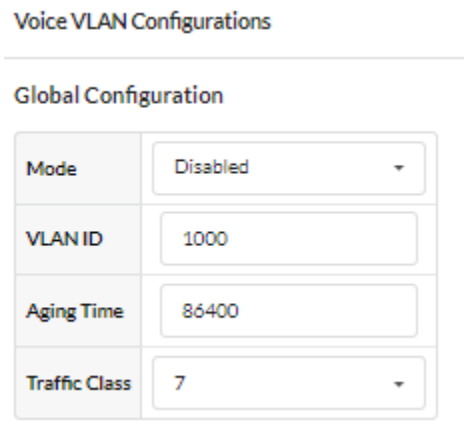
Click “Add New Entry” button to add a new IP subnet to VLAN ID mapping entry. An empty row is added to the table, and the mapping can be configured as needed. Any IP address/mask can be configured for the mapping. Legal values for the VLAN ID are 1 to 4095. The IP subnet to VLAN ID mapping entry is enabled when you click on "Save". The maximum possible IP subnet to VLAN ID mappings are limited to 128.

4.22 Voice VLAN

4.22.1 Voice VLAN 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.

Global Configuration



Setting	Description
Mode	Indicates the Voice VLAN mode operation. We must disable the MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are: **Enabled**: Enable Voice VLAN mode operation. **Disabled**: Disable 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 Class	Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply to this class.

Port Configuration

Port Configuration

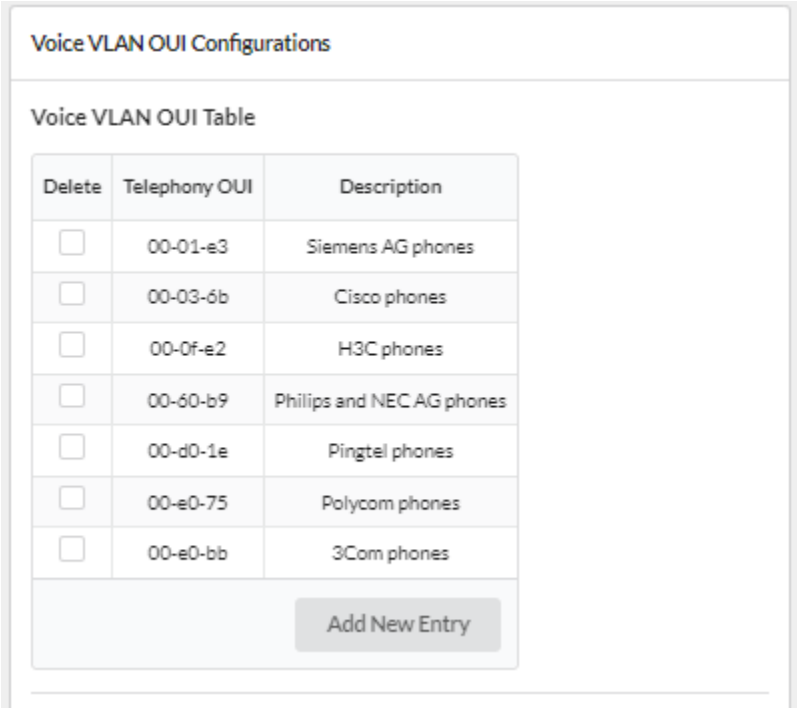
Port	Mode	Security	Discovery Protocol
*	<>	<>	<>
1	Disabled	Disabled	OUI
2	Disabled	Disabled	OUI
3	Disabled	Disabled	OUI
4	Disabled	Disabled	OUI
5	Disabled	Disabled	OUI
6	Disabled	Disabled	OUI
7	Disabled	Disabled	OUI
8	Disabled	Disabled	OUI
9	Disabled	Disabled	OUI
10	Disabled	Disabled	OUI

Setting	Description
Port	The port number for which the configuration applies.
Port Mode	Indicates the Voice VLAN port mode. Possible port modes are: **Disabled**: Disjoin from Voice VLAN. **Auto**: Enable auto detect mode. It detects whether there is a VoIP phone attached to the specific port and configures the Voice VLAN members automatically. **Forced**: Force join to Voice VLAN.
Port 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 (or blocked for 300 seconds if changing the aging time). Possible port modes are: **Enabled**: Enable Voice VLAN security mode operation. **Disabled**: Disable Voice VLAN security mode operation.

Port Discovery Protocol	Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable the LLDP feature before configuring the discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart the auto detect process. Possible discovery protocols are: **OUI**: Detect telephony device by OUI address. **LLDP**: Detects telephony device by LLDP. **Both**: Both OUI and LLDP.

4.22.2 Voice VLAN OUI

Configure VOICE VLAN OUI table on this page. The maximum number of entries is 16. Modifying the OUI table will restart auto detection of the OUI process.



Setting	Description
Delete	Check to delete the entry. It will be deleted during the next apply.
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", "xx:xx:xx", "xx.xx.xx" or "xxxxxx" (x is a hexadecimal digit).
Description	The description of the OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is **0 to 32**

4.23 QoS

4.23.1 Port Classification

QoS Port Classification

Port	Ingress						
	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	Address Mode
*	<>	<>	<>	<>			<>
1	0	0	0	0	Disabled		Source
2	0	0	0	0	Disabled		Source
3	0	0	0	0	Disabled		Source
4	0	0	0	0	Disabled		Source
5	0	0	0	0	Disabled		Source
6	0	0	0	0	Disabled		Source
7	0	0	0	0	Disabled		Source
8	0	0	0	0	Disabled		Source
9	0	0	0	0	Disabled		Source
10	0	0	0	0	Disabled		Source

Setting	Description
Port	The port number for which the configuration below applies.
CoS	Controls the default CoS value. All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority. If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default CoS. The classified CoS can be overruled by a QCL entry. **Note**: If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.

DPL	Controls the default DPL value. All frames are classified to a Drop Precedence Level. If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL. The classified DPL can be overruled by a QCL entry.
PCP	Controls the default PCP value. All frames are classified to a PCP value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.
DEI	Controls the default DEI value. All frames are classified to a DEI value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.
Tag Class.	Shows the classification mode for tagged frames on this port. ● **Disabled:** Use default CoS and DPL for tagged frames. ● **Enabled:** Use mapped versions of PCP and DEI for tagged frames. Click on the mode in order to configure the mode and/or mapping. **Note:** This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL.
DSCP Based	Click to Enable DSCP Based QoS Ingress Port Classification.
Address Mode	The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. The allowed values are: ● **Source**: Enable SMAC/SIP matching. ● **Destination**: Enable DMAC/DIP matching.

4.23.2 Port Policing

This page allows you to configure the Policer settings for all switch ports.

QoS Ingress Port Policers

Port	Enable	Rate	Unit	Flow Control
*	☐		<>	☐
1	☐	500	kbps	☐
2	☐	500	kbps	☐
3	☐	500	kbps	☐
4	☐	500	kbps	☐
5	☐	500	kbps	☐
6	☐	500	kbps	☐
7	☐	500	kbps	☐
8	☐	500	kbps	☐
9	☐	500	kbps	☐
10	☐	500	kbps	☐

Setting	Description
Port	The port number for which the configuration below applies.
Enable	Enable or disable the port policer for this switch port.
Rate	Controls the rate for the port policer. This value is restricted to 100-3276700 when "Unit" is kbps or fps, and 1-3276 when "Unit" is Mbps or kfps. The rate is internally rounded up to the nearest value supported by the port policer.
Unit	Controls the unit of measure for the port policer rate as kbps, Mbps, fps or kfps.
Flow Control	If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

4.23.3 Queue Policing

QoS Ingress Queue Policers

Port	Queue 0	Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable
-	☐	☐	☐	☐	☐	☐	☐	☐
1	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐
9	☐	☐	☐	☐	☐	☐	☐	☐
10	☐	☐	☐	☐	☐	☐	☐	☐

Setting	Description
Port	The port number for which the configuration below applies.
Enable	Enable or disable the queue policer for this switch port.
Rate	Controls the rate for the queue policer. This value is restricted to 100-3276700 when "Unit" is kbps, and 1-3276 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue policer. This field is only shown if at least one of the queue policers are enabled.
Unit	Controls the unit of measure for the queue policer rate as kbps or Mbps. This field is only shown if at least one of the queue policers are enabled.

4.23.4 Port Scheduler

QoS Egress Port Schedulers

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

Setting	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.
Mode	Shows the scheduling mode for this port.
Qn	Shows the weight for this queue and port.

4.23.5 Port Shaping

QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-	-
9	-	-	-	-	-	-	-	-	-
10	-	-	-	-	-	-	-	-	-

Setting	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure the shapers.
Qn	Shows "-" for disabled or actual queue shaper rate - e.g. "800 Mbps".
Port	Shows "-" for disabled or actual port shaper rate - e.g. "800 Mbps".

4.23.6 Port Tag Remarking

QoS Egress Port Tag Remarking

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified

Setting	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure tag remarking.
Mode	Shows the tag remarking mode for this port. • **Classified:** Use classified PCP/DEI values. • **Default:** Use default PCP/DEI values. • **Mapped:** Use mapped versions of CoS class and DP level.

4.23.7 Port DSCP

QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
-	☐	<>	<>
1	☐	Disable	Disable
2	☐	Disable	Disable
3	☐	Disable	Disable
4	☐	Disable	Disable
5	☐	Disable	Disable
6	☐	Disable	Disable
7	☐	Disable	Disable
8	☐	Disable	Disable
9	☐	Disable	Disable
10	☐	Disable	Disable

Setting	Description
Port	The Port column shows the list of ports for which you can configure DSCP ingress and egress settings.
Ingress	In Ingress settings you can change ingress translation and classification settings for individual ports.There are two configuration parameters available in Ingress: **Translate:** To Enable the Ingress Translation click the checkbox. **Classify:** Classification for a port having 4 different values. 1. **Disable:** No Ingress DSCP Classification. 2. **DSCP=0:** Classify if incoming (or translated if enabled) DSCP is 0. 3. **Selected:** Classify only selected DSCP for which classification is enabled as specified in the DSCP Translation window for the specific DSCP. 4. **All:** Classify all DSCP.
Egress	Port Egress Rewriting can be one of - **Disable:** No Egress rewrite. **Enable:** Rewrite enabled without remapping.

	Remap DP Unaware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table. **Remap DP Aware:** DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation->Egress Remap DP0' table or from the 'DSCP Translation->Egress Remap DP1' table.

4.23.8 DSCP-Based QoS

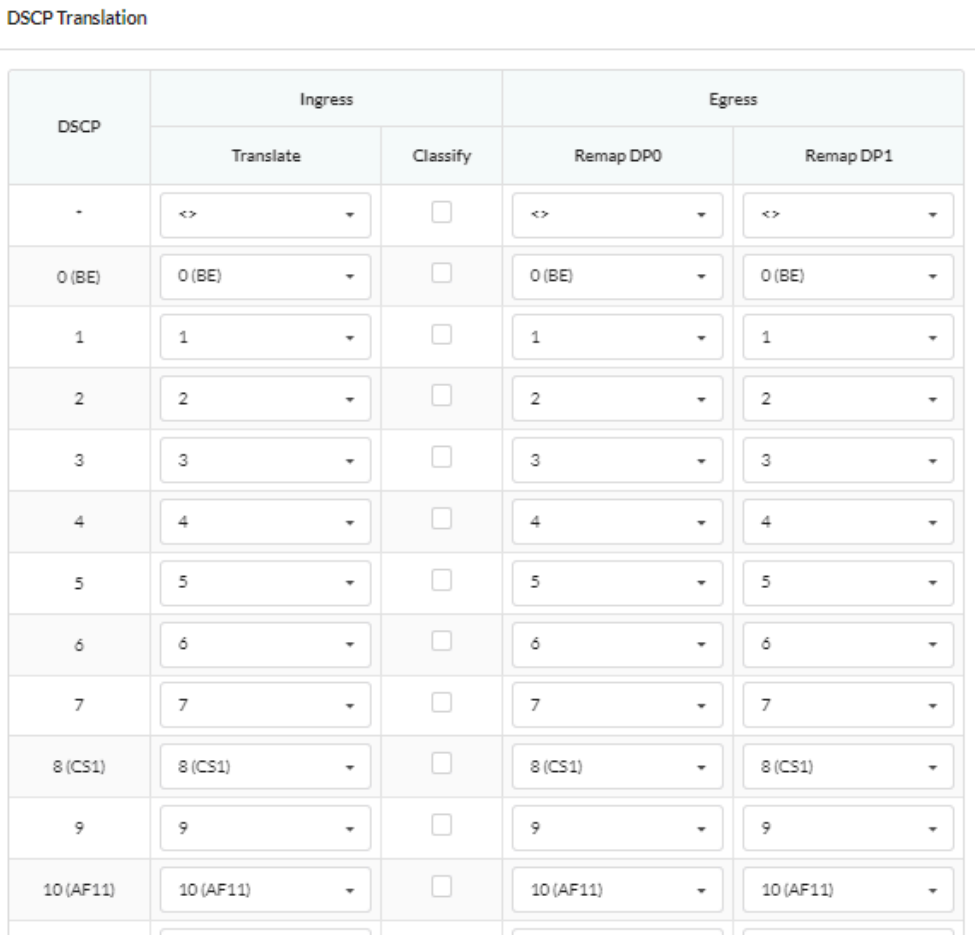
DSCP-Based QoS Ingress Classification

DSCP	Trust	CoS	DPL
-	☐	<>	<>
0 (BE)	☐	0	0
1	☐	0	0
2	☐	0	0
3	☐	0	0
4	☐	0	0
5	☐	0	0
6	☐	0	0
7	☐	0	0
8 (CS1)	☐	0	0
9	☐	0	0
10 (AF11)	☐	0	0

28 (AF32)	☐	0	0
29	☐	0	0
30 (AF33)	☐	0	0
31	☐	0	0
32 (CS4)	☐	0	0
33	☐	0	0
34 (AF41)	☐	0	0
35	☐	0	0
36 (AF42)	☐	0	0
37	☐	0	0
38 (AF43)	☐	0	0
39	☐	0	0
40 (CS5)	☐	0	0
41	☐	0	0
42	☐	0	0
43	☐	0	0

Setting	Description
DSCP	Maximum number of supported DSCP values is 64.
Trust	Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.
QoS Class	QoS class value can be any of (0-7)
DPL	Drop Precedence Level (0-3)

4.23.9 DSCP Translation



Setting	Description
DSCP	Maximum number of supported DSCP values are 64 and valid DSCP values range from 0 to 63.
Ingress	Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two configuration parameters for DSCP Translation - • **Translate:** DSCP at Ingress side can be translated to any of (0-63) DSCP values. • **Classify:** Click to enable Classification at Ingress side.
Egress	There are the following configurable parameters for Egress side - • **Remap DP0:** Controls the remapping for frames with DP level 0. Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63. • **Remap DP1:** Controls the remapping for frames with DP level 1. Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.

4.23.10 DSCP Classification

This page allows you to configure the mapping of CoS and DPL to DSCP value.

DSCP Classification

CoS	DSCP DP0	DSCP DP1
*	<>	<>
0	0 (BE)	0 (BE)
1	0 (BE)	0 (BE)
2	0 (BE)	0 (BE)
3	0 (BE)	0 (BE)
4	0 (BE)	0 (BE)
5	0 (BE)	0 (BE)
6	0 (BE)	0 (BE)
7	0 (BE)	0 (BE)

CoS Class	Actual Class of Service
DSCP DP0	Select the classified DSCP value (0-63) for Drop Precedence Level 0.
DSCP DP1	Select the classified DSCP value (0-63) for Drop Precedence Level 1.

4.23.11 QoS Control List

This page shows the QoS Control List(QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is **256** on each switch.Click on the lowest plus sign to add a new QCE to the list.

QoS Control List Configuration

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action					
									CoS	DPL	DSCP	PCP	DEI	Policy

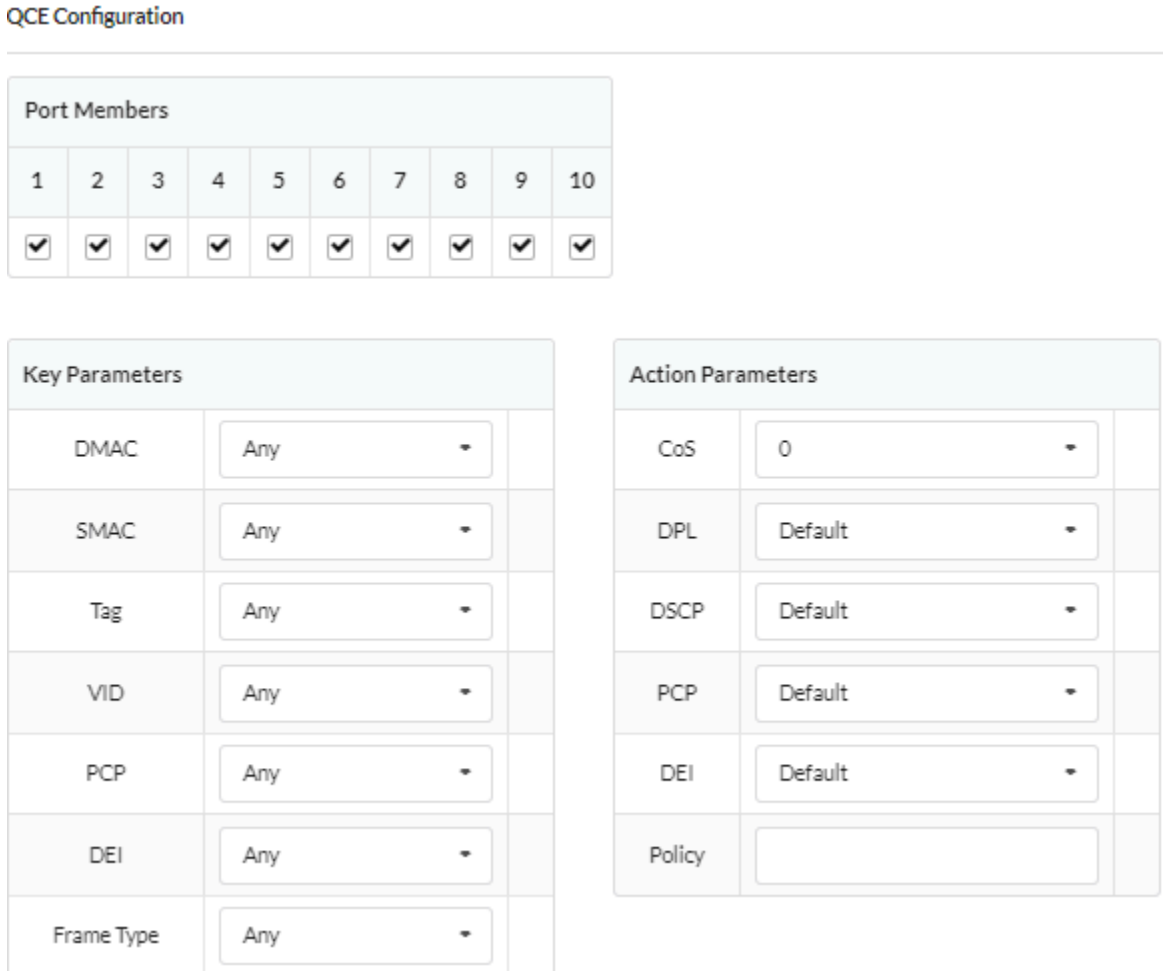
Add QCE to end of list

Setting	Description
QCE	Indicates the QCE id.
Port	Indicates the list of ports configured with the QCE or 'Any'.
DMAC	Indicates the destination MAC address. Possible values are: • **Any:** Match any DMAC. • **Unicast:** Match unicast DMAC.

	• **Multicast:** Match multicast DMAC. • **Broadcast:** Match broadcast DMAC. The default value is 'Any'.
SMAC	Match specific source MAC address or 'Any'. If a port is configured to match on destination addresses, this field indicates the DMAC.
Tag Type	Indicates tag type. Possible values are: • **Any:** Match tagged and untagged frames. • **Untagged:** Match untagged frames. • **Tagged:** Match tagged frames. The default value is 'Any'.
VID	Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'
PCP	Priority Code Point: Valid values of PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.
DEI	Drop Eligible Indicator: Valid values of DEI are 0, 1 or 'Any'.
Frame Type	Indicates the type of frame. Possible values are: 1. **Any:** Match any frame type. 2. **Ethernet:** Match EtherType frames. 3. **LLC:** Match (LLC) frames. 4. **SNAP:** Match (SNAP) frames. 5. **IPv4:** Match IPv4 frames. 6. **IPv6:** Match IPv6 frames.
Action	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are: 1. **CoS:** Classify Class of Service. 2. **DPL:** Classify Drop Precedence Level. 3. **DSCP:** Classify DSCP value. 4. **PCP:** Classify PCP value. 5. **DEI:** Classify DEI value. 6. **Policy:** Classify ACL Policy number.

Add QCE to the end of list

Allows to edit/insert a single QoS Control Entry at a time. A QCE consists of several parameters. These parameters vary according to the frame type that you select.



Port Members

Check the checkbox button to include the port in the QCL entry. By default all ports are included.

Key Parameters

Setting	Description
DMAC	Destination MAC address: Possible values are **Unicast**, **Multicast**, **Broadcast** or **Any**.
SMAC	Source MAC address: **xx-xx-xx-xx-xx-xx** or **Any**. If a port is configured to match on DMAC/DIP, this field is the Destination MAC address.
Tag	Value of the Tag field can be **Untagged, Tagged, C-Tagged, S-Tagged** or **Any**.
VID	Valid value of VLAN ID can be any value in the range **1-4095** or **Any**; user can enter either a specific value or a range of VIDs.
PCP	Valid value PCP are specific (**0, 1, 2, 3, 4, 5, 6, 7**) or range (**0-1, 2-3, 4-5, 6-7, 0-3, 4-7**) or **Any**.
DEI	Valid value of DEI can be **0**, **1** or **Any**.

Frame Type	Frame Type can have any of the following. 1. **Any** 2. **EtherType** 3. **LLC** 4. **SNAP** 5. **IPv4** 6. **IPv6**

All frame types are explained below.

1. **Any:** Allow all types of frames.
2. **EtherType:** Ether Type Valid Ether Type can be 0x600-0xFFFF excluding 0x800(IPv4) and 0x86DD(IPv6) or 'Any'.
3. **LLC:**
   - ***DSAP Address:*** Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any'.
   - ***SSAP Address:*** Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any'.
   - ***Control:*** Valid Control field can vary from 0x00 to 0xFF or 'Any'.
4. **SNAP:** PID Valid PID(a.k.a Ether Type) can be 0x0000-0xFFFF or 'Any'.
5. **IPv4:**
   - ***Protocol:*** IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.
   - ***Source IP:*** Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero. If a port is configured to match on DMAC/DIP, this field is the Destination IP address.
   - ***IP Fragment:*** IPv4 frame fragmented option: 'Yes', 'No' or 'Any'.
   - ***DSCP:*** Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.
   - ***Sport:*** Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.
   - ***Dport:*** Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.
6. **IPv6**
   - ***Protocol:*** IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.
   - ***Source IP:*** 32 LS bits of IPv6 source address in value/mask format or 'Any'. If a port is configured to match on DMAC/DIP, this field is the Destination IP address.
   - ***DSCP:*** Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.
   - ***Sport:*** Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

- ***Dport:*** Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Action Parameters

Setting	Description
CoS	Class of Service: (**0-7**) or **Default**.
DP	Drop Precedence Level: (**0-1**) or **Default**.
DSCP	DS1CP: (**0-63, BE, CS1-CS7, EF** or **AF11-AF43**) or **Default**.
PCP	PCP: (**0-7**) or **Default**. Note: PCP and DEI cannot be set individually.
DEI	DEI: (**0-1**) or **Default**.
Policy	ACL Policy number: (**0-255**) or **Default** (empty field).

Note: "Default" means that the default classified value is not modified by this QCE.

4.23.12 Storm Policing

Global storm policers for the switch are configured on this page.

There is a unicast storm policer, multicast storm policer, and a broadcast storm policer.
These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present in the MAC Address table.

Global Storm Policer Configuration

Frame Type	Enable	Rate	Unit
Unicast	☐	1	fps
Multicast	☐	1	fps
Broadcast	☐	1	fps

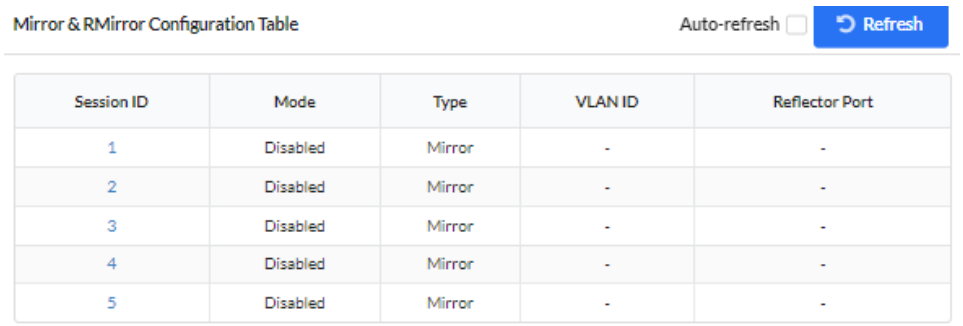
Setting	Description
Frame Type	The frame type for which the configuration below applies.
Enable	Enable or disable the global storm policer for the given frame type.
Rate	Controls the rate for the global storm policer. This value is restricted to 1-1024000 when **Unit** is fps, and 1-1024 when **Unit** is kfps. The rate is internally rounded up to the nearest value supported by the global storm policer. Supported rates are 1, 2, 4, 8, 16, 32, 64, 128, 256 and 512 fps for rates <= 512 fps and 1, 2, 4, 8, 16, 32, 64, 128, 256, 512 and 1024 kfps for rates > 512 fps.
Unit	Controls the unit of measure for the global storm policer rate as fps or kfps.

4.24 Mirroring

Mirroring is a feature for switched port analyzers. The administrator can use the Mirroring to debug network problems. The selected traffic can be mirrored or copied on a destination port where a network analyzer can be attached to analyze the network traffic.

Remote Mirroring is an extended function of Mirroring. It can extend the destination port in other switches. So the administrator can analyze the network traffic on the other switches.

If you want to get the tagged mirrored traffic, you have to set VLAN egress tagging as "Tag All" on the reflector port. On the other hand,
If you want to get untagged mirrored traffic, you have to set VLAN egress tagging as "Untag ALL" on the reflector port.

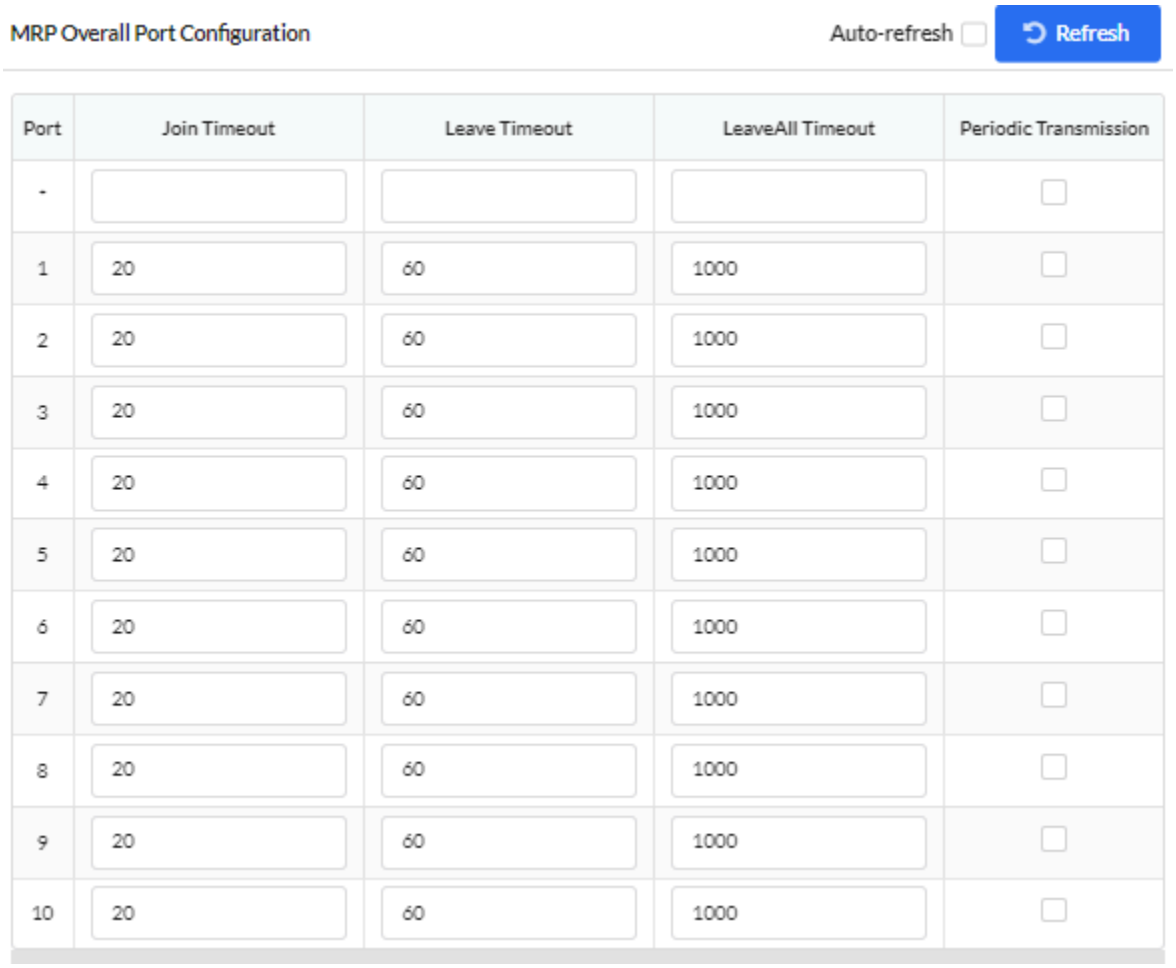


Setting	Description
Session	Select session ID to configure.
Mode	To **Enabled/Disabled** the mirror or Remote Mirroring function.
Type	Select switch type. • **Mirror:** The switch is running in mirror mode. The source port(s) and destination port are located on this switch. • **Rmirror source:** The switch is a source node for monitor flow. The source port(s), reflector ports are located on this switch. • **Rmirror destination:** The switch is an end node for monitor flow. The destination port(s) is located on this switch.
VLAN ID	The VLAN ID points out where the monitor packet will copy to. The default VLAN ID is 200.
Reflector Port	The **reflector port** is a method to redirect the traffic to Remote Mirroring VLAN. Any device connected to a port set as a reflector port loses connectivity until the Remote Mirroring is disabled. In the stacking mode, you need to select the switch ID to select the correct device. If you shut down a port, it cannot be a candidate for a **reflector port**. If you shut down the port which is a **reflector port**, the remote mirror function cannot work. **Note1: The reflector port needs to select only on Source switch type.** **Note2: The reflector port needs to disable MAC Table learning and STP.**

	Note3: The reflector port only supports pure copper ports.

4.25 MRP

4.25.1 Ports

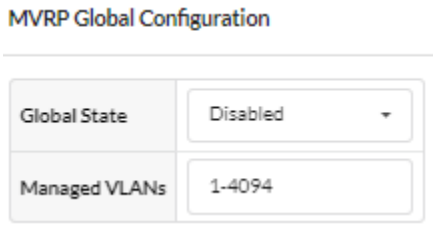


Setting	Description
Port	The port number for which the following configuration applies.
Join Timeout	Controls the timeout of the Join Timer for all MRP Applications on this switch port. This value is restricted to 1-20 centiseconds
Leave Timeout	Controls the timeout of the Leave Timer for all MRP Applications on this switch port. This value is restricted to 60 - 300 centiseconds.
LeaveAll Timeout	Controls the timeout of the LeaveAll Timer for all MRP Applications on this switch port. This value is restricted to 1000-5000 centiseconds.
Periodic Transmission	Enable or disable the PeriodicTransmission feature for all MRP Applications on this switch port.

4.25.2 MVRP

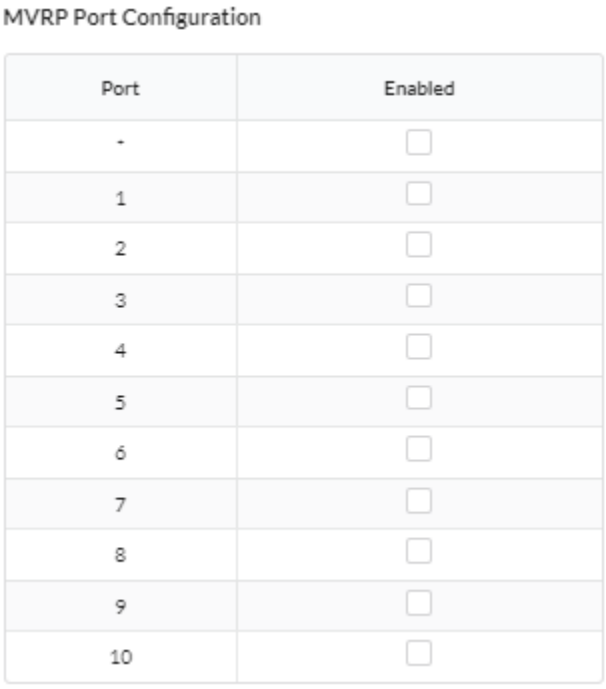
This page allows you to configure the MVRP global and per port settings altogether. The page is divided into a global section and a per-port configuration section.

MVRP Global Configuration



Setting	Description
Global State	Enable or disable the MVRP protocol globally. This will enable or disable the protocol globally and at the same time on the switch ports that are MVRP enabled
Managed VLANs	This field shows the managed VLANs, i.e. the VLANs that MVRP will operate upon. By default, only VLANs 1- 4094 are managed, i.e. the entire range as defined in IEEE802.1Q-2014 for MVRP. However this range can be limited 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.

MVRP Port Configuration

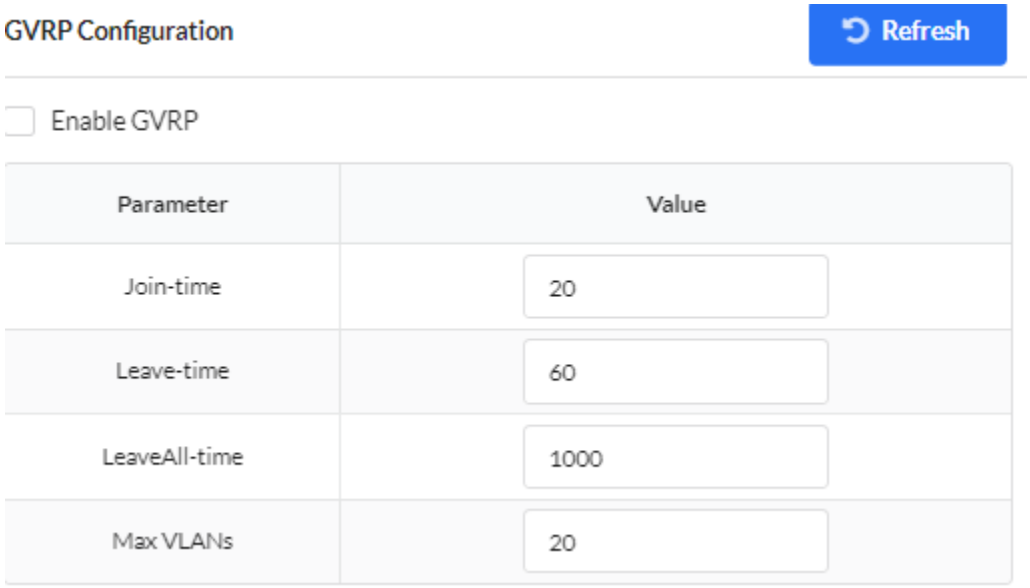


Setting	Description
Port	The port number for which the following configuration applies.
Enabled	Enabled or disable the MVRP protocol on this switch port. This will enable or disable the protocol on the switch port given that MVRP is also globally enabled.

4.26 GVRP

4.26.1 Global Config

This page allows you to configure the global GVRP configuration settings that are commonly applied to all GVRP enabled ports.



Enable GVRP

The GVRP feature is globally enabled by setting the check mark in the checkbox named Enable GVRP and pressing the Apply button.

Join-time

Setting	Description	Factory Default
1 ~ 20	Join-time is a value in the range of 1-20cs, i.e. in units of one hundredth of a second.	20

Leave-time

Setting	Description	Factory Default
60 ~ 300	Leave-time is a value in the range of 60-300cs, i.e. in units of one hundredth of a second.	60

LeaveAll-time

Setting	Description	Factory Default
1000 ~ 5000	LeaveAll-time is a value in the range of 1000-5000cs, i.e. in units of one hundredth of a second. The default is 1000cs.	1000

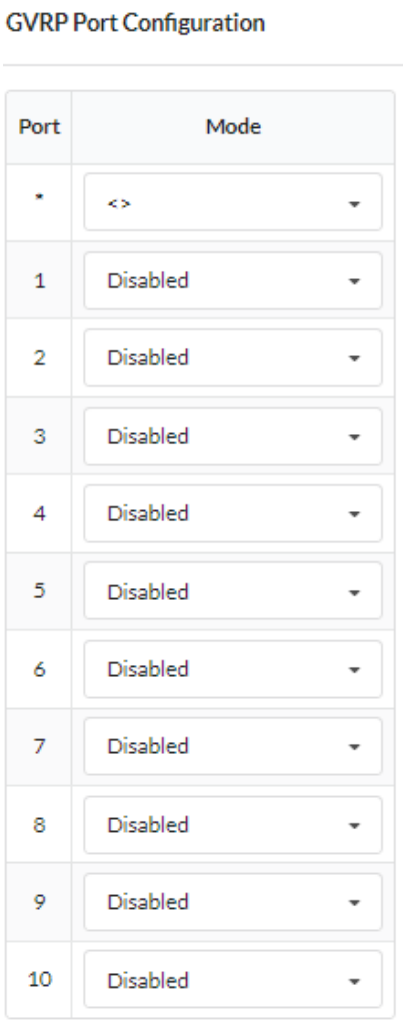
Max VLANs

Setting	Description	Factory Default
1 ~ 4094	When GVRP is enabled, a maximum number of VLANs supported by GVRP is specified. This number can only be changed when GVRP is turned off.	20

4.26.2 Port Config

This page allows you to enable or disable a port for GVRP operation.

This configuration can be performed either before or after GVRP is configured globally - the protocol operation will be the same.



Setting	Description
Port	The logical port that is to be configured.
Mode	Mode can be either **Disabled** or **Enabled**. These values turn the GVRP feature off or on respectively for the port in question.

4.27 sFLOW

sFLOW Configuration

This page allows for configuring sFlow. The configuration is divided into two parts: Configuration of the sFlow receiver (a.k.a. sFlow collector) and configuration of per-port flow and counter samplers.
sFlow configuration is not persisted to non-volatile memory, which means that a reboot will disable sFlow sampling.

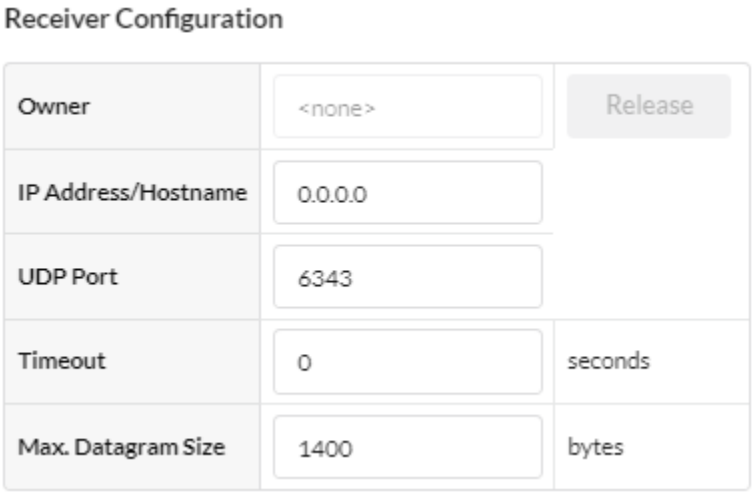
Agent Configuration



IP Address

Setting	Description	Factory Default
IP Address	The IP address used as Agent IP address in sFlow datagrams. It serves as a unique key that will identify this agent over extended periods of time. Both IPv4 and IPv6 addresses are supported.	127.0.0.1

Receiver Configuration



Owner

Basically, sFlow can be configured in two ways: Through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows:

- If sFlow is currently unconfigured/unclaimed, Owner contains **none**.
- If sFlow is currently configured through Web or CLI, Owner contains **Configure through local management**.
- If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.

If sFlow is configured through SNMP, all controls - except for the Release-button - are disabled to avoid inadvertent reconfiguration.
The "**Release"** button allows for releasing the current owner and disables sFlow sampling. The button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will appear).

IP Address/Hostname

Setting	Description	Factory Default
IP Address	The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.	0.0.0.0

UDP Port

Setting	Description	Factory Default
port number	The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0, the default port (6343) is used.	6343

Timeout

Setting	Description	Factory Default
0 ~ 2147483647	The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh button. If locally managed, the timeout can be changed on the fly without affecting other settings. The valid range is 0 to 2147483647 seconds.	0

Max. Datagram Size

Setting	Description	Factory Default
200 ~ 1468	The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. The valid range is 200 to 1468 bytes.	1400

Port Configuration

Port Configuration

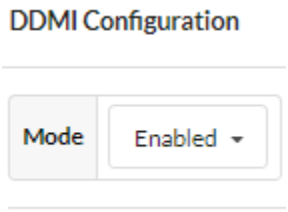
Port	Flow Sampler			Counter Poller	
	Enabled	Sampling Rate	Max. Header	Enabled	Interval
*	☐			☐	
1	☐	0	128	☐	0
2	☐	0	128	☐	0
3	☐	0	128	☐	0
4	☐	0	128	☐	0
5	☐	0	128	☐	0
6	☐	0	128	☐	0
7	☐	0	128	☐	0
8	☐	0	128	☐	0
9	☐	0	128	☐	0
10	☐	0	128	☐	0

Setting	Description
Port	The port number for which the configuration below applies.
Flow Sampler Enabled	Enables/disables flow sampling on this port.
Flow Sampler Sampling Rate	The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port. Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field. Valid range is 1 to 4294967295.
Flow Sampler Max. Header	The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes. To have room for any frame, the maximum datagram size should be roughly 100 bytes

	larger than the maximum header size. If the maximum datagram size does not take into account the maximum header size, samples may be dropped.
Counter Poller Enabled	Enables/disables counter polling on this port.
Counter Poller Interval	With counter polling enabled, this specifies the interval - in seconds - between counter poller samples. Valid range is 1 to 3600 seconds.

4.28 DDMI

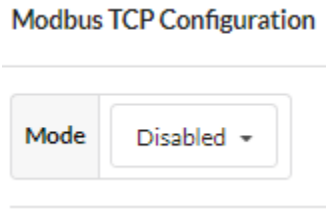
DDMI Configuration



Setting	Description	Factory Default
Mode	Indicates the DDMI mode operation. Possible modes are: **Enabled**: Enable DDMI mode operation. **Disabled**: Disable DDMI mode operation.	Enabled

4.29 Modbus TCP

Modbus TCP Configuration



Setting	Description	Factory Default
Mode	Indicates the MODBUS TCP mode operation. Possible modes are: **Enabled**: Enable MODBUS TCP mode operation. **Disabled**: Disable MODBUS TCP mode operation.	Disabled

Modbus TCP Register Table

Address Offset	Data Size (Words)	Interpretation	Read/Write	Description
System Information				
0x0000	1	HEX	Read	0x964D Antaira

				(This value refers to SNMP private enterprise number.)
0x0001	32	ASCII	Read	Model Name
0x0021	32	ASCII	Read	System Name
0x0041	32	ASCII	Read	System Location
0x0061	20	ASCII	Read	Version Code Ex. FW VERSION = “3.0.a1” Word 0 Hi byte = “3” Word 0 Lo byte = “.” Word 1 Hi byte = “0” Word 1 Lo byte = “.” Word 2 Hi byte = “a” Word 2 Lo byte = “1” Word 3 Hi byte = “\0” Word 3 Lo byte = “\0”
0x0075	5	ASCII	Read	FW Release Date: yyMMddHHmm
0x007a	32	ASCII	Read	Serial Number
0x009a	3	HEX	Read	MAC Address Ex. 00:11:22:33:44:55 Byte 0: 00 Byte 1: 11 Byte 2: 22 Byte 3: 33 Byte 4: 44 Byte 5: 55
0x009d	1	HEX	Read	Power 1 Status 0x0000: ON 0x0001: OFF
0x009e	1	HEX	Read	Power 2 Status 0x0000: ON 0x0001: OFF
0x009f	1	HEX	Read	Relay Status 0x0000: Open 0x0001: Close

Address Offset	Data Size (Words)	Interpretation	Read/Write	Description
Port Information				
0x1000 ~ 0x103F	1	HEX	Read	Port 1~64 Status 0x0000: link down 0x0001: link up 0x0002: disabled 0xFFFF: no port
0x1100 ~ 0x113F	1	HEX	Read	Port 1~64 Speed 0x0000: 10M-Half

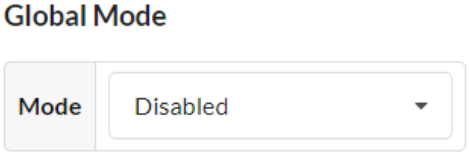
				0x0001: 10M-Full 0x0002: 100M-Half 0x0003: 100M-Full 0x0004: 1G 0x0005: 10G 0xFFFF: no port
0x1200 ~ 0x123F	1	HEX	Read	Port 1~64 Flow Control 0x0000: off 0x0001: tx on 0x0002: rx on 0x0003: tx on and rx on 0xFFFF: no port
Packets Information				
0x2000 ~ 0x20FF	4	HEX	Read	Port 1~64 TX Packets Ex: port 1 Tx Packets = 1234605616436508552 MODBUS response: 0x1122334455667788 Word 0 = 1122 Word 1 = 3344 Word 2 = 5566 Word 3 = 7788
0x2200 ~ 0x22FF	4	HEX	Read	Port 1~64 RX Packets
0x2400 ~ 0x24FF	4	HEX	Read	Port 1~64 TX Error Packets
0x2600 ~ 0x26FF	4	HEX	Read	Port 1~64 RX Error Packets

4.30 NAT

4.30.1 Global Config

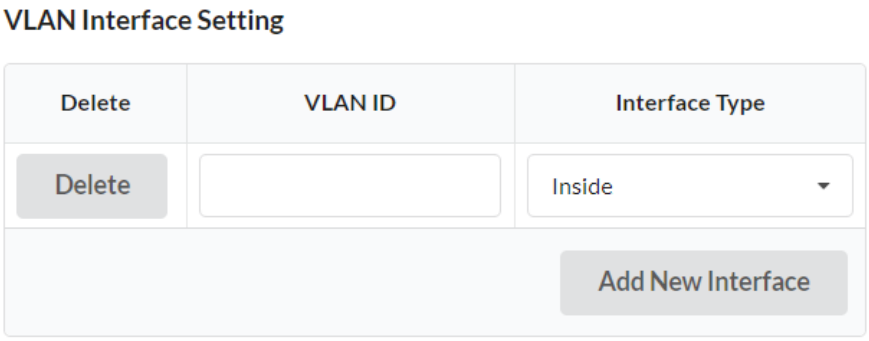
Network Address Translation(NAT) is a method that can translate (a) private IP address(es) to another public IP address(es), in an attempt to provide transparent routing to hosts. NAT allows users on private networks to access public networks.
The NAT mode can turn on/off NAT operation.
The VLAN interface setting can set VLAN interface with NAT interface type. Please make sure the VLAN is already set IP and bind one or more physical ports.

Global Mode



Setting	Description	Factory Default
Mode	Indicates the NAT global mode operation. If turn off the NAT global mode, the VLAN interface setting and Rules configuration will not be removed, but the NAT function cannot work. Otherwise, if the NAT mode is turned on, the NAT function will work and the valid rules will also work well. Possible modes are: **Enabled**: Enable NAT global mode operation. When NAT global mode operation is enabled, all the valid rules will work. **Disabled**: Disable NAT global mode operation.	Disabled

VLAN Interface Setting

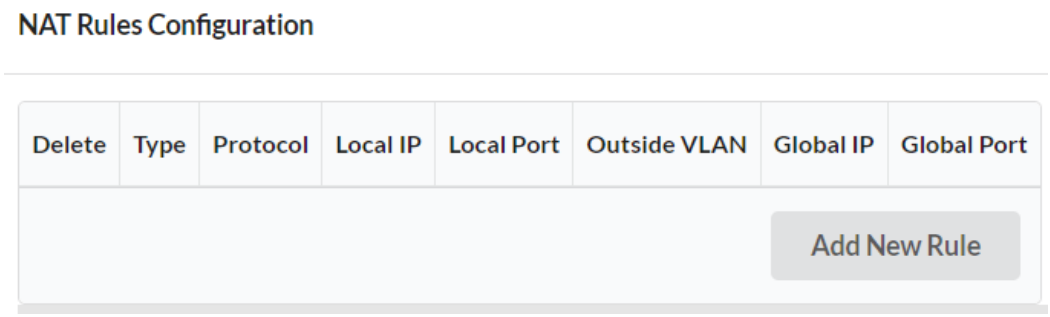


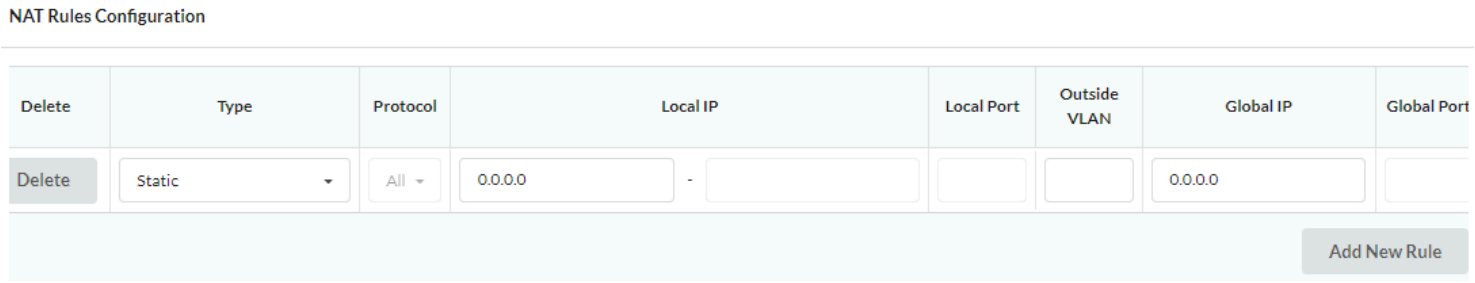
Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	Choose an ID VLAN as NAT VLAN inside or outside interface. The chosen VLAN interface should be created, and have a valid IP address and bind with a physical port. There are some rules for using the settings shown as following: ***Case1***. If delete an existing VLAN interface, the related rules configuration will not be removed, but the related rules configuration cannot work. However, if you add the VLAN interface with the **same** IP address back, the related rules configuration will work. ***Case2***. If delete an existing VLAN interface and then add the VLAN interface with a **different** IP address back, the related rules configuration which is matched the IP address or VLAN ID will work. However, the related rules configuration which does not match the IP address or VLAN IP will not work. For the situation, please remove the invalid or un-worked rules configuration manually. ***Case 3***. When the VLAN, IP address or ports have been changed, please clear the NAT interface first, and then please set the NAT interface to the VLAN again once the changing has been finished.

Interface Type	Indicates the NAT interface type. **Inside:** Indicates the VLAN ID belongs to NAT inside interface type. The number of ports which are inside the interface cannot exceed “total port – 4.” **Outside:** Indicates the VLAN ID belongs to NAT outside interface type. The number of ports which is outside interface cannot exceed ‘4’

4.30.2 Rules Config

Network Address Translation(NAT) is a method that can translate (a) private IP address(es) to another public IP address(es), in an attempt to provide transparent routing to hosts. NAT allows users on private networks to access public networks.
This configuration can set NAT rules.





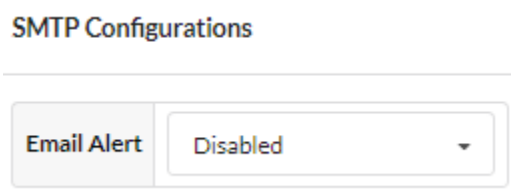
Setting	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Type	Indicates the NAT type. **Static**: Indicates NAT Static type which can implement one-to-one translation between one private IP address and one public IP address. **Overloading**: Indicates NAT overloading (also called dynamic port address translation(PAT)) type which can implement one-to-many translation between one public IP address and multiple private IP addresses. **Port-Forwarding**: Indicates port-forwarding type which allows remote computers with a public IP address to connect to a specific computer or service within a private IP address.
Protocol	Indicates protocol type for port-forwarding.

	ALL: Indicates both TCP and UDP protocols. **UDP**: Indicates UDP protocol. **TCP**: Indicates TCP protocol.
Local IP	Indicates inside local IP address. The local IP should be in the range of IP addresses that matched NAT VLAN with the inside interface. The local IP range is displayed for the NAT overloading type.
Local Port	Indicates inside local socket port number for port-forwarding type.
Outside VLAN	Indicates VLAN interface for global address. Please choose the VLAN ID which is NAT VLAN with outside interface.
Global IP	Indicates inside global IP address. The global IP should be the IP address of the global VLAN interface. Please write the matched IP address of the global VLAN ID interface for static NAT type.
Global Port	Indicates inside global socket port number for port-forwarding type.

4.31 SMTP

Configure SMTP on this page. Before sending SMTP configuration, you need to set DNS Server, IP Routes and enable SMTP access in your Email account settings.

SMTP Configuration

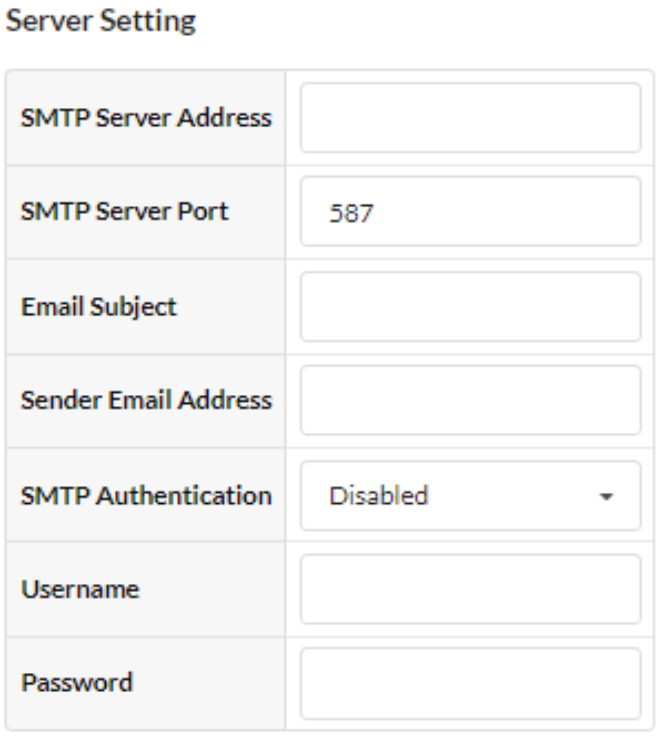


Setting	Description
Email Alert	Indicates the SMTP mode operation. Possible modes are:

	Enabled: Enable sending Email when event mode operation. **Disabled**: Disable to send Email when event mode operation.

Note: When Email Alert is "Enabled", users should configure the **Server Setting** and **Recipient Setting** completely before clicking on the "Save" or "Test" button. The related fields should not be blank.

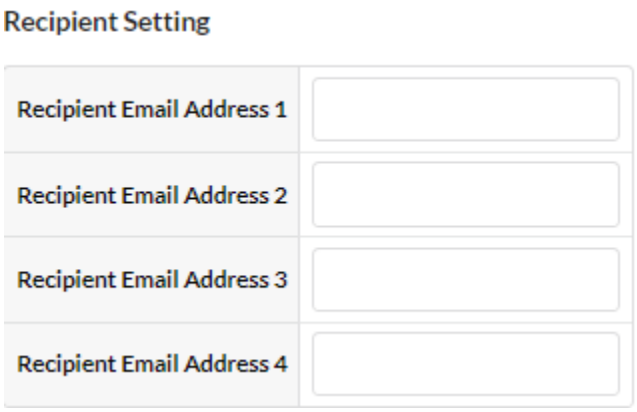
Server Setting



Setting	Description
SMTP Server Address	This is the IP address or URL of the SMTP Server. The allowed string length is 0 to 253. Example: smtp.gmail.com
SMTP Server Port	This field is the port listening on the server for the SMTP request. The default Server Port is **587**. Common Port: 25 or 587 (SMTP STARTTLS), don't support 465 (SMTP SSL). The allowed value is 1 to 65535.
Email Subject	The first text you see when you receive the Email. The allowed string length is 0 to 255.
Sender Email Address	When an event warning is triggered, the notification Email will be sent from the configured Sender Email Address. The allowed string length is 0 to 255.

	Email Address = "account@domain". The maximum string length of the account is 64.
SMTP Authentication	Indicates the SMTP authentication mode operation. Possible modes are: **Enabled:** Enable if the SMTP server needs authentication. **Disabled**: Disable if the SMTP server doesn't need authentication. ***Note:*** When **SMTP Authentication** is "**Enabled**", users should configure the **Username** and **Password** completely before clicking on the "Apply" or "Test" button. It's not allowed to leave the fields blank.
Username	When an event warning is triggered and SMTP authentication is enabled, the configured Username is used in authentication with the SMTP server. The allowed string length is 0 to 255.
Password	When an event warning is triggered and SMTP authentication is enabled, the configured Password is used in authentication with the SMTP server. The allowed string length is 0 to 100. ***Note:*** If the Email server supports "Application Passwords", it's also allowed to use "Application Passwords" to authenticate users without providing the passwords directly.

Recipient Setting



Recipient Email Address

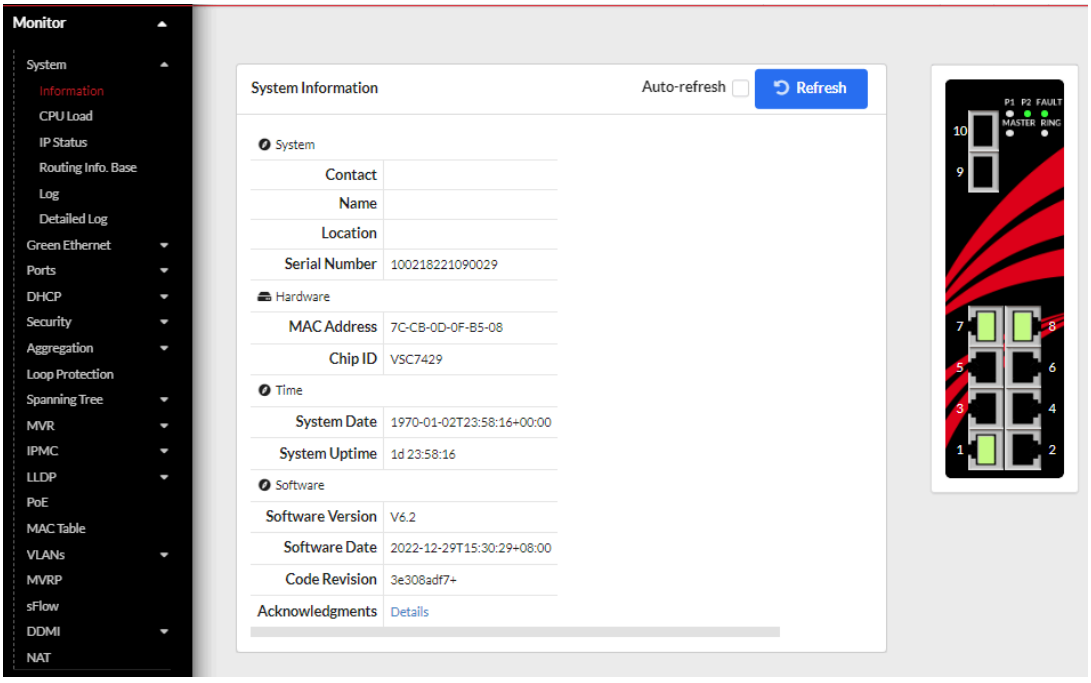
When an event warning is triggered, the system will send Email to the recipient(s). The allowed string length is 0 to 255. When Email Alert is enabled, this field should be filled with at least one recipient Email address.

Email address = "account@domain". The maximum string length of the account is 64.

5 Monitor

5.1 System

5.1.1 Information



System Information

Check Box	Description
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Port Status

Check Box	Description
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Check Box

Check Box	Description
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

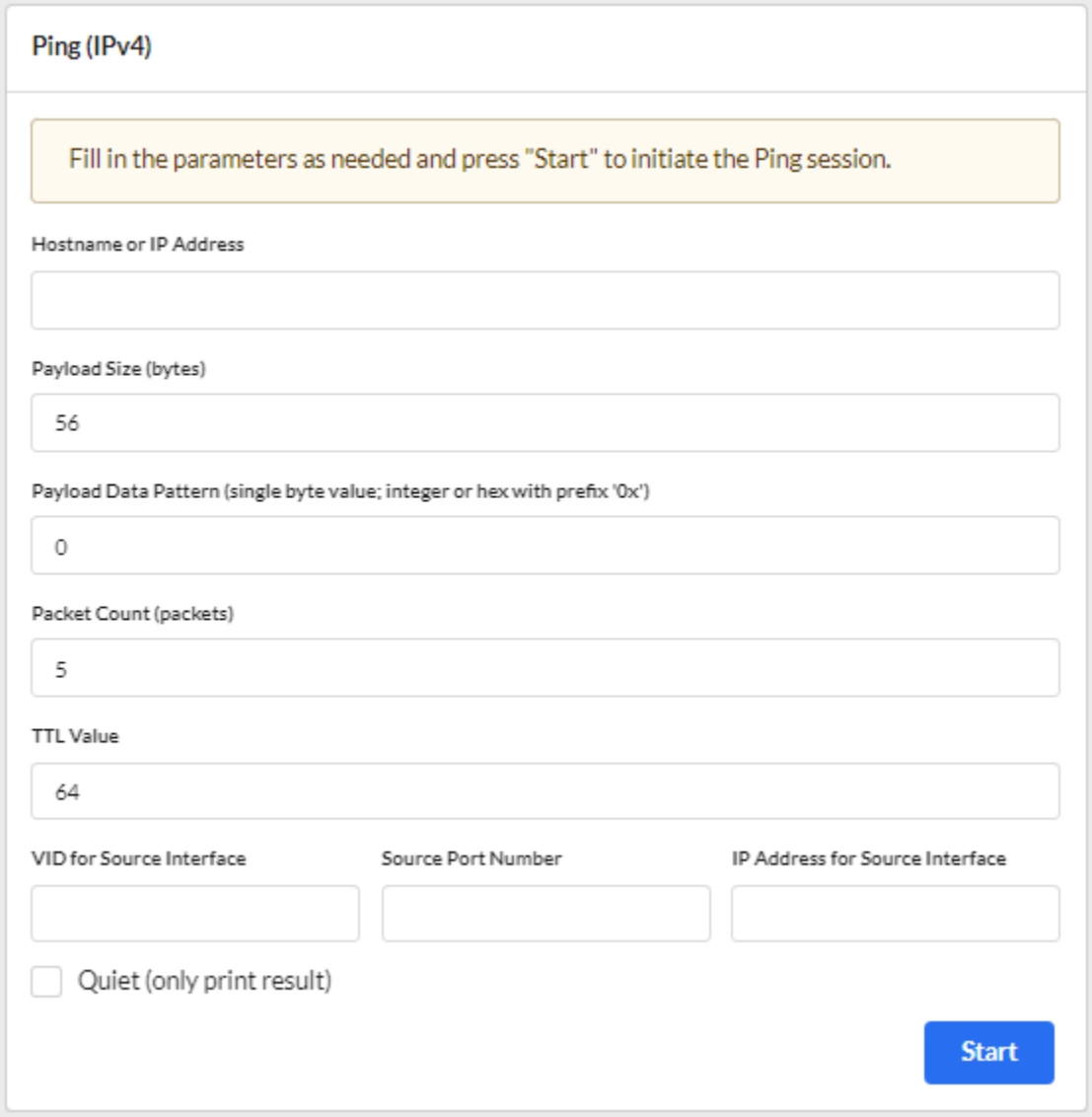
Buttons

Button	Description
Refresh	Click to refresh the page.

6 Diagnostics

6.1 Ping (IPv4)

This page allows you to issue ICMP (IPv4) PING packets to troubleshoot IP connectivity issues.



Setting	Description
Hostname or IP Address	The address of the destination host, either as a symbolic hostname or an IP Address.
Payload Size	Determines the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP and ICMP headers). The default value is 56 bytes. The valid range is 2-1452 bytes.
Payload Data Pattern	Determines the pattern used in the ICMP data payload. The default value is 0. The valid range is 0-255.

Packet Count	Determines the number of PING requests sent. The default value is 5. The valid range is 1-60.
TTL Value	Determines the Time-To-Live /TTL) field value in the IPv4 header. The default value is 64. The valid range is 1-255.
VID for Source Interface	This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.
Source Port Number	This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the Source Port Number or the IP Address for the source interface.
Address for Source Interface	This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.
Quiet (only print result)	Checking this option will not print the result of each ping request but will only show the final result.

After you press **Start**, ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply.

The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested payload data size (the difference is the ICMP header).

The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

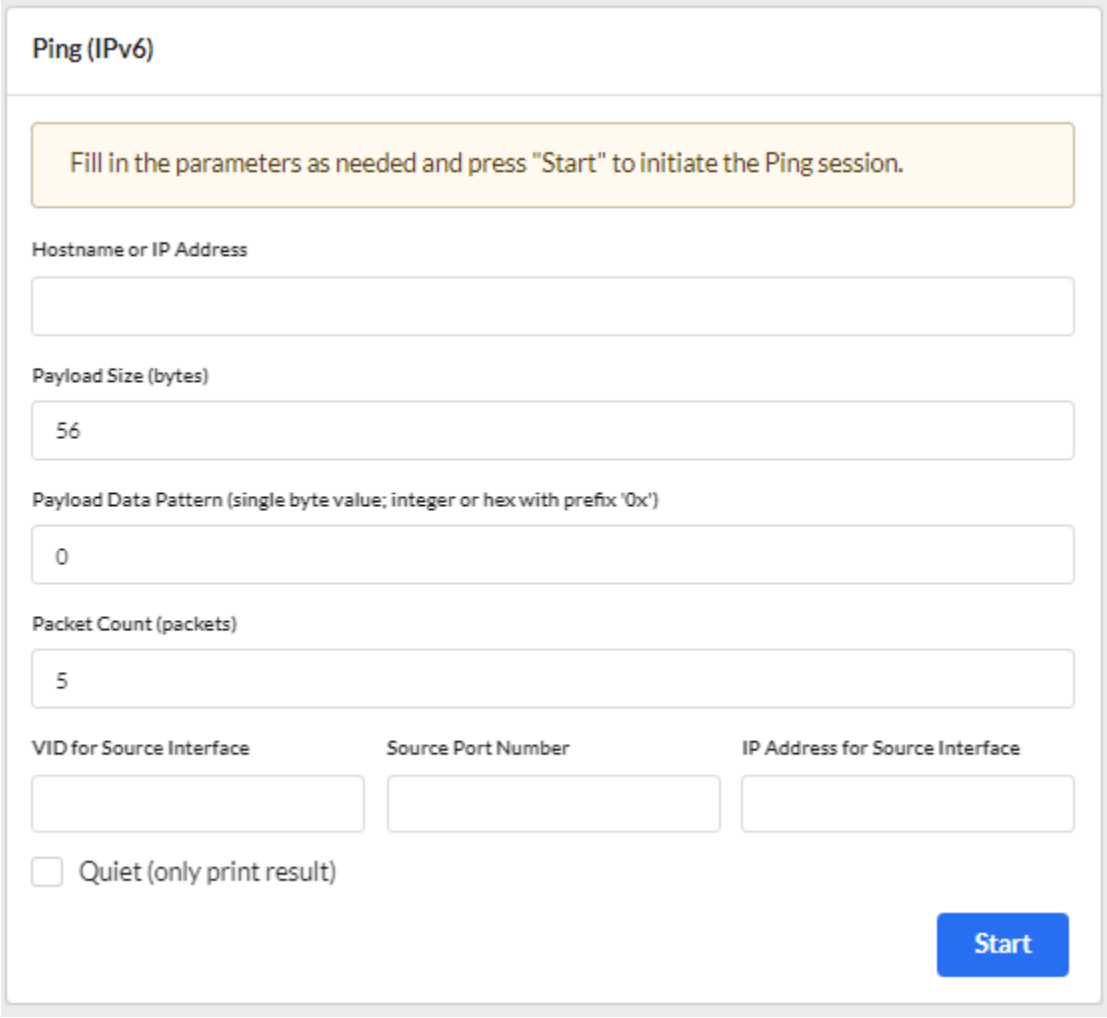
The output from the command will look like the following:

PING 172.16.1.1 (172.16.1.1) from 172.16.1.10: 56 data bytes
64 bytes from 172.16.1.1: seq=0 ttl=64 time=2.034 ms
64 bytes from 172.16.1.1: seq=1 ttl=64 time=1.729 ms
64 bytes from 172.16.1.1: seq=2 ttl=64 time=1.954 ms
64 bytes from 172.16.1.1: seq=3 ttl=64 time=1.699 ms
64 bytes from 172.16.1.1: seq=4 ttl=64 time=1.916 ms

--- 172.16.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.699/1.866/2.034 ms

6.2 Ping (IPv6)

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.



Setting	Description
Hostname or IP Address	The address of the destination host, either as a symbolic hostname or an IP Address.
Payload Size	Determines the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP and ICMP headers). The default value is 56 bytes. The valid range is 2-1452 bytes.
Payload Data Pattern	Determines the pattern used in the ICMP data payload. The default value is 0. The valid range is 0-255.
Packet Count	Determines the number of PING requests sent. The default value is 5. The valid range is 1-60.
VID for Source Interface	This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration.

	Note: You may only specify either the VID or the IP Address for the source interface.
Source Port Number	This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the Source Port Number or the IP Address for the source interface.
Address for Source Interface	This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.
Quiet (only print result)	Checking this option will not print the result of each ping request but will only show the final result.

After you press **Start** ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply.

The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested payload data size (the difference is the ICMP header).

The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

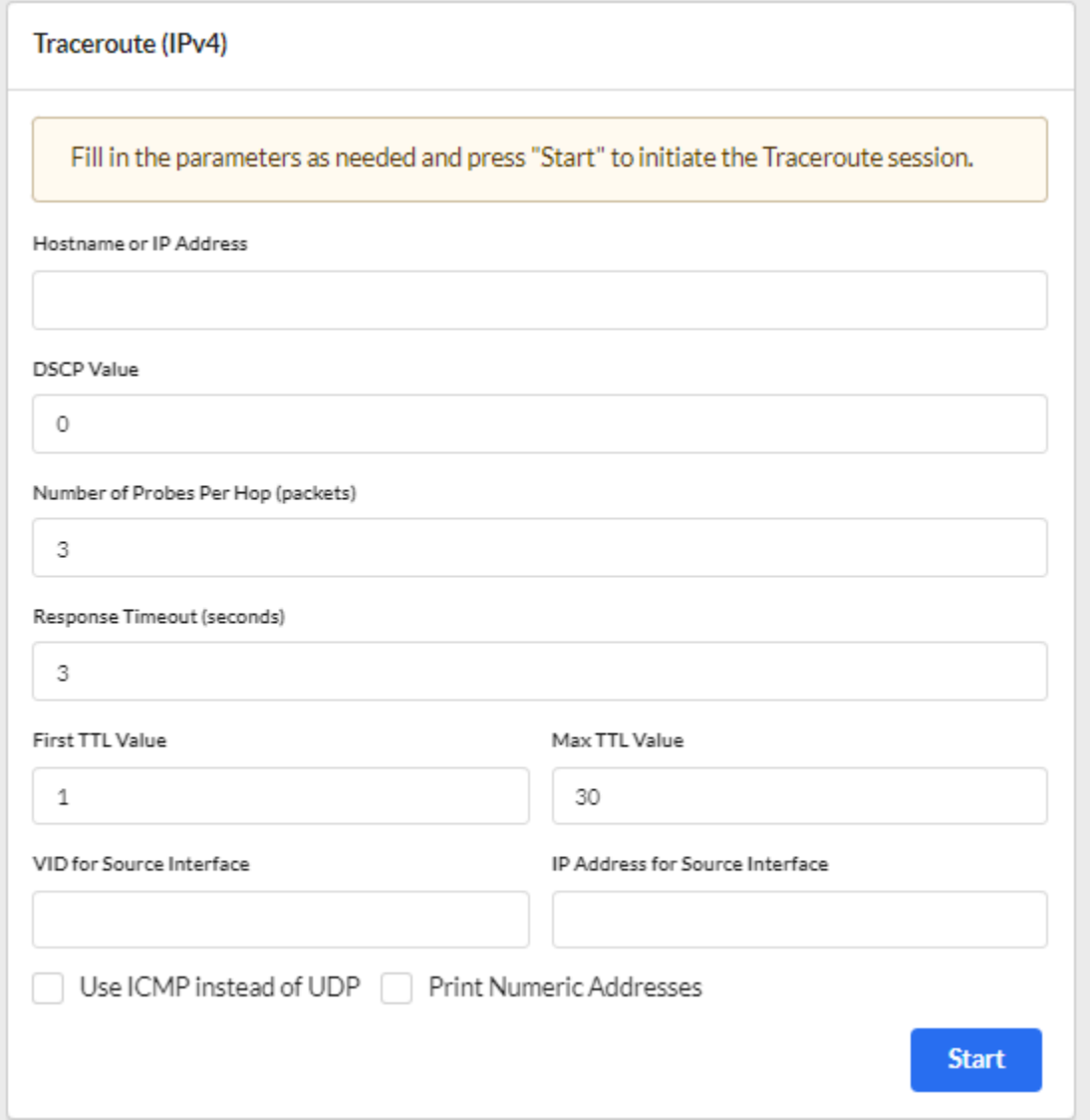
The output from the command will look like the following:

PING 2001::01 (2001::1) from 2001::3: 56 data bytes
64 bytes from 2001::1: seq=0 ttl=64 time=2.118 ms
64 bytes from 2001::1: seq=1 ttl=64 time=2.009 ms
64 bytes from 2001::1: seq=2 ttl=64 time=1.852 ms
64 bytes from 2001::1: seq=3 ttl=64 time=2.869 ms
64 bytes from 2001::1: seq=4 ttl=64 time=1.845 ms

--- 2001::01 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.845/2.138/2.869 ms

6.3 Traceroute (IPv4)

This page allows you to perform a traceroute test over IPv4 towards a remote host. traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv4 network.

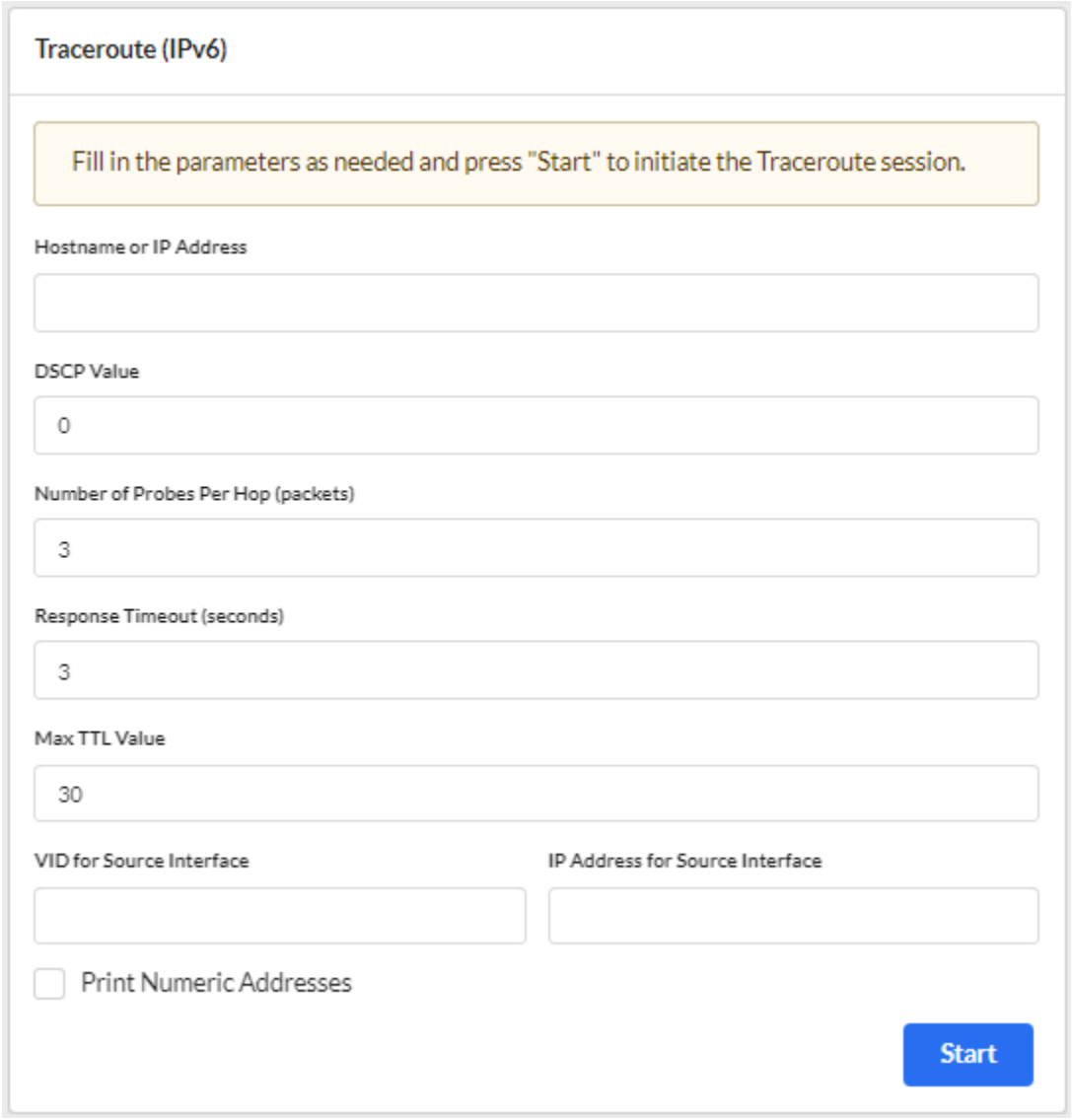


Setting	Description
Hostname or IP Address	The destination IP Address.
DSCP Value	This value is used for the DSCP value in the IPv4 header. The default value is 0. The valid range is 0-63.
Number of Probes Per Hop	Determines the number of probes (packets) sent for each hop. The default value is 3. The valid range is 1-60.
Response Timeout	Determines the number of seconds to wait for a reply to a sent request. The default number is 3. The valid range is 1-86400.
First TTL Value	Determines the value of the Time-To-Live (TTL) field in the IPv4 header in the first packet sent. The default number is 1. The valid range is 1-30.

Max TTL Value	Determines the maximum value of the Time-To-Live (TTL) field in the IPv4 header. If this value is reached before the specified remote host is reached the test stops. The default number is 30. The valid range is 1-255.
VID for Source Interface	This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.
Address for Source Interface	This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.
Use ICMP instead of UDP	By default the traceroute command will use UDP datagrams. Selecting this option forces it to use ICMP ECHO packets instead.
Print Numeric Addresses	By default the **traceroute** command will print out hop information using a reverse DNS lookup for the acquired host ip addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the traceroute command to print numeric IP addresses instead.

6.4 Traceroute (IPv6)

This page allows you to perform a traceroute test over IPv6 towards a remote host. traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv6 network.

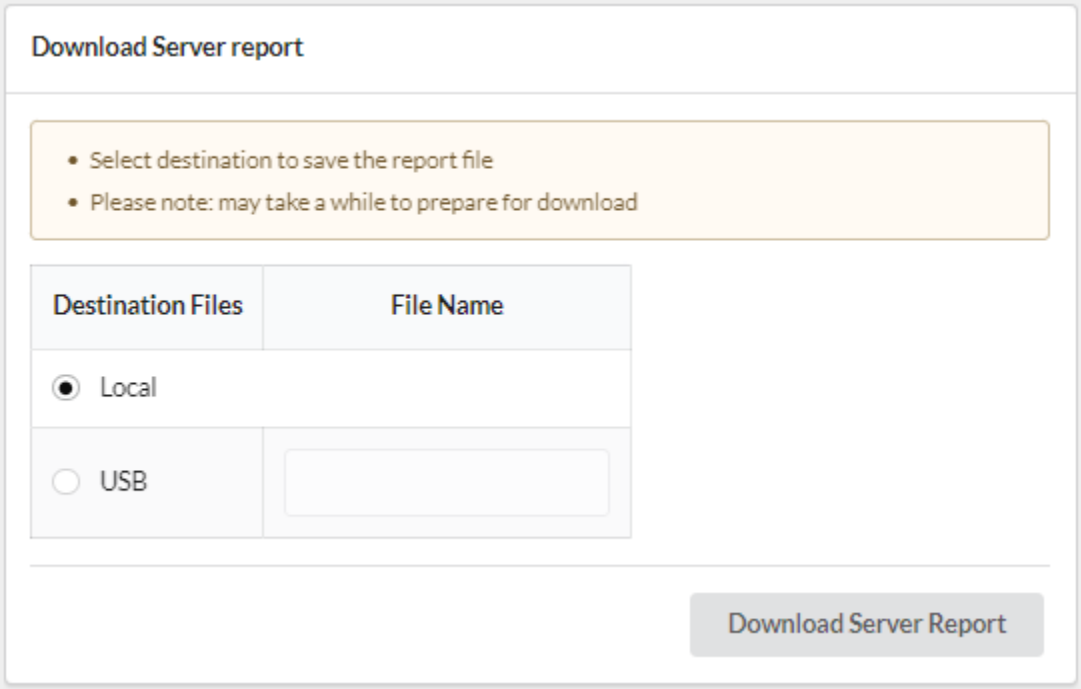


Setting	Description
Hostname or IP Address	The destination IP Address.
DSCP Value	This value is used for the DSCP value in the IPv4 header. The default value is 0. The valid range is 0-255.
Number of Probes Per Hop	Determines the number of probes (packets) sent for each hop. The default value is 3. The valid range is 1-60.
Response Timeout	Determines the number of seconds to wait for a reply to a sent request. The default number is 3. The valid range is 1-86400.
Max TTL Value	Determines the maximum value of the Time-To-Live (TTL) field in the IPv4 header. If this value is reached before the specified remote host is reached the test stops. The default number is 30. The valid range is 1-255.

VID for Source Interface	This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.
Address for Source Interface	This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.
Print Numeric Addresses	By default the **traceroute** command will print out hop information using a reverse DNS lookup for the acquired host ip addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the traceroute command to print numeric IP addresses instead.

6.5 Server Report

It is possible to download a server report file of the switch from the web browser.



Downloading server-report.txt may take a little while to complete, as the file must be prepared for download.

- Local: Download the file with the default file name server-report.txt to the local file destination.
- USB: Download the file to the USB Drive. Users can choose the file name from the default options or enter the file name of the target server report file.

  Please note valid files names can only contain the following characters, use of other characters will produce an invalid name.

  A-Z, a-z (English Alphabet)

  0-9 (Arabic Numerals)

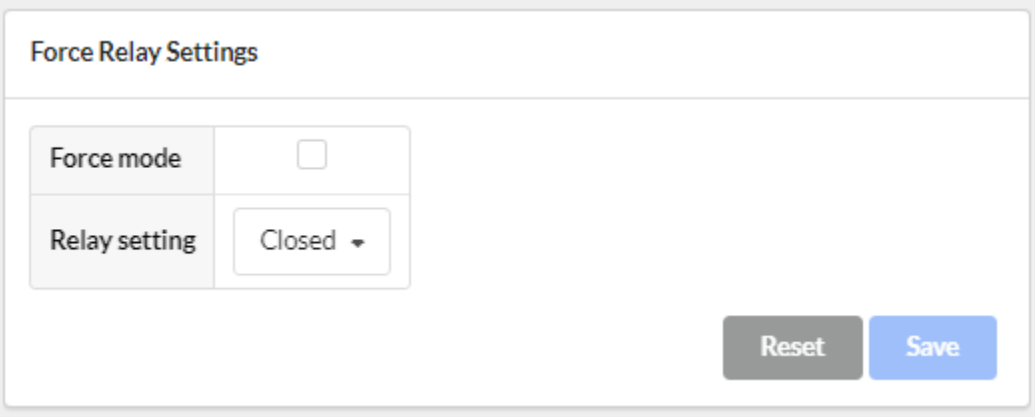
  . (Period)

  - (Dash)

  _ (Underline)

When the USB Drive mode is disabled, the file destination of USB will become invalid.

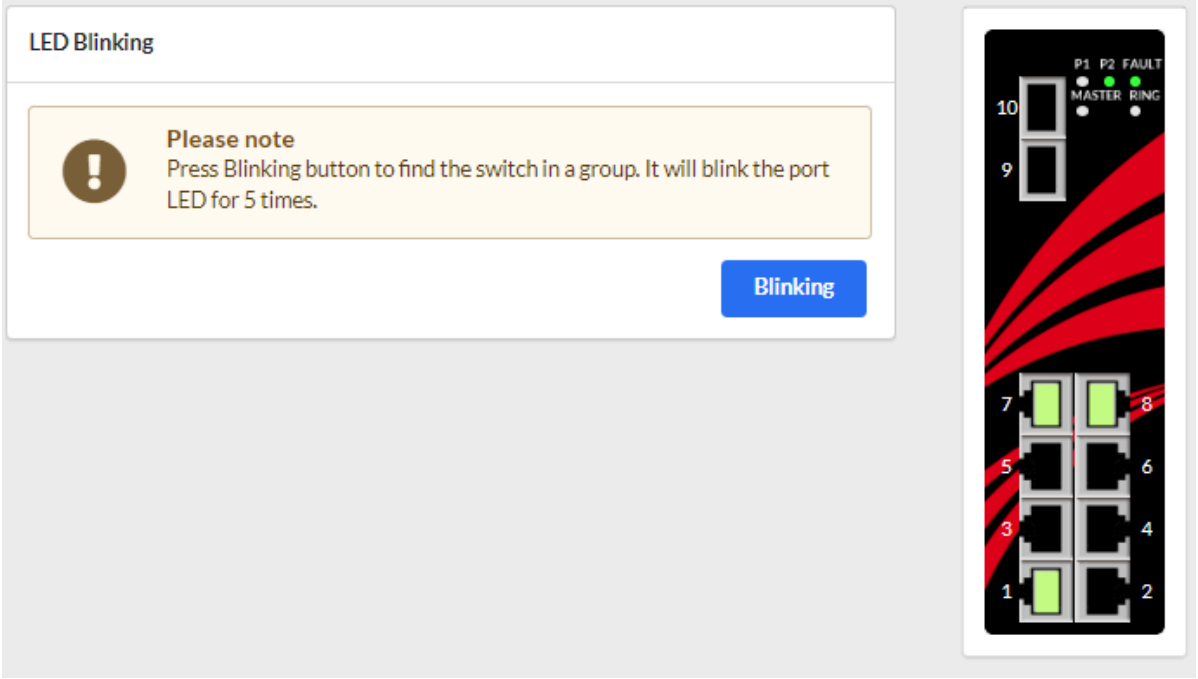
6.6 Relay



Setting	Description
Force mode	Force relay into debug mode. In force mode, the relay will keep in one status that users set (Opened/Closed). In other words, it can not be switch from other events
Relay Setting	**Opened:** Set Fault Contact in the opened state. **Closed**: Set Fault Contact in the closed state.

6.7 LED Blinking

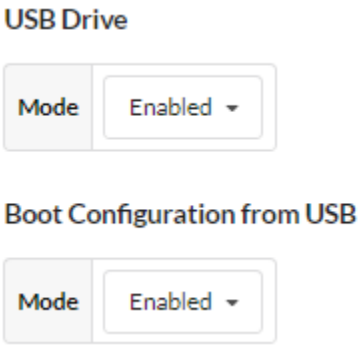
This feature helps users find the specific switch in a group. It will blink the port LED 5 times after users press the Blinking button.



7 Maintenance

7.1 USB

The switch supports the configuration backup and restore features with USB Drive.



USB Drive

USB Drive feature is used for backing up and restoring configuration files to the USB drive.

Setting	Description	Factory Default
Enabled	Enable the USB Drive for configuration backup and restore.	Enabled
Disabled	Disable the USB Drive for configuration backup and restore.	

Additionally, by disabling this feature the ability to write the running configuration file to the USB drive by tapping on the reset button will also be disabled.

Boot Configuration from USB

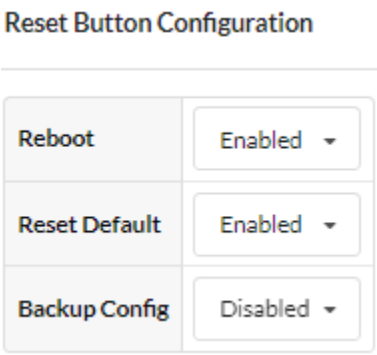
Boot Configuration from USB is to allow the switch to boot up using the configuration file on the USB drive.

The switch will first look for a configuration file containing the model name plus the MAC address of the specific switch, if that is not found it will look for a file name with just the model number, if that fails it will use the configuration file found in the switch's memory .

Setting	Description	Factory Default
Enabled	Enable the Boot Configuration from USB.	Enabled
Disabled	Disable the Boot Configuration from USB.	

7.2 Reset Button

Reset Button Configuration

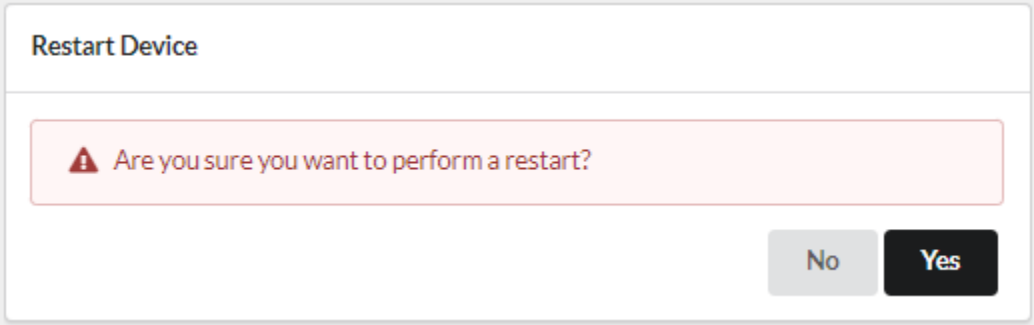


Configure operation mode of Reset Button to enable/disable.

Setting	Description	Factory Default
Reboot	Reboot: 0 < t(press time) < 4 seconds, Status LED is flashing with green color. **Enabled**: Enable reboot operation. **Disabled**: Disable reboot operation.	Enabled
Reset Default	Reset to factory default: 4 < t(press time) < 8 seconds, Status LED is flashing with green and red color. **Enabled**: Enable reset default operation. **Disabled**: Disable reset default operation.	
Backup Config	Backup configuration to USB: 8 < t(press time), Status LED is flashing with red color. (for startup-config) **Enabled**: Enable backup config operation. **Disabled**: Disable backup config operation.	Disabled

7.3 Restart Device

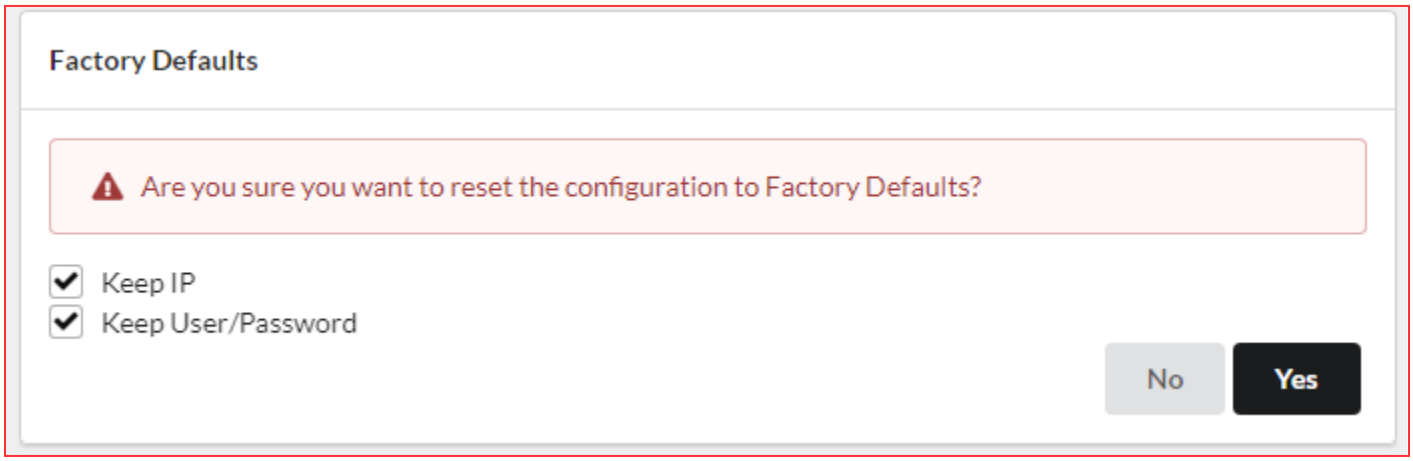
Restart Device



You can restart the switch on this page. After restart, the switch will boot normally.
Click **Yes** to restart the device.
Click **No** to return to the Dashboard page without restarting.

7.4 Factory Defaults

You can reset the configuration of the switch on this page. Only the IP configuration is retained. The new configuration is available immediately, which means that no restart is necessary.



Click **Yes** to reset the configuration to Factory Defaults.
Click **No** to return to the Dashboard page without resetting the configuration.

Keep IP

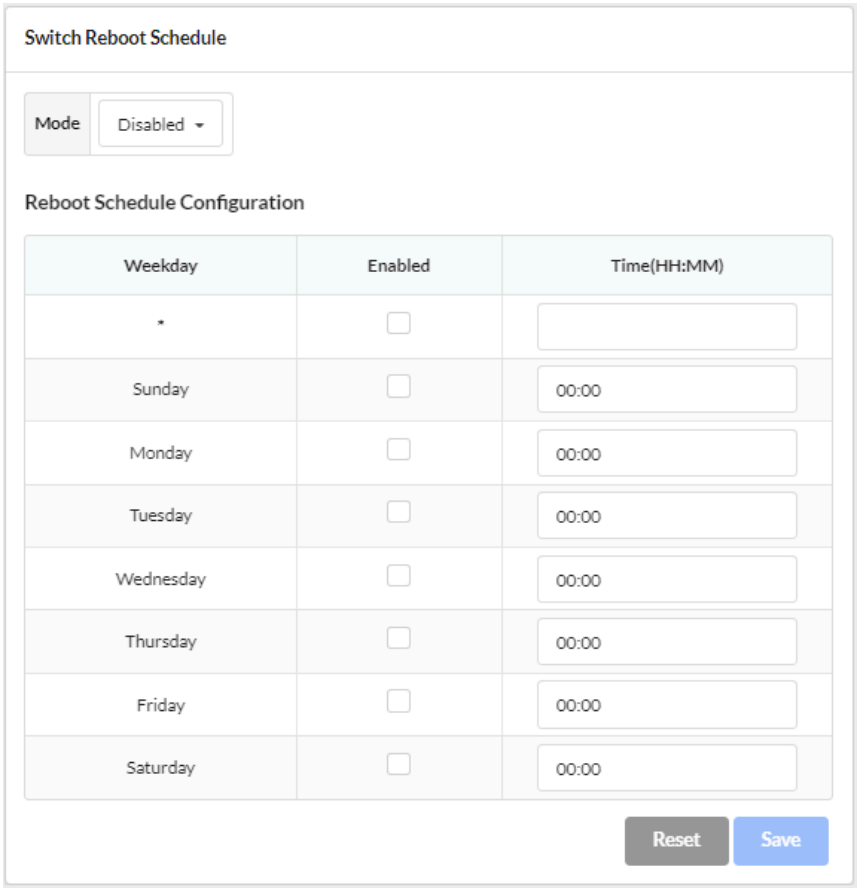
Keep the IP Address after you reset the configuration to the state of factory default.

Keep User/Password

Keep all usernames and passwords that you created in the system.

7.5 Reboot Schedule

This page allows the user to configure the reboot schedule time.



Setting	Description	Factory Default
Mode	**Enabled**: Enable switch reboot scheduling. **Disabled**: Disable switch reboot scheduling.	Disabled
Reboot Schedule Configuration	**Weekday**: The day to reboot this switch. **Enabled**: Activate this schedule on the day of the week. **Time**: Timetabling. Format: hh:mm; hh: 00 ~ 23, mm: 00 ~ 59.	

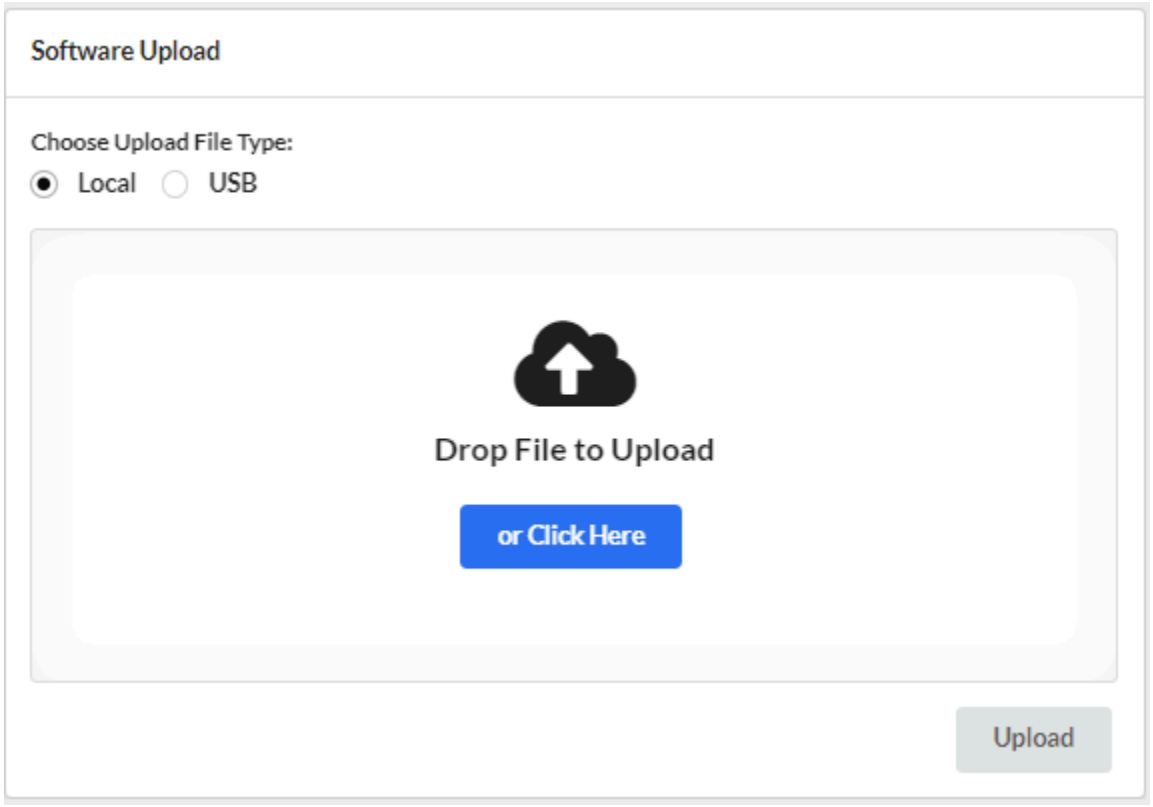
7.6 Software

7.6.1 Upload

This page facilitates an update of the firmware controlling the switch.

The file source can be:
Local: Upload the file from the local server.
USB: Upload the file from the USB Drive.

Please note that when the USB Drive mode is disabled, the file destination of USB will become invalid.



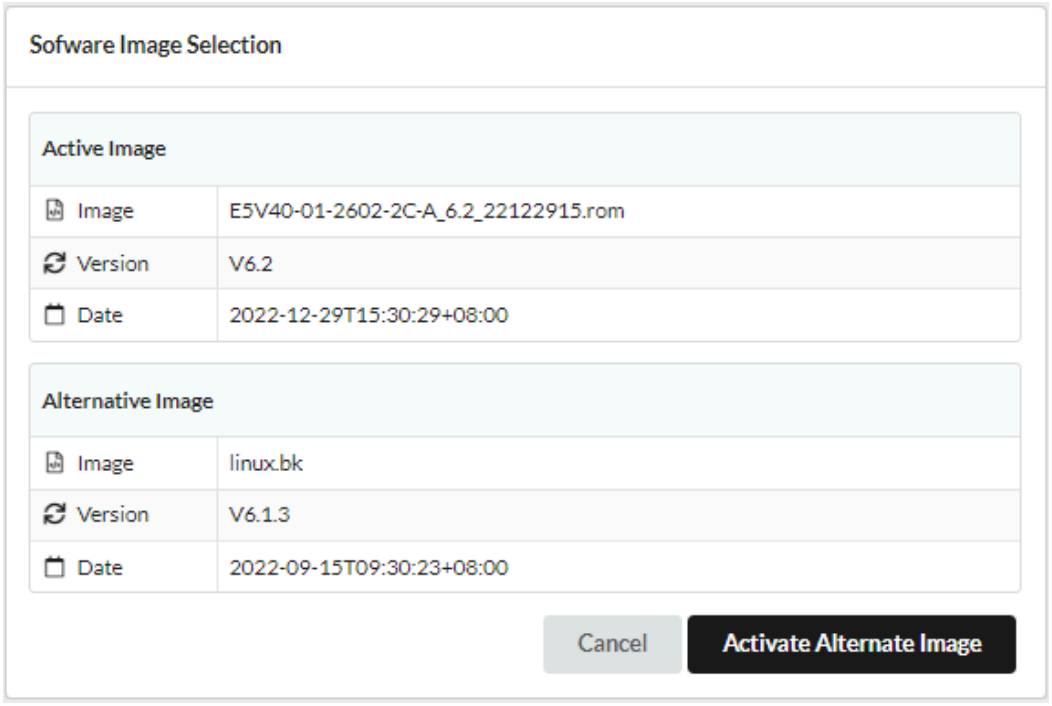
WARNING:

Warning: *While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress.* ***Do not restart or power off the device at this time*** *or the switch may fail to function afterwards.*

7.6.2 Image Select

This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.

The web page displays two tables with information about the active and alternate firmware images.



NOTE:

1. In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the **Activate Alternate Image** button is also disabled.
2. If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.
3. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

Image Information

Setting	Description
Image	The file name of the firmware image, from when the image was last updated.
Version	The version of the firmware image.
Date	The date where the firmware was produced.

Click **Activate Alternate Image** to use the alternate image. This button may be disabled depending on system state.
Click **Cancel** to activate the backup image. Navigates away from this page.

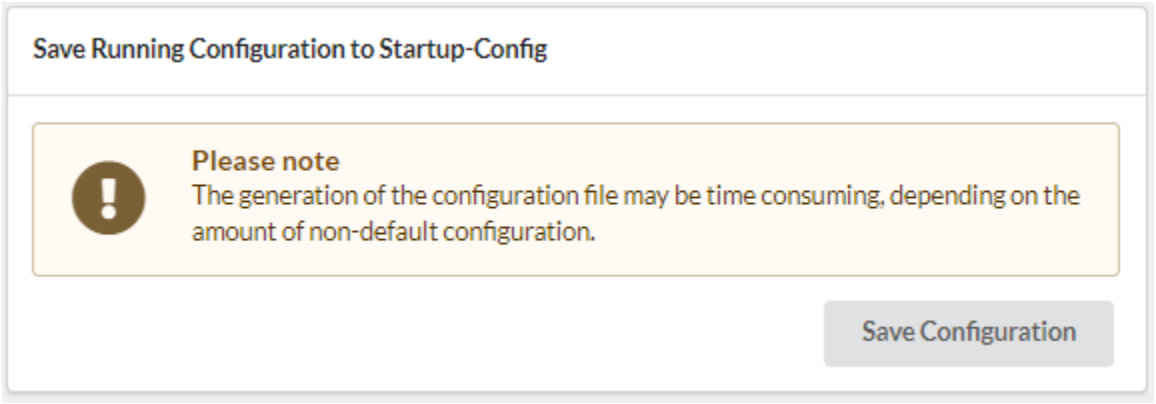
7.7 Configuration

The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch.
The available files are:

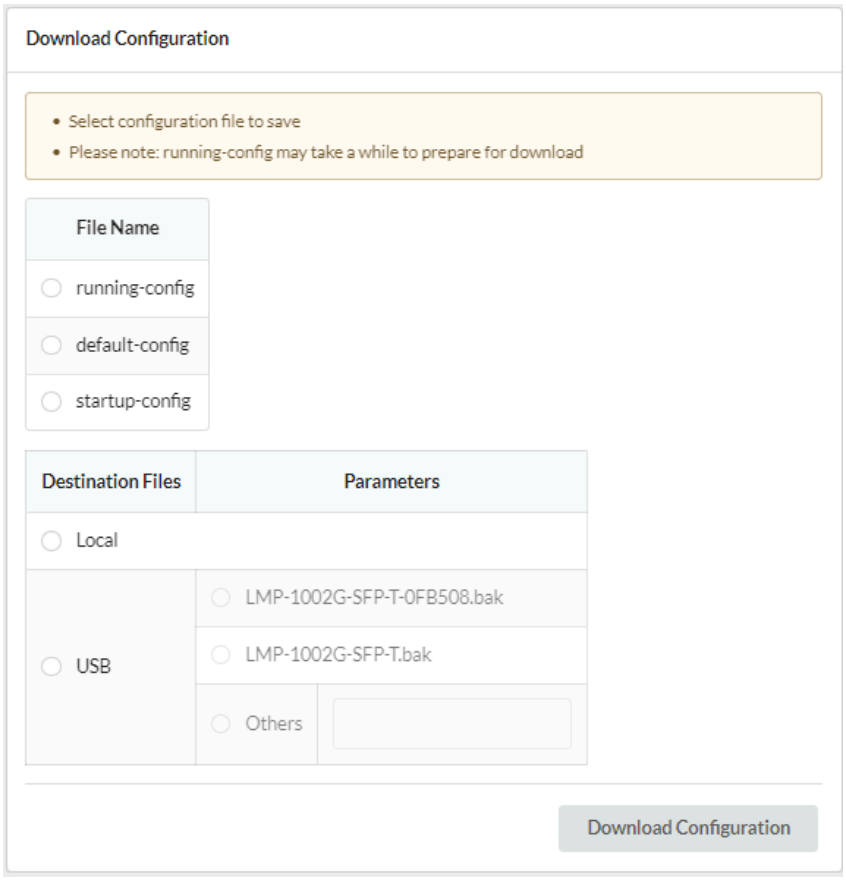
- running-config: A virtual file that represents the currently active configuration on the switch. This file is volatile.
- startup-config: The startup configuration for the switch, read at boot time. If this file doesn't exist at boot time, the switch will start up in default configuration.
- default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.
- Up to 31 other files, typically used for configuration backups or alternative configurations.

7.7.1 Save Start-up Config

This copies running-config to startup-config, thereby ensuring that the currently active configuration will be used at the next reboot.



7.7.2 Download



It is possible to download any of the files on the switch to the web browser or the USB Drive. Select the file and click **Download Configuration**.

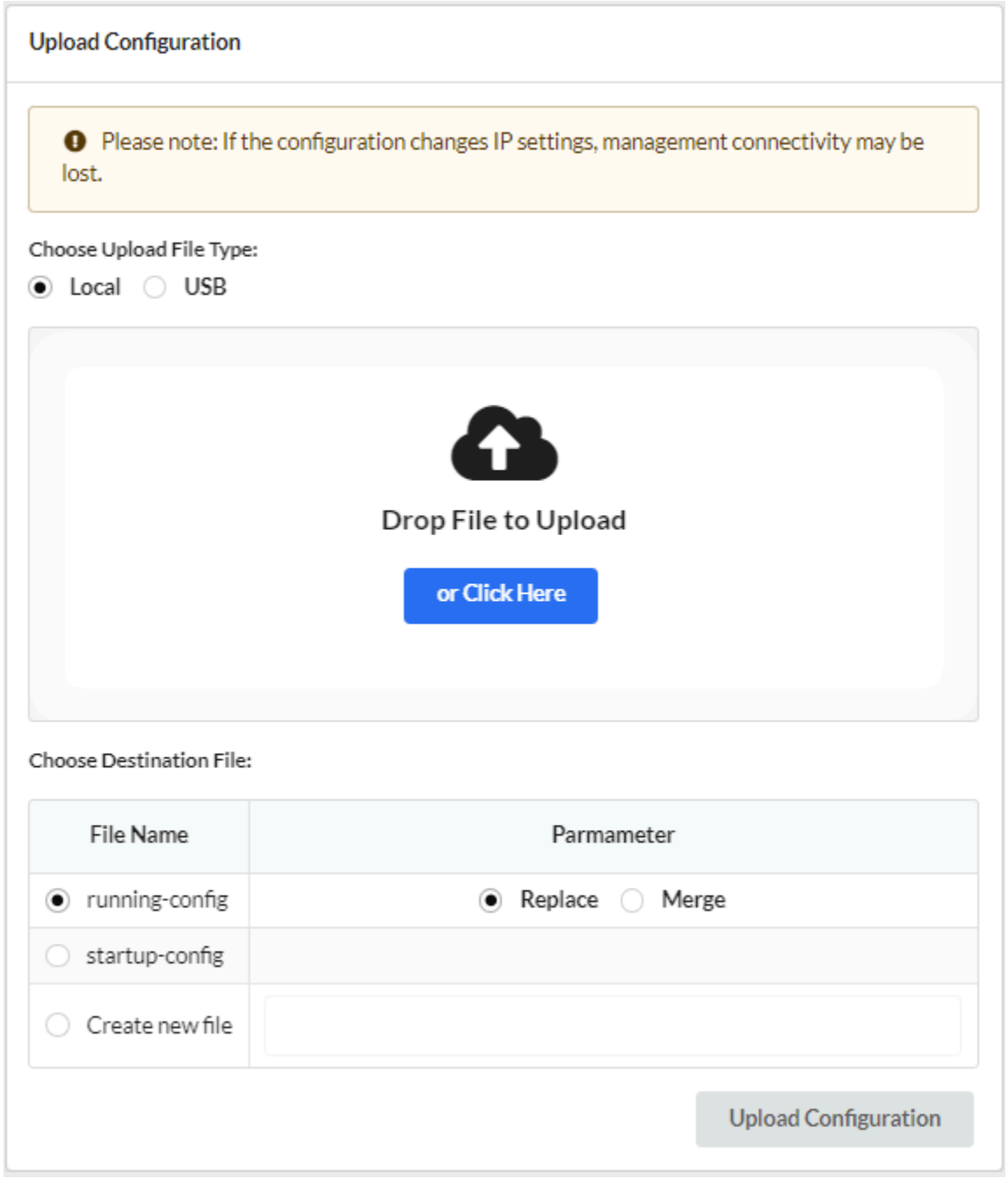
Download of *running-config* may take a little while to complete, as the file must be prepared for download. The file destination can be:

- **Local**: Download the file with default file name with model name and Mac Address to the local file destination.
- **USB**: Download the file to the USB Drive. Users can choose the file name from the default options or enter the file name of the target configuration file.

When the USB Drive mode is disabled, the file destination of USB will become invalid.

NOTE: A valid file name is a text string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), and under score(_). Use of other characters will produce an invalid name.

7.7.3 Upload



It is possible to upload a file from the local source or the USB Drive to all the files on the switch, except default-config which is read-only.

Drop File to Upload "or Click Here" to the location of a configuration file , select the destination file on the target, then click “Upload Configuration”.

- **Local**: Upload the file from the local source
- **USB**: Upload the file from the USB Drive. Users can choose the file sources from the default options or enter the file name of the target configuration file for upload.

When the USB Drive mode is disabled, the file source of USB will become invalid.

NOTE: A valid file name is a text string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), and under score(_). Use of other characters will produce an invalid name.

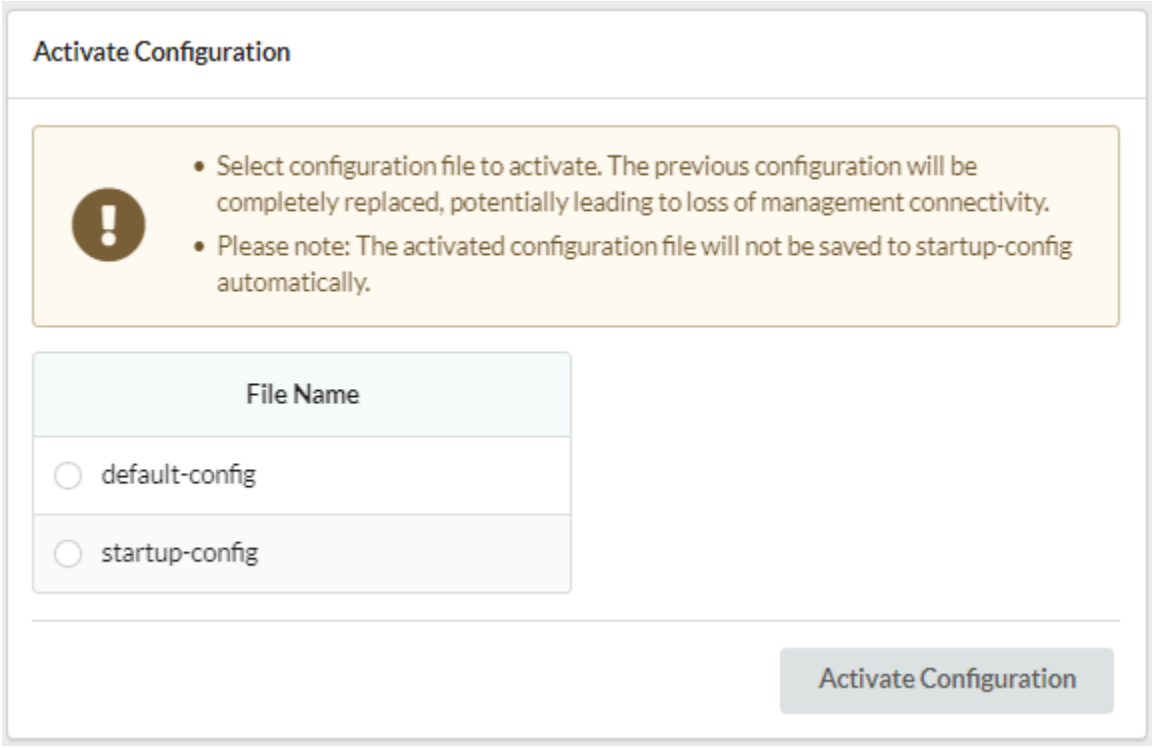
If the destination is *running-config*, the file will be applied to the switch configuration. This can be done in two ways:

- **Replace mode**: The current configuration is fully replaced with the configuration in the uploaded file.
- **Merge mode**: The uploaded file is merged into running-config. Besides, in merge mode, conflicting configurations will default to the new file.

If the flash file system is full (i.e. contains *default-config* and 32 other files, usually including *startup-config*), it is not possible to create new files. Instead an existing file must be overwritten or another file must be deleted.

7.7.4 Activate

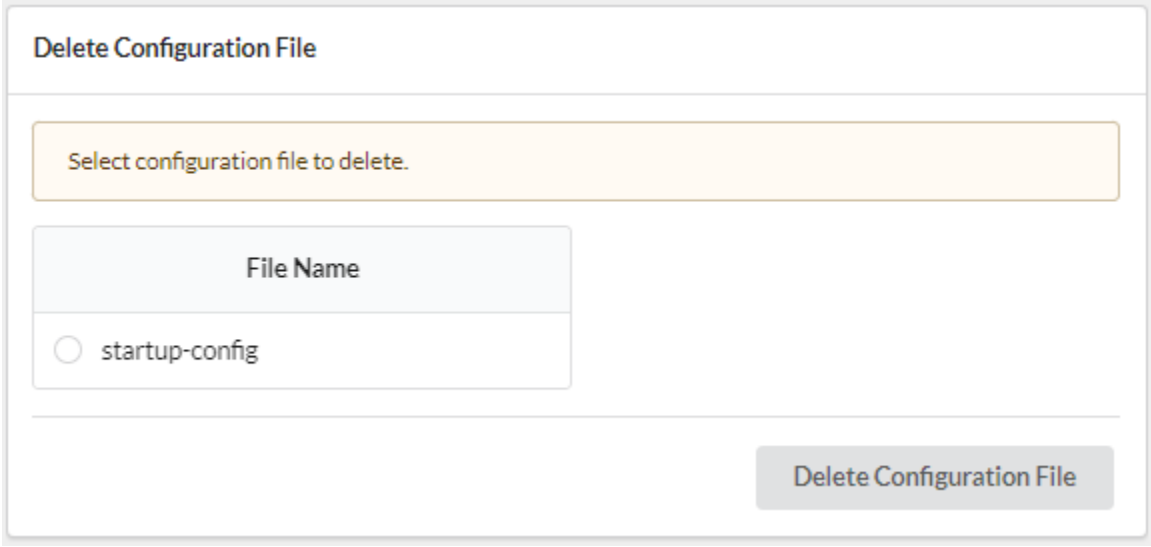
It is possible to activate any of the configuration files present on the switch, except for running-config which represents the currently active configuration.



Select the file(**default- config** or **startup-config**) to activate and click **Activate Configuration**. This will initiate the process of completely replacing the existing configuration with that of the selected file.

7.7.5 Delete

It is possible to delete any of the writable files stored in flash, including startup-config.



Selecting File name and clicking **Delete Configuration File** the switch will reboot without prior Save operation, this effectively resets the switch to default configuration.

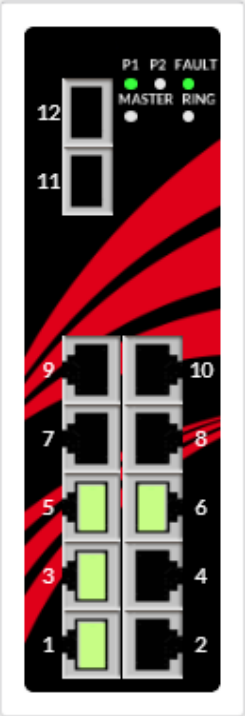
Appendix A - Routing and VLANs

Static Routing/VLANs

This appendix notes on how to configure static routing through the web UI.

This appendix consists of these sections:

- IP Configuration
- VLANs



The process of configuring Antaria's Layer 3 Lite switch with static routing entails the establishment of static routes to facilitate the movement of traffic between distinct subnets or VLANs.

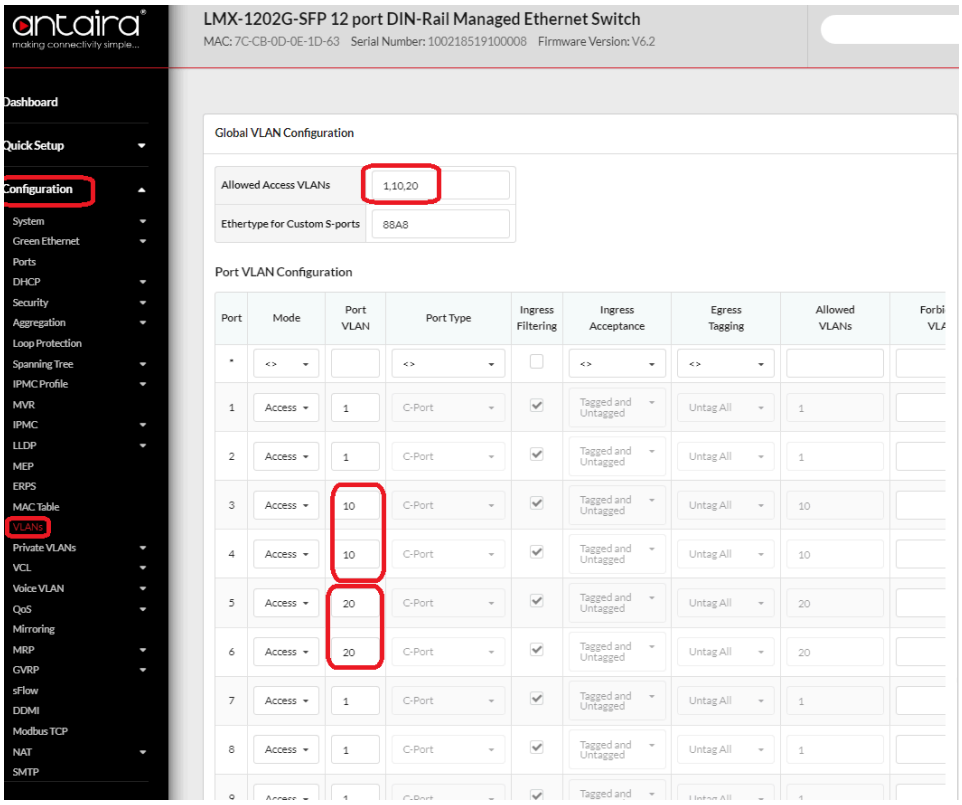
For instance, let's consider the following scenario:

- VLAN1: IP 192.168.102.0/24 - GigabitEthernet 1/1-2
- VLAN10: IP 10.0.10.0/24 - GigabitEthernet 1/3-4
- VLAN20: IP 192.168.112.0/24 - GigabitEthernet 1/5-6

In this specific scenario, PC-1, PC-2, and PC-3 are all within the same switch but belong to different networks. Our objective is to enable seamless communication among these PCs. Given that each port on the switch operates within the same network domain, we achieve network segregation by implementing VLANs. Notably, users do not need to manually add routing tables because all source and destination networks are directly connected to the same switch.

Configuration > VLANs

1. Go to Configuration>VLANs page
2. Create VLAN 1,2,3 in the "Allowed Access VLAN"
3. Configure the PVID for port 1 & 2 as VLAN 1. (All ports is VLAN 1 by default)
4. Configure the PVID for port 3 & 4 as VLAN 10.
5. Configure the PVID for port 5 & 6 as VLAN 20.
6. Click Save Button



Configuration > System > IP > IP Routes

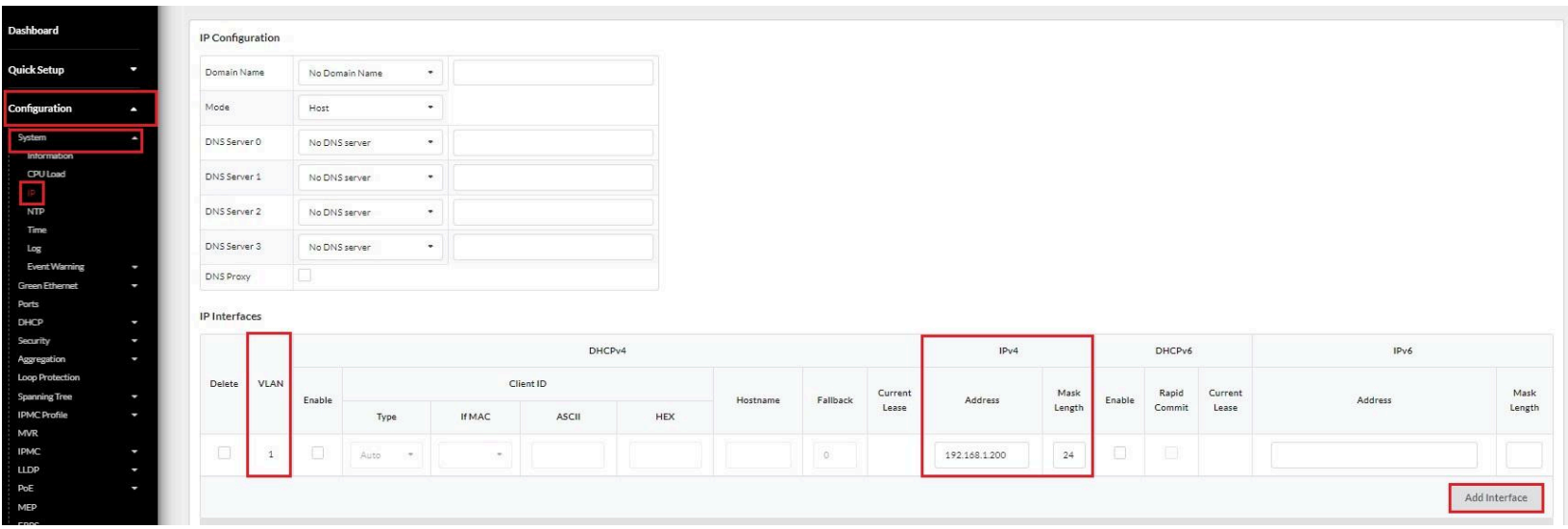
1. Go to Configuration>System>IP page
2. Change the mode from Host to “Router”

(Note : by default VLAN 1 IP address is 192.168.1.254 /24)

3. Click Add interface for VLAN 10, with IP address 10.0.10.1 /24
4. Click Add interface for VLAN 20, with IP address 192.168.112.2 /24

(Note : maximum interfaces can added is 8)

5. Click Save Button



Configuration via CLI

In the Command Line Interface (CLI), the initial step entails accessing the configuration mode and establishing Virtual LANs (VLANs). In this specific illustration, we are in the process of creating two VLANs with identifiers 10 and 20, while keeping in mind that VLAN 1 is the default.

Following this, the subsequent step involves configuring each VLAN to correspond with its respective port interface. This configuration must be performed individually for each range of ports and VLANs. For each port interface within the specified range, it is imperative to enable access with the following command: "switchport access vlan [ID]." Additionally, the command "ip routing" should be executed to enable IP routing.

Subsequently, for each VLAN, an IP address network should be established with the appropriate subnet mask.

```
switch#
# configure terminal
(config)#
(config)# interface GigabitEthernet 1/3-4
(config-if)# switchport access vlan 10
(config-if)# exit
(config)#
(config)# int Gi 1/5-6
(config-if)# sw acc vlan 20
(config-if)# ip routing
(config)#
(config)# interface vlan 10
(config-if-vlan)# ip address 10.0.10.1 255.255.255.0
(config-if-vlan)# int vlan 20
(config-if-vlan)# ip address 192.168.112.2 255.255.255.0
(config-if-vlan)#exit
(config)#
(config)# do show vlan
VLAN  Name                                Interfaces
----  ----------------------------------  ----------
1     default                             Gi 1/1-2,7-12
10    VLAN0010                            Gi 1/3-4
20    VLAN0020                            Gi 1/5-6
(config)# end
#
# show ip int br
Interface  Address              Method   Status
---------- -------------------- -------- ------
VLAN 1     192.168.12.1/24      Manual   UP
VLAN 10    10.0.10.1/24         Manual   UP
VLAN 20    192.168.112.2/24     Manual   UP
```

Appendix B - ERPS

Setting up ERPS in Quick Setup

This appendix describes how to setup the ERPS ring on the switch using Quick Setup.

This appendix consists of these sections:

- Ring Configuration,
- Ethernet Ring Protection
- VLANs

Setting up Ethernet Ring Protection Switching (ERPS) on network switches is a critical task for creating a resilient and fault-tolerant network infrastructure. ERPS is a standardized protocol (IEEE 802.17) used to provide rapid network recovery in the event of link or node failures in a ring topology. It ensures that data traffic continues to flow with minimal disruption.

Physical Network Topology:

- Create a physical network ring topology by connecting switches in a ring, either using fiber or copper cables.
- Each switch in the ring should have two connections (uplinks) to adjacent switches.

Ethernet Ring Protection:

Before you begin with the ERPS Quick Setup, it's important to set up VLANs and assign IP addresses to each switch. These VLANs are the Control VLAN and Data VLAN, and their IP addresses should align with their respective VLAN IDs. This is a prerequisite for ERPS setup.

Define ERPS Domains:

ERPS operates within domains, and each switch in the ring must be part of the same ERPS domain for proper functionality. Follow these steps:

- Assign a unique Domain ID to each switch within the same ERPS domain. This unique ID helps switches identify their role within the ring and coordinate during failure scenarios.

Please note that the specific steps and commands for setting up ERPS using Quick Setup may vary depending on your switch's manufacturer and model. Refer to the switch's user manual or documentation for detailed instructions tailored to your equipment.

Setting up ERPS using Quick Setup streamlines the process and simplifies the configuration of this crucial feature, making it easier for network administrators to ensure network reliability and fault tolerance in ring topologies.

Appendix C - DHCP

DHCP per Port

This appendix provides information on DHCP and highlights the advantages of implementing DHCP per port, offers a convenient solution for managing devices such as IP cameras, which are primarily accessed via their respective IP addresses. In this context, maintaining consistent IP addresses becomes crucial, especially when devices fail, need replacement, or undergo upgrades.

This appendix consists of these sections:

- IP Configuration
- VLANs
- DHCP
- Private VLANS

Here are the available options for achieving this:

Hard-Coded IP Addresses(Static IP): This method involves manually configuring the IP address for each device. While effective, it necessitates the involvement of a technically proficient individual for the setup and configuration of each device.

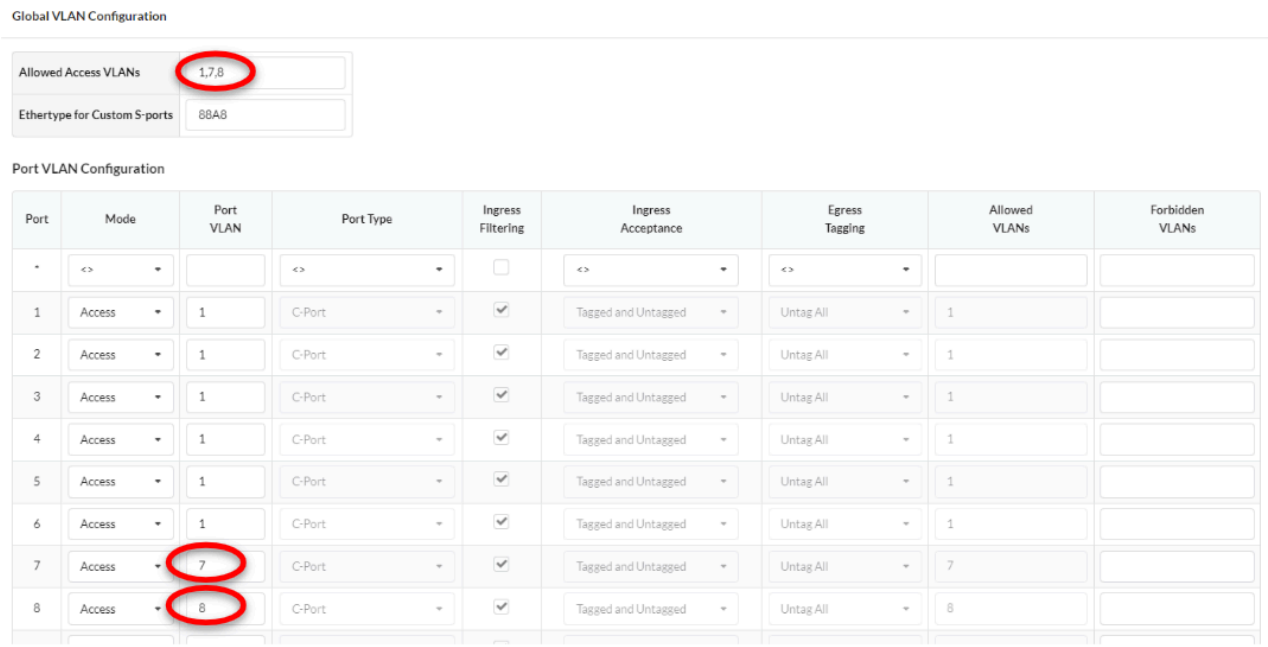
IP Address Reservation (Based on MAC Address): Each device possesses a unique MAC address. With this approach, IP addresses are reserved and assigned based on the device's MAC address. However, a drawback is that whenever a device is replaced, the DHCP server configuration must be updated accordingly. This feature is typically found on more advanced DHCP servers.

DHCP per Port: This method simplifies IP address allocation. Irrespective of the device connected to a specific port on the switch, the switch consistently assigns the same IP address to that port. This approach ensures a seamless and straightforward management of IP addresses without the need for constant DHCP server configuration adjustments.

Configuration > VLANs

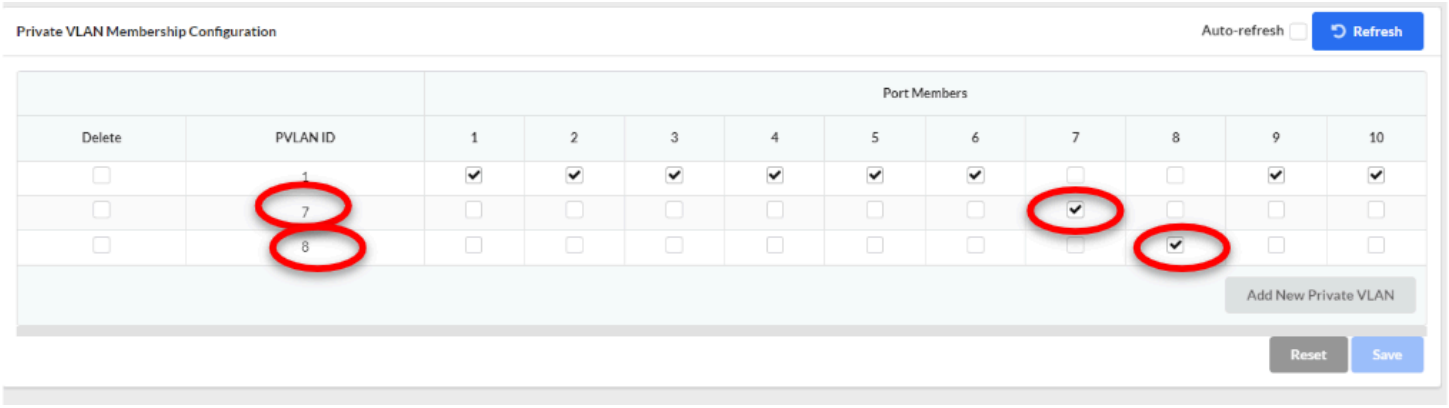
Create VLANS

1. Go to Configuration>VLANs page
2. Create VLAN 1,2,3 in the “Allowed Access VLAN”
3. Configure the PVID for port 7as VLAN 7. (All ports is VLAN 1 by default)
4. Configure the PVID for port 8 as VLAN 8.
5. Click Save Button



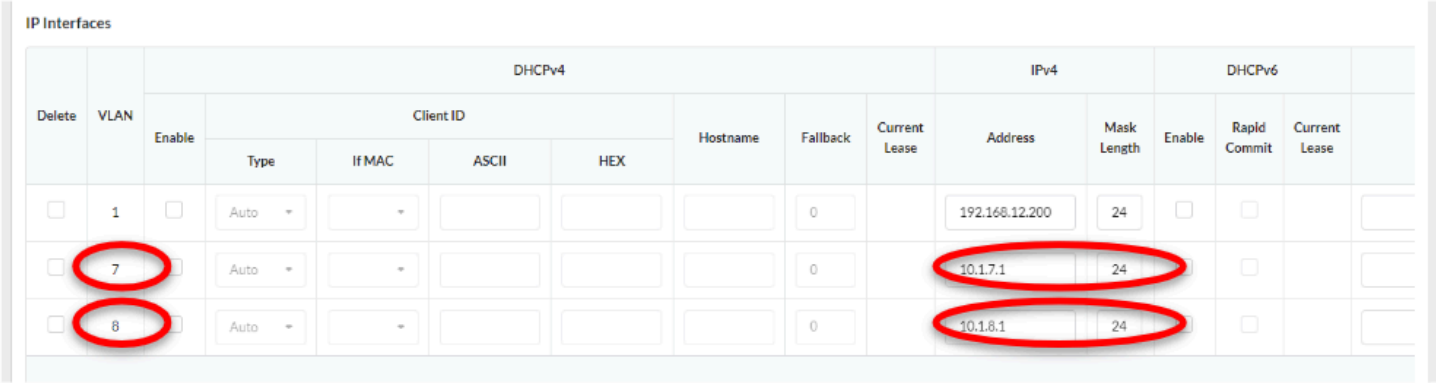
Configuration > **Private VLANS** > **Memberships**

Under Private VLANs, Add new private vlan with VLAN ID corresponding to port in this senerio it is to Port 7 and port 8



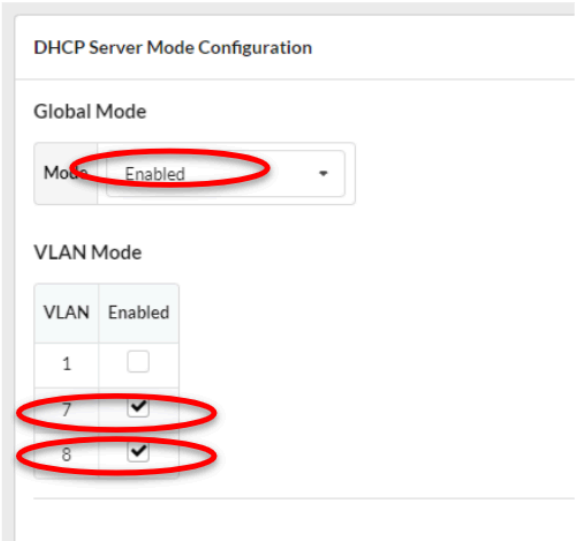
Configuration > System > IP

Under IP configuration, IP interfaces we need to create an Interface



Configuration > DHCP > Server

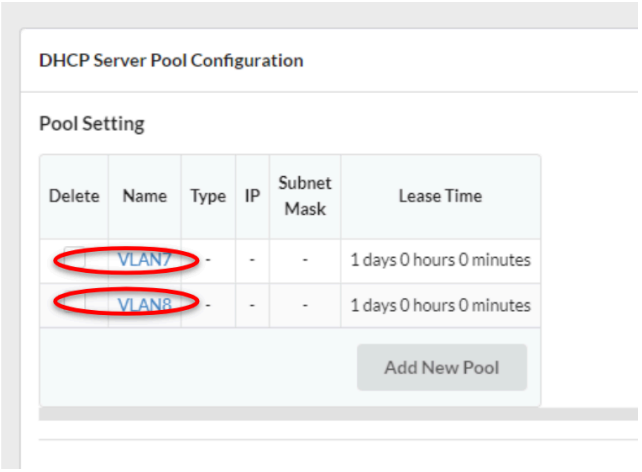
Now enabling DHCP server globally and per VLAN enabled.

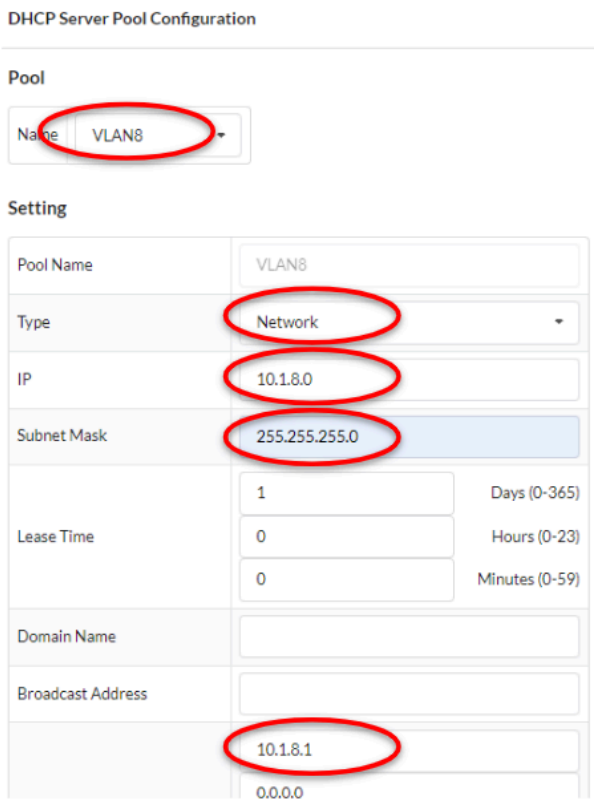


Configuration > DHCP > Pools

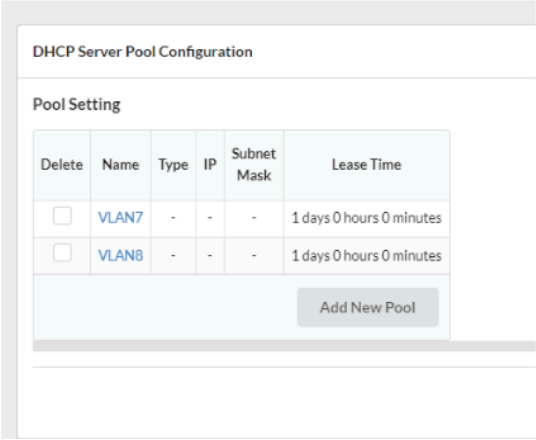
Create pools with names that are meaningful to your setup. After creating these pools, you can configure them by saving your changes and then clicking on the respective pool name.

Then Click the pool name to configure the DHCP server pool

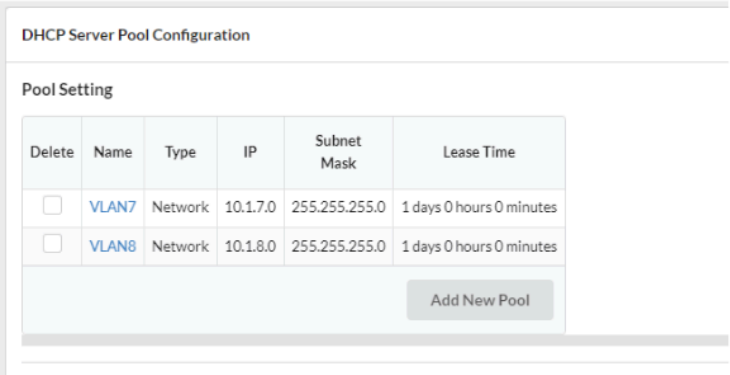




Unconfigured



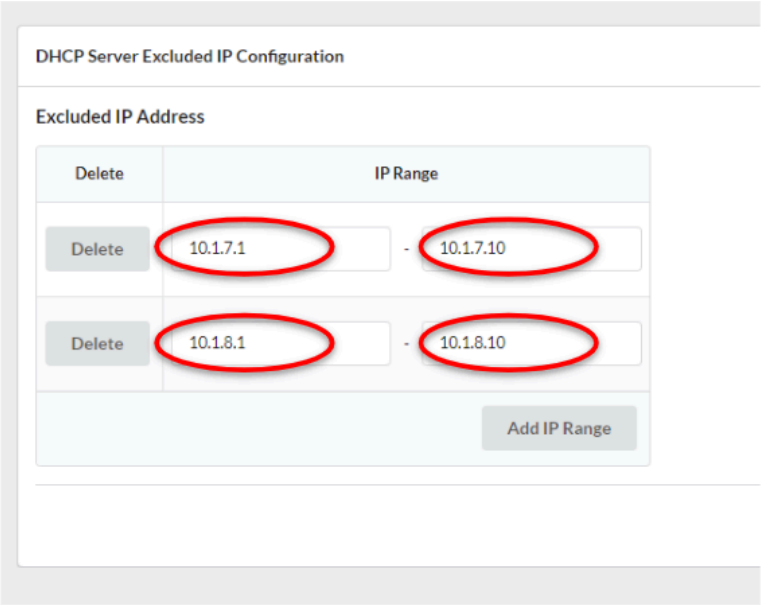
Configured



Configuration > DHCP > Server > Exclusions

To set up ranges of IP addresses that you don't want the DHCP server to automatically allocate to a system, you can configure DHCP address exclusions. This prevents the DHCP server from assigning specific IP addresses within a range to any device.

After setting up these exclusions, the DHCP server will avoid assigning the specified IP addresses to any system, ensuring that they remain available for other purposes or for manual assignment.



Configuration > DHCP > Server > Port Address

To assign a range of IP addresses to a specific port in a VLAN using the Configuration menu, follow these steps: Access your network device or router's configuration interface.

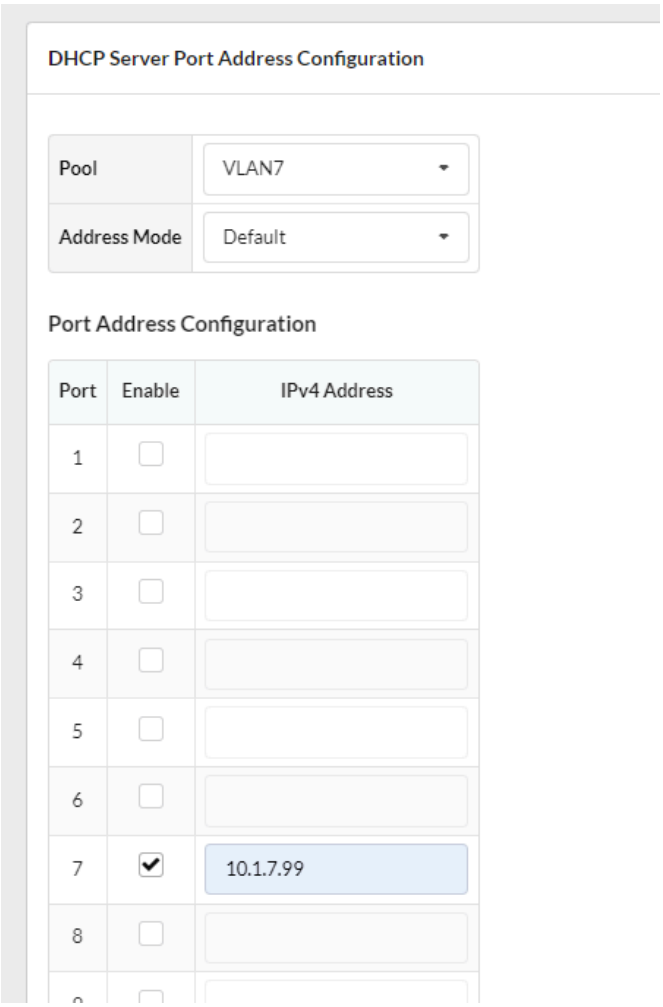
Look for the option "Port Address" thats allows you to associate an IP address range with a specific port or VLAN. The exact wording may vary depending on your device or router.

Choose the DHCP pool (or "Pool" in some cases) that corresponds to the range you want to assign to the port. This pool should be associated with the specific VLAN you're interested in.

Enable the port within that VLAN where you want to assign the IP addresses. This typically involves specifying the port number or VLAN ID.

Assign an IP address to the port within the selected VLAN. This IP address should be within the range of the DHCP pool you've associated with the VLAN.

By following these steps, you will configure the port to use a specific range of IP addresses from the DHCP pool associated with the VLAN. This ensures that devices connected to that port will receive IP addresses from the designated range.



Appendix - Supported CLI Commands

Command Line Interface

This appendix shows supported Command-line interface (CLI) commands which is used for configuring, monitoring, and maintaining Managed switch over the ***CLI, Telnet, SSH***. It is essential to utilze a baud rate of **115200** whenever utilizing the front panel console serial interface.

NOTE:

- It is strongly recommended utilizing the Web interface (Web GUI) whenever possible to simplify user configuration and reduce the chances of configuration mismatches.
- The CLI may contain a broader range of configuration commands compared to those affected by changes made via the web GUI.

In the CLI, every command you input necessitates values, parameters, or a combination of both. Parameters can fall into several categories, including mandatory values, optional values, choices, or a combination of these.

- When you encounter a parameter enclosed within angle brackets "**<>**", such as "***<parameter>***", it signifies that you must input a mandatory parameter in place of the brackets and the text within them.
- Square brackets "**[]**" denote optional parameters, allowing you the flexibility to enter them or omit them as needed, as in "[parameter]".
- When you see a vertical bar "|" between parameters, like "***choice1*** | ***choice2***," it indicates that you can select only one of the specified parameters.
- The presence of curly braces "**{}**" signifies that you must select a parameter from the provided list of choices.
- Values can take various forms, including six hexadecimal numbers separated by colons (e.g., MAC address like 00:0A:BC:3F:82:70), dotted-decimal notation (e.g., Area IDs like 0.0.0.1), slot/port numbers (e.g., 1/1), or logical slot/port designations (applicable in the case of link-aggregation).

Partial Command

To initiate command auto-completion, begin by entering the initial characters of the command and then press the Tab key. The command line parser will finalize the command if the entered string is exclusive to that command. Alternatively, you can opt to type the first few letters of the command followed by a question mark "**?**," which will display all commands that commence with the letters you've already entered.

Command History

Using the Up and Down arrow keys to navigate through previously entered commands. To view the entire command history, you can employ the "***# show history***" command.\

General Maintenance Commands

Configure terminal

Description – Start unit configuration. Terminal display will switch from # to (config)#
configure terminal

	parameter	description
Parameter	-	N/A
Default	N/A	
Mode	EXEC	
Usage	Enter Configuration mode whenever starting unit configuration	
Example	# configure terminal **NOTE** - You may also use the shortcut # conf t	

Interface

Description – Start interface (port) configuration. Terminal display will switch from ***(config)#*** to ***(configif)# interface <port_type> [<port_type_list>]***

	parameter	description
	<port_type>	Port Type GigabitEthernet, vlan
Parameter	[<port_type_list>]	List of Port ID, ex 1/1,3-5 1/1-8
Default	N/A	
Mode	Global Configuration	
Usage	Enter interface configuration mode to start configuring port parameters	
Example	Example#1 (enter configuration mode for ports 1, 3,4 and 5): (config)# interface GigabitEthernet 1/1,3-5 (config-if)# Example#2 (enter configuration mode vlan 10) (config)# interface vlan 10 (config-if-vlan)#	

exit

Description - Go up one level in the configuration process. Logout from terminal/telnet/SSH session in case user was at top level.

	parameter	description
Parameter	-	N/A
Default	N/A	
Mode	Exit from current mode	

Usage	Whenever end in-depth configuration and need to go up one levelm or to log out of the serial interface
Example	(config-if)# exit (config)# (config)# exit #

End

Description - End any in-depth configuration mode and go back to EXEC mode.

Parameter	parameter	description
	-	N/A
Default	N/A	
Mode	Go back to EXEC mode	
Usage	Whenever need to end in-depth configuration and go back to EXEC mode	
Example	(config-if)# end #	

show running-config

Description - View unit running configuration (the configuration being in use by the unit). User may change unit configuration without saving the changes, meaning that upon unit power down-up cycle it may operate completely different.

Parameter	parameter	description
	-	-
Default	N/A	
Mode	EXEC	
Usage	Use this command to view the current configuration	
Example	# show running-config	

show running-config all-default

Description - View unit running configuration plus omitted default configuration

Parameter	parameter	description
	-	-
Default	N/A	
Mode	EXEC	
Usage	Use this command to view the current configuration including all default	

	values
Example	# show running-config all-default

dir

Description - Show all optional configuration files stored inside the unit.

Parameter	parameter	description
	-	-
Default	N/A	
Mode	EXEC	
Usage	Use this command to view all configuration files stored in the flash.	
Example	# dir r- 2022-12-29 07:31:43 649 default-config rw 1970-01-01 00:38:10 1511 startup-config 2 files, 2160 bytes total.	

copy running-config startup-config

Description– update (save) unit configuration to be used after reset or power-up.
copy running-config startup-config

Parameter	parameter	description
	-	-
Default	N/A	
Mode	EXEC	
Usage	Use this command to view all configuration files stored in the flash.	
Example	# copy running-config startup-config Building configuration... % Saving 1648 bytes to flash:startup-config	

copy running-config flash:<file-name>

Description- copy running (or startup) configuration files to another file name or to TFTP server. Also vice versa from TFTP Server to unit local file
copy <running config | startup-config | flash:file-name | tftp://server/filename>

Parameter	parameter	description
	-	-
Default	N/A	
Mode	EXEC	

Usage	Use this command to copy unit configuration to another file or to TFTP Server or from TFTP Server to unit local file
Example	Example#1 - save current configuration stored in unit flash to another file named “test” also inside unit FLASH. # copy running-config flash:test Example#2 - save unit running configuration file to TFTP Server under name “test” # copy running-config tftp://192.168.12.40/test

del flash:<file-name>

Description - delete configuration file stored in flash

	parameter	description
Parameter	-	-
Default	N/A	
Mode	EXEC	
Usage	Use this command to delete unit configuration stored in flash	
Example	# del flash:test	

reload cold

Description – Unit performs software reset, turning Ethernet ports down and back up.

reload cold

NOTE:

- Unit software reset may or may-not effect PoE power being delivered to PD devices.
- Use the command “poe uninterruptible-power” , “no poe uninterruptible-power” to configure PoE power state during software reset cycle.

	parameter	description
Parameter	-	-
Default	N/A	
Mode	EXEC	
Usage	Use this command to restart the unit	
Example	# reload cold	

reload defaults

Description – restore to full factory default configuration

reload defaults

	parameter	description
Parameter	-	-
Default	N/A	
Mode	EXEC	
Usage	Use this command to restore to factory default	
Example	# reload defaults	

reload defaults keep-ip

Description - Semi factory defaults, keeping IP and VLAN configuration unchanged
reload defaults keep-ip

	parameter	description
Parameter	-	-
Default	N/A	
Mode	EXEC	
Usage	Use this command to restore to factory default but keep IP address unchanged	
Example	# reload defaults keep-ip	

show version

Description – Display unit software and hardware information

	parameter	description
Parameter	-	-
Default	N/A	
Mode	EXEC	
Usage	Use this command to display unit information	
Example	# sh version MAC Address : 7C-CB-0D-0E-1D-63 Serial Number : 100218519100008 Previous Restart : Cold System Contact : System Name : System Location : System Time : 1970-01-01T22:27:55+00:00 System Uptime : 22:27:55 ---------- SID : 1	

	---------- Chipset ID : VSC7429 Port Count : 12 Product : LMX-1202G-SFP Software Version : V6.2 Build Date : 2022-12-29T15:30:29+08:00 Code Revision : 3e308adf7+

Network

Ethernet ports - configuration commands

Configure Ethernet ports Link speed, max Ethernet packet size and flow control

shutdown

Description - Enable/disable Ethernet port (has no effect on PoE power)

shutdown
no shut

	parameter	description
Parameter	-	-
Default	N/A	
Mode	Port List Interface configuration mode	
Usage	Use the command to disable the specified interface and use no form of this command to enable the interface	
Example	Example#1 (disable port 1) # configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# shutdown Example#2 (disable ports 1 through 8) # configure terminal (config)# interface GigabitEthernet 1/1-8 (config-if)# shutdown Example#3 (enable all ports) # configure terminal (config)# interface * (config-if)# no shutdown	

speed

Description - configure port speed

speed {1000 | 100| 10 | auto }

	parameter	description
	10	10Mbps

Parameter

	100	100Mbps
	1000	1Gbps
	auto	Auto negotation
Default	All ports are set to Auto	
Mode	Port List Interface Mode	
Usage	Use to set the speed of the specified interface.	
Example	Example#1 (set speed for port 1 to 100Mbps) # configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# speed 100 Example#2 (set all ports to 1Gbps) # configure terminal (config)# interface * (config-if)# speed 1000	

duplex

Description - configure interface duplex mode

duplex { half | full | auto }

no duplex

	parameter	description
	half	Forced half duplex
	full	Forced full duplex
Parameter	auto	Auto negotation of duplex mode
Default	All ports are set to Auto	
Mode	Port List Interface Mode	
Usage	Use to set the duplex mode of the specified interface. Use the no form of the command to set duplex to default.	
Example	Example#1 (set duplex for port 1 to half) # configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# duplex half Example#2 (set all ports to 1Gbps) # configure terminal (config)# interface * (config-if)# speed 1000	

Flowcontrol

Description- configures flow control for the interface (slow temporarily packet transition upon request, or for packet reception, signal the remote transmitter to slow down temporarily its packet transition whenever Switch reception buffer becomes to full).

flowcontrol { on | off }

no flowcontrol

	parameter	description
Parameter	on	Enable flow control
	off	Disable flow control
Default	All ports flow control receive and send is off	
Mode	Port List Interface Mode	
Usage	Use to set the flow control for the interface. Use the no form of the command to return to defaults.	
Example	Example#1 (enable flow control for port 1) # configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# flowcontrol on Example#2 (enable flow control for all ports) # configure terminal (config)# interface * (config-if)# flowcontrol on	

MTU

Description- specify maximum Ethernet frame size for the interface

mtu <max_length>
no mtu

	parameter	
Parameter	<max_length>	Maximum frame size in bytes (1518-9600 bytes)
Default	All ports mtu 9600 bytes	
Mode	Port List Interface Mode	
Usage	Use to set the maximum frame size for the interface. Use the no form of the command to return to defaults.	
Example	Example#1 (set mtu for port 1 to 1518) # configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# mtu 1518 Example#2 (set mtu for all ports to 1518) # configure terminal (config)# interface * (config-if)# mtu 1518	

Ethernet ports - view commands

View link status (up/down/speed), flow control, max frame size and mode.

show interface status

Description- display status and configuration information for any port.

show interface <port_type> [<v_port_type_list>] **status**

	parameter	description
Parameter	<port_type>	Port type in GigbitEthernet
	<v_port_type_list>	List of Port ID, ex 1/1,3-5; 1/6
Default	N/A	
Mode	EXEC mode	
Usage	Use to display current status of the specified interface.	
Example	show interface gi 1/1-5 status Interface Mode Speed & Duplex Flow Control Max Frame Excessive Link ---------- ------- ------------ ------------ --------- --------- ------- GigabitEthernet 1/1 enabled Auto disabled 9600 Discard 100fdx GigabitEthernet 1/2 enabled Auto disabled 9600 Discard Down GigabitEthernet 1/3 enabled Auto disabled 9600 Discard 100fdx GigabitEthernet 1/4 enabled Auto disabled 9600 Discard Down GigabitEthernet 1/5 enabled Auto disabled 9600 Discard 1Gfdx	

IPv4, IPv6

Configure static/dynamic IPv4, IPv6 address and mask, default gateway, DNS.

ip name-server - DNS Server

Description- Set the DNS server for resolving domain names

ip name-server [<order>] { <v_ipv4_ucast> | { <v_ipv6_ucast> [interface vlan <v_vlan_id_static>] } | dhcp [ipv4 | ipv6] [interface vlan <v_vlan_id_dhcp>] }

no ip name-server

	parameter	description
Parameter	<order>	Preference of DNS server. Default selection is 0
	<v_ipv4_ucast>	A valid IPv4 unicast address
	<v_ipv6_ucast>	A valid IPv6 unicast address
	dhcp	Dynamic Host Configuration Protocol
Default	No DNS server configured	
Mode	Global Configuration mode	
Usage	Set the DNS for resolving domain names. Use the no version of the command to return to default.	
Example	Example#1 (DNS Server 0 setting is derived from any DHCPv4 VLANs-ID) (config)# ip name-server 0 dhcp Example#2 (DNS Server 1 configured as a static IPv4 address) (config)# ip name-server 1 192.168.0.10 Example#3 (DNS Server 1 setting is derived from DHCPv4 VLANs-ID 1) (config)#ip name-server 1 dhcp ipv4 interface vlan 1	

ip (ipv6) address - IPv4,IPv6 interface

Description - add IPv4, IPv6 interface

ip address { { <address> <netmask> } | { dhcp [fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]] [client-id { <port_type> <client_id_interface> | ascii <ascii_str> | hex <hex_str> }] [hostname <hostname>] } }
no ip address
ipv6 address <subnet>
no ipv6 address

	parameter	description
	<address>	IPv4 Address
	<netmask>	IP netmask
	dhcp	Enable Dynamic Host Configuration Protocol
	fallback	DHCP fallback settings
	client-id	DHCP client identifier
	hostname	DHCP host name
Parameter	<subnet>	IPv6 prefix x:x::y/z
Default	N/A	
Mode	Vlan interface configuration mode	
Usage	Add VLAN interface and set all IPv4, IPv6 parameters. Use the no version of the command to disable the selectred VLAN interface. To remove it completely use **no interface vlan** <id> for Global Config mode.	
Example	Example#1 (Set VLAN2 static IP address to 192.168.1.50 mask length 24) (config)#interface vlan 2 (config-if-vlan)# ip address 192.168.1.50 255.255.255.0 Example#2 (Add VLAN 3 and set it to get IP address from DHCP using MAC of port 1 as Client ID with a hostname test) (config)#interface vlan 3 (config-if-vlan)# ip address dhcp client-id GigabitEthernet 1/1 hostname test	

IP Routes (Default gateway)

Description - Add new IP route.

ip route <ipv4_addr> <ipv4_netmask> <ipv4_gw> [<distance>]
no ip route <ipv4_addr> <ipv4_netmask> <ipv4_gw>

	parameter	description
	<ipv4_addr>	Network
	<ipv4_netmask>	Netmask
	<ipv4_gw>	Gateway
Parameter	<distance>	Distance value for this route

Default	N/A
Mode	Global Configuration
Usage	To route all unknown destination IP to default gateway use the following parameters: Network=0.0.0.0 Netmask=0.0.0.0 and Distance=1 To remove the route use **no ip route** command with all parameters for the selected route.
Example	Example#1 (add IP route to gateway 192.168.1.1): (config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1 1 Example#2 (remove IP route) (config)#no ip route 0.0.0.0 0.0.0.0 192.168.1.1

Show interface vlan

Description - View VLAN interface status and configuration.

show interface vlan [<vlist>]

	parameter	description
Parameter	<vlist>	vlan list
Default	N/A	
Mode	EXEC mode	
Usage	Use to display current status and configuration of the specified interface	
Example	# show interface vlan 10 VLAN10 LINK: 7c-cb-0d-0e-1d-63 Mtu:1500 <UP BROADCAST MULTICAST> IPv4: 10.0.10.1/24 10.0.10.255 IPv6: fe80::7ecb:dff:fe0e:1d63/64 <>	

NTP (Network Time Protocol)

Configure the unit NTP Servers IP. The NTP Server updates the unit with the correct GMT (Greenwich Mean Time).

ntp server - Configure NTP server

Description- Enable or disable NTP server and specify its parameters. Up to 5 NTP servers can be configured.

ntp
no ntp
ntp server <index_var> ip-address { <ipv4_var> | <ipv6_var> | <name_var> }
no ntp server <index_var>

	parameter	description
Parameter	<index_var>	NTP Server index (1-5)
	<ipv4_var>	IPv4 address of NTP server
	<ipv6_var>	IPv6 address of NTP server
	<name_var>	Domain name of NTP server
Default	N.A	
Mode	Global Configuration mode	

Usage	Enable NTP server by entering ntp command. Use a no version of the command to disable it. Specify the parameters of NTP server by entering ntp server command. Use a no version of the command to delete the specified NTP server.
Example	Example#1 (add NTP server 1 with IP address 192.168.1.2) (config)#ntp server 1 ip-address 192.168.1.2 Example#2 (add NTP server 2 with domain name ntp.google.com) (config)#ntp server 2 ip-address ntp.google.com Example#3 (enable NTP server) (config)#ntp

show ntp status - view NTP status

Description - View NTP status and all configured NTP servers

show ntp status

	parameter	description
Parameter	-	-
Default	N.A	
Mode	EXEC mode	
Usage	Use the command view status and configuration of NTP servers	
Example	#show ntp status	

Time Zone

Configure unit local time zone and daylight saving.

clock timezone - time zone configuration

Description - configure time zone.

clock timezone <word16> <hour_var> [<minute_var> [<subtype_var>]]

no clock timezone

	parameter	description
Parameter	<word16>	Name of time zone up to 16 characters. Use “ for null input
	< hour_var >	Hours offset from UTC -23-23
	<minute_var>	Minutes offset from UTC 0-59
	<subtype_var>	Sub type of time zone 0-9
Default	(UTC) Coordinated Universal Time	
Mode	Global Configuration mode	
Usage	Specify the time zone and offsets from UTC. Use the no form of the command to return to default	
Example	Example#1 (Configure Eastern time zone with -05:00 from UTC) (config)#clock timezone Eastern -05 0	

clock summer-time - Daylight Savings Time configuration

Description - Configure daylight savings time.

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

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

no clock summer-time

Parameter	parameter	description
	<word16>	Name of time zone in summer up to 16 characters. Use " for null input
	<start_month_var>	Month to start (1-12)
	<start_date_var>	Date to start (1-31)
	<start_year_var>	Year to start (2000-2097)
	<start_hour_var>	Time to start (hh:mm)
	<end_month_var>	Month to end (1-12)
	<end_date_var>	Date to end (1-31)
	<end_year_var>	Year to end (2000-2097)
	<end_hour_var>	Time to end (hh:mm)
	<offset_var>	Offset to add in minutes (1-1439)
	<start_week_var>	Week number to start (1-5)
	<start_day_var>	Weekday to start (1-7)
	<end_week_var>	Week number to end (1-5)
	<end_day_var>	Weekday to end (1-7)
Default	Daylight savings time mode disabled	
Mode	Global Configuration mode	
Usage	Configure summer (daylight savings) time in absolute non-recurring mode (**date**) and recurring mode (**recurring**). Use the no form of the command to go back to default.	
Example	Example#1 (Configure non-recurring Daylight Savings Time to start on March 10 2019 at 02:00AM and finish on November 3 2019 at 02:00AM) (config)#clock summer-time " date 3 10 2019 02:00 11 3 2019 02:00	

Time zone - view commands

show clock detail

Description - Display the detailed clock information

show clock detail

Parameter	parameter	description
	N.A	N.A
Default	N.A	
Mode	EXEC mode	
Usage	Use to display clock information	

Example	# show clock detail

SysLog report

Configure SysLog Server IP address. The unit sends SysLog messages during Power-Up and normal operation. The SysLog events are send by the unit over the Network to SysLog Server. The user has the option to filter some of the SysLog messages being send by the unit by configuring from what severity/importance SysLog messages the message should be send.

logging - Enable and configure SysLog

Description - System Log configuration commands

logging on

logging host { <ipv4_addr> | <domain_name> } **logging level** { informational | notice | warning | error } **no logging on**

Parameter	parameter	description
	<ipv4_addr>	Name of time zone up to 16 characters. Use " for null input
	<domain_name>	Hours offset from UTC -23-23
	informational	Severity 6: Informational messages
	notice	Severity 5: Normal but significant condition
	warning	Severity 4: Warning conditions
	error	Severity 3: Error conditions
Default	N.A	
Mode	Global Configuration mode	
Usage	Enable SysLog server, specify its address and what level of messages will be sent to it. Use the no logging on command to disable SysLog server.	
Example	Example#1 (Enable SysLog server at 192.168.0.1 with Warning level messages) (config)#logging on (config)#logging host 192.168.0.1 (config)#logging level warning Example#2 (Disable SysLog server) (config)#no logging on	

show logging

Description - Show logging configuration and message summary. **show logging** [informational] [notice] [warning] [error]

show logging <log_id> [switch <switch_list>]

Parameter	parameter	description
	informational	Severity 6: Informational messages
	notice	Severity 5: Normal but significant condition
	warning	Severity 4: Warning conditions

	error	Severity 3: Error conditions
	<log_id>	Message logging ID
	<switch_list>	List of switch ID (in a stacked system) ex, 1,3-5,7
Default	N.A	
Mode	EXEC mode	
Usage	Display SysLog server status and configuration and detailed logging messages.	
Example	Example#1 (Show SysLog configuration on switch 1 and detailed log message 1) #show logging 1 switch 1 Example#2 (Show SysLog configuration and detailed Error log messages) #show logging error	

MAC Table Learning – configuration commands

Provides various options regarding the way MAC address learning should be processed by the Ethernet Switch, and how to process a packet with unknown source MAC address, unknown destination MAC address, etc.

When a packet is received, it is classified by its Source-MAC, Destination-MAC, VLAN-ID and Port number. As part of Ethernet Switch forwarding algorithm, the switch will look for Destination-MAC and VLAN inside the MAC learning table. If it was found, then the packet will be forwarded to the specified port, otherwise the packet is flooded to all ports on same VLAN

mac address-table aging-time

Description - By default, dynamic entries are removed from the Mac table after 300 seconds. This process is called aging. Aging time can be configured to be in the range of 10 to 1000000 seconds or 0 to disable automatic aging.

mac address-table aging-time <v_0_10_to_1000000>

no mac address-table aging-time

	parameter	description
Parameter	<v_0_10_to_1000000>	Aging time in seconds, 0 disables aging
Default	Aging time is 300 seconds	
Mode	Global Configuration mode	
Usage	Set MAC address table aging time in seconds. Use the no version of the command to reset to default (300 seconds)	
Example	Example#1 (Set aging time to 400 seconds) (config)# mac address-table aging-time 400 Example#2 (Disable automatic aging) (config)# mac address-table aging-time 0	

mac address-table learning

Description - Each port can do learning in Auto mode (done automatically as soon as the frame with unknown MAC is received) or Secured mode (only static MAC entries are learned and all other frames are dropped). MAC learning can also be disabled and no learning is done. Specific VLANs can also be learning-disabled.

mac address-table learning [secure]

no mac address-table learning

mac address-table learning vlan <vlan_list>

no mac address-table learning vlan <vlan_list>

	parameter	description
Parameter	[secure]	Port Secure mode
Default	All ports are in Auto learning mode	
Mode	Port List Interface Mode (for specific port), Global Configuration Mode (for VLANs)	
Usage	Set MAC address table learning mode to Secure or back to Auto (command without [secure] parameter). Use the no version of the command to Disable learning.	
Example	Example#1 (Set MAC address learning to Secure on port 1) (config)# interface GigabitEthernet 1/1 (config-if)#mac address-table learning secure Example#2 (Disable MAC address learning on ports 2-5) (config)# interface GigabitEthernet 1/2-5 (config-if)#no mac address-table learning Example#3 (add VLAN2 to the list of learning disabled VLANs) (config)# no mac address-table learning vlan 2	

mac address-table static

Description - Assign a static mac address to the specific port or ports

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

no mac address-table static <v_mac_addr> vlan <v_vlan_id> { [interface <port_type> [<v_port_type_list>]] }

	parameter	description
Parameter	<v_mac_addr>	48 bit MAC address: xx:xx:xx:xx:xx:xx
	<v_vlan_id>	VLAN IDs 1-4095
	<port_type>	GigabitEthernet
	<v_port_type_list>	List of Port ID, ex, 1/1,3-5
Default	N.A	
Mode	Global Configuration Mode	
Usage	Assigns a static MAC address to a port. Use the no version of the command to remove it.	

Example	Example#1 (Assign static MAC address 00:11:22:33:44:55 to port 1 on VLAN 1) (config)#mac address-table static 00:11:22:33:44:55 vlan 1 interface Gi 1/1

show mac address-table

Description - Display MAC address table entries.

show mac address-table [conf | static | aging-time | { { learning | count } [interface <port_type> [<v_port_type_list>] | vlan <v_vlan_id_2>] } | { address <v_mac_addr> [vlan <v_vlan_id>] } | vlan <v_vlan_id_1> | interface <port_type> [<v_port_type_list_1>]]

	parameter	description
Parameter	conf	User added static MAC addresses
	static	All static MAC addresses
	aging-time	Display MAC address aging time
	learning	MAC address learning state (Learn/Secure/Disable)
	count	Total number of MAC addresses
Default	N.A	
Mode	EXEC Mode	
Usage	Show MAC address table entries in various views based on the specific parameter.	
Example	**Example#1 (display all static MAC addresses)** #show mac address-table static **Example#2 (display the MAC table entry for MAC address 00:11:22:33:44:55)** #show mac address-table address 00:11:22:33:44:55 **Example#3 (display the MAC table entry for port 2)** #show mac address-table interface GigabitEthernet ½ **Example#4 (display all MAC table entries)** #show mac address-table	

```
# show mac address-table
Type    VID  MAC Address       Ports
Static  1    00:00:00:00:00:11 GigabitEthernet 1/3-5
Dynamic 1    00:05:5a:03:99:b6 GigabitEthernet 1/9
Static  1    00:05:5a:98:67:23  CPU
Dynamic 1    00:0a:cd:2d:b1:ed GigabitEthernet 1/10
Dynamic 1    18:68:cb:b5:85:03 GigabitEthernet 1/1
Static  1    33:33:00:00:00:01 GigabitEthernet 1/1-11 CPU
Static  1    33:33:ff:98:67:23 GigabitEthernet 1/1-11 CPU
Static  1    ff:ff:ff:ff:ff:ff GigabitEthernet 1/1-11 CPU
```

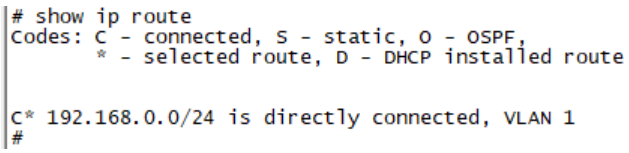
Routing

show ip route

Description - Display IPv4 route entry table with status information.

show ip route

	parameter	description
Parameter	N.A	N.A
Default	N.A	
Mode	EXEC Mode	

Usage	display routing information
Example	#show ip route 

```
# show ip route
Codes: C - connected, S - static, O - OSPF,
       * - selected route, D - DHCP installed route


C* 192.168.0.0/24 is directly connected, VLAN 1
#
```

ACCESS CONTROL

Control who can access the unit, from what type of Network interface, who will verify remote user username and password (by the unit locally, or by RADIUS/TACACS+ Authentication Server), etc.

Local Users - configuration commands

Allows changing 'admin' user password, adding or removing additional users and changing users' password.

username - Add local user or change password

Description- Add, remove or change password of local users. Up to 20 users can be configured.

username { default-administrator | <input_username> } **privilege** <priv> **password** { unencrypted<unencry_password> | encrypted <encry_password> | none }

no username <username>

Parameter	parameter	description
	<input_username>	User name allows letters, numbers and underscores
	<priv>	User privilege level 0-15. **NOTE** - **Please use only privilege level 15**
	<unencry_password>	The UNENCRYPTED (Plain Text) user password. Any printable characters including space are accepted. Notice that you have no chance to get the Plain Text password after this command. The system will always display the ENCRYPTED password.
	<encry_password>	The ENCRYPTED (hidden) user password. Notice the ENCRYPTED password will be decoded by system internally. You cannot directly use it as same as the Plain Text and it is not human-readable text normally.
	none	NULL password
Default	N.A	
Mode	Global Configuration Mode	
Usage	Add a new user for the local switch access and add/change password.	
Example	Example#1 (add a user named usertest with unencrypted password of testuser) (config)# username usertest privilege 15 password unencrypted testuser Example#2 (remove user named usertest) (config)# no username usertest Example#3 (change the password of usertest to testuser123) (config)# username usertest privilege 15 password unencrypted testuser123	

NOTE:

- The unit is shipped with default username 'admin' and with no password. It is strongly recommended to assign a strong password instead.
- Username 'admin' can't be removed or be changed, only its password.

Local Users

show user-privilege

Description- Display all local users, privilege levels and passwords

show user-privilege

	parameter	description
Parameter	N.A	N.A
Default	N.A	
Mode	EXEC Mode	
Usage	display information about all local user accounts	
Example	# show user-privilege # show user-privilege username admin privilege 15 password encrypted 64d0dfc93d6b24b6ad00 0dc81cb0e9865f737d4d7d1fb8e83be6cb687dd5fce85a26d9d21a754b753d1a1 #	

show users

Description- Display information on how remote users are connected at the moment to the unit. Serial is represented as "con", Telnet is represented as "vty".

show users

	parameter	description
Parameter	N.A	N.A
Default	N.A	
Mode	EXEC Mode	
Usage	Display information on how remote users are connected	
Example	# show users Line is vty 0. * You are at this line now. Connection is from 192.168.12.50:61054 by SSH. User name is admin. Privilege is 15. Elapsed time is 0 day 0 hour 0 min 14 sec. Idle time is 0 day 0 hour 0 min 0 sec.	

Web Server

Controls whether unit embedded Web Server should operate in HTTP or HTTPS mode. HTTPS use TLS v1.2 encryption to encrypt all Web Network traffic between the user web browser and the unit Web Server.

ip http secure-server

Description- Configure Web Server to use only HTTPS (secure and encrypted operation mode) or HTTP (unsecure operation mode) as well.

ip http secure-server

no ip http secure-server

Parameter	parameter	description
	N.A	N.A
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure Web Server to use HTTPS. Use the no version of the command to use HTTP	
Example	(config)# ip http secure-server (config)# no ip http secure-server	

ip http secure-certificate

Description - Manage Web Server certificate. Use this command to delete the current certificate, generate a new self-signed RSA certificate or upload a PEM certificate using URL over http, tftp or ftp.

ip http secure-certificate { upload <url_file> [pass-phrase <pass_phrase>] | delete | generate }

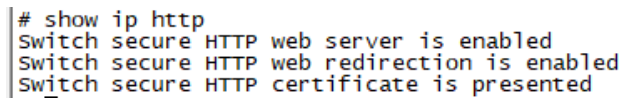
Parameter	parameter	description
	<url_file>	Uniform Resource Locator. It is a specific character string that constitutes a reference to a resource. Syntax: <protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>]/<file_name> If the following special characters: space !\"#$%&'()*+,/:;<=>?@[\\]^`{|}~ need to be contained in the input URL string, they should be percent-encoded. A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under score (_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains '.' is not allowed.
	<pass_phrase>	Privacy key pass phrase string if uploading certificate protected by a specific passphrase.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Manage the HTTPS certificate (PEM format)	

Example	Example#1 (upload the HTTPS certificate from TFTP server) (config)# ip http secure-certificate upload tftp://10.9.52.103/test_ca.pem Example#2 (delete current certificate) (config)# ip http secure-certificate delete

show ip http

Description - Use this command to show status information about the secure HTTP web server.

show ip http

Parameter	parameter	description
	N.A	N.A
Default	N.A	
Mode	EXEC Mode	
Usage	Display the secure HTTP web server status	
Example	# show ip http 	

```
# show ip http
Switch secure HTTP web server is enabled
Switch secure HTTP web redirection is enabled
Switch secure HTTP certificate is presented
```

Telnet/SSH/Web

Authentication Method Configuration - Configures Which Network interface as telnet, SSH, Web or local console should be enabled or disable, and how remote user username + password will be authenticated. Should it be done locally by the unit or by remote RADIUS/TACACS+ Authentication Server.

Accounting Method Configuration - Configures if the unit should send Accounting messages to remote TACACS+ Accounting server whenever remote user login/logout, and report any CLI command typed by the user over Console, Telnet or SSH

aaa authentication login

Description - Configure how a user is authenticated when logging into the switch via one of the management client interfaces - console, telnet, ssh or web. Each one of the interfaces may have up to 3 authentication servers. In case the first authentication server is down, then second authentication server will be accessed instead. Same for the third authentication server in case both the first and second authentication servers are down.

NOTE:

- Rejection of remote user by any of the authentication servers will reject the remote user. The three remote authentication servers are used only as a backup in case one of the authentication services is down.
- disabling authentication by all three authentication services will disable management interface

Local- use the Switch local user database.

radius- use remote RADIUS server

tacacs- use remote TACACS+ server.

aaa authentication login { console | telnet | ssh | http } { { local | radius | tacacs } [{ local | radius | tacacs } [{ local | radius | tacacs }]] }
no aaa authentication login { console | telnet | ssh | http }

	parameter	description
Parameter	N.A	N.A
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure user authentication method for a specific management interface. Use the no version of the command to disable the interface.	
Example	Example#1 (configure SSH to be authenticated 1st by RADIUS Server. In case it is down, then by TACACS Server, and in case it is also down, then be authenticated locally) (config)#aaa authentication login ssh radius tacacs localconfig)# aaa authentication login ssh radius tacacs local Example#2 (disable Telnet remote access) (config)# no aaa authentication login telnet	

aaa accounting

Description - Configure what type of activity over a specific interface (console, telnet or ssh) is reported to the TACACS+ accounting server. Possible options are “CLI Commands”, and Exec=Login/Logout.

CLI Commands - every CLI command entered by the user will be mirrored to the accounting server. Exe (Login/Logout) – every login/logout of remote user will be reported to the accounting server.

aaa accounting { console | telnet | ssh } tacacs { [commands <priv_lvl>] [exec] }

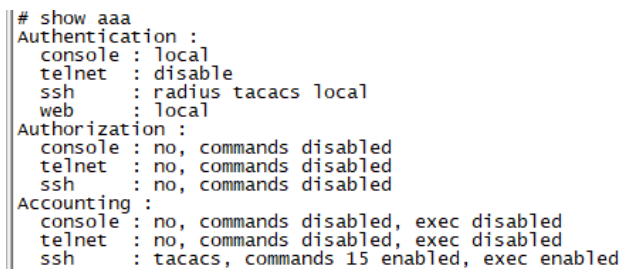
no aaa accounting { console | telnet | ssh }

Parameter	parameter	description
	[commands <priv_lvl>]	all CLI commands equal and above the privilege level are accounted
	[exec]	only remote user login/logout is reported
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure accounting method and reporting. Use the no version of the command to disable accounting.	
Example	Example#1 (configure accounting for ssh to report all CLI activity and any login/logout) (config)# aaa accounting ssh tacacs commands 15 exec Example#1 (disable accounting for Telnet) (config)# no aaa accounting telnet	

show aaa

Description - Display the current authentication, authorization and accounting statuses and methods for all interfaces.

show aaa

Parameter	parameter	description
	N.A	N.A
Default	N.A	
Mode	EXEC Mode	
Usage	Display the current status of authentication, authorization and accounting.	
Example	# show aaa 	

```
# show aaa
Authentication :
  console : local
  telnet  : disable
  ssh     : radius tacacs local
  web     : local
Authorization :
  console : no, commands disabled
  telnet  : no, commands disabled
  ssh     : no, commands disabled
Accounting :
  console : no, commands disabled, exec disabled
  telnet  : no, commands disabled, exec disabled
  ssh     : tacacs, commands 15 enabled, exec enabled
```

Access Control List

Access Control List - configures from what remote IP address remote user will be able to access the Switch management interface over Web, SNMP, Telnet/SSH.

access management

Description - Enable/disable access management mode and configure up to 16 entries.

access management

no access management

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

no access management <access_id_list>

Parameter	parameter	description
	<access_id>	ID of access management entry (1-16)
	<access_vid>	VLAN ID for the access management entry (1-4095)
	<start_addr>	start IPv4 or IPv6 unicast address
	<end_addr>	end IPv4 or IPv6 unicast address
Default	N.A	
Mode	Global Configuration Mode	
Usage	Enable access management mode and configure up to 16 entries. Use the no version of the command to disable access management globally or a specific entry.	
Example	Example#1 (configure access management entry 1 on VLAN4 for IPv4 address 192.168.0.40 – 192.168.0.70 on all interfaces) (config)# access management 1 4 192.168.0.40 to 192.168.0.70 all Example#1 (disable access management entry 1) (config)# no access management 1	

show access management

show access management [statistics | <access_id_list>]

Parameter	parameter	description
	<access_id_list>	ID of access management entry (1~16)
Default	N.A	
Mode	EXEC Mode	
Usage	Display access management status and all entries or statistics or a specific entry.	

Example	**Example#1 (show access management configuration)** # show access management **Example#2 (show access management statistics)** #show access management statistics

```
# show access management
Switch access management mode is disabled

W: WEB/HTTPS
S: SNMP
T: TELNET/SSH

Idx VID  Start IP Address                End IP Address                W S T
--- ---  ------------------------------ ------------------------------ - - -
1   4    192.168.0.40                   192.168.0.70                   Y Y Y
```

```
# show access management statistics

Access Management Statistics:
------------------------------
HTTP      Receive:          0    Allow:          0    Discard:          0
HTTPS     Receive:          0    Allow:          0    Discard:          0
SNMP      Receive:          0    Allow:          0    Discard:          0
TELNET    Receive:          0    Allow:          0    Discard:          0
SSH       Receive:          0    Allow:          0    Discard:          0
```

VLAN

VLAN configuration commands and port types

VLAN Access - VLAN is a mean to split Switch ports into sub port groups while each group is totally isolated from the other as if we are using two or more independent Switches. Such splitting is done by assigning different VLAN-IDs to various groups of ports, each group is assigned a different VLAN-ID and the ports for each group are configured as Access ports meaning that VLAN tagging and port splitting is done internally by the switch. The packets transmitted over Access ports are the normal Ethernet ports with no VLAN tagging.

VLAN Trunk – VLAN Trunk port configuration allow multiple VLAN-IDs to travel over the same Ethernet cable or local LAN Network with absolute isolation between the VLANs traveling over the same infrastructure

VLAN port types: 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.

VLAN port type - 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.

VLAN port type - 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.

VLAN port type - S-Port:On egress, if frames must be tagged, they will be tagged with an S-tag.On ingress, frames with a VLAN tag with TPID = 0x88A8 get classified to the VLAN ID embedded in the tag.Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped.

If the S-port is configured to accept Untagged Only frames, S-tagged frames will be discarded (except for priority S-tagged frames). C-tagged frames are initially considered untagged and will therefore not be discarded. Later on in the ingress classification process, they will get classified to the VLAN embedded in the tag instead of the port VLAN ID.

VLAN port type - S-Custom-Port:

On egress, if frames must be tagged, they will be tagged with the custom S-tag.

On ingress, frames with a VLAN tag with a TPID equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped.

If the Custom S-port is configured to accept Untagged Only frames, custom S-tagged frames will be discarded (except for priority custom S-tagged frames). C-tagged frames are initially considered untagged and will therefore not be discarded. Later on in the ingress classification process, they will get classified to the VLAN embedded in the tag instead of the port VLAN ID

vlan - create VLAN

Description - Create one or more VLANs in **Access mode**. By default, only single VLAN #1 is enabled with all ports assigned to this VLAN in Access mode..

vlan <vlist>

no vlan <vlist>

Parameter	parameter	description
	<vlist>	ISL VLAN IDs. Individual elements are separated by commas and ranges are specified with a dash.
Default	None	
Mode	Global Configuration mode	
Usage	Create allowed Access VLANs. Use the no version of the command to delete VLANs.	
Example	Example#1 (Create Access VLANs 10,11,12,200 and 300) (config)# vlan 10-12,200,300 Example#2 (Delete VLAN 12) (config)# no vlan 12	

vlan ethertype s-custom-port

Description - Specifies the Ethertype/TPID (specified in hexadecimal) used for Custom S-Ports. The setting is in force for all ports set to S-Custom port type.

vlan ethertype s-custom-port <etype>

Parameter	parameter	description
	<etype>	EtherType (Range: 0x0600-0xffff)
Default	TPID is set to 0x88A8	
Mode	Global Configuration mode	
Usage	Specifies the ethertype/TPID for Custom S-Ports	
Example	(config)# vlan ethertype s-custom-port 0x8888	

switchport mode

Description - Defines the port mode as access (default), trunk or hybrid unconditionally.

switchport mode { access | trunk | hybrid }

Parameter	parameter	description
	access	Configure a switch port mode is access
	trunk	Configure a switch port mode is trunk
	hybrid	Configure a switch port mode is hybrid
Default	The switch port default mode is access	
Mode	Port List Interface Mode	
Usage	Set port mode	
Example	# configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode trunk	

switchport trunk native vlan

Description - Configure VLAN ID to be added internally by the Switch whenever native VLAN packet (packet with no VLAN header) is received.

switchport trunk native vlan <pvid>

no switchport trunk native vlan

Parameter	parameter	description
	<pvid>	VLAN ID of the native VLAN when this port is in trunk mode
Default	Trunk native default VLAN is VLAN1	
Mode	Port List Interface Mode	
Usage	Configure a port VLAN ID for a trunk port. use the no version of the command to revert to default.	
Example	# configure terminal (config)# interface GigabitEthernet ⅓ (config-if)# switchport mode trunk (config-if)# switchport trunk native vlan 4	

switchport trunk vlan tag native

Description - Port in Trunk mode may control the tagging of frames on egress. Options are default Untag Port VLAN (frames classified to the Port VLAN are transmitted untagged and all other frames are transmitted with the relevant tag) and Tag all (all frames transmitted with a tag).

switchport trunk vlan tag native

no switchport trunk vlan tag native

Parameter	parameter	description
	N.A	N.A
Default	Frames classified to the Port VLAN (Native VLAN) do not get tagged on egress.	
Mode	Port List Interface Mode	
Usage	Set the trunk port egress tagging to all. Use the no version of the command to revert to default (untag native VLAN)	
Example	# configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode trunk (config-if)# switchport trunk native vlan 4 (config-if)# switchport trunk vlan tag native	

switchport trunk allowed vlan

Description - Ports in Trunk mode may control which VLANs they are allowed to become members of. By default, Trunk port will become a member of all VLANs (1-4095).

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

no switchport trunk allowed vlan

Parameter	parameter	description
	all	all VLANs are allowed (1-4095)
	none	Port will not become member of any VLAN
	add	Add VLANs to the current list
	remove	Remove VLANs from the current list
	except	All VLANs except the following (VLAN ID or list)
	<vlan_list>	VLAN IDs of the allowed VLANs. Individual elements are separated by commas and ranges are specified with a dash.
Default	All VLANs are allowed (1-4095)	
Mode	Port List Interface Mode	
Usage	Configure allowed VLANs for a trunk port. Use the no version of the command to revert to default.	
Example	# configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan except 10,30-32	

switchport forbidden vlan

Description - Configure the port to never become a member of one or more VLANs.

switchport forbidden vlan { add | remove } <vlan_list>

no switchport forbidden vlan

Parameter	parameter	description
	add	Add forbidden VLANs to the current list of forbidden VLANs
	remove	Remove forbidden VLANs from the current list of forbidden VLANs
Default	Trunk Port may become a member of all possible VLANs	
Mode	Port List Interface Mode	
Usage	Configure VLANs that a trunk port may not become a member. Use the no version of the command to revert to default.	

Example	# configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode trunk (config-if)# switchport forbidden vlan add 4

switchport hybrid native vlan

Description - Configure VLAN ID (PVID) for the hybrid port (Native VLAN).

switchport hybrid native vlan <pvid>

no switchport hybrid native vlan

Parameter	parameter	description
	<pvid>	VLAN ID of the native VLAN when this port is in hybrid mode
Default	Hybrid native default VLAN is VLAN1	
Mode	Port List Interface Mode	
Usage	Configure a port VLAN ID for a hybrid port. Use the no version of the command to revert to default	
Example	# configure terminal (config)# interface GigabitEthernet 1/4 (config-if)# switchport mode hybrid (config-if)# switchport hybrid native vlan 5	

switchport hybrid port-type

Description - Specifies the port type in hybrid mode.

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

no switchport hybrid port-type

Parameter	parameter	description
	unaware	Port is not aware of VLAN tags. No matter the received frame is tagged or untagged, port adds a tag (based on PVID) to the frame and then forward it.
	c-port	Customer port. If the received frame is untagged, C-port adds a tag (based on PVID) to the frame and then forward it; If the frame is already tagged, it will be forwarded without adding a tag.
	s-port	Provider port. Port only accepts untagged frames. If the received frame is untagged, S-port adds a tag (based on PVID) to the frame and then forward it; If the frame is already tagged, it will be discarded.

	s-custom-port	Custom provider port. When Ethertype is set to 0x8100, S-custom ports do the same as C-ports: If the received frame is untagged, S-custom port adds a tag (based on PVID) to the frame and then forward it; If the frame is already tagged, it will be forwarded without adding a tag.
Default	Hybrid Port type is C-port	
Mode	Port List Interface Mode	
Usage	Configure hybrid port type. Use the no version of the command to revert to default.	
Example	# configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode hybrid (config-if)# switchport hybrid port-type unaware	

switchport hybrid ingress-filtering

Description - enable/disable ingress filtering

switchport hybrid ingress-filtering

no switchport hybrid ingress-filtering

Parameter	parameter	description
	N.A	N.A
Default	Ingress filtering disabled	
Mode	Port List Interface Mode	
Usage	Enable ingress filtering Use the no version of the command to revert to default.	
Example	# configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode hybrid (config-if)# switchport hybrid ingress-filtering	

switchport hybrid acceptable-frame-type

Description - Set Ingress acceptance criteria.

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

no switchport hybrid acceptable-frame-type

Parameter	parameter	description
	all	Both tagged and untagged frames are accepted
	tagged	Only frames tagged with the corresponding port type tag are accepted.

	untagged	Only untagged frames are accepted.
Default	Hybrid Port is set to accept all frames (tagged and untagged)	
Mode	Port List Interface Mode	
Usage	Configure type of frames accepted on ingress. use the no version of the command to revert to default.	
Example	# configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode hybrid (config-if)# switchport hybrid acceptable-frame-type tagged	

switchport hybrid egress-tag

Description - Configure Egress tagging.

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

no switchport hybrid egress-tag

Parameter	parameter	description
	none	No Egress tagging. All frames transmitted without a tag.
	all	Tag all frames. All frames are transmitted with a tag.
	except-native	Tag all frames except frames classified to native VLAN.
Default	Hybrid Port is set to tag all frames except frames classified to native VLAN.	
Mode	Port List Interface Mode	
Usage	Configure egress tagging. Use the no version of the command to revert to default.	
Example	# configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode hybrid (config-if)# switchport hybrid egress-tag all	

switchport trunk allowed vlan

Description - Ports in Hybrid mode may control which VLANs they are allowed to become members of. By default Hybrid port will become a member of all VLANs (1-4095).

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

no switchport hybrid allowed vlan

Parameter	parameter	description
	all	all VLANs are allowed (1-4095)
	none	Port will not become member of any VLAN
	add	Add VLANs to the current list

	remove	Remove VLANs from the current list
	except	All VLANs except the following (VLAN ID or list)
	<vlan_list>	VLAN IDs of the allowed VLANs. Individual elements are separated by commas and ranges are specified with a dash.
Default	All VLANs are allowed (1-4095)	
Mode	Port List Interface Mode	
Usage	Configure allowed VLANs for a hybrid port. Use the no version of the command to revert to default.	
Example	# configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode hybrid (config-if)# switchport hybrid allowed vlan except 10,30-32	

show vlan

Description- provides overview of membership status of VLAN users and VLANs configured for each interface.

show vlan [id <vlan_list> | name <name> | brief] [all]

Parameter	parameter	description
	id <vlan_list>	VLAN status by VLAN ID
	name <name>	VLAN status by VLAN name
	brief	VLAN summary informatin
	all	Show all VLANs (if left out only access VLANs are shown)
Default	N.A	
Mode	EXEC mode	
Usage	Display VLAN membership status overview.	
Example	Example#1 (Show VLAN summary information for all vlans) #show vlan brief all Example#2 (Show VLAN information for port 1 configured by Admin) #show vlan status interface GigabitEthernet 1/1 admin	

show vlan status

Description - Shows VLAN status for a specific interface (port) configured by a specific user.

show vlan status [interface <port_type> [<plist>]] [admin | all | combined | conflicts | mstp | nas | rmirror]

Parameter	parameter	description
	interface <port_type>	Show the VLANs configured for a specific interface or interfaces and port type (GigabitEthernet)
	<plist>	List of Port ID, ex, 1/1,3-5

	admin	Show the VLANs configured by administrator.
	all	Show VLANs configured VLANs for all VLAN users.
	combined	Show the combined set of configured VLANs.
	mstp	Show the VLANs configured by MSTP.
	nas	Show the VLANs configured by NAS.
	rmirror	Show the VLANs configured by Remote mirroring.
Default	N.A	
Mode	EXEC mode	
Usage	Display VLAN membership status overview.	
Example	#show vlan status interface GigabitEthernet 1/1 admin	

POE **(Feature Supported on PoE switches only)

PoE-BT Power (Only supported on PoE BT switches)

PoE-BT (IEEE 802.3-bt) is the latest PoE (Power Over Ethernet) specification offering up to 90[W] of power whenever power is delivered over all four RJ45 cable pairs.

poe extended-bt-power-mode

Description - Global configuration of Extended Power Mode. When enabled the switch will extend slightly the maximum power provided to PD beyond its classification. For example, class 8 will be extended from 90W to 95W.

poe extended-bt-power-mode

no poe extended-bt-power-mode

	parameter	description
Parameter	N.A	N.A
Default	Extended mode disabled.	
Mode	Global Configuration Mode	
Usage	Enable extended power mode. Use the no version of the command to disable extended power mode.	
Example	(config)# poe extended-bt-power-mode	

poe uninterruptible-power

Description - Global configuration of uninterruptable power mode. When enabled, the switch will provide seamless uninterruptable power to PD devices even when the switch performs software reset.

poe uninterruptible-power

no poe uninterruptible-power

	parameter	description

Parameter	N.A	N.A
Default	Uninterruptable power enabled	
Mode	Global Configuration Mode	
Usage	Enable uninterruptable power mode. Use the no version of the command to disable uninterruptable power mode.	
Example	**Example** (config)# poe uninterruptible-power	

poe power

Description - Enable/Disable poe power for the specific port

poe power

no poe power

Parameter	parameter	description
	N.A	N.A
Default	N.A	
Mode	Port List Interface Mode	
Usage	Enable/Disable PoE power for the port.	
Example	Example#1 (enable PoE power for port (config)# interface GigabitEthernet1/1 (config-if)# poe power Example#2 (disable PoE power for port 2) (config)# interface GigabitEthernet1/2 (config-if)# no poe power	

poe mode

Description - Set PoE mode to control what PD devices may receive power.

poe mode { bt | bt-plus-legacy }

Parameter	parameter	description
	bt	Power only PoE-BT compliant PDs.
	bt-plus-legacy	Power PoE-BT compliant and legacy PDs.
Default	N.A	
Mode	Port List Interface Mode	
Usage	Set PoE mode	
Example	Example#1 (set PoE mode for port 1 to BT only) (config)# interface GigabitEthernet1/1 (config-if)# poe mode bt	

poe priority

Description - Configure PoE priority

poe priority { low | high | critical }

Parameter	parameter	description
	low	Low priority. Ports will be powered last upon startup and disconnected first whenever power budget is exceeded.
	high	High priority. Ports will be powered second upon startup and disconnected second whenever power budget is exceeded.
	critical	Critical priority. Ports will be powered first upon startup and disconnected last whenever power budget is exceeded.
Default	All ports priority is Low.	
Mode	Port List Interface Mode	
Usage	Set PoE priority	
Example	(config)# interface GigabitEthernet1/1 (config-if)# poe priority high	

poe terminal-description

Description - Textual description for each PoE-PD device connected to the port.

poe terminal-description <term_desc>

Parameter	parameter	description
	<term_desc>	PD device description (32 characters).
Default	N.A	
Mode	Port List Interface Mode	
Usage	Set terminal description	
Example	Example#1 (set description for port 1 to ipcamera) (config)# interface GigabitEthernet1/1 (config-if)# poe terminal description “ipcamera”	

show poe

Description - Display detailed PoE status for the switch.

show poe [interface <port_type> [<v_port_type_list>]]

Parameter	parameter	description
	interface <port_type>	Specify interfaces and port type (GigabitEthernet)
	<v_port_type_list>	List of Port ID, ex, 1/1,3-5
Default	N.A	
Mode	EXEC Mode	
Usage	Display PoE status for the switch.	

Example	Example#1 (show poe status for port 1) # show poe interface GigabitEthernet 1/1 Example#2 (show poe status for all ports) # show poe

```
# show poe
    Interface          PD     Power                  Port Status      Power     Current
                       Class  Alloc [w]              Used [w]  Used [mA]  Internal status
-------------------- ------ ---------- ---------------- --------- ---------- ----------------------------------------
GigabitEthernet 1/1  2      7          PoE-ON (2Pair)   2.7       50         0x85 PoE-On : 4P Pwr on 2P IEEE SSPD
GigabitEthernet 1/2  ---    0          ---              0         0          0xA8 PoE-Off: No Device (open)
GigabitEthernet 1/3  4, 4   60         PoE-ON           2.8       53         0x89 PoE-On : 4P Pwr on 4P IEEE DSPD
GigabitEthernet 1/4  ---    0          ---              0         0          0xA8 PoE-Off: No Device (open)
GigabitEthernet 1/5  ---    0          PoE-OFF-fault    0         0          0x41 PoE-Off: PD Class > PoE-IC max Class
GigabitEthernet 1/6  ---    0          PoE-OFF-fault    0         0          0x25 PoE-Off: PD Capacitor out of range
GigabitEthernet 1/7  ---    0          ---              0         0          0xA8 PoE-Off: No Device (open)
GigabitEthernet 1/8  ---    0          ---              0         0          0xA8 PoE-Off: No Device (open)
-------------------- ------ ---------- ---------------- --------- ---------- ----------------------------------------
    Total                   67                          5.5       103
```

Spanning tree Protocol

STP Bridge Configuration commands

The Spanning Tree Protocol (STP) and its variations, such as RSTP and MSTP, serve to prevent network loops that can lead to broadcast storms. Additionally, they provide redundancy paths between switches or multiple paths across multiple switches while maintaining control over network loops through STP.

The STP algorithm ensures that, at any given moment, only one path out of several possible loops remains active. This enables switches to utilize multiple backup paths in the event that the primary connection path becomes unavailable.

spanning-tree mode

Description - Configure STP protocol version.

spanning-tree mode { stp | rstp | mstp }

no spanning-tree mode

Parameter	parameter	description
	stp	Spaning Tree protocol 802.1D
	rstp	Rapid Spanning Tree protocol 802.1w
	mstp	Multiple Spanning Tree protocol 802.1s
Default	Default protocol is MSTP	
Mode	Global Configuration Mode	
Usage	Set STP protocol version. Use the no version of the command to revert to default.	
Example	# configure terminal (config)# spanning-tree mode rstp	

spanning-tree system settings

Description - Configure STP system settings used by all STP Bridge instances in the switch. Basic STP global setting commands:

spanning-tree mst <instance=0> **priority** <prio>

spanning-tree mst hello-time <hellotime>
spanning-tree mst forward-time <fwdtime>
spanning-tree mst max-age <maxage> [forward-time <fwdtime>]
spanning-tree mst max-hops <maxhops>
spanning-tree transmit hold-count <holdcount>

Parameter	parameter	description
	<instance>	STP bridge instance. Must be 0 (zero)
	priority <prio>	Bridge Priority. Supported values are 0-61440. Only values divisible by 4096 are allowed. For example, 4096, 8192, etc. . Default value is 32768
	<hellotime>	Interval between sending STP BPDUs. Valid values are 1-10 seconds. Default is 2 seconds.
	<fwdtime>	Forward delay used by STP Bridges to transit Root and Designated Ports to Forwarding. Valid values are 4-30 seconds. Default is 15.
	<maxage>	Maximum age of the information transmitted by the Bridge when it is a Root Bridge. Valid values are 6-40 seconds. Default is 20.
	<maxhops>	Defines how many bridges a root bridge can distribute its BPDU information. Valid values are 6-40 hops. Default is 20.
	<holdcount>	Number of BPDUs a bridge port can send per second. Valid range 1-10 BPDUs per second. Default is 6.
	<interval>	Time to pass before a port in error-disabled state can be enabled. Values are 30-86400 seconds (24 hours). Default is port error recovery disabled.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure STP system settings. Use the no version of the command to revert to default.	
Example	**Example (Configure STP settings)** # configure terminal (config)# spanning-tree mode mstp (config)# spanning-tree mst 0 priority 36864 (config)# spanning-tree mst hello-time 3 (config)# spanning-tree mst max-age 25 forward-time 16 (config)# spanning-tree mst max-hops 25 (config)# spanning-tree transmit hold-count 7 (config)# spanning-tree edge bpdu-filter (config)# spanning-tree edge bpdu-guard (config)# spanning-tree recovery interval 120	

Advanced STP global setting commands:

spanning-tree edge bpdu-filterspanning-tree edge

bpdu-guard spanning-tree recovery interval

<interval>

spanning-tree port settings

Description- Configure STP CIST settings for the specific physical and aggregated ports

spanning-tree *Enable STP on the port*

no spanning-tree *Disable STP on the port*

spanning-tree mst <instance=0> **cost** { <cost> | auto }

spanning-tree mst <instance=0> **port-priority** <prio>

spanning-tree edge

spanning-tree auto-edge spanning-tree restricted-role

spanning-tree restricted-tcn spanning-tree bpdu-guard

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

Parameter	parameter	description
	<instance>	STP bridge instance. Must be 0 (zero)
	cost { <cost> | auto }	Controls the path cost incurred by the port. Auto setting will set the cost as appropriate by link speed using 802.1D recommended values. User defined value can also be entered and the valid range is 1-200000000. Default is auto.
	port-priority <prio>	Represents the port priority. Must be divisible by 16, supported values are 0-240. For example, 16, 32, etc. Default value is 128
	link-type { point-to-point | shared | auto }	Controls whether the port connects to a point-to-point LAN rather than to a shared medium. Default is auto.
	edge	Defines whether the port is is connecting directly to edge devices. Default is non-edge.
	auto-edge	Enables auto edge detection on the port.
	restricted-role	If enabled causes the port not to be selected as Root port.
	restricted-tcn	If enabled causes the port not to propagate received topology change notifications to other ports.
	bpdu-guard	If enabled causes the port to disable itself upon receiving valid BPDUs.
Default	N.A	
Mode	Port List Interface Mode	
Usage	Configure STP CIST settings for the specific physical and aggregated ports. Use the no version of the command to revert to default.	

Example	# configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# spanning-tree (config-if)# spanning-tree mst 0 cost auto (config-if)# spanning-tree mst 0 port-priority16 (config-if)# spanning-tree egde

show spanning-tree

Description - Provides a detailed status information on a STP bridge instance, along with port state for all active ports associated.

show spanning-tree [summary | active | { interface <port_type> [<v_port_type_list>] } | { detailed [interface <port_type> [<v_port_type_list_1>]] } | { mst [configuration | { <instance> [interface<port_type> [<v_port_type_list_2>]] }] }]

Parameter	parameter	description
	summary	STP sumary
	active	STP active interfaces
	interface <port_type>	Choose port and type in GigabitEthernet
	<v_port_type_list>	List of Port ID, ex, 1/1,3-5
	detailed	STP statistics
	mst	Multiple STP
	configuration	Show MSTI to VLAN mapping
	<instance>	STP bridge instance (CIST=0, MSTI1=1...)
Default	N.A	
Mode	EXEC Mode	
Usage	Display information on STP	
Example	**Example (Display CIST port state for port 8)** # show spanning-tree interface GigabitEthernet 1/8 **Example (Display STP detailed Bridge status)** #show spanning-tree mst 0	

SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)

Application-layer protocol used to manage and monitor network devices and their functions. It enables network management systems to learn network problems by receiving traps or change notices from network devices.

NOTE: By default, SNMP is disabled for security concerns. In case SNMPv2 will be used then please change SNMPv2 default 'public', 'private' community strings (passwords) prior enabling SNMPv2.

Enable/Disable SNMP and configure MIB-II system OiDs

snmp-server

Description - Enable/Disable SNMP server

snmp-server

no snmp-server

	parameter	description
Parameter	N.A	N.A
Default	N.A	
Mode	Global Configuration Mode	
Usage	Enable SNMP server. Use the no version of the command to disable SNMP.	
Example	# configure terminal (config)# snmp-server	

snmp-server contact, System-Name (host) and location

Description- Specify SNMP MIB-II contact person, system name and system location

snmp-server contact <v_line255>

no snmp-server contact host<conf_name>

snmp-server location <v_line255>

	parameter	description
Parameter	<v_line255>	String length is 0-255 and valid ASCII characters range 32-126
	<conf_name>	Administratively assigned name for this system. By convention this is fully-qualified domain name. String length is 0-255 and no spaces are permitted.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Specify system contact, name and location Use the no version of the command to delete it.	
Example	Example (Set system contact as "testcontact", name as "microchip" and location as "server room") # configure terminal (config)# snmp-server contact testcontact (config)# host microchip microchip(config)# snmp-server location server room	

snmp-server view

Description - Configure which SNMP OiDs should be included/excluded from the entire SNMP OiD tree.

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

no snmp-server view <view_name> <oid_subtree>

Parameter	parameter	description
	<view_name>	Name identifying the vew OiD branch to be included/excluded. String length is 1-32 and valid ASCII characters range 33-126
	<.oid_subtree>	OiD defining the root of the subtree to add to the named view. String length is 1-128. Allowed string content is number or asterisk (*).
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure SNMP View OiD-range.	
Example	Example (Create SNMP view OiD-range named “mib-ii” with access to all SNMP OiDs exept for MIB-II system branch .1.3.6.1.2.1.1) # configure terminal (config)# snmp-server view mib-ii .1.3.6.1.2.1.1 excluded	

snmp-server community

Description- Configure SNMP community table used as part of SNMP group configuration.

snmp-server community <comm> [{ ip-range <v_ipv4_addr> <v_ipv4_netmask> }] { <sec> | encrypted <sec_enc> }

Parameter	parameter	description
	<comm>	Community Name to map to the SNMP Groups configuration. String length is 1-32 and valid ASCII characters range 33-126.
	ip-range <v_ipv4_addr> <v_ipv4_netmask>	Indicates SNMP access source address. A range of source addresses can be used to restrict source subnet when combined with source netmask.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure SNMP community	
Example	# configure terminal (config)# snmp-server community c-name secret	

snmp-server user

Description - Configure SNMPv3 user.

snmp-server user <username> engine-id <engineID> [{ md5 { <md5_passwd> | { encrypted<md5_passwd_encrypt> } } |

sha { <sha_passwd> | { encrypted <sha_passwd_encrypt> } } } [priv{ des | aes } { <priv_passwd> | { encrypted <priv_passwd_encrypt> } }]]

	parameter	description
Parameter	<username>	User name. String length is 1-32 and valid ASCII characters range 33-126
	<engineID>	Octet string. Must contain an even number (in hexadecimal format) between 10 and 64 digits.
	md5 <md5_passwd>	Authentication protocol MD5 and password length 8-32 ASCII characters 33-126
	sha <sha_passwd>	Authentication protocol SHA and password length 8-40 ASCII characters 33-126
	priv { des | aes }	Privacy protocol DES or AES
	<priv_passwd>	Privacy password length 8-32 ASCII characters 33-126.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure SNMPv3 user.	
Example	# configure terminal (config)# snmp-server user testuser engine-id 800019ab12345 md5 testpassword	

snmp-server security-to-group model

Description - Configure SNMP group-name based on Security Model and Security name.

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

	parameter	description
Parameter	v1 | v2c | v3	Security model the entry should belong to.
	<security_name>	One of the security names created in SNMP Community for v1 and v2c or one of the SNMPv3 users.
	<group_name>	Group name. String length is 1-32 and valid ASCII characters range 33-126.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure SNMP group name.	
Example	# configure terminal (config)# snmp-server security-to-group model v2c name public group ro_group	

snmp-server access

Description - Configure SNMP access.

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

Parameter	parameter	description
	<group_name>	Group name previously configured by security-to-group command. String length is 1-32 and valid ASCII characters range 33-126.
	model {v1 | v2c | v3 | any}	Security model the entry should belong to.
	level {auth | noauth | priv}	Security level. authNoPriv, noAuthNoPriv, authPriv
	read <view_name>	Name of the MIB view defining the MIB objects for which this request may read OiD values
	write <write_name>]	Name of the MIB view defining the MIB objects for which this request may set OiD new values
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure SNMP group name.	
Example	Example (Configure SNMPv2 access) # configure terminal (config)# snmp-server access ro_group model v2c level noauth read mib-ii	

snmp-server trap

Description - SNMP Trap source configuration. Provides the list for all events that may cause SNMP Trap to be sent.

snmp-server trap <source_name>

no snmp-server trap <source_name>

Parameter	parameter	description
	<source_name>	Name of the event. Possible options are: coldStart, warmStart, linkUp, linkDown, authenticationFailure, newRoot, topologyChage, lldpRemTablesChange.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure SNMP source. Use the no version of the command to delete the entry.	

Example	Example (Add “Remote SNMP client was trying to access the unit using invalid username/password values” event to the trap source configuration) # configure terminal (config)# snmp-server trap authenticationfailure

snmp-server host

Description - Add/delete SNMP trap server.

snmp-server host <conf_name>

no snmp-server host <conf_name>

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

Parameter	parameter	description
	<conf_name>	Group name previously configured by security-to-group command. String length is 1-32 and valid ASCII characters range 33-126.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Add SNMP trap server. Use the no version of the command to delete trap server.	
Example	# configure terminal (config)# snmp-server host trapserver	

Configure SNMP Trap server

version { v1 [{ <v1_comm> | encrypted <v1_comm_sec> }] | v2 [{ <v2_comm> | encrypted <v2_comm_sec> }] | v3 engineID <v_word10_to_64> [<securityname>] }

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

informs retries<retries> timeout <timeout>

Parameter	parameter	description
	<v1_comm>, <v2_comm>, <v_word10_to_64>	SNMP version 1 and 2 community or version 3 engine ID
	<v_ipv4_ucast>	IP address of SNMP trap host
	<v_word>	hostname of SNMP trap host
	<udp_port>	UDP port of the trap messages
	traps	Send Trap messages to this host
	informs	Send Inform messages to this host
	<retries>	inform retry times 0-255
	<timeout>	inform timeout interval 0-2147 seconds
Default	N.A	
Mode	SNMP Server Host Mode	

Usage	Configure SNMP trap server.
Example	**Example (Configure SNMP Trap server)** # configure terminal (config)# snmp-server host trapserver (config-snmp-host)# version v2 c-name (config-snmp-host)# host my.traphost.com 162 informs (config-snmp-host)# informs retries 6 timeout 3

show snmp

Description - Display SNMP configuration.

show snmp view - Display OiD-range configuration

show snmp community -Display SNMP Community configuration

show snmp security-to-group -Display SNMP Group configuration

show snmp access - Display SNMP access configuration

show snmp user - Display SNMPv3 users

show snmp trap - Display configured SNMP Trap sources

show snmp host - Display SNMP Trap server list and configuration

Parameter	parameter	description
	N.A	N.A
Default	N.A	
Mode	EXEC Mode	
Usage	Display PoE status for the switch.	
Example	# show snmp host	

RADIUS TACACS+

RADIUS Server configuration commands

RADIUS (Remote Authentication Dial-In User Service) and TACACS+ (Terminal Access Controller Access Control System) are networking protocols designed to centralize the management of Authentication, Authorization, and Accounting (commonly referred to as AAA or Triple A) for users connecting to a unit via Web, Telnet, or SSH.

Instead of locally checking the remote username and password against the unit's configuration file, these protocols send the remote username and password to a RADIUS or TACACS+ server for authentication (checking if the user and password match) and authorization (determining privilege levels).

Global configuration commands

Description - Set default values to be used for every new RADIUS server being added when the same

parameters are left blank.

radius-server timeout <seconds>

radius-server retransmit <retries>

radius-server deadtime <minutes>

radius-server key { [unencrypted] <unencrypted_key> | encrypted <encrypted_key> }

Parameter	parameter	description
	timeout <seconds>	Time to wait for a RADIUS server to reply in seconds 1-1000 before retransmitting the request
	retransmit <retries>	Number of times 1-1000 a request is retransmitted to a server that is not responding.
	deadtime <minutes>	Period between 0-1440 minutes during which the switch will not send a new request to a server that failed to respond to previous requests (dead).
	key	Specify the encryption key up to 63 characters long.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure default global parameters for RADIUS Server	
Example	**Example** # configure terminal (config)# radius-server timeout 10 (config)# radius-server retransmit 3 (config)# radius-server deadtime 10 (config)# radius-server key unencrypted secret	

Radius server configuration

Description - Add a new RADIUS server. Up to 5 servers can be added.

radius-server host <host_name> [auth-port <auth_port>] [acct-port <acct_port>] [timeout<seconds>] [retransmit <retries>] [key { [unencrypted] <unencrypted_key> | encrypted<encrypted_key> }]

Parameter	parameter	description
	<host_name>	IPv4/IPv6 address or the hostname of the radius server
	<auth_port>	UDP port number to use on the RADIUS server for authentication. Set to 0 to disable authentication.
	<acct_port>	UDP port number to use on the RADIUS server for accounting. Set to 0 to disable accounting.
	timeout <seconds>	Time to wait for this RADIUS server to reply (overrides default).
	retransmit <retries>	Specify the number of retries to active server (overrides

		default).
	<unencrypted_key>	The UNENCRYPTED (Plain Text) secret key (overrides default)
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure custom parameters for RADIUS Server.	
Example	# configure terminal (config)# radius-server host radiusserver auth-port 1812 timeout 20 retransmit 5	

show radius-server

Description - Display overview status of the current RADIUS servers configuration and statistics

show radius-server [statistics]

	parameter	description
Parameter	[statistics]	provides detailed statistics for the RADIUS servers
Default	N.A	
Mode	EXEC Mode	
Usage	Show current RADIUS servers configuration and statistics	
Example	# show radius-server # show radius-server statistics	

tacacs Global configuration commands

Description - Set default values to be used for every new TACACS+ server being added when the same parameters are left blank.

tacacs-server timeout <seconds>

tacacs-server deadtime <minutes>

tacacs-server key { [unencrypted] <unencrypted_key> | encrypted <encrypted_key> }

	parameter	description
Parameter	**timeout** <seconds>	Time to wait for a TACACS+ server to reply in seconds 1-1000 before retransmitting the request
	deadtime <minutes>	Period between 0-1440 minutes during which the switch will not send a new request to a server that failed to respond to previous requests (dead).
	key	Specify the encryption key up to 63 characters long.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure default global parameters for TACACS Server	

Example	# configure terminal (config)# tacacs-server timeout 10 (config)# tacacs-server deadtime 3 (config)# tacacs-server key unencrypted secret

TACACS+ Server configuration

Description - Add a new TACACS+ server. Up to 5 servers can be added.

tacacs-server host <host_name> [port <port>] [timeout <seconds>] [key { [unencrypted]<unencrypted_key> | encrypted <encrypted_key> }]

Parameter	parameter	description
	<host_name>	IPv4/IPv6 address or the hostname of the radius server
	<port>	TCP port number to use on the TACACS+ server for authentication.
	timeout <seconds>	Time to wait for this TACACS+ server to reply (overrides default).
	<unencrypted_key>	The UNENCRYPTED (Plain Text) secret key (overrides default)
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure custom parameters for TACACS+ Server.	
Example	# configure terminal (config)# tacacs-server host tacacsserver port 50 timeout 20 key unencrypted secret	

show tacacs-server

Description - Display current TACCAS+ servers configuration.

show tacacs-server

Parameter	parameter	description
	N.A	
Default	N.A	
Mode	EXEC Mode	
Usage	View the current TACACS+ server configuration.	
Example	# show tacacs-server	

AGGREGATION/LACP

Aggregation Group Configuration commands

Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

aggregation mode

Description - Specify parameters that contribute to the way Aggregation is done. Applies to the whole network element.

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

no aggregation mode

Parameter	parameter	description
	[smac]	Source MAC address can be used to calculate the destination port for the frame (enabled by default)
	[dmac]	Destination MAC address can be used to calculate the destination port for the frame (disabled by default)
	[ip]	IP address can be used to calculate the destination port for the frame (enabled by default)
	[port]	TCP/UDP port number can be used to calculate the destination port for the frame (enabled by default)
Default	smac,ip and port enabled, dmac disabled	
Mode	Global Configuration Mode	
Usage	Configure aggregation parameters. Use the no version of the command to reset to default.	
Example	# configure terminal (config)# aggregation mode smac dmac	

aggregation group

Description - Create and configure aggregation group. Each port can be a member of one aggregation group only and ports must be full duplex and have the same speed.

aggregation group <v_uint> mode { [active | on | passive] }

no aggregation group <v_uint>

Parameter	parameter	description
	<v_uint>	The aggregation group id
	[active]	Group operates in LACP active aggregation mode.
	[on]	Group operates in a static aggregation mode
	[passive]	Group operates in LACP passive aggregation mode
Default	N.A.	
Mode	Port List Interface Mode	

Usage	Configure aggregation group (add port to it). Use the no version of the command to remove the port from the aggregation group.
Example	# configure terminal (config)# interface GigabiitEthernet 1/1 (config-if)# aggregation group 1 mode active

lacp failover

Description - This parameter determines if the group will perform automatic link (re-)calculation when links with higher priority becomes available.

lacp failover { revertive | non-revertive }

no lacp failover

Parameter	parameter	description
	revertive	group will perform automatic link (re-)calculation
	non-revertive	group will not perform automatic link (re-)calculation
Default	Revertive failover is enabled.	
Mode	LLAG Mode	
Usage	Specify if the group will perform automatic link (re-)calculation. Use the no version of the command to revert to default.	
Example	# configure terminal (config)# interface llag 1 (config-llag)# lacp failover non-revertive	

lacp max-bundle

Description - This parameter determines the maximum number of active bundled LACP ports allowed in an aggregation.

lacp max-bundle <v_uint>

no lacp max-bundle

Parameter	parameter	description
	<v_uint>	The aggregation group id
Default	Maximum number of active bundled ports 16.	
Mode	LLAG Mode	
Usage	Specify the maximum number of active bundled LACP ports allowed in an aggregation. Use the no version of the command to revert to default.	
Example	# configure terminal (config)# interface llag 1 (config-llag)# lacp max-bundle 10	

show aggregation

Description - Display current status of ports in aggregation group and view parameters that contribute to the way Aggregation is done.

show aggregation

show aggregation mode

Parameter	parameter	description
	N.A	
Default	N.A	
Mode	EXEC Mode	
Usage	View the current aggregation status and parameters	
Example	# show aggregation	

lacp system-priority

Description - Set the system LACP priority **lacp system-priority** <v_1_to_65535> **no lacp system-priority** <v_1_to_65535>

Parameter	parameter	description
	<v_1_to_65535>	Priority value, lower means higher priority
Default	System priority 32768	
Mode	Global Configuration Mode	
Usage	Configure LACP system priority. Use the no version of the command to revert to default.	
Example	Example#1 (set lacp system priority to 16384) # configure terminal (config)# lacp system-priority 16384 Example#2 (set lacp system priority to default) # configure terminal (config)# no lacp system-priority 1	

lacp port-priority

Description - Set LACP priority of the port.

lacp port-priority <v_1_to_65535>

no lacp port-priority <v_1_to_65535>

Parameter	parameter	description
	<v_1_to_65535>	Priority value, lower means higher priority
Default	Port priority 32768	
Mode	Port List Interface Mode	
Usage	Configure LACP system priority. Use the no version of the command to revert to default.	

Example	Example#1 (set lacp priority to 16384 for port#1) # configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# lacp port-priority 16384 Example#2 (set lacp priority to default for port#1) # configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# no lacp port-priority 1

lacp timeout

Description - Specifies time period between BPDU transmissions.

lacp timeout { fast | slow }

no lacp timeout { fast | slow }

Parameter	parameter	description
	fast	Transmit BPDU each second (fast timeout)
	slow	Transmit BPDU each 30th second (slow timeout)
Default	Fast	
Mode	Port List Interface Mode	
Usage	Set the LACP timeout, i.e. how fast to transmit BPDUs, once a sec or once each 30 sec.	
Example	Example#1 (set lacp timeout to slow for port#1) # configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# lacp timeout slow Example#1 (set lacp timeout to default (fast) port#1) # configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# no lacp timeout slow	

show lacp system-id

Description -Display local system priority and MAC address which forms the local LACP System ID

show lacp system-id

Parameter	parameter	description
	N.A	
Default	N.A	
Mode	EXEC Mode	
Usage	Display local system priority and MAC address	
Example	#show lacp system-id	

show lacp internal details

Description- Display status overview for LACP internal (local system) status for all ports that are part of the

LACP group.

show lacp internal details

Parameter	parameter	description
	N.A	
Default	N.A	
Mode	EXEC Mode	
Usage	Display status overview for LACP ports	
Example	#show lacp internal details	

show lacp neighbor details

Description - Display status overview for the LACP neighbor status for all ports.

show lacp neighbor details

Parameter	parameter	description
	N.A	
Default	N.A	
Mode	EXEC Mode	
Usage	Display status overview for the LACP neighbor status for all ports.	
Example	#show lacp neighbor details	

show lacp statistics details

Description - Display overview for LACP statistics for all ports.

show lacp statistics details

Parameter	parameter	description
	N.A	
Default	N.A	
Mode	EXEC Mode	
Usage	Display overview for LACP statistics for all ports	
Example	#show lacp statistics details	

LLDP (LINK LAYER DISCOVERY PROTOCOL)

LLDP Configuration commands

The Link Layer Discovery Protocol allows stations to advertise their identity, capabilities and neighbors connected within the same network.

LLDP parameters

Description - Configure LLDP parameters.

lldp timer <val>

lldp holdtime <val>

lldp transmission-delay <val>

lldp reinit <val>

Parameter	parameter	description
	timer<val>	Sets LLDP TX interval. The time between each LLDP frame transmitted in 5-32768 seconds
	holdtime<val>	Sets LLDP hold time. The neighbor switch will discard the LLDP information after 'hold time' multiplied with 'timer' 2-10seconds.
	transmission-delay<val>	Sets LLDP transmission-delay. The amount of time that the transmission of LLDP frames will be delayed after LLDP configuration has changed in 1-8192 seconds.
	reinit<val>	LLDP TX reinitialization delay in 1-10seconds
Default	Timer 30, Holdtime 4, transmission-delay 2, reinit 2	
Mode	Global Configuration Mode	
Usage	Configure LLDP parameters. Use the no version of the command to reset to default.	
Example	# configure terminal (config)# lldp timer 125 (config)# lldp holdtime 3 (config)# lldp transmision-delay 5 (config)# lldp reinit 5	

LLDP Interface configuration

Description - Configure LLDP parameters of the interface.

lldp receive lldp transmit lldp

cdp-aware lldp trap

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

Parameter	parameter	description
	receive	Enable/Disable decoding of received LLDP frames.
	transmit	Enable/Disabled transmission of LLDP frames.
	cdp-aware	Configures if the interface shall be CDP aware (CDP discovery information is added to the LLDP neighbor table)
	trap	Configures if an SNMP trap shall be emitted when the LLDP neighbor table changes for the interface
	tlv-select	Enable/Disable transmission of optional TLVs

Default	N.A.
Mode	Port List Interface Mode
Usage	Enable LLDP parameters of the interface. Use the no version of the command to disable.
Example	# configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# lldp receive (config-if)# lldp cdp-aware (config-if)# lldp trap (config-if)# lldp tlv-select system-capabilities system-name

show lldp neighbors

Description - Display status overview of all LLDP neighbors.

show lldp neighbors [interface <port_type> [<v_port_type_list>]]

Parameter	parameter	description
	<port_type>	Gigabit Ethernet port
	<v_port_type_list>	Port list 1/1-11
Default	N.A	
Mode	EXEC Mode	
Usage	Display status overview of all LLDP neighbors	
Example	#show lldp neighbors	

show lldp statistics

Description - Display status overview of all LLDP traffic.

show lldp statistics [interface <port_type> [<v_port_type_list>]]

Parameter	parameter	description
	<port_type>	Gigabit Ethernet port
	<v_port_type_list>	Port list 1/1-11
Default	N.A	
Mode	EXEC Mode	
Usage	Display status overview of all LLDP neighbors	
Example	#show lldp statistics	

PRIVATE VLAN / PORT ISOLATION

Private VLAN

Private VLAN (has nothing to do with traditional VLAN) filters outgoing destination port traffic. Packet received on port X can be send only to destination ports which are marked as part of port X group.

pvlan

Description - Add or remove a port from a PVLAN

pvlan <range_list>

no pvlan <range_list>

	parameter	description
Parameter	<range_list>	List of PVLANs. Range is from 1 to number of ports.
Default	N.A.	
Mode	Port List Interface Mode	
Usage	Add port to PVLAN. Use the no version of the command to remove the port from PVLAN.	
Example	# configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# pvlan 1-3 (config-if)# no pvlan 2	

show pvlan

Description- View the PVLAN configuration information.

show pvlan [<range_list>]

	parameter	description
Parameter	<range_list>	List of PVLANs. Range is from 1 to number of ports.
Default	N.A	
Mode	EXEC Mode	
Usage	Display PVLAN configuration	
Example	**Example** #show pvlan	

Port Isolation

Isolated ports are prevented from sending packets to each other. However, they can communicate normally with all the other Switch ports.

pvlan isolation

Description - Add the port to isolation group.

pvlan isolation

no pvlan isolation

	parameter	description
Parameter	N.A	
Default	N.A.	
Mode	Port List Interface Mode	
Usage	Add port to isolation group. Use the no version of the command to remove the port from isolation group.	
Example	# configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# pvlan isolation	

show pvlan isolation

Description - View port isolation configuration

show pvlan isolation [interface <port_type_list>]

	parameter	description
Parameter	<port_type_list>	List of Port ID, ex, GigabitEthernet 1/1,3-5
Default	N.A	
Mode	EXEC Mode	
Usage	Display port isolation configuration	
xample	Example (show port isolation configuration for port 2) #show pvlan isolation interface GigabitEthernet 1/2 Example (show port isolation configuration for all ports) #show pvlan isolation	

LOOP PROTECTION

Loop protection configuration commands

Loop protect feature can prevent Layer2 loops by sending loop protect protocol packets and shutting down interfaces in case they receive loop protect packets originated from themselves.

loop-protect (general settings)

Description - Configure Loop protection general parameters.

loop-protect no loop-protect

loop-protect transmit-time <t>

no loop-protect transmit-time

loop-protect shutdown-time <t>

no loop-protect shutdown-time

Parameter	parameter	description
	transmit-time <t>	Interval between each loop protection PDU sent on each port. Valid values are 1-10 seconds.
	shutdown-time <t>	Period for which the port will be kept disabled if a loop is detected. Valid values 0-604800 seconds (7 days). A value of 0 will keep the port disabled until the next device restart.
Default	Transmission time 5 seconds. Shutdown time 180 seconds.	
Mode	Global Configuration Mode	
Usage	Enable/Disable Loop protection (globally) and configure Loop protection parameters. Use the no version of the command to reset to default.	
Example	Example (Enable Loop protection and set transmit time to 8 seconds, shutdown time to 500 seconds) # configure terminal (config)# loop-protect (config)# loop-protect transmit-time 8 (config)# loop-protect shutdown-time 500	

loop-protect (port settings)

Description - Configure Loop protection parameters for the switch port

loop-protect

no loop-protect

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

no loop-protect action

loop-protect tx-mode

no loop-protect tx-mode

Parameter	parameter	description
	shutdown	Shutdown the port when the Loop is detected
	log	Log only when the Loop is detected
	tx-mode	Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.
Default	N.A	
Mode	Port List Interface Mode	
Usage	Enable/Disable Loop protection on a switch port and configure Loop protection parameters.	

Example	# configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# loop-protect (config-if)# loop-protect action shutdown log (config-if)# no loop-protect tx-mode

show loop-protect

Description - View Loop protection status

show loop-protect [interface <port_type> [<plist>]]

Parameter	parameter	description
	<port_type>	Gigabit Ethernet port
	<plist>	List of Port ID, ex, GigabitEthernet 1/1,3-5
Default	N.A	
Mode	EXEC Mode	
Usage	Display Loop protection configuration and status.	
Example	Example (show Loop protection configuration for port 2) #show loop-protect interface GigabitEthernet 1/2 Example (show Loop protection configuration for all ports) #show loop-protect	

IGMP (INTERNET GROUP MANAGEMENT PROTOCOL)

IGMP Snooping Configuration commands

Snooping is the process of listening to IGMP (Internet Group Management Protocol) network traffic to control delivery of IP multicast packets. Network switches supporting IGMP snooping listen to IGMP conversation between hosts and routers and maintain a map of the ports that the IP multicast traffic should go through, while filter the IP multicast traffic from other Switch ports which do not need those IP Multicast packets, conserving bandwidth on those links.

ip igmp (global parameters)

Description - Enable/disable IGMP Snooping and configure global parameters

ip igmp snooping

no ip igmp snooping

ip igmp unknown-flooding

no ip igmp unknown-flooding

ip igmp ssm-range <v_ipv4_mcast> <ipv4_prefix_length>

no ip igmp ssm-range

ip igmp host-proxy [leave-proxy]

no ip igmp host-proxy [leave-proxy]

Parameter	parameter	description
	snooping	Enable Global IGMP Snooping. Use the no version of the command to disable.
	unknown-flooding	Enable unregistered IPMCv4 traffic flooding. Use the no version of the command to disable.
	ssm-range	Source-Specific Multicast range. Use the no version of the command to set to default (232.0.0.0/8)
	<v_ipv4_mcast>	Valid IPv4 multicast address
	<ipv4_prefix_length>	Prefix length ranges from 4 to 32
	host-proxy	Enable IGMP Proxy. Use the no version of the command to disable.
	[leave-proxy]	Enable IGMP Leave Proxy. Use the no version of the command to disable.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Enable/Disable IGMP Snooping on a switch and configure global parameters.	
Example	Example (Enable IGMP Snooping, unregistered IPMCv4 traffic flooding, proxy and leave proxy) # configure terminal (config)# ip igmp snooping (config)# ip igmp unknown-flooding (config)# ip igmp host-proxy (config)# ip igmp host-proxy leave-proxy	

ip igmp snooping (port parameters)

Description - Configure IGMP Snooping on a specific port.

ip igmp snooping mrouter

no ip igmp snooping mrouter

ip igmp snooping immediate-leave

no ip igmp snooping immediate-leave

ip igmp snooping max-groups <throttling>

no ip igmp snooping max-groups

Parameter	parameter	description
	mrouter	Multicast router port configuration. Specify which ports act as a router ports (lead toward Layer 3 multicast device or IGMP querier)
	immediate-leave	Enable/Disable Fast Leave on the port.

	max-groups	Maximum number of multicast groups to which a switch port can belong (default unlimited)
	<throttling>	Number of multicast groups 1-10.
Default	N.A	
Mode	Port List Interface Mode	
Usage	Configure IGMP Snooping parameters on a port.	
Example	# configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# ip igmp snooping mrouter (config-if)# ip igmp snooping immediate-leave (config-if)# ip igmp snooping max-groups 5	

ip igmp snooping (vlan parameters)

Description- Configure IGMP Snooping on a VLAN.

ip igmp snooping

no ip igmp snooping

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

no ip igmp snooping querier { election | address }

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

ip igmp snooping priority <cos_priority>

no ip igmp snooping priority

ip igmp snooping robustness-variable <ipmc_rv>

no ip igmp snooping robustness-variable

ip igmp snooping query-interval <ipmc_qi> \

no ip igmp snooping query-interval

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

no ip igmp snooping query-max-response-time

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

no ip igmp snooping last-member-query-interval

ip igmp snooping unsolicited-report-interval <ipmc_uri>

no ip igmp snooping unsolicited-report-interval

	parameter	description
Parameter	**snooping**	Enable IGMP Snooping on a VLAN interface. Use the no version of the command to disable.
	querier { election }	Enable to join IGMP Querier election in the VLAN. Use the no version of the command to disable.
	querier { address <v_ipv4_ucast> }	Define IPv4 unicast address as source address used in IP header for IGMP Querier election.

	compatibility { auto | v1 | v2 | v3 }	IGPM interface compatibility. Forced IGMPv1, IGMPv2, IGMPv3 or auto (compatible with IGMPv1, IGMPv2, IGMPv3)
	priority <cos_priority>	Interface CoS Priority 0-7 with default value 0.
	robustness-variable <ipmc_rv>	Allows tuning for the expected packet loss tolerance count from 1 to 255. Default value is 2.
	query-interval <ipmc_qi>	Query Interval in 1-31744 seconds. Default value is 125.
	query-max-response-time <ipmc_qri>	Query Response Interval in 0-31744 tenths of seconds. Default value is 100 in tenth of seconds.
	last-member-query-interval <ipmc_lmqi>	Last Member Query Interval in 0-31744 tenths of seconds. Default value is 10 in tenth of seconds (1 second).
	unsolicited-report-interval <ipmc_uri>	Unsolicited Report Interval in 0-31744 seconds. Default value is 1 second.
Default	N.A	

Mode	VLAN Interface Mode
Usage	Enable/Disable IGMP Snooping on a switch and configure global parameters.
Example	Example (Enable IGMP Snooping on a VLAN 2 interface with CoS priority 5 and all other default parameters) # configure terminal (config)# interface vlan 2 (config-if)# ip igmp snooping (config-if)# ip igmp snooping priority 5

show ip igmp snooping group-database

Description - View IGMP Snooping Group Information and statistics.

show ip igmp snooping [vlan <v_vlan_list>] [group-database [interface <port_type> [<v_port_type_list>]] [sfm-information]] [detail]

	parameter	description
Parameter	<v_vlan_list>	VLAN identifier (VLAN ID)
	<port_type>	Gigabit Ethernet port
	<v_port_type_list>	List of Port ID, ex, GigabitEthernet 1/1,3-5
Default	N.A	
Mode	EXEC Mode	
Usage	Display IGMP Snooping Group Information.	
Example	Example (show detailed IGMP Snooping Group Information for vlan 2) #show ip igmp snooping vlan 2 group-database detail Example (show detailed running information and statistics if IGMP Snooping) #show ip igmp snooping detail	

show ip igmp snooping mrouter

Description - Display which ports act as a router ports and the status.

show ip igmp snooping mrouter [detail]

	parameter	description
Parameter	N.A	
Default	N.A	
Mode	EXEC Mode	
Usage	Display Multicast router port status in IGMP	
Example	**Example** #show ip igmp snooping mrouter detail	

PORT MIRRORING

Port mirroring configuration

Port Mirroring allows the user to mirror (duplicate) Rx/Tx/Both traffic from one or more ports to another dedicated debug port where a network analyzer can be attached to analyze the network traffic.

monitor session

Description - Enable Port Mirroring

monitor session <session_number = 1>

no monitor session <session_number = 1>

	parameter	description
Parameter	<session_number= 1>	Mirror session number. Must set as 1
Default	N.A	
Mode	Global Configuration Mode	
Usage	Enable traffic mirroring from one or more ports to a dedicated mirroring port. Use the no version of the command to disable.	
Example	# configure terminal (config)# monitor session 1	

Port configuration

Description - Configure port mirroring parameters

monitor session <session_number> [**destination** { interface <port_type> [<di_list>] } | **source** { interface <port_type> [<si_list>] [both | rx | tx] | **cpu** [both | rx | tx] }]

	parameter	description
Parameter	<session_number = 1>	Mirror session number. Must set as 1
	destination	Mirror destination port
	<port_type>	Port type in GigaEthernet

	<di_list>	Port ID, ex, 1/1
	source	Mirror source ports
	<si_list>	List of Port ID, ex, 1/1,3-5
	both	Received and transmitted frames are mirrored on the destination port.
	rx	Only received frames are mirrored to the destination port.
	tx	Only transmitted frames are mirrored to the destination port.
	cpu	Mirror source CPU
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure which Switch ports to mirror, and to which port to mirror it to. Please disable MAC address learning for the destination port.	
Example	# configure terminal (config)# monitor session 1 destination interface GigabitEthernet 1/11 (config)# monitor session 1 source interface GigabitEthernet 1/1-5 rx (config)# monitor session 1	

NOTE: NOTE – Please disable MAC address learning to the port used to mirror the traffic of the monitored ports.
To do please select the port to be configured, and type the command: no mac address-table learning

Unit Configuration

Software update

Upload new version

Description – Upload a new software version to the Switch.

firmware upgrade <url_file>

Parameter	parameter	description
	<url_file>	Specific character string that constitutes a reference to a resource. Syntax:<protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>]/<file_name> If the following special characters: space !\"#$%&'()*+,/:;<=>?@[\\]^`{|}~ need to be contained in the input URL string, they should be percent-encoded.
Default	N.A	

Mode	EXEC
Usage	Use this command to upgrade Switch software version.
Example	# firmware upgrade tftp://192.168.0.40/new_image.mfi

Select active Image

Description – Swap the active and alternative image

firmware swap

Parameter	parameter	description
	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to activate alternative (backup) image	
Example	# firmware swap	

NOTE: Backup software version is the one used before latest software update was performed. Please note that using this command again will switch to the new software version that was just uploaded.

DIAGNOSTICS

View log file

Description – Show System Log Information. Please note that the system log file starts clean after each Switch RESET.

show logging [informational] [notice] [warning] [error]

show logging <log_id> [switch <switch_list>]

Parameter	parameter	description
	informational	Severity 6: Informational messages
	notice	Severity 5: Normal but significant condition
	warning	Severity 4: Warning conditions
	error	Severity 3: Error conditions
	<log_id>	Message logging ID
	<switch_list>	List of switch ID (in a stacked system) ex, 1,3-5,7
Default	N.A	
Mode	EXEC mode	

Usage	Display SysLog server status and configuration and detailed logging messages.
Example	Example#1 – show all switch log messages # show logging#show logging 10 switch 1 Example#2 – show all log messages with severity level of “notice” #show logging notice

Ping

Description – Test network connectivity between the unit and the remote network device.

ping ip { <domain_name> | <ip_addr> } [repeat <count>] [size <size>]

ping ipv6 { <domain_name> | <ip_addr> } [repeat <count>] [size <size>]

Parameter	parameter	description
	<domain_name>	Destination host name
	<ip_addr>	Destination IPv4 or IPv6 address
	repeat <count>	Number of PING requests sent. Packets: 1-60; Default is 5
	size <size>	Size (bytes): 2-1452; Default is 56 (excluding MAC, IP and ICMP headers)
Default	N.A	
Mode	EXEC mode	
Usage	Ping remote host	
Example	Example (ping my.computer.com 10 times with 100 bytes packets) #ping ip my.computer.com repeat 10 size 100	

View CPU Load

Description – Show CPU load. The load is measured as average over the last 100ms, 1sec and 10 seconds intervals.

show system cpu status

Parameter	parameter	description
	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to display cpu status	
Example	# show system cpu status Average load in 100 ms : 0% Average load in 1 sec : 0% Average load in 10 sec : 8%	