



# Software Manual

Version 1.0  
(April 2022)

## LMX-3228G-10G-SFP

<b>CLI Management</b>	<b>1</b>
Configuration by serial console	1
Configuration by Telnet console	1
<b>Web Management</b>	<b>2</b>
<b>Connecting to the Web Console Interface</b>	<b>3</b>
<b>Monitor</b>	<b>4</b>
Monitor > System > Information	4
Switch State Overview	4
Contact	4
Name	4
Location	4
MAC Address	4
Hardware Version	4
System Date	4
System Uptime	5
Software Version	5
Software Date	5
Buttons	5
<b>Configuration</b>	<b>6</b>
Configuration > System > Information	6
System Information Configuration	6
System Contact	6
System Name	6
System Location	6
Configuration > System > IP	7
IP Configuration	7
Mode	7
DNS Server	7
DNS Proxy	8
IP Interfaces	8
IP Routes	11
Configuration > System > NTP	12
NTP Configuration	12
Configuration > System > Time	13
Time Zone Configuration	13
Daylight Saving Time Configuration	13
Daylight Saving Time Mode	13
Start time settings	14

End time settings	14
Offset settings	14
Configuration > System > Log	15
System Log Configuration	15
Server Mode	15
Server Address	15
Syslog Level	15
Configuration > System > CLI Logger	16
CLI Logger Configuration	16
Mode	16
Log Level	16
Log Content Configuration	16
Configuration > Green Ethernet > Port Power Savings	17
What is EEE	17
Port Configuration	17
Configuration > Ports	19
Port Configuration	19
Configuration > DHCP > Server > Mode	22
DHCP Server Mode Configuration	22
Global Mode	22
Mode	22
VLAN Mode	22
Configuration > DHCP > Server > Excluded IP	23
DHCP Server Excluded IP Configuration	23
Excluded IP Address	23
Configuration > DHCP > Server > Pool	24
DHCP Server Pool Configuration	24
Pool Setting	24
Configuration > Option 82 > Global Configuration	25
Option 82 Format	25
Option 82 Policy	25
Configuration > Option 82 > VLAN Configuration	26
Configuration > Option 82 > Port Configuration	28
Configuration > Option 82 > Snooping	30
DHCP Snooping Configuration	30
Snooping Mode	30
Port Mode Configuration	31
Configuration > Option 82 > Relay	32
DHCP Relay Configuration	32

Relay Mode	32
Relay Server	32
Configuration > Security > Switch > Users	33
Add/Edit User	33
Configuration > Security > Switch > Privilege Levels	35
Privilege Level Configuration	35
Configuration > Security > Switch > Auth Method	37
Authentication Method Configuration	37
Command Authorization Method Configuration	37
Accounting Method Configuration	38
Configuration > Security > Switch > SSH	39
SSH Configuration	39
Configuration > Security > Switch > HTTPS	40
HTTPS Configuration	40
Configuration > Security > Switch > Access Management	42
Access Management Configuration	42
Configuration > Security > Switch > SNMP > System	43
SNMP System Configuration	43
Mode	43
Version	43
Read Community	43
Write Community	43
Engine ID	43
Configuration > Security > Switch > SNMP > Trap	44
Trap Configuration	44
Global Settings	44
Mode	44
Trap Destination Configurations	44
SNMP Trap Configuration	45
SNMP Trap Event	47
Configuration > Security > Switch > SNMP > Communities	49
SNMPv3 Community Configuration	49
Configuration > Security > Switch > SNMP > Users	50
SNMPv3 User Configuration	50
Configuration > Security > Switch > SNMP > Groups	52
SNMPv3 Group Configuration	52
Configuration > Security > Switch > SNMP > Views	53
SNMPv3 View Configuration	53
Configuration > Security > Switch > SNMP > Access	54

SNMPv3 Access Configuration	54
Configuration > Security > Switch > RMON > Statistics	55
RMON statistics Configuration	55
Configuration > Security > Switch > RMON > History	56
RMON History Configuration	56
Configuration > Security > Switch > RMON > Alarm	57
RMON Alarm Configuration	57
Configuration > Security > Switch > RMON > Event	59
RMON Event Configuration	59
Configuration > Security > Network > Limit Control	60
System Configuration	60
Port Configuration	60
Configuration > Security > Network > NAS	64
Network Access Server Configuration	64
System Configuration	64
Port Configuration	67
Configuration > Security > Network > ACL > Ports	74
ACL Ports Configuration	74
Configuration > Security > Network > ACL > Rate Limiters	76
ACL Rate Limiter Configuration	76
Configuration > Security > Network > ACL > Access Control List	77
Access Control List Configuration	77
ACE Configuration	77
MAC Parameters	80
VLAN Parameters	81
ARP Parameters	81
IP Parameters	84
IPv6 Parameters	87
ICMP Parameters	88
TCP/UDP Parameters	89
Ethernet Type Parameters	92
Configuration > Security > Network > IP Source Guard > Configuration	93
IP Source Guard Configuration	93
Port Mode Configuration	93
Configuration > Security > Network > IP Source Guard > Static Table	96
Static IP Source Guard Table	96
Configuration > Security > Network > ARP Inspection > Port Configuration	97
ARP Inspection Configuration	97
Port Mode Configuration	97

Configuration > Security > Network > ARP Inspection > VLAN Configuration	99
VLAN Mode Configuration	99
Configuration > Security > Network > ARP Inspection > Static Table	100
Static ARP Inspection Table	100
Configuration > Security > Network > ARP Inspection > Dynamic Table	101
Dynamic ARP Inspection Table	101
Configuration > Security > AAA > RADIUS	102
RADIUS Server Configuration	102
Global Configuration	102
Server Configuration	102
Configuration > Security > AAA > TACACS+	104
TACACS+ Server Configuration	104
Global Configuration	104
Server Configuration	104
Configuration > Aggregation > Static	104
Aggregation Mode Configuration	105
Aggregation Group Configuration	105
Configuration > Aggregation > LACP	105
LACP Port Configuration	106
Configuration > Loop Protection	107
Loop Protection Configuration	108
Configuration > Spanning Tree > Bridge Settings	110
STP Bridge Configuration	110
Configuration > Spanning Tree > MSTI Mapping	112
MSTI Configuration	112
Configuration > Spanning Tree > MSTI Priorities	113
MSTI Configuration	113
Configuration > Spanning Tree > CIST Ports	113
STP CIST Port Configuration	114
Configuration > Spanning Tree > MSTI Ports	115
MSTI Port Configuration	116
(MSTn) MSTI Port Configuration	116
Configuration > IPMC Profile > Profile Table	117
IPMC Profile Configurations	117
IPMC Profile Table Setting	117
Configuration > IPMC Profile > Address Entry	118
IPMC Profile Address Configuration	118
Configuration > MVR	118
MVR Configurations	118

VLAN Interface Setting	119
Configuration > IPMC > IGMP Snooping > Basic Configuration	121
IGMP Snooping Configuration	121
Port Related Configuration	121
Configuration > IPMC > IGMP Snooping > VLAN Configuration	123
IGMP Snooping VLAN Configuration	123
Configuration > IPMC > IGMP Snooping > Port Filtering Profile	125
IGMP Snooping Port Filtering Profile Configuration	125
Configuration > IPMC > MLD Snooping > Basic Configuration	126
MLD Snooping Configuration	126
Port Related Configuration	126
Configuration > IPMC > MLD Snooping > VLAN Configuration	128
MLD Snooping VLAN Configuration	128
Configuration > IPMC > MLD Snooping > Port Filtering Profile	130
MLD Snooping Port Filtering Profile Configuration	130
Configuration > LLDP > LLDP	130
LLDP Configuration	130
LLDP Parameters	131
LLDP Interface Configuration	132
Configuration > LLDP > LLDP-MED	133
LLDP-MED Configuration	134
Fast start repeat count	134
LLDP-MED Interface Configuration	134
Coordinates Location	136
Civic Address Location	136
Emergency Call Service	137
Policies	137
Policies Interface Configuration	140
Configuration > MAC Table	140
Aging Configuration	141
MAC Table Learning	141
Static MAC Table Configuration	141
Configuration > VLANs	142
Global VLAN Configuration	143
Port VLAN Configuration	143
Configuration > Private VLANs > Membership	147
Private VLAN Membership Configuration	148
Configuration > Private VLANs > Port Isolation	149
Port Isolation Configuration	149

Configuration > VCL > MAC-based VLAN	150
MAC-Based VLAN Membership Configuration	150
Configuration > VCL > Protocol-based VLAN > Protocol to Group	151
Protocol to Group Mapping Table	151
Configuration > VCL > Protocol-based VLAN > Group to VLAN	153
Group Name to VLAN mapping Table	153
Configuration > VCL > IP Subnet-based VLAN	153
IP Subnet-based VLAN Membership Configuration	154
Configuration > Voice VLAN > Configuration	154
Configuration > Voice VLAN > OUI	156
Voice VLAN OUI Configuration	156
Configuration > QoS > Port Classification	156
QoS Ingress Port Classification	157
QoS Ingress Port Tag Classification Port n	158
Tagged Frames Settings	158
(PCP, DEI) to (QoS class, DP level) Mapping	159
Configuration > QoS > Port Policing	159
QoS Ingress Port Policers	160
Configuration > QoS > Queue Policing	161
QoS Ingress Queue Policers	161
Configuration > QoS > Port Scheduler	162
QoS Egress Port Schedulers	162
Configuration > QoS > Port Shaping	164
QoS Egress Port Shapers	164
Configuration > QoS > Port Tag Remarking	164
QoS Egress Port Tag Remarking	165
Configuration > QoS > Port DSCP	165
QoS Port DSCP Configuration	166
Configuration > QoS > DSCP-Based QoS	167
DSCP-based QoS Ingress Classification	168
Configuration > QoS > DSCP Translation	169
DSCP Translation	169
Configuration > QoS > DSCP Classification	169
DSCP Classification	170
Configuration > QoS > QoS Control List	170
QoS Control List Configuration	171
QCE Configuration	172
Key Parameters	173
Action Parameters	174

Configuration > QoS > Storm Policing	174
Global Storm Policer Configuration	175
Configuration > QoS > WRED	176
QoS Weighted Random Early Detection Configuration	178
RED Drop Probability Function	179
Configuration > Mirroring	179
Mirroring & Remote Mirroring Configuration	180
Source VLAN(s) Configuration	180
Port Configuration	181
Configuration Guideline for All Features	182
Configuration > UPnP	184
Configuration > GVRP > Global config	184
GVRP Configuration	185
Configuration > GVRP > Port config	185
GVRP Port Configuration	186
Configuration > sFlow	186
Agent Configuration	188
Receiver Configuration	188
Port Configuration	189
Configuration > UDLD	191
<b>Diagnostics</b>	<b>193</b>
Diagnostics > Ping/Ping6	193
Diagnostics > VeriPHY	195
Port	195
Cable Status	196
<b>Maintenance</b>	<b>196</b>
Maintenance > Restart Device	196
Restart Device	197
Maintenance > Factory Defaults	197
Factory Defaults	198
Maintenance > Software > Upload	198
Software Upload	199
Maintenance > Software > Image Select	199
Software Image Selection	200
Maintenance > Configuration > Save startup-config	201
Save Running Configuration to startup-config	201
Maintenance > Configuration > Download	201
Download Configuration	202
Upload Configuration	203

Maintenance > Configuration > Activate	203
Activate Configuration	204
Maintenance > Configuration > Delete	204
Delete Configuration File	205

© Copyright 2022 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.

### **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 1.0 (April 2022)

The manual supports the following models:

- LMX-3228G-10G-SFP-AC
- LMX-3228G-10G-SFP-DC
- LMX-3228G-10G-SFP-AA
- LMX-3228G-10G-SFP-DD
- LMX-3228G-10G-SFP-AD

# CLI Management

---

## Configuration by serial console

ANTAIRA Ethernet switches support CLI management. You can use console or telnet to manage the switch by CLI.

Before configuring the RS-232 serial console, connect the RS-232 port of the switch to your PC Com port using a RJ45 to DB9-Female cable.



1. Connect your PC to the switches' Console port.
2. Launch the serial terminal program.
3. Configure the port settings of the serial terminal program to match the console port:
  - ❖ 115200 baud
  - ❖ 8 data bits
  - ❖ No parity
  - ❖ 1 stop bit
  - ❖ No flow control
4. The administrator username/ password are admin/admin by default. Enter the username and password to login to the serial console.

```
Press ENTER to get started
Username: admin
Password:
# configure terminal
```

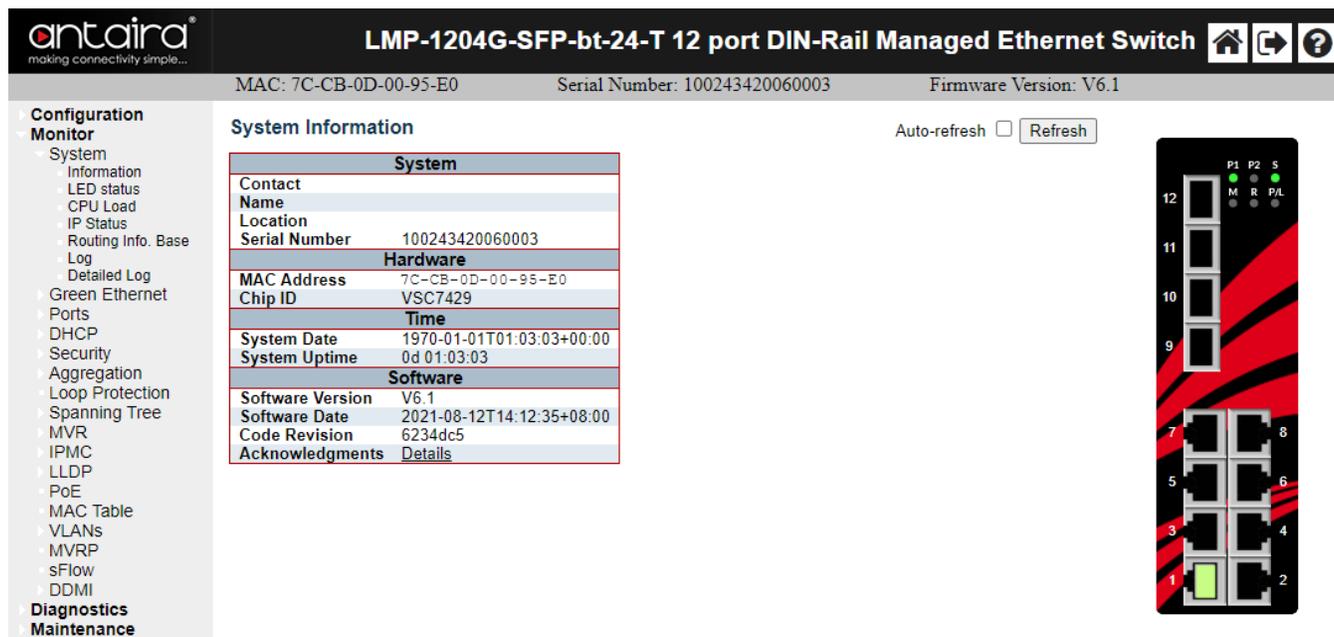
## Configuration by Telnet console

1. Connect your PC and the switches on the same logical subnetwork.
2. Launch the Telnet program.
3. Configure the switches default settings of the Telnet program:
  - **IP Address:** 192.168.1.254
  - **Subnet Mask:** 255.255.255.0
  - **Default Gateway:** none
4. The administrator username/ password are admin/admin by default. Enter the username and password to login to the Telnet console.

```
Press ENTER to get started
Username: admin
Password:
# configure terminal
```

# Web Management

Besides CLI-based management, ANTAIRA Ethernet switches also supports Web-based management. This section describes the Web console interface for a series Industrial Management Switch. This is a **user friendly** design with advanced management features that allow you to manage switches through Internet browser.



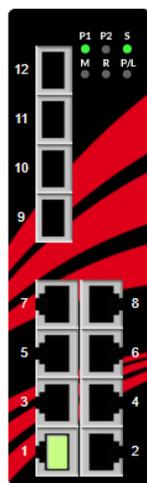
**antaira** making connectivity simple...  
**LMP-1204G-SFP-bt-24-T 12 port DIN-Rail Managed Ethernet Switch**   

MAC: 7C-CB-0D-00-95-E0      Serial Number: 100243420060003      Firmware Version: V6.1

**Configuration**  
**Monitor**  
 System  
 Information  
 LED status  
 CPU Load  
 IP Status  
 Routing Info. Base  
 Log  
 Detailed Log  
 Green Ethernet  
 Ports  
 DHCP  
 Security  
 Aggregation  
 Loop Protection  
 Spanning Tree  
 MVR  
 IPMC  
 LLDP  
 PoE  
 MAC Table  
 VLANs  
 MVRP  
 sFlow  
 DDMI  
**Diagnostics**  
**Maintenance**

**System Information**      Auto-refresh

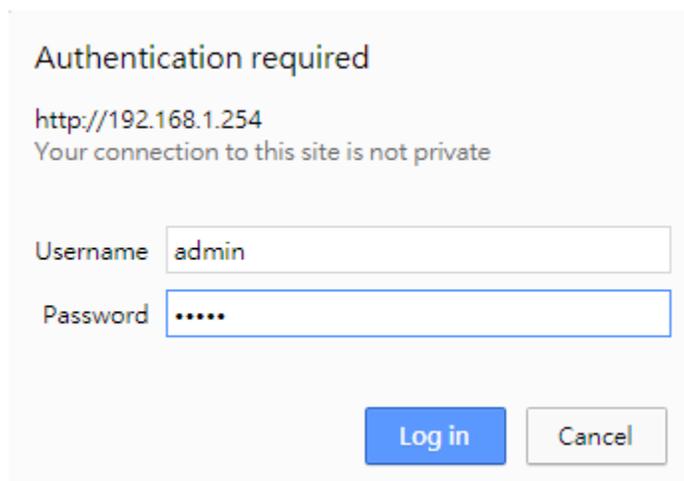
System	
Contact	
Name	
Location	
Serial Number	100243420060003
Hardware	
MAC Address	7C-CB-0D-00-95-E0
Chip ID	VSC7429
Time	
System Date	1970-01-01T01:03:03+00:00
System Uptime	0d 01:03:03
Software	
Software Version	V6.1
Software Date	2021-08-12T14:12:35+08:00
Code Revision	6234dc5
Acknowledgments	<a href="#">Details</a>



## Connecting to the Web Console Interface

---

1. Initiate a connection from a browser to the default IP address: <http://192.168.1.254> The Login page appears.
2. The administrator username/password is admin/admin by default. Enter the username and password and then click the Login button.



Authentication required

<http://192.168.1.254>  
Your connection to this site is not private

Username

Password

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

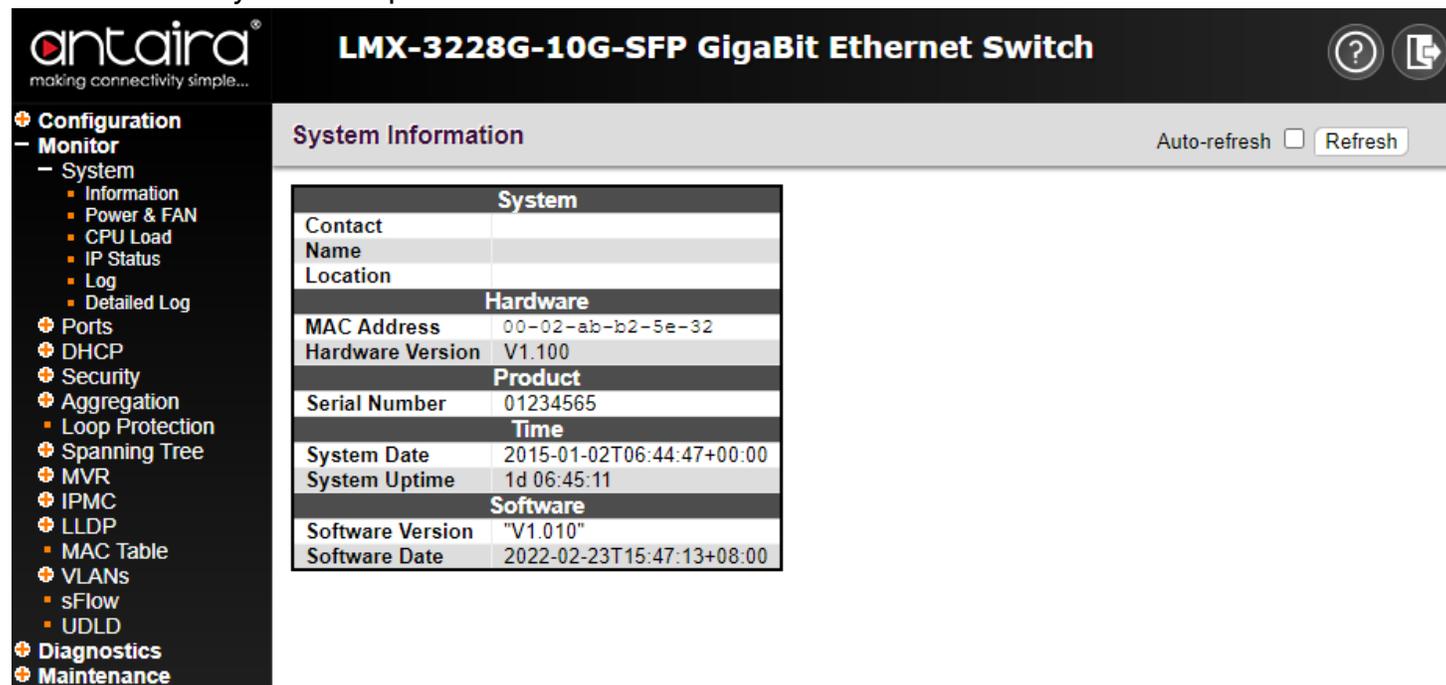
---

# Monitor

## Monitor > System > Information

### Switch State Overview

When logged into the Web GUI Interface, Switch State Overview page provides an overview of the current switch system and port states.



**antaira** making connectivity simple... **LMX-3228G-10G-SFP GigaBit Ethernet Switch**

**System Information** Auto-refresh  Refresh

System	
Contact Name	
Contact Location	
Hardware	
MAC Address	00-02-ab-b2-5e-32
Hardware Version	V1.100
Product	
Serial Number	01234565
Time	
System Date	2015-01-02T06:44:47+00:00
System Uptime	1d 06:45:11
Software	
Software Version	"V1.010"
Software Date	2022-02-23T15:47:13+08:00

### Contact

The system contact configured in Configuration | System | Information | System Contact.

### Name

The system name configured in Configuration | System | Information | System Name.

### Location

The system location configured in Configuration | System | Information | System Location.

### MAC Address

The MAC Address of this switch.

### Hardware Version

The hardware version of this switch.

### System Date

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

**System Uptime**

The period of time the device has been operational.

**Software Version**

The software version of this switch.

**Software Date**

The date when the switch software was produced.

**Buttons**

Button	Description
<b>Auto-refresh</b>	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
<b>Refresh</b>	Click to refresh the page.

# Configuration

---

## Configuration > System > Information

### System Information Configuration

The switch system information is provided here.

System Information Configuration	
System Contact	<input type="text"/>
System Name	<input type="text"/>
System Location	<input type="text"/>

#### System Contact

The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

#### System Name

An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-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.

#### System Location

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.

## Configuration > System > IP

### IP Configuration

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

The maximum number of interfaces supported is 128 and the maximum number of routes is 128.

<b>Mode</b>	Host ▾
<b>DNS Server 0</b>	No DNS server ▾
<b>DNS Server 1</b>	No DNS server ▾
<b>DNS Server 2</b>	No DNS server ▾
<b>DNS Server 3</b>	No DNS server ▾
<b>DNS Proxy</b>	<input type="checkbox"/>

#### Mode

Configure whether the IP stack should act as a Host or a Router. In Host mode, IP traffic between interfaces will not be routed. In Router mode 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.

System selects the active DNS server from configuration in turn, if the preferred server does not respond in five attempts.

Setting	Description	Factory Default
<b>From any DHCPv4 interfaces</b>	The first DNS server offered from a DHCPv4 lease to a DHCPv4-enabled interface will be used.	No DNS Server
<b>No DNS server</b>	No DNS server will be used.	
<b>Configured IPv4</b>	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.	
<b>From this DHCPv4 interface</b>	Specify from which DHCPv4-enabled interface a provided DNS server should be preferred.	
<b>Configured IPv6</b>	Explicitly provide the valid IPv6 unicast (except linklocal) address of the DNS Server. Make sure the configured DNS server could be reachable (e.g. via PING6) for activating DNS service.	
<b>From this DHCPv6 interface</b>	Specify from which DHCPv6-enabled interface a provided DNS server should be preferred.	

<b>From any DHCPv6 interfaces</b>	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 128 interfaces is supported.

Delete	VLAN	DHCPv4			IPv4		DHCPv6			IPv6	
		Enable	Fallback	Current Lease	Address	Mask Length	Enable	Rapid Commit	Current Lease	Address	Mask Length
<input type="checkbox"/>	1	<input type="checkbox"/>	0		192.168.1.205	24	<input type="checkbox"/>	<input type="checkbox"/>			

[Add Interface](#)

Setting	Description
<b>Delete</b>	Select this option to delete an existing IP interface.
<b>VLAN</b>	The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface.
<b>IPv4 DHCP Enabled</b>	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 hostname to provide DNS lookup.
<b>IPv4 DHCP Fallback Timeout</b>	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.
<b>IPv4 DHCP Current Lease</b>	For DHCP interfaces with an active lease, this column shows the current interface address, as provided by the DHCP server.
<b>IPv4 Address</b>	The IPv4 address of the interface 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.
<b>IPv4 Mask</b>	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.
<b>DHCPv6 Enable</b>	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.

<b>DHCPv6 Rapid Commit</b>	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.
<b>DHCPv6 Current Lease</b>	For DHCPv6 interface with an active lease, this column shows the interface address provided by the DHCPv6 server.
<b>IPv6 Address</b>	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. 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.
<b>IPv4 Mask</b>	The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for a IPv4 address. If DHCP is enabled, this field 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.
<b>DHCPv6 Enable</b>	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.
<b>DHCPv6 Rapid Commit</b>	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.
<b>DHCPv6 Current Lease</b>	For DHCPv6 interface with an active lease, this column shows the interface address provided by the DHCPv6 server.
<b>IPv6 Address</b>	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. 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.
<b>IPv6 Mask</b>	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.
<b>Resolving IPv6 DAD</b>	The link-local address is formed from an interface identifier based on the hardware address which is supposed to be uniquely assigned. Once the DAD (Duplicate Address Detection) detects the address duplication, the operation on the interface SHOULD be disabled. At this moment, manual intervention is required to resolve the address duplication. For example, check whether the loop occurs in the VLAN or there is

indeed another device occupying the same hardware address as the device in the VLAN.

After making sure the specific link-local address is unique on the IPv6 link in use, delete and then add the specific IPv6 interface to restart the IPv6 operations on this interface.

## IP Routes

Click the **Add Route** button to add a new IP route. A maximum of 128 routes is supported.

Delete	Network	Mask Length	Gateway	Next Hop VLAN
<input type="checkbox"/>	0.0.0.0	0	192.168.1.1	0

Add Route

Setting	Description
<b>Delete</b>	Select this option to delete an existing IP route.
<b>Network</b>	The destination IP network or host address of this route. Valid format is dotted decimal notation or a valid IPv6 notation. A default route can use the value 0.0.0.0 or IPv6 :: notation.
<b>Mask Length</b>	The destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bits respectively 128 for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything).
<b>Gateway</b>	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.
<b>Distance (Only for IPv4)</b>	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.
<b>Next Hop VLAN (Only for IPv6)</b>	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.

## Configuration > System > NTP

### NTP Configuration

<b>Mode</b>	Disabled <input type="button" value="v"/>
<b>Server 1</b>	<input type="text"/>
<b>Server 2</b>	<input type="text"/>
<b>Server 3</b>	<input type="text"/>
<b>Server 4</b>	<input type="text"/>
<b>Server 5</b>	<input type="text"/>

#### Mode

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

#### Server #

Setting	Description	Factory Default
<b>IPv4 or IPv6 address of a NTP server</b>	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

## Configuration > System > Time

### Time Zone Configuration

Time Zone Configuration	
Time Zone	None <input type="button" value="v"/>
Acronym	<input type="text"/> ( 0 - 16 characters )

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.	None
Acronym	The 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 )	None

### Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Disabled <input type="button" value="v"/>
<b>Start Time settings</b>	
Month	Jan <input type="button" value="v"/>
Date	1 <input type="button" value="v"/>
Year	2014 <input type="button" value="v"/>
Hours	0 <input type="button" value="v"/>
Minutes	0 <input type="button" value="v"/>
<b>End Time settings</b>	
Month	Jan <input type="button" value="v"/>
Date	1 <input type="button" value="v"/>
Year	2097 <input type="button" value="v"/>
Hours	0 <input type="button" value="v"/>
Minutes	0 <input type="button" value="v"/>
<b>Offset settings</b>	
Offset	1 (1 - 1440) Minutes

### 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 1440)	1

## Configuration > System > Log

### System Log Configuration

Server Mode	Disabled	▼
Server Address		
Syslog Level	Informational	▼



#### 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 which severity code is less or equal than Error(3).	Informational
Warning	Send the specific messages which severity code is less or equal than Warning(4).	
Notice	Send the specific messages which severity code is less or equal than Notice(5).	
Informational	Send the specific messages which severity code is less or equal than Informational(6).	

## Configuration > System > CLI Logger

### CLI Logger Configuration

Mode	Disabled ▾
Log Level	Informational ▾

#### Mode

Indicates whether the CLI capture operation is enabled or not.

Setting	Description	Factory Default
Enabled	CLI capture operation is enabled	Disabled
Disabled	CLI capture operation is disabled	

#### Log Level

Indicates what level will be assigned to the log.

Setting	Description	Factory Default
Info	Indicate the specific messages where severity code is Informational(6).	Informational
Warning	Indicate the specific messages where severity code is Warning(4).	
Error	Indicate the specific messages where severity code is Error(3).	

### Log Content Configuration

Indicates what information should be logged, default only logs commands.

Connected Line	<input type="checkbox"/>
User Information	<input type="checkbox"/>
View Level	<input type="checkbox"/>

Setting	Description
Connected Line	The log indicates which VTY or console the user is using.
User Information	The log indicates which user issued this command.
View Level	The log indicates the view level that the command works at.

## Configuration > Green Ethernet > Port Power Savings

### What is EEE

EEE is a power saving option that reduces the 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 wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange wakeup 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 are 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.

## Port Configuration

Port	ActiPHY	PerfectReach
*	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	<input type="checkbox"/>
11	<input type="checkbox"/>	<input type="checkbox"/>
12	<input type="checkbox"/>	<input type="checkbox"/>
13	<input type="checkbox"/>	<input type="checkbox"/>
14	<input type="checkbox"/>	<input type="checkbox"/>
15	<input type="checkbox"/>	<input type="checkbox"/>
16	<input type="checkbox"/>	<input type="checkbox"/>
17	<input type="checkbox"/>	<input type="checkbox"/>
18	<input type="checkbox"/>	<input type="checkbox"/>
19	<input type="checkbox"/>	<input type="checkbox"/>
20	<input type="checkbox"/>	<input type="checkbox"/>
21	<input type="checkbox"/>	<input type="checkbox"/>
22	<input type="checkbox"/>	<input type="checkbox"/>
23	<input type="checkbox"/>	<input type="checkbox"/>
24	<input type="checkbox"/>	<input type="checkbox"/>
25	<input type="checkbox"/>	<input type="checkbox"/>
26	<input type="checkbox"/>	<input type="checkbox"/>
27	<input type="checkbox"/>	<input type="checkbox"/>
28	<input type="checkbox"/>	<input type="checkbox"/>
29	<input type="checkbox"/>	<input type="checkbox"/>
30	<input type="checkbox"/>	<input type="checkbox"/>
31	<input type="checkbox"/>	<input type="checkbox"/>
32	<input type="checkbox"/>	<input type="checkbox"/>
33	<input type="checkbox"/>	<input type="checkbox"/>

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.

## Configuration > Ports

### Port Configuration

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

Port	Description	Link	Current	Speed Configured	Adv Duplex			Adv speed			Flow Control			PFC		Maximum Frame Size	Excessive Collision Mode	Frame Length Check
					Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx	Enable	Priority				
1		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240	<>	☐	
2		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
3		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
4		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
5		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
6		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
7		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
8		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
9		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
10		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
11		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
12		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
13		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
14		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
15		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
16		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
17		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
18		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
19		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
20		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
21		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
22		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
23		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
24		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
25		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240	Discard ▼	☐	
26		● 100fdx	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240	Discard ▼	☐	
27		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240	Discard ▼	☐	
28		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240	Discard ▼	☐	
29		● Down	10Gbps FDX	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
30		● Down	10Gbps FDX	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
31		● Down	10Gbps FDX	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
32		● Down	10Gbps FDX	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240		☐	
33		● Down	Auto	▼	☑	☑	☑	☑	☑	☐	☐	☐	☐	0-7	10240	Discard ▼	☐	

Save Reset

#### Port

This is the logical port number for this row.

#### Description

The description of the port. It is an ASCII string no longer than 34 characters .

#### Link

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

#### Current Link Speed

Provides the current link speed of the port.

#### Configured Link Speed

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

Setting	Description	Factory Default
Disabled	Disables the switch port operation.	

Auto

<b>Auto</b>	Port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner.
<b>10Mbps HDX</b>	Forces the cu port in 10Mbps half-duplex mode.
<b>10Mbps FDX</b>	Forces the cu port in 10Mbps full-duplex mode.
<b>100Mbps HDX</b>	Forces the cu port in 100Mbps half-duplex mode.
<b>100Mbps FDX</b>	Forces the cu port in 100Mbps full-duplex mode.
<b>1Gbps FDX</b>	Forces the port in 1Gbps full-duplex.
<b>SFP_Auto_AMS</b>	Automatically determines the speed of the SFP. <b>Note:</b> There is no standardized way to do SFP auto detect, so here it is done by reading the SFP rom. Due to the missing standardized way of doing SFP auto detect some SFPs might not be detectable. The port is set in AMS mode. Cu port is set in Auto mode.
<b>100-FX</b>	SFP port in 100-FX speed. Cu port disabled.
<b>1000-X</b>	SFP port in 1000-X speed. Cu port disabled.

Ports in AMS mode with 1000-X speed has Cu port preferred.

Ports in AMS mode with 1000-X speed has fiber port preferred.

Ports in AMS mode with 100-FX speed has fiber port preferred.

### 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**) 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**.

### PFC

When PFC (802.1Qbb Priority Flow Control) is enabled on a port then flow control on a priority level is enabled. Through the **Priority** field, a range (one or more) of priorities can be configured, e.g. '0-3,7'

which equals '0,1,2,3,7'. PFC is not supported through auto negotiation. PFC and Flowcontrol cannot both be enabled on the same port.

### Maximum Frame Size

Setting	Description	Factory Default
1518-9600	Enter the maximum frame size allowed for the switch port, including FCS. The range is 1518-10240 bytes.	10240

### 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 actually 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.

## Configuration > DHCP > Server > 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

Configure operation mode to enable/disable DHCP server per system.

##### Global Mode

Mode | Disabled ▾

#### Mode

Configure the operation mode per system.

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

#### VLAN Mode

Configure operation mode to enable/disable DHCP server per VLAN.

##### VLAN Mode

Delete | VLAN Range | Mode

Add VLAN Range

#### VLAN Range

Indicate the VLAN range in which DHCP server is enabled or disabled. The first VLAN ID must be smaller than or equal to the second VLAN ID. BUT, if the VLAN range contains only 1 VLAN ID, then you can just input it into either one of the first and second VLAN ID or both.

On the other hand, if you want to disable the existing VLAN range, then you can follow the steps.

1. press **Add VLAN Range** to add a new VLAN range.
2. input the VLAN range that you want to disable.
3. choose Mode to be Disabled.
4. press **Save** to apply the change.

Then, you will see the disabled VLAN range is removed from the DHCP Server mode configuration page.

#### Mode

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

## Configuration > DHCP > Server > Excluded IP

### DHCP Server Excluded IP Configuration

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

### Excluded IP Address

#### Excluded IP Address

Delete | IP Range

Add IP Range

### 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.

## Configuration > DHCP > Server > Pool

### DHCP Server Pool Configuration

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

Delete	Name	Type	IP	Subnet Mask	Lease Time
--------	------	------	----	-------------	------------

[Add New Pool](#)

[Save](#) [Reset](#)

#### Pool Setting

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 into the configuration page.

Setting	Description
<b>Name</b>	Configure the pool name that accepts all printable characters, except white space. If you want to configure the detail settings, you can click the pool name to go into the configuration page.
<b>Type</b>	Display which type of the pool is. <b>Network:</b> the pool defines a pool of IP addresses to service more than one DHCP client. <b>Host:</b> the pool services for a specific DHCP client identified by client identifier or hardware address. If - is displayed, it means not defined.
<b>IP</b>	Display network number of the DHCP address pool. If - is displayed, it means not defined.
<b>Subnet Mask</b>	Display subnet mask of the DHCP address pool. If - is displayed, it means not defined.
<b>Lease Time</b>	Display lease time of the pool.

## Configuration > Option 82 > Global Configuration

These configurations apply to a DHCP relay or snooping enabled device

Option 82 Format	Disabled	▼
Option 82 Policy	Keep	▼

Save Reset

### Option 82 Format

Indicates the DHCP option 82 information mode option operation.

Setting	Description	Factory Default
Disabled	Disable DHCP option 82 information mode operation.	Disabled
Default	The option 82 circuit ID is formatted as "[vlan_id][module_id][port_no]" in hexadecimal notation. The first four bytes represent the VLAN ID, the fifth and sixth bytes are the module ID(in standalone devices it always equals 0), and the last two bytes are the port number. For example, "00030008" means the DHCP message was received from VLAN ID 3, module ID 0, port No 8. And the option 82 remote ID value is equal to the switch MAC address.	
Configured	Indicates the user-defined format of the option 82 field.	

### Option 82 Policy

Indicates the DHCP option 82 policy. When DHCP option 82 mode operation is enabled, if the switch receives a DHCP message that already contains option 82 information it will enforce the policy. The 'Replace' policy is invalid when option 82 mode is disabled.

Setting	Description	Factory Default
Replace	Replace the original option 82 information when a DHCP message that already contains it is received.	Keep
Keep	Keep the original option 82 information when a DHCP message that already contains it is received.	
Drop	Drop the package when a DHCP message that already contains option 82 information is received.	

## Configuration > Option 82 > VLAN Configuration

This function applies to a DHCP relay agent or a DHCP snooping-enabled device. The Option 82 field records the location of a DHCP client. A device inserts the Option 82 field to a DHCP Request message to notify the DHCP server of the DHCP client location. The DHCP server can assign an IP address and other configurations to the DHCP client, ensuring DHCP client security. The user can configure the device to insert one or two of the circuit-id suboption and remote-id suboption.

You can use the following keywords to define the option 82 field. The format string can use the hexadecimal notation, ASCII format, or combination of the two formats:

- %vlan: Indicates the VLAN ID. The value ranges from 1 to 4095. This keyword is valid in ASCII format or in hexadecimal notation.
- %port: Indicates the port number. This keyword is valid in ASCII format or in hexadecimal notation.
- %portname: Indicates the name of a port. This keyword is valid only in ASCII format.
- %sysname: Indicates the name of the system. This keyword is valid only in ASCII format.
- %sysmac: Indicates the MAC address of the system. In ASCII format, the value is in the format of 'hhhhhhhhhhhh' of twelve bytes; in hexadecimal notation, the value is a number of six bytes.

**Note:** The keywords of content in quotation marks (" ") are encapsulated in a character string ASCII format, and the keywords outside the quotation marks are encapsulated in hexadecimal notation.

Start from VLAN  with  entries per page.

VLAN	Format String	
	Circuit ID	Remote ID
1	Disabled	Disabled
2	Disabled	Disabled
3	Disabled	Disabled
4	Disabled	Disabled
5	Disabled	Disabled
6	Disabled	Disabled
7	Disabled	Disabled
8	Disabled	Disabled
9	Disabled	Disabled
10	Disabled	Disabled
11	Disabled	Disabled
12	Disabled	Disabled
13	Disabled	Disabled
14	Disabled	Disabled
15	Disabled	Disabled
16	Disabled	Disabled
17	Disabled	Disabled
18	Disabled	Disabled
19	Disabled	Disabled
20	Disabled	Disabled

Setting	Description
<b>VLAN ID</b>	Indicates the ID of this particular VLAN.
<b>Circuit ID</b>	Indicates the circuit ID (CID) in the Option 82 field.
<b>Remote ID</b>	Indicates the remote ID (RID) in the Option 82 field.

## Configuration > Option 82 > Port Configuration

This function applies to a DHCP relay agent or a DHCP snooping-enabled device. The Option 82 field records the location of a DHCP client. A device inserts the Option 82 field to a DHCP Request message to notify the DHCP server of the DHCP client location. The DHCP server can assign an IP address and other configurations to the DHCP client, ensuring DHCP client security. The user can configure the device to insert one or two of the circuit-id suboption and remote-id suboption.

You can use the following keywords to define the option 82 field. The format string can use the hexadecimal notation, ASCII format, or combination of the two formats:

- %vlan: Indicates the VLAN ID. The value ranges from 1 to 4095. This keyword is valid in ASCII format or in hexadecimal notation.
- %port: Indicates the port number. This keyword is valid in ASCII format or in hexadecimal notation.
- %portname: Indicates the name of a port. This keyword is valid only in ASCII format.
- %sysname: Indicates the name of the system. This keyword is valid only in ASCII format.
- %sysmac: Indicates the MAC address of the system. In ASCII format, the value is in the format of 'hhhhhhhhhhhhhh' of twelve bytes; in hexadecimal notation, the value is a number of six bytes.

**Note:** The keywords of content in quotation marks (" ") are encapsulated in a character string ASCII format, and the keywords outside the quotation marks are encapsulated in hexadecimal notation.

Port	Format String	
	Circuit ID	Remote ID
*	Disabled	Disabled
1	Disabled	Disabled
2	Disabled	Disabled
3	Disabled	Disabled
4	Disabled	Disabled
5	Disabled	Disabled
6	Disabled	Disabled
7	Disabled	Disabled
8	Disabled	Disabled
9	Disabled	Disabled
10	Disabled	Disabled
11	Disabled	Disabled
12	Disabled	Disabled
13	Disabled	Disabled
14	Disabled	Disabled
15	Disabled	Disabled
16	Disabled	Disabled
17	Disabled	Disabled
18	Disabled	Disabled
19	Disabled	Disabled
20	Disabled	Disabled
21	Disabled	Disabled
22	Disabled	Disabled
23	Disabled	Disabled
24	Disabled	Disabled
25	Disabled	Disabled
26	Disabled	Disabled
27	Disabled	Disabled
28	Disabled	Disabled
29	Disabled	Disabled
30	Disabled	Disabled
31	Disabled	Disabled
32	Disabled	Disabled
33	Disabled	Disabled



Setting	Description
<b>Port</b>	This is the logical port number of this row.
<b>Circuit ID</b>	Indicates the circuit ID (CID) in the Option 82 field. This setting will overwrite the setting in VLAN.
<b>Remote ID</b>	Indicates the remote ID (RID) in the Option 82 field. This setting will overwrite the setting in VLAN.

## Configuration > Option 82 > Snooping

### DHCP Snooping Configuration

Snooping Mode Disabled ▾

#### Snooping Mode

Indicates the DHCP snooping mode operation.

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

Indicates the DHCP snooping port mode.

Port	Mode
*	<> ▼
1	Trusted ▼
2	Trusted ▼
3	Trusted ▼
4	Trusted ▼
5	Trusted ▼
6	Trusted ▼
7	Trusted ▼
8	Trusted ▼
9	Trusted ▼
10	Trusted ▼
11	Trusted ▼
12	Trusted ▼
13	Trusted ▼
14	Trusted ▼
15	Trusted ▼
16	Trusted ▼
17	Trusted ▼
18	Trusted ▼
19	Trusted ▼
20	Trusted ▼
21	Trusted ▼
22	Trusted ▼
23	Trusted ▼
24	Trusted ▼
25	Trusted ▼
26	Trusted ▼
27	Trusted ▼
28	Trusted ▼
29	Trusted ▼
30	Trusted ▼
31	Trusted ▼
32	Trusted ▼
33	Trusted ▼

Save Reset

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

<b>Untrusted</b>	Configures the port as an untrusted source of the DHCP messages.	
------------------	--	--

## Configuration > Option 82 > Relay

### DHCP 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.

<b>Relay Mode</b>	Disabled
<b>Relay Server</b>	0.0.0.0

#### Relay Mode

Indicates the DHCP relay mode operation.

Setting	Description	Factory Default
<b>Enabled</b>	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
<b>Disabled</b>	Disable DHCP relay mode operation.	

#### Relay Server

Indicates the DHCP relay server IP address.

## Configuration > Security > Switch > 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 Name	Privilege Level
admin	15

[Add New User](#)

Setting	Description	Factory Default
<b>User Name</b>	The name identifying the user.	None
<b>Privilege Level 0~15</b>	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 fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most 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 and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.	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 Settings	
User Name	<input type="text"/>
Password	<input type="password"/>
Password (again)	<input type="password"/>
Privilege Level	0 <input type="button" value="v"/>

### User Name

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

### Password

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

### Privilege Level

Setting	Description	Factory Default
<b>0~15</b>	The privilege level of the user. The allowed range is <b>0 to 15</b> . If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most 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 and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.	0

## Configuration > Security > Switch > Privilege Levels

### Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5 ▾	10 ▾	5 ▾	10 ▾
Debug	15 ▾	15 ▾	15 ▾	15 ▾
DHCP	5 ▾	10 ▾	5 ▾	10 ▾
DHCPv6_Client	5 ▾	10 ▾	5 ▾	10 ▾
Diagnostics	5 ▾	10 ▾	5 ▾	10 ▾
IP	5 ▾	10 ▾	5 ▾	10 ▾
IPMC_Snooping	5 ▾	10 ▾	5 ▾	10 ▾
JSON_RPC	5 ▾	10 ▾	5 ▾	10 ▾
JSON_RPC_Notification	5 ▾	10 ▾	5 ▾	10 ▾
LACP	5 ▾	10 ▾	5 ▾	10 ▾
LLDP	5 ▾	10 ▾	5 ▾	10 ▾
Loop_Protect	5 ▾	10 ▾	5 ▾	10 ▾
MAC_Table	5 ▾	10 ▾	5 ▾	10 ▾
Maintenance	15 ▾	15 ▾	15 ▾	15 ▾
MVR	5 ▾	10 ▾	5 ▾	10 ▾
NTP	5 ▾	10 ▾	5 ▾	10 ▾
Ports	5 ▾	10 ▾	1 ▾	10 ▾
Private_VLANs	5 ▾	10 ▾	5 ▾	10 ▾
QoS	5 ▾	10 ▾	5 ▾	10 ▾
RMirror	5 ▾	10 ▾	5 ▾	10 ▾
Security	5 ▾	10 ▾	5 ▾	10 ▾
sFlow	5 ▾	10 ▾	5 ▾	10 ▾
Spanning_Tree	5 ▾	10 ▾	5 ▾	10 ▾
System	5 ▾	10 ▾	1 ▾	10 ▾
UDLD	5 ▾	10 ▾	5 ▾	10 ▾
UPnP	5 ▾	10 ▾	5 ▾	10 ▾
VCL	5 ▾	10 ▾	5 ▾	10 ▾
VLANs	5 ▾	10 ▾	5 ▾	10 ▾
Voice_VLAN	5 ▾	10 ▾	5 ▾	10 ▾
XXRP	5 ▾	10 ▾	5 ▾	10 ▾

Save Reset

#### 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.

## Configuration > Security > Switch > Auth Method

### Authentication Method Configuration

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

Client	Methods		
console	local ▼	no ▼	no ▼
telnet	local ▼	no ▼	no ▼
ssh	local ▼	no ▼	no ▼
http	local ▼	no ▼	no ▼

Setting	Description
<b>Client</b>	The management client for which the configuration below applies.
<b>Methods</b>	<p>Method can be set to one of the following values:</p> <ul style="list-style-type: none"> <li>• <b>no</b>: Authentication is disabled and login is not possible.</li> <li>• <b>local</b>: Use the local user database on the switch for authentication.</li> <li>• <b>radius</b>: Use remote RADIUS server(s) for authentication.</li> <li>• <b>tacacs</b>: Use remote TACACS+ server(s) for authentication.</li> </ul> <p>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.</p>

### Command Authorization Method Configuration

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

Client	Method	Cmd Lvl	Cfg Cmd
console	no ▼	0	<input type="checkbox"/>
telnet	no ▼	0	<input type="checkbox"/>
ssh	no ▼	0	<input type="checkbox"/>

Setting	Description
<b>Client</b>	The management client for which the configuration below applies.
<b>Methods</b>	<p>Method can be set to one of the following values:</p> <ul style="list-style-type: none"> <li>• <b>no</b>: Command authorization is disabled. User is granted access to CLI commands according to his privilege level.</li> <li>• <b>tacacs</b>: 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.</li> </ul>
<b>Cmd Lvl (0~15)</b>	Authorize all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15.
<b>Cfg Cmd</b>	Also authorize configuration commands.

## Accounting Method Configuration

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

Client	Method	Cmd Lvl	Exec
console	no ▼	<input type="text"/>	<input type="checkbox"/>
telnet	no ▼	<input type="text"/>	<input type="checkbox"/>
ssh	no ▼	<input type="text"/>	<input type="checkbox"/>

Setting	Description
<b>Client</b>	The management client for which the configuration below applies.
<b>Methods</b>	Method can be set to one of the following values: <ul style="list-style-type: none"> <li>• <b>no</b>: Accounting is disabled.</li> <li>• <b>tacacs</b>: Use remote TACACS+ server(s) for accounting.</li> </ul>
<b>Cmd Lvl (0~15)</b>	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.
<b>Exec</b>	Enable exec (login) accounting.

## Configuration > Security > Switch > SSH

### SSH Configuration

Mode

Setting	Description	Factory Default
<b>Enabled</b>	Enable SSH mode operation.	Enabled
<b>Disabled</b>	Disable SSH mode operation.	

## Configuration > Security > Switch > HTTPS

### HTTPS Configuration

This page allows you to configure the HTTPS settings and maintain the current certificate on the switch.

<b>Mode</b>	Disabled
<b>Automatic Redirect</b>	Disabled
<b>Certificate Maintain</b>	None
<b>Certificate Status</b>	Switch secure HTTP certificate is presented

#### Mode

Setting	Description	Factory Default
<b>Enabled</b>	Enable HTTPS mode operation.	Disabled
<b>Disabled</b>	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
<b>Enabled</b>	Enable HTTPS redirect mode operation.	Disabled
<b>Disabled</b>	Disable HTTPS redirect mode operation.	

#### Certificate Maintain

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

### Certificate Pass Phrase

Setting	Description	Factory Default
Pass phrase	Enter the pass phrase 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 certificate, e.g. Firefox v37 and Chrome v39.

Setting	Description	Factory Default
Web Browser	Upload a certificate via Web browser.	Web Browser
URL	<p>Upload a certificate via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP. The URL format is &lt;protocol&gt;://[&lt;username&gt;[:&lt;password&gt;]@]&lt;host&gt;[:&lt;port&gt;][/&lt;path&gt;]/&lt;file_name&gt;. For example,</p> <p>tftp://10.10.10.10/new_image_path/new_image.dat,</p> <p>http:// username:password@10.10.10.10:80/new_image_path/new_image.dat.</p> <p>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.</p>	

### Certificate Status

Display the current status of certificate on the switch.

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

## Configuration > Security > Switch > Access Management

### Access Management Configuration

Configure access management table on this page. The maximum number of entries is **16**. If the application's type matches any one of the access management entries, it will allow access to the switch.

Mode

Delete |  VLAN ID |  Start IP Address |  End IP Address |  HTTP/HTTPS |  SNMP |  TELNET/SSH

#### 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.

## Configuration > Security > Switch > SNMP > System

### SNMP System Configuration

Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	800007e5017f000001

#### Mode

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

#### Read Community

Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.

The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

#### Write Community

Indicates the community write access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.

The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

#### 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. Change of the Engine ID will clear all original local users.

## Configuration > Security > Switch > SNMP > Trap

### Trap Configuration

#### Global Settings

#### Global Settings

Mode

#### Mode

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

#### Trap Destination Configurations

#### 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 allow 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 message via this port, the port range is 1~65535.

## SNMP Trap Configuration

Trap Config Name	<input type="text"/>
Trap Mode	Disabled ▾
Trap Version	SNMP v2c ▾
Trap Community	Public
Trap Destination Address	<input type="text"/>
Trap Destination Port	162
Trap Inform Mode	Disabled ▾
Trap Inform Timeout (seconds)	3
Trap Inform Retry Times	5
Trap Probe Security Engine ID	Enabled ▾
Trap Security Engine ID	<input type="text"/>
Trap Security Name	None ▾

### 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 255, and the allowed content is ASCII characters from 33 to 126.	Public

### Trap 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'.

### Trap Destination port

Setting	Description	Factory Default
1~65535	Indicates the SNMP trap destination port. SNMP Agent will send SNMP message 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 inform timeout. The allowed range is 0 to 2147.	3

### Trap Inform Retry Times

Setting	Description	Factory Default
0~255	Indicates the SNMP trap inform 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 informs using USM for authentication and privacy. A unique engine ID for these traps and informs 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 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 informs are enabled.

## SNMP Trap Event

<b>System</b>	<input type="checkbox"/> * <input type="checkbox"/> Warm Start <input type="checkbox"/> Cold Start
<b>Interface</b>	Link up <input checked="" type="radio"/> none <input type="radio"/> specific <input type="radio"/> all switches <input type="checkbox"/> * Link down <input checked="" type="radio"/> none <input type="radio"/> specific <input type="radio"/> all switches LLDP <input checked="" type="radio"/> none <input type="radio"/> specific <input type="radio"/> all switches
<b>Authentication</b>	<input type="checkbox"/> * <input type="checkbox"/> SNMP Authentication Fail
<b>Switch</b>	<input type="checkbox"/> * <input type="checkbox"/> STP <input type="checkbox"/> RMON

### System

Setting	Description	Factory Default
Warm Start	Enable/disable Warm Start trap.	Unchecked
Cold Start	Enable/disable Cold Start trap.	

### Interface

Setting	Description	Factory Default
Link Up	Enable/disable Link up trap.	None
Link Down	Enable/disable Link down trap.	
LLDP	Enable/disable LLDP trap.	

### Authentication

Setting	Description	Factory Default
SNMP Authentication Fail	Enable/disable SNMP trap authentication failure trap.	Unchecked

### Switch

Setting	Description	Factory Default
STP	Enable/disable STP trap.	Unchecked
RMON	Enable/disable RMON trap.	

## Configuration > Security > Switch > SNMP > Communities

### SNMPv3 Community Configuration

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

Delete	Community	Source IP	Source Mask
<input type="checkbox"/>	public	0.0.0.0	0.0.0.0
<input type="checkbox"/>	private	0.0.0.0	0.0.0.0




#### Add New Entry

Setting	Description
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>Community</b>	Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.
<b>Source IP</b>	Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.
<b>Source Prefix</b>	Indicates the SNMP access source address prefix.

## Configuration > Security > Switch > SNMP > Users

### SNMPv3 User Configuration

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

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
<input type="checkbox"/>	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None




#### Add New Entry

Setting	Description
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>Engine ID</b>	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user.
<b>User Name</b>	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.
<b>Security Level</b>	Indicates the security model that this entry should belong to. Possible security models are: <ul style="list-style-type: none"> <li>• <b>NoAuth, NoPriv:</b> No authentication and no privacy.</li> <li>• <b>Auth, NoPriv:</b> Authentication and no privacy.</li> <li>• <b>Auth, Priv:</b> Authentication and privacy.</li> </ul> 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.
<b>Authentication Protocol</b>	Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are: <ul style="list-style-type: none"> <li>• <b>None:</b> No authentication protocol.</li> <li>• <b>MD5:</b> An optional flag to indicate that this user uses MD5 authentication protocol.</li> <li>• <b>SHA:</b> An optional flag to indicate that this user uses SHA authentication protocol.</li> </ul> The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.
<b>Authentication Password</b>	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.
<b>Privacy Protocol</b>	Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are: <ul style="list-style-type: none"><li>• <b>None:</b> No privacy protocol.</li><li>• <b>DES:</b> An optional flag to indicate that this user uses DES authentication protocol.</li><li>• <b>AES:</b> An optional flag to indicate that this user uses AES authentication protocol.</li></ul>
<b>Privacy Password</b>	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.

## Configuration > Security > Switch > SNMP > Groups

### SNMPv3 Group Configuration

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

Delete	Security Model	Security Name	Group Name
<input type="checkbox"/>	v1	public	default_ro_group
<input type="checkbox"/>	v1	private	default_rw_group
<input type="checkbox"/>	v2c	public	default_ro_group
<input type="checkbox"/>	v2c	private	default_rw_group
<input type="checkbox"/>	usm	default_user	default_rw_group




#### Add New Entry

Setting	Description
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>Security Model</b>	Indicates the security model that this entry should belong to. Possible security models are: <ul style="list-style-type: none"> <li>• <b>v1</b>: Reserved for SNMPv1.</li> <li>• <b>v2c</b>: Reserved for SNMPv2c.</li> <li>• <b>usm</b>: User-based Security Model (USM).</li> </ul>
<b>Security Name</b>	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.
<b>Group Name</b>	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.

## Configuration > Security > Switch > SNMP > Views

### SNMPv3 View Configuration

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

Delete	View Name	View Type	OID Subtree
<input type="checkbox"/>	default_view	included ▾	.1




#### Add New Entry

Setting	Description
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>View Name</b>	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.
<b>View Type</b>	<p>Indicates the view type that this entry should belong to. Possible view types are:</p> <ul style="list-style-type: none"> <li>● <b>included:</b> An optional flag to indicate that this view subtree should be included.</li> <li>● <b>excluded:</b> An optional flag to indicate that this view subtree should be excluded.</li> </ul> <p>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.</p>
<b>OID Subtree</b>	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

## Configuration > Security > Switch > SNMP > Access

### SNMPv3 Access Configuration

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

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
<input type="checkbox"/>	default_ro_group	any	NoAuth, NoPriv	default_view ▼	None ▼
<input type="checkbox"/>	default_rw_group	any	NoAuth, NoPriv	default_view ▼	default_view ▼

#### Add New Entry

Setting	Description
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>Group Name</b>	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.
<b>Security Model</b>	Indicates the security model that this entry should belong to. Possible security models are: <ul style="list-style-type: none"> <li>• <b>any</b>: Any security model accepted(v1 v2c usm).</li> <li>• <b>v1</b>: Reserved for SNMPv1.</li> <li>• <b>v2c</b>: Reserved for SNMPv2c.</li> <li>• <b>usm</b>: User-based Security Model (USM).</li> </ul>
<b>Security Level</b>	Indicates the security model that this entry should belong to. Possible security models are: <ul style="list-style-type: none"> <li>• <b>NoAuth, NoPriv</b>: No authentication and no privacy.</li> <li>• <b>Auth, NoPriv</b>: Authentication and no privacy.</li> <li>• <b>Auth, Priv</b>: Authentication and privacy.</li> </ul>
<b>Read View Name</b>	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.
<b>Write View Name</b>	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.

## Configuration > Security > Switch > RMON > Statistics

### RMON statistics Configuration

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

**Delete | ID | Data Source**

Add New Entry

Save

Reset

#### Add New Entry

Setting	Description
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>ID</b>	Indicates the index of the entry. The range is from 1 to 65535.
<b>Data Source</b>	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.

## Configuration > Security > Switch > RMON > History

### RMON History Configuration

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

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
--------	----	-------------	----------	---------	-----------------

#### Add New Entry

Setting	Description
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>ID</b>	Indicates the index of the entry. The range is from 1 to 65535.
<b>Data Source</b>	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.
<b>Interval</b>	Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.
<b>Buckets</b>	Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600, default value is 50.
<b>Buckets Granted</b>	The number of data shall be saved in the RMON.

## Configuration > Security > Switch > RMON > Alarm

### RMON Alarm Configuration

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

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
--------	----	----------	----------	-------------	-------	---------------	------------------	--------------	-------------------	---------------




#### Add New Entry

Setting	Description
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>ID</b>	Indicates the index of the entry. The range is from 1 to 65535.
<b>Interval</b>	Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2 <sup>31</sup> -1.
<b>Variable</b>	<p>Indicates the particular variable to be sampled, the possible variables are:</p> <ul style="list-style-type: none"> <li>● <b>InOctets</b>: The total number of octets received on the interface, including framing characters.</li> <li>● <b>InUcastPkts</b>: The number of uni-cast packets delivered to a higher-layer protocol.</li> <li>● <b>InNUcastPkts</b>: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.</li> <li>● <b>InDiscards</b>: The number of inbound packets that are discarded even if the packets are normal.</li> <li>● <b>InErrors</b>: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.</li> <li>● <b>InUnknownProtos</b>: the number of the inbound packets that were discarded because of the unknown or un-support protocol.</li> <li>● <b>OutOctets</b>: The number of octets transmitted out of the interface, including framing characters.</li> <li>● <b>OutUcastPkts</b>: The number of uni-cast packets that request to transmit.</li> <li>● <b>OutNUcastPkts</b>: The number of broad-cast and multi-cast packets that request to transmit.</li> <li>● <b>OutDiscards</b>: The number of outbound packets that are discarded even if the packets are normal.</li> <li>● <b>OutErrors</b>: The number of outbound packets that could not be transmitted because of errors.</li> <li>● <b>OutQLen</b>: The length of the output packet queue (in packets).</li> </ul>
<b>Sample Type</b>	<p>The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:</p> <ul style="list-style-type: none"> <li>● <b>Absolute</b>: Get the sample directly.</li> <li>● <b>Delta</b>: Calculate the difference between samples (default).</li> </ul>
<b>Value</b>	The value of the statistic during the last sampling period.
<b>Startup Alarm</b>	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:

	<ul style="list-style-type: none"><li>● <b>Rising:</b> Trigger alarm when the first value is larger than the rising threshold.</li><li>● <b>Falling:</b> Trigger alarm when the first value is less than the falling threshold.</li><li>● <b>RisingOrFalling:</b> Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).</li></ul>
<b>Rising Threshold</b>	Rising threshold value (-2147483648-2147483647).
<b>Rising Index</b>	Rising event index (1-65535).
<b>Falling Threshold</b>	Falling threshold value (-2147483648-2147483647).
<b>Falling Index</b>	Falling event index (1-65535).

## Configuration > Security > Switch > RMON > Event

### RMON Event Configuration

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

Delete	ID	Desc	Type	Community	Event Last Time
--------	----	------	------	-----------	-----------------




#### Add New Entry

Setting	Description
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>ID</b>	Indicates the index of the entry. The range is from 1 to 65535.
<b>Desc</b>	Indicates this event, the string length is from 0 to 127, default is a null string.
<b>Type</b>	Indicates the notification of the event, the possible types are: <b>none</b> : No SNMP log is created, no SNMP trap is sent. <b>log</b> : Create SNMP log entry when the event is triggered. <b>snmptrap</b> : Send SNMP trap when the event is triggered. <b>logandtrap</b> : Create SNMP log entry and send SNMP trap when the event is triggered.
<b>Community</b>	Specify the community when trap is sent, the string length is from 0 to 127, default is "public".
<b>Event Last Time</b>	Indicates the value of sysUpTime at the time this event entry last generated an event.

## Configuration > Security > Network > Limit Control

Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of the four different actions as described below.

The Limit Control module utilizes a lower-layer module, Port Security module, which manages MAC addresses learnt on the port.

The Limit Control configuration consists of two sections, a system- and a port-wide.

### System Configuration

<b>Mode</b>	Disabled ▾
<b>Aging Enabled</b>	<input type="checkbox"/>
<b>Aging Period</b>	3600 seconds

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

## Port Configuration

The table has one row for each port on the switch and a number of columns.

Port	Mode	Limit	Action	State	Re-open
*	<>	4	<>		
1	Disabled	4	None	Disabled	Reopen
2	Disabled	4	None	Disabled	Reopen
3	Disabled	4	None	Disabled	Reopen
4	Disabled	4	None	Disabled	Reopen
5	Disabled	4	None	Disabled	Reopen
6	Disabled	4	None	Disabled	Reopen
7	Disabled	4	None	Disabled	Reopen
8	Disabled	4	None	Disabled	Reopen
9	Disabled	4	None	Disabled	Reopen
10	Disabled	4	None	Disabled	Reopen
11	Disabled	4	None	Disabled	Reopen
12	Disabled	4	None	Disabled	Reopen
13	Disabled	4	None	Disabled	Reopen
14	Disabled	4	None	Disabled	Reopen
15	Disabled	4	None	Disabled	Reopen
16	Disabled	4	None	Disabled	Reopen
17	Disabled	4	None	Disabled	Reopen
18	Disabled	4	None	Disabled	Reopen
19	Disabled	4	None	Disabled	Reopen
20	Disabled	4	None	Disabled	Reopen
21	Disabled	4	None	Disabled	Reopen
22	Disabled	4	None	Disabled	Reopen
23	Disabled	4	None	Disabled	Reopen
24	Disabled	4	None	Disabled	Reopen
25	Disabled	4	None	Disabled	Reopen
26	Disabled	4	None	Disabled	Reopen
27	Disabled	4	None	Disabled	Reopen
28	Disabled	4	None	Disabled	Reopen
29	Disabled	4	None	Disabled	Reopen
30	Disabled	4	None	Disabled	Reopen
31	Disabled	4	None	Disabled	Reopen
32	Disabled	4	None	Disabled	Reopen
33	Disabled	4	None	Disabled	Reopen

Setting	Description
<b>Port</b>	The port number to which the configuration below applies.
<b>Mode</b>	Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.
<b>Limit</b>	<p>The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.</p> <p>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.</p> <p><b>Default: 4</b></p>
<b>Action</b>	<p>If Limit is reached, the switch can take one of the following actions:</p> <ul style="list-style-type: none"> <li>• <b>None:</b> Do not allow more than Limit MAC addresses on the port, but take no further action.</li> <li>• <b>Trap:</b> If Limit + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded.</li> <li>• <b>Shutdown:</b> If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port: <ul style="list-style-type: none"> <li>1) Boot the switch,</li> <li>2) Disable and re-enable Limit Control on the port or the switch,</li> <li>3) Click the Reopen button.</li> </ul> </li> <li>• <b>Trap &amp; Shutdown:</b> If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.</li> </ul>
<b>State</b>	<p>This column shows the current Port Security state of the port. The state takes one of four values:</p> <p><b>Disabled:</b> Port Security is disabled on the port.</p> <p><b>Ready:</b> The limit is not yet reached. This can be shown for all violation modes.</p> <p><b>Limit Reached:</b> Indicates that the limit is reached on this port. This can be shown for all violation modes.</p> <p><b>Shutdown:</b> Indicates that the port is shut down by Port Security. This state can only be shown if violation mode is set to <b>Shutdown</b>.</p>

**Re-open Button**

If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to Shutdown in the Action section.

Note that clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost.

## Configuration > Security > Network > NAS

### Network Access Server Configuration

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

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

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

#### System Configuration

<b>Mode</b>	Disabled ▾	
<b>Reauthentication Enabled</b>	<input type="checkbox"/>	
<b>Reauthentication Period</b>	3600	seconds
<b>EAPOL Timeout</b>	30	seconds
<b>Aging Period</b>	300	seconds
<b>Hold Time</b>	10	seconds
<b>RADIUS-Assigned QoS Enabled</b>	<input type="checkbox"/>	
<b>RADIUS-Assigned VLAN Enabled</b>	<input type="checkbox"/>	
<b>Guest VLAN Enabled</b>	<input type="checkbox"/>	
<b>Guest VLAN ID</b>	1	
<b>Max. Reauth. Count</b>	2	
<b>Allow Guest VLAN if EAPOL Seen</b>	<input type="checkbox"/>	

Setting	Description
<b>Mode</b>	Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.

<b>Reauthentication Enabled</b>	<p>If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.</p> <p>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).</p>
<b>Reauthentication Period</b>	<p>Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.</p>
<b>EAPOL Timeout</b>	<p>Determines the time for retransmission of Request Identity EAPOL frames.</p> <p>Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports.</p>
<b>Aging Period</b>	<p>This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:</p> <ul style="list-style-type: none"> <li>● <b>Single 802.1X</b></li> <li>● <b>Multi 802.1X</b></li> <li>● <b>MAC-Based Auth.</b></li> </ul> <p>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.</p> <p>If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries.</p> <p>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.</p>

<b>Hold Time</b>	<p>This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:</p> <ul style="list-style-type: none"> <li>● <b>Single 802.1X</b></li> <li>● <b>Multi 802.1X</b></li> <li>● <b>MAC-Based Auth.</b></li> </ul> <p>If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the <b>Configuration &gt; Security &gt; AAA</b> page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication.</p> <p>In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time.</p> <p>The Hold Time can be set to a number between 10 and 1000000 seconds</p>
<b>RADIUS-Assigned QoS Enabled</b>	<p>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).</p> <p>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 setting determine whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.</p>
<b>RADIUS-Assigned VLAN Enabled</b>	<p>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 <b>RADIUS-Assigned VLAN Enabled</b> below for a detailed description).</p> <p>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 setting determine whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.</p>
<b>Guest VLAN Enabled</b>	<p>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.</p> <p>The <b>Guest VLAN Enabled</b> 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.</p>

<b>Guest VLAN ID</b>	<p>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.</p> <p>Valid values are in the range [1; 4095].</p>
<b>Max. Reauth. Count</b>	<p>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.</p> <p>Valid values are in the range [1; 255].</p>
<b>Allow Guest VLAN if EAPOL Seen</b>	<p>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.</p> <p>The value can only be changed if the Guest VLAN option is globally enabled.</p>

### ***Port Configuration***

The table has one row for each port on the switch and a number of columns

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
*	<>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
1	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
6	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
7	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
8	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
9	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
10	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
11	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
12	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
13	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
14	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
15	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
16	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
17	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
18	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
19	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
20	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
21	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
22	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
23	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
24	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
25	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
26	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
27	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
28	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
29	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
30	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
31	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
32	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
33	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize

Save Reset

## Port

The port number for which the configuration below applies.

## Admin State

If NAS is globally enabled, this selection controls the port's authentication mode.

Setting	Description
<b>Force Authorized</b>	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.
<b>Force Unauthorized</b>	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.

<p><b>Port-based 802.1X</b></p>	<p>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.</p> <p>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.</p> <p><b>Note:</b> 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.</p>
<p><b>Single 802.1X</b></p>	<p>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.</p> <p>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.</p>

<p><b>Multi 802.1X</b></p>	<p>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.</p> <p>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.</p> <p>The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.</p>
<p><b>MAC-based Auth.</b></p>	<p>Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.</p> <p>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.</p> <p>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.</p>

### **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 (ordinal 6).
  - Value of **Tunnel-Type** must be set to **VLAN** (ordinal 13).
  - 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.

## Configuration > Security > Network > ACL > Ports

### ACL Ports 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

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

<b>Enabled</b>	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
<b>Disabled</b>	Port shut down is disabled.	Disabled
<b>Enabled</b>	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
<b>Disabled</b>	To close ports by changing the volatile port configuration of the ACL user module.	Enabled
<b>Enabled</b>	To reopen ports by changing the volatile port configuration of the ACL user module.	

### Counter

Counts the number of frames that match this ACE.

## Configuration > Security > Network > ACL > Rate Limiters

### ACL Rate Limiter Configuration

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

#### Rate Limiter ID

The rate limiter ID for the settings contained in the same row and its range is 1 to 16.

#### Rate

Setting	Description	Factory Default
0-5000000	The valid rate is 0, 10, 20, 30, ..., 5000000 in pps or 0, 25, 50, 75, ..., 10000000 in kbps.	1

#### Unit

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

## Configuration > Security > Network > ACL > 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 512 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.

You can modify each ACE (Access Control Entry) in the table using the following buttons:

- : Inserts a new ACE before the current row.
- : Edits the ACE row.
- : Moves the ACE up the list.
- : Moves the ACE down the list.
- : Deletes the ACE.
- : The lowest plus sign adds a new entry at the bottom of the ACE listings.

### ACE Configuration

Ingress Port	All Port 1 Port 2 Port 3 Port 4
Policy Filter	Any
Frame Type	Any

Action	Permit
Rate Limiter	Disabled
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

#### VLAN Parameters

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

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
<b>Any</b>	No policy filter is specified. (policy filter status is "don't-care".)	Any
<b>Specific</b>	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
<b>0~255</b>	When <b>Specific</b> 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
<b>0x0 ~ 0xff</b>	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
<b>Any</b>	Any frame can match this ACE.	Any
<b>Ethernet Type</b>	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).	
<b>ARP</b>	Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type.	
<b>IPv4</b>	Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type.	
<b>IPv6</b>	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 of 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).

### 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.

## MAC Parameters

### SMAC Filter

(Only displayed when the frame type is Ethernet Type or ARP.)

Setting	Description	Factory Default
Any	No SMAC filter is specified.	Any
Specific	If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.	

### SMAC Value

Setting	Description	Factory Default
MAC address	When <b>Specific</b> is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is <b>xx-xx-xx-xx-xx-xx</b> or <b>xx.xx.xx.xx.xx.xx</b> or <b>xxxxxxxxxxxx</b> (x is a hexadecimal digit). A frame that hits this ACE matches this SMAC value.	00-00-00-00-00-01

### DMAC Filter

Setting	Description	Factory Default
Any	No DMAC filter is specified. (DMAC filter status is "don't-care".)	Any
MC	Frame must be multicast.	
BC	Frame must be broadcast.	
UC	Frame must be unicast.	

<b>Specific</b>	If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.	
-----------------	---	--

### DMAC Value

Setting	Description	Factory Default
<b>MAC address</b>	When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value.	00-00-00-00-00-02

## VLAN Parameters

### 802.1Q Tagged

Setting	Description	Factory Default
<b>Any</b>	Any value is allowed. ("don't-care").	Any
<b>Enabled</b>	Tagged frame only.	
<b>Disabled</b>	Untagged frame only.	

### VLAN ID Filter

Setting	Description	Factory Default
<b>Any</b>	No VLAN ID filter is specified.	Any
<b>Specific</b>	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
<b>1~4095</b>	When <b>Specific</b> 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
<b>Any</b>	No tag priority is specified. ("don't-care").	Any
<b>0~7, 0-1, 2-3, 4-5, 6-7, 0-3, 4-7</b>	Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority.	

## ARP Parameters

The ARP parameters can be configured when Frame Type "ARP" is selected.

### ARP/RARP

Setting	Description	Factory Default
Any	No ARP/RARP OP flag is specified. (OP is "don't-care".)	Any
ARP	Frame must have ARP opcode set to ARP.	
RARP	Frame must have RARP opcode set to RARP.	
Other	Frame has unknown ARP/RARP Opcode flag.	

### Request/Reply

Setting	Description	Factory Default
Any	No Request/Reply OP flag is specified. (OP is "don't-care".)	Any
Request	Frame must have ARP Request or RARP Request OP flag set.	
Reply	Frame must have ARP Reply or RARP Reply OP flag.	

### Sender IP Filter

Setting	Description	Factory Default
Any	No sender IP filter is specified. (OP is "don't-care".)	Any
Host	Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears.	
Network	Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.	

### Sender IP Address

Setting	Description	Factory Default
IP address	When <b>Host</b> or <b>Network</b> is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.	0.0.0.0

### Sender IP Mask

Setting	Description	Factory Default
IP address	When <b>Network</b> is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.	255.255.255.0

### Target IP Filter

Setting	Description	Factory Default
<b>Any</b>	No target IP filter is specified. (OP is "don't-care".)	Any
<b>Host</b>	Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears.	
<b>Network</b>	Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.	

### Target IP Address

Setting	Description	Factory Default
<b>IP address</b>	When <b>Host</b> or <b>Network</b> is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly add a deny action.	0.0.0.0

### Target IP Mask

Setting	Description	Factory Default
<b>IP address</b>	When <b>Network</b> is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.	255.255.255.0

### ARP Sender MAC Match

Specify whether frames can hit the action according to their sender hardware address field (SHA) settings.

Setting	Description	Factory Default
<b>0</b>	ARP frames where SHA is not equal to the SMAC address.	Any
<b>1</b>	ARP frames where SHA is equal to the SMAC address.	
<b>Any</b>	Any value is allowed. ("don't-care").	

### RARP Target MAC Match

Specify whether frames can hit the action according to their target hardware address field (THA) settings.

Setting	Description	Factory Default
<b>0</b>	RARP frames where THA is not equal to the target MAC address.	Any
<b>1</b>	RARP frames where THA is equal to the target MAC address.	
<b>Any</b>	Any value is allowed. ("don't-care").	

### IP/Ethernet Length

Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.

Setting	Description	Factory Default
0	ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04).	Any
1	ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04).	
Any	Any value is allowed. ("don't-care").	

## IP

Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.

Setting	Description	Factory Default
0	ARP/RARP frames where the HLD is not equal to Ethernet (1).	Any
1	ARP/RARP frames where the HLD is equal to Ethernet (1).	
Any	Any value is allowed. ("don't-care").	

## Ethernet

Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.

Setting	Description	Factory Default
0	ARP/RARP frames where the PRO is not equal to IP (0x800).	Any
1	ARP/RARP frames where the PRO is equal to IP (0x800).	
Any	Any value is allowed. ("don't-care").	

## IP Parameters

The IP parameters can be configured when Frame Type IPv4 is selected.

### IP Protocol Filter

Setting	Description	Factory Default
Any	No IP protocol filter is specified	Any
Specific	If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears.	
ICMP	Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file.	
UDP	Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file.	

<b>TCP</b>	Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.	
------------	--	--

### IP Protocol Value

Setting	Description	Factory Default
<b>0~255</b>	When <b>Specific</b> is selected for the IP protocol value, you can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IP protocol value.	255

### IP TTL

Specify the Time-to-Live settings for this ACE.

Setting	Description	Factory Default
<b>zero</b>	IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.	Any
<b>non-zero</b>	IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.	
<b>Any</b>	Any value is allowed. ("don't-care").	

### IP Fragment

Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.

Setting	Description	Factory Default
<b>No</b>	IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.	Any
<b>Yes</b>	IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.	
<b>Any</b>	Any value is allowed. ("don't-care").	

### IP Option

Specify the options flag setting for this ACE.

Setting	Description	Factory Default
<b>No</b>	IPv4 frames where the options flag is set must not be able to match this entry.	Any
<b>Yes</b>	IPv4 frames where the options flag is set must be able to match this entry.	
<b>Any</b>	Any value is allowed. ("don't-care").	

### SIP Filter

Specify the source IP filter for this ACE.

Setting	Description	Factory Default
<b>Any</b>	No source IP filter is specified. ("don't-care").	Any
<b>Host</b>	Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears.	
<b>Network</b>	Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.	

### SIP Address

Setting	Description	Factory Default
<b>IP address</b>	When <b>Host</b> or <b>Network</b> is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly add a deny action.	0.0.0.0

### SIP Mask

Setting	Description	Factory Default
<b>IP address</b>	When <b>Network</b> is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.	255.255.255.0

### DIP Filter

Specify the destination IP filter for this ACE.

Setting	Description	Factory Default
<b>Any</b>	No source IP filter is specified. (Destination IP filter is "don't-care".)	Any
<b>Host</b>	Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears.	
<b>Network</b>	Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.	

### DIP Address

Setting	Description	Factory Default
---------	-------------	-----------------

<b>IP address</b>	When <b>Host</b> or <b>Network</b> is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly add a deny action.	0.0.0.0
-------------------	---	---------

### DIP Mask

Setting	Description	Factory Default
<b>IP address</b>	When <b>Network</b> is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.	255.255.255.0

## IPv6 Parameters

The IP parameters can be configured when Frame Type **IPv6** is selected.

### Next Header Filter

Setting	Description	Factory Default
<b>Any</b>	No IPv6 next header filter is specified. ("don't-care").	Any
<b>Specific</b>	If you want to filter a specific IPv6 next header filter with this ACE, choose this value. A field for entering an IPv6 next header filter appears.	
<b>ICMP</b>	Select ICMP to filter IPv6 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file.	
<b>UDP</b>	Select UDP to filter IPv6 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file.	
<b>TCP</b>	Select TCP to filter IPv6 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help f	

### Next Header Value

Setting	Description	Factory Default
<b>0~255</b>	When <b>Specific</b> is selected for the IPv6 next header value, you can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IPv6 protocol value.	255

### SIP Filter

Specify the source IPv6 filter for this ACE.

Setting	Description	Factory Default
<b>Any</b>	No source IPv6 filter is specified. (Source IPv6 filter is "don't-care".)	Any
<b>Specific</b>	Source IPv6 filter is set to Network. Specify the source IPv6 address and source IPv6 mask in the SIP Address fields that appear.	

### SIP Address

Setting	Description	Factory Default
IPv6 address	When <b>Specific</b> is selected for the source IPv6 filter, you can enter a specific SIPv6 address. The field only supported last 32 bits for IPv6 address.	::

### SIP BitMask

Setting	Description	Factory Default
IPv6 address	When <b>Specific</b> is selected for the source IPv6 filter, you can enter a specific SIPv6 mask. The field only supported last 32 bits for IPv6 address. 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 [sipv6_address & sipv6_bitmask] (last 32 bits). For example, if the SIPv6 address is 2001::3 and the SIPv6 bitmask is 0xFFFFFFFFE(bit 0 is "don't-care" bit), then SIPv6 address 2001::2 and 2001::3 are applied to this rule.	0xFFFFFFFF

### Hop Limit

Setting	Description	Factory Default
Zero	IPv6 frames with a hop limit field greater than zero must not be able to match this entry.	Any
Non-zero	IPv6 frames with a hop limit field greater than zero must be able to match this entry.	
Any	Any value is allowed. ("don't-care").	

## ICMP Parameters

### ICMP Type Filter

Setting	Description	Factory Default
Any	No ICMP filter is specified. (ICMP filter status is "don't-care").	Any
Specific	If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears.	

### ICMP Type Value

Setting	Description	Factory Default
0~255	When <b>Specific</b> is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP value.	255

### ICMP Code Filter

Setting	Description	Factory Default
<b>Any</b>	No ICMP code filter is specified	Any
<b>Specific</b>	If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears.	

### ICMP Code Value

Setting	Description	Factory Default
<b>0~255</b>	When <b>Specific</b> is selected for the ICMP code filter, you can enter a specific ICMP code value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP code value.	255

## TCP/UDP Parameters

### TCP/UDP Source Filter

Setting	Description	Factory Default
<b>Any</b>	No TCP/UDP source filter is specified. (TCP/UDP source filter status is "don't-care").	Any
<b>Specific</b>	If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears.	
<b>Range</b>	If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.	

### TCP/UDP Source No.

Setting	Description	Factory Default
<b>0 ~ 65535</b>	When <b>Specific</b> is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.	0

### TCP/UDP Source Range

Setting	Description	Factory Default
<b>0 ~ 65535</b>	When <b>Range</b> is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.	0-65535

### TCP/UDP Destination Filter

Setting	Description	Factory Default
---------	-------------	-----------------

<b>Any</b>	No TCP/UDP destination filter is specified	Any
<b>Specific</b>	If you want to filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears.	
<b>Range</b>	If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears.	

### TCP/UDP Destination Number

Setting	Description	Factory Default
<b>0 ~ 65535</b>	When <b>Specific</b> is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.	0

### TCP/UDP Destination Port Range

Setting	Description	Factory Default
0 ~ 65535	When <b>Range</b> is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.	0-65535

### TCP FIN

Specify the TCP "No more data from sender" (FIN) value for this ACE.

Setting	Description	Factory Default
0	TCP frames where the FIN field is set must not be able to match this entry.	Any
1	TCP frames where the FIN field is set must be able to match this entry.	
Any	Any value is allowed. ("don't-care").	

### TCP SYN

Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE.

Setting	Description	Factory Default
0	TCP frames where the SYN field is set must not be able to match this entry.	Any
1	TCP frames where the SYN field is set must be able to match this entry.	
Any	Any value is allowed. ("don't-care").	

### TCP RST

Specify the TCP "Reset the connection" (RST) value for this ACE.

Setting	Description	Factory Default
0	TCP frames where the RST field is set must not be able to match this entry.	Any
1	TCP frames where the RST field is set must be able to match this entry.	
Any	Any value is allowed. ("don't-care").	

### TCP PSH

Specify the TCP "Push Function" (PSH) value for this ACE.

Setting	Description	Factory Default
0	TCP frames where the PSH field is set must not be able to match this entry.	Any
1	TCP frames where the PSH field is set must be able to match this entry.	
Any	Any value is allowed. ("don't-care").	

### TCP ACK

Specify the TCP "Acknowledgement field significant" (ACK) value for this ACE.

Setting	Description	Factory Default
0	TCP frames where the ACK field is set must not be able to match this entry.	Any
1	TCP frames where the ACK field is set must be able to match this entry.	
Any	Any value is allowed. ("don't-care").	

### TCP URG

Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.

Setting	Description	Factory Default
0	TCP frames where the URG field is set must not be able to match this entry.	Any
1	TCP frames where the URG field is set must be able to match this entry.	
Any	Any value is allowed. ("don't-care").	

## Ethernet Type Parameters

The Ethernet Type parameters can be configured when Frame Type Ethernet Type is selected.

### EtherType Filter

Setting	Description	Factory Default
Any	No EtherType filter is specified. (EtherType filter status is "don't-care").	Any
Specific	If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering an EtherType value appears.	

### Ethernet Type Value

Setting	Description	Factory Default
0x600 ~ 0xFFFF excluding 0x800, 0x806, 0x86DD	When <b>Specific</b> is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is 0x600 to 0xFFFF but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value.	0xFFFF

## Configuration > Security > Network > IP Source Guard > Configuration

### IP Source Guard Configuration

Mode

[Translate dynamic to static](#)

#### 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

Port	Mode	Max Dynamic Clients
*	<> ▾	<> ▾
1	Disabled ▾	Unlimited ▾
2	Disabled ▾	Unlimited ▾
3	Disabled ▾	Unlimited ▾
4	Disabled ▾	Unlimited ▾
5	Disabled ▾	Unlimited ▾
6	Disabled ▾	Unlimited ▾
7	Disabled ▾	Unlimited ▾
8	Disabled ▾	Unlimited ▾
9	Disabled ▾	Unlimited ▾
10	Disabled ▾	Unlimited ▾
11	Disabled ▾	Unlimited ▾
12	Disabled ▾	Unlimited ▾
13	Disabled ▾	Unlimited ▾
14	Disabled ▾	Unlimited ▾
15	Disabled ▾	Unlimited ▾
16	Disabled ▾	Unlimited ▾
17	Disabled ▾	Unlimited ▾
18	Disabled ▾	Unlimited ▾
19	Disabled ▾	Unlimited ▾
20	Disabled ▾	Unlimited ▾
21	Disabled ▾	Unlimited ▾
22	Disabled ▾	Unlimited ▾
23	Disabled ▾	Unlimited ▾
24	Disabled ▾	Unlimited ▾
25	Disabled ▾	Unlimited ▾
26	Disabled ▾	Unlimited ▾
27	Disabled ▾	Unlimited ▾
28	Disabled ▾	Unlimited ▾
29	Disabled ▾	Unlimited ▾
30	Disabled ▾	Unlimited ▾
31	Disabled ▾	Unlimited ▾
32	Disabled ▾	Unlimited ▾
33	Disabled ▾	Unlimited ▾

Save Reset

### Mode

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

### Max Dynamic Clients

Setting	Description	Factory Default
<b>0,1,2,Unlimited</b>	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

## Configuration > Security > Network > IP Source Guard > Static Table

### Static IP Source Guard Table

The maximum number of rules is 112 on the switch.

Delete	Port	VLAN ID	IP Address	MAC address
--------	------	---------	------------	-------------

Add New Entry

Save Reset

#### 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.

## Configuration > Security > Network > ARP Inspection > Port Configuration

### ARP Inspection Configuration

Mode

#### Mode

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

#### Translate dynamic to static button

Click to translate all dynamic entries to static entries.

### Port Mode Configuration

Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port.

Port	Mode	Check VLAN	Log Type
*	<>	<>	<>
1	Disabled	Disabled	None
2	Disabled	Disabled	None
3	Disabled	Disabled	None
4	Disabled	Disabled	None
5	Disabled	Disabled	None
6	Disabled	Disabled	None
7	Disabled	Disabled	None
8	Disabled	Disabled	None
9	Disabled	Disabled	None
10	Disabled	Disabled	None
11	Disabled	Disabled	None
12	Disabled	Disabled	None
13	Disabled	Disabled	None
14	Disabled	Disabled	None
15	Disabled	Disabled	None
16	Disabled	Disabled	None
17	Disabled	Disabled	None
18	Disabled	Disabled	None
19	Disabled	Disabled	None
20	Disabled	Disabled	None
21	Disabled	Disabled	None
22	Disabled	Disabled	None
23	Disabled	Disabled	None
24	Disabled	Disabled	None
25	Disabled	Disabled	None
26	Disabled	Disabled	None
27	Disabled	Disabled	None
28	Disabled	Disabled	None
29	Disabled	Disabled	None
30	Disabled	Disabled	None
31	Disabled	Disabled	None
32	Disabled	Disabled	None
33	Disabled	Disabled	None

### 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.

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

## Configuration > Security > Network > ARP Inspection > VLAN Configuration

### VLAN Mode Configuration

Start from VLAN  with  entries per page.

**Delete | VLAN ID | Log Type**

#### Navigating the VLAN Configuration

Each page shows up to 9999 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 Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on VLAN mode configuration web page. The log type also can be configured on per VLAN setting.

Possible types are:

- **None:** Log nothing.
- **Deny:** Log denied entries.
- **Permit:** Log permitted entries.
- **ALL:** Log all entries.

#### Add New Entry Button

Click to add a new VLAN to the ARP Inspection VLAN table.

## Configuration > Security > Network > ARP Inspection > Static Table

### Static ARP Inspection Table

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

Delete	Port	VLAN ID	MAC Address	IP Address
--------	------	---------	-------------	------------

Add New Entry

Save Reset

#### 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.

## Configuration > Security > Network > ARP Inspection > 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.

Start from  , VLAN  , MAC address  and IP address  with  entries per page.

Port	VLAN ID	MAC Address	IP Address	Translate to static
No more entries				

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

Item	Description
<b>Port</b>	Switch Port Number for which the entries are displayed.
<b>VLAN ID</b>	VLAN-ID in which the ARP traffic is permitted.
<b>MAC Address</b>	User MAC address of the entry.
<b>IP Address</b>	User IP address of the entry.
<b>Translate to static</b>	Select the checkbox to translate the entry to static entry.

## Configuration > Security > AAA > RADIUS

### RADIUS Server Configuration

#### Global Configuration

#### Global Configuration

<b>Timeout</b>	5	seconds
<b>Retransmit</b>	3	times
<b>Deadtime</b>	0	minutes
<b>Key</b>		
<b>NAS-IP-Address</b>		
<b>NAS-IPv6-Address</b>		
<b>NAS-Identifier</b>		

Setting	Description	Factory Default
<b>Timeout</b>	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
<b>Retransmit</b>	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
<b>Deadtime</b>	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
<b>Key</b>	The secret key - up to 63 characters long - shared between the RADIUS server and the switch.	None
<b>NAS-IP-Address</b>	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
<b>NAS-IPv6-Address</b>	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
<b>NAS-Identifier</b>	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

The table has one row for each RADIUS server and a number of columns.

### Server Configuration

**Delete | Hostname | Auth Port | Acct Port | Timeout | Retransmit | Key**

Add New Server

Save Reset

Setting	Description
<b>Delete</b>	To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.
<b>Hostname</b>	The IP address or hostname of the RADIUS server.
<b>Auth Port</b>	The UDP port to use on the RADIUS server for authentication. Set to 0 to disable authentication.
<b>Acct Port</b>	The UDP port to use on the RADIUS server for accounting. Set to 0 to disable accounting.
<b>Timeout</b>	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
<b>Retransmit</b>	This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.
<b>Key</b>	This optional setting overrides the global key. Leaving it blank will use the global key.

### “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.

## Configuration > Security > AAA > TACACS+

### TACACS+ Server Configuration

#### Global Configuration

#### Global Configuration

Timeout	5	seconds
Deadtime	0	minutes
Key		

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.
Key	The secret key - up to 63 characters long - shared between the TACACS+ server and the switch.

#### Server Configuration

The table has one row for each TACACS+ server and a number of columns.

#### Server Configuration

Delete	Hostname	Port	Timeout	Key
<input type="button" value="Add New Server"/>				
<input type="button" value="Save"/> <input type="button" value="Reset"/>				

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.
Key	This optional setting overrides the global key. Leaving it blank will use the global key.

#### “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.

## Configuration > Aggregation > Static

### Aggregation Mode Configuration

Hash Code Contributors	
Source MAC Address	<input checked="" type="checkbox"/>
Destination MAC Address	<input type="checkbox"/>
IP Address	<input checked="" type="checkbox"/>
TCP/UDP Port Number	<input checked="" type="checkbox"/>

#### 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

### Aggregation Group Configuration

Group ID	Port Members																																		
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33		
Normal	<input checked="" type="radio"/>																																		
1	<input type="radio"/>																																		
2	<input type="radio"/>																																		
3	<input type="radio"/>																																		
4	<input type="radio"/>																																		
5	<input type="radio"/>																																		
6	<input type="radio"/>																																		
7	<input type="radio"/>																																		
8	<input type="radio"/>																																		
9	<input type="radio"/>																																		
10	<input type="radio"/>																																		
11	<input type="radio"/>																																		
12	<input type="radio"/>																																		
13	<input type="radio"/>																																		
14	<input type="radio"/>																																		
15	<input type="radio"/>																																		
16	<input type="radio"/>																																		

Save Reset

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.

## Configuration > Aggregation > LACP

### LACP Port Configuration

Port	LACP Enabled	Key	Role	Timeout	Prio
*	<input type="checkbox"/>	<> ▾	<> ▾	<> ▾	32768
1	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
2	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
3	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
4	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
5	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
6	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
7	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
8	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
9	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
10	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
11	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
12	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
13	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
14	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
15	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
16	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
17	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
18	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
19	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
20	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
21	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
22	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
23	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
24	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
25	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
26	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
27	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
28	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
29	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
30	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
31	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
32	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768
33	<input type="checkbox"/>	Auto ▾	Active ▾	Fast ▾	32768

Setting	Description
Port	The switch port number.
LACP Enabled	Show whether LACP is currently enabled on this switch port.
Key	The Key value incurred by the port, range 1-65535 . The <b>Auto</b> setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the <b>Specific</b> setting, a user-defined value can be entered. Ports

	with the same Key value can participate in the same aggregation group, while ports with different keys cannot.
<b>Role</b>	The <b>Role</b> shows the LACP activity status. <b>Active</b> will transmit LACP packets each second, while <b>Passive</b> will wait for a LACP packet from a partner (speak if spoken to).
<b>Timeout</b>	The <b>Timeout</b> controls the period between BPDU transmissions. <b>Fast</b> will transmit LACP packets each second, while <b>Slow</b> will wait for 30 seconds before sending a LACP packet.
<b>Prio</b>	The <b>Prio</b> 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.

## Configuration > Loop Protection

### Loop Protection Configuration

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

#### General Settings

Setting	Description	Factory Default
<b>Enable Loop Protection</b>	Controls whether loop protections are enabled (as a whole).	Disabled
<b>Transmission Time</b>	The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds.	5
<b>Shutdown Time</b>	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 next device restart).	180

Port	Enable	Action	Tx Mode
*	<input checked="" type="checkbox"/>	<>	<>
1	<input checked="" type="checkbox"/>	Shutdown Port	Enable
2	<input checked="" type="checkbox"/>	Shutdown Port	Enable
3	<input checked="" type="checkbox"/>	Shutdown Port	Enable
4	<input checked="" type="checkbox"/>	Shutdown Port	Enable
5	<input checked="" type="checkbox"/>	Shutdown Port	Enable
6	<input checked="" type="checkbox"/>	Shutdown Port	Enable
7	<input checked="" type="checkbox"/>	Shutdown Port	Enable
8	<input checked="" type="checkbox"/>	Shutdown Port	Enable
9	<input checked="" type="checkbox"/>	Shutdown Port	Enable
10	<input checked="" type="checkbox"/>	Shutdown Port	Enable
11	<input checked="" type="checkbox"/>	Shutdown Port	Enable
12	<input checked="" type="checkbox"/>	Shutdown Port	Enable
13	<input checked="" type="checkbox"/>	Shutdown Port	Enable
14	<input checked="" type="checkbox"/>	Shutdown Port	Enable
15	<input checked="" type="checkbox"/>	Shutdown Port	Enable
16	<input checked="" type="checkbox"/>	Shutdown Port	Enable
17	<input checked="" type="checkbox"/>	Shutdown Port	Enable
18	<input checked="" type="checkbox"/>	Shutdown Port	Enable
19	<input checked="" type="checkbox"/>	Shutdown Port	Enable
20	<input checked="" type="checkbox"/>	Shutdown Port	Enable
21	<input checked="" type="checkbox"/>	Shutdown Port	Enable
22	<input checked="" type="checkbox"/>	Shutdown Port	Enable
23	<input checked="" type="checkbox"/>	Shutdown Port	Enable
24	<input checked="" type="checkbox"/>	Shutdown Port	Enable
25	<input checked="" type="checkbox"/>	Shutdown Port	Enable
26	<input checked="" type="checkbox"/>	Shutdown Port	Enable
27	<input checked="" type="checkbox"/>	Shutdown Port	Enable
28	<input checked="" type="checkbox"/>	Shutdown Port	Enable
29	<input checked="" type="checkbox"/>	Shutdown Port	Enable
30	<input checked="" type="checkbox"/>	Shutdown Port	Enable
31	<input checked="" type="checkbox"/>	Shutdown Port	Enable
32	<input checked="" type="checkbox"/>	Shutdown Port	Enable
33	<input checked="" type="checkbox"/>	Shutdown Port	Enable

### Port Configuration

Setting	Description
<b>Port</b>	The switch port number of the port.
<b>Enable</b>	Controls whether loop protection is enabled on this switch port.
<b>Action</b>	Configures the action performed when a loop is detected on a port. Valid values are <b>Shutdown Port</b> , <b>Shutdown Port and Log</b> or <b>Log Only</b> .
<b>Tx Mode</b>	Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

## Configuration > Spanning Tree > Bridge Settings

### STP Bridge Configuration

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

Protocol Version	MSTP ▼
Bridge Priority	128 ▼
Hello Time	2
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

#### Basic Settings

Setting	Description	Factory Default
<b>Protocol Version</b>	The MSTP / RSTP / STP protocol version setting. Valid values are <b>STP</b> , <b>RSTP</b> and <b>MSTP</b> .	MSTP
<b>Bridge Priority</b>	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 <b>MSTP</b> operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.	32768
<b>Hello Time</b>	The interval between sending STP BPDU's. Valid values are in the range 1 to 10 seconds. <b>NOTE:</b> Changing this parameter from the default value is not recommended, and may have adverse effects on your network.	2
<b>Forward Delay</b>	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
<b>Max Age</b>	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 $\leq (FwdDelay-1)*2$ .	20
<b>Maximum Hop Count</b>	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
<b>Transmit Hold Count</b>	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

Edge Port BPDU Filtering	<input type="checkbox"/>
Edge Port BPDU Guard	<input type="checkbox"/>
Port Error Recovery	<input type="checkbox"/>
Port Error Recovery Timeout	

### Advanced Settings

Setting	Description
<b>Edge Port BPDU Filtering</b>	Control whether a port explicitly configured as <b>Edge</b> will transmit and receive BPDUs.
<b>Edge Port BPDU Guard</b>	Control whether a port explicitly configured as <b>Edge</b> will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.
<b>Port Error Recovery</b>	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.
<b>Port Error Recovery Timeout</b>	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).

## Configuration > Spanning Tree > MSTI Mapping

### MSTI Configuration

This page allows the user to inspect the current STP MSTI bridge instance priority configurations.

Configuration Name	00-02-ab-b2-5e-32
Configuration Revision	0

### Configuration Identification

Setting	Description
Configuration Name	The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.
Configuration Revision	The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

### 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 ( <b>xx</b> , xx being between 1 and 4094) VLAN, or a range ( <b>xx-yy</b> ), 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: <b>2,5,20-40</b> .

## Configuration > Spanning Tree > MSTI Priorities

### MSTI Configuration

This page allows the user to inspect the current STP MSTI bridge instance priority configurations.

MSTI	Priority
*	<> ▼
CIST	128 ▼
MSTI1	128 ▼
MSTI2	128 ▼
MSTI3	128 ▼
MSTI4	128 ▼
MSTI5	128 ▼
MSTI6	128 ▼
MSTI7	128 ▼

### MSTI Priority Configuration

Setting	Description
<b>MSTI</b>	The bridge instance. The CIST is the default instance, which is always active.
<b>Priority</b>	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.

## Configuration > Spanning Tree > CIST Ports

### STP CIST Port Configuration

This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well.

This page contains settings for physical and aggregated ports.

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
-	<input type="checkbox"/>	Auto ▾	128 ▾	Non-Edge ▾	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forced True ▾

### CIST Aggregated/ Normal Port Configuration

Setting	Description
<b>Port</b>	The switch port number of the logical STP port.
<b>STP Enabled</b>	Controls whether STP is enabled on this switch port.
<b>Path Cost</b>	Controls the path cost incurred by the port. The <b>Auto</b> setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the <b>Specific</b> setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.
<b>Priority</b>	Controls the port priority. This can be used to control priority of ports having identical port cost.
<b>operEdge (state flag)</b>	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.
<b>AdminEdge</b>	Controls whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized).
<b>AutoEdge</b>	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.
<b>Restricted Role</b>	If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.
<b>Restricted TCN</b>	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.
<b>BPDU Guard</b>	If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port <b>Edge</b> status does not effect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.
<b>Point-to-Point</b>	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.

## Configuration > Spanning Tree > MSTI Ports

### MSTI Port Configuration



#### Select MSTI

Select **MSTI port number** and Click “**Get**” Button to configuration.

### (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.

This page contains MSTI port settings for physical and aggregated ports.

Port	Path Cost	Priority
-	Auto	128

#### MSTI Aggregated/ Normal Ports Configuration

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

## Configuration > IPMC Profile > 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

#### Global Profile Mode

Enable/Disable the Global IPMC Profile.

### IPMC Profile Table Setting

Delete	Profile Name	Profile Description	Rule
Delete	<input type="text"/>	<input type="text"/>	 

#### “Add New IPMC Profile” button

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

Setting	Description
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>Profile Name</b>	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.
<b>Profile Description</b>	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.
<b>Rule</b>	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.

## Configuration > IPMC Profile > Address Entry

### IPMC Profile Address Configuration

This page provides address range settings used in IPMC profile.

The address entry is used to specify the address range that will be associated with IPMC Profile. It is allowed to create at maximum 128 address entries in the system.

Navigate Address Entry Setting in IPMC Profile by  entries per page.

**Delete | Entry Name | Start Address | End Address**

#### “Add New Address (Range) Entry” button

Setting	Description
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>Entry Name</b>	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.
<b>Start Address</b>	The starting IPv4/IPv6 Multicast Group Address that will be used as an address range.
<b>End Address</b>	The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.

## Configuration > 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 to connect on the source port. By giving the static membership of MVR VLAN, 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.

After the MVR VLAN members are properly configured, it is required to associate an IPMC profile with the specific MVR VLAN to be the expected channel. The channel profile is defined by the IPMC Profile which provides the filtering conditions. Notice that the profile only work when the global profile mode is enabled. It is allowed to create at maximum 4 MVR VLANs with corresponding channel profile.



### 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

Delete	MVR VID	MVR Name	IGMP Address	Mode	Tagging	Priority	LLQI	Interface Channel Profile
Delete			0.0.0.0	Dynamic	Tagged	0	5	
Port	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33							
Role	[Progress bar]							

Add New MVR VLAN

### “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. <b>Caution:</b> 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.
IGMP Address	Define the IPv4 address as source address used in IP header for IGMP control frames. The default IGMP address is not set (0.0.0.0).

	<p>When the IGMP address is not set, system uses IPv4 management address of the IP interface associated with this VLAN.</p> <p>When the IPv4 management address is not set, system uses the first available IPv4 management address.</p> <p>Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.</p>
<b>Mode</b>	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.
<b>Tagging</b>	Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is Tagged.
<b>Priority</b>	Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.
<b>LLQI</b>	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.
<b>Interface Channel Profile</b>	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. Profile selected for designated interface channel is not allowed to have overlapped permit group address.
<b>Profile Management Button</b> 	List the rules associated with the designated profile.
<b>Port</b>	The logical port for the settings.
<b>Port Role</b>	<p>Configure an MVR port of the designated MVR VLAN as one of the following roles.</p> <p><b>Inactive:</b> The designated port does not participate MVR operations.</p> <p><b>Source:</b> Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports.</p> <p><b>Receiver:</b> 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.</p> <p><b>Caution:</b> MVR source ports are not recommended to be overlapped with management VLAN ports.</p> <p>Select the port role by clicking the Role symbol to switch the setting. I indicates Inactive; S indicates Source; R indicates Receiver</p> <p>The default Role is Inactive.</p>

### Immediate Leave Setting

Enable the fast leave on the port.

## Configuration > IPMC > IGMP Snooping > Basic Configuration

### IGMP Snooping Configuration

Global Configuration	
Snooping Enabled	<input type="checkbox"/>
Unregistered IPMCv4 Flooding Enabled	<input checked="" type="checkbox"/>
IGMP SSM Range	<input type="text" value="232.0.0.0"/> / <input type="text" value="8"/>
Leave Proxy Enabled	<input type="checkbox"/>
Proxy Enabled	<input type="checkbox"/>

#### Global Configuration

Setting	Description
<b>Snooping Enabled</b>	Enable the Global IGMP Snooping.
<b>Unregistered IPMCv4 Flooding Enabled</b>	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.
<b>IGMP SSM Range</b>	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers 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.
<b>Leave Proxy Enabled</b>	Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
<b>Proxy Enabled</b>	Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

## Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	<input type="checkbox"/>	<input type="checkbox"/>	<> ▼
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
9	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
10	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
11	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
12	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
13	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
14	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
15	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
16	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
17	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
18	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
19	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
20	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
21	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
22	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
23	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
24	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
25	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
26	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
27	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
28	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
29	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
30	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
31	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
32	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
33	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼

Save Reset

Setting	Description
<b>Router Port</b>	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.
<b>Fast Leave</b>	Enable the fast leave on the port.
<b>Throttling</b>	Enable to limit the number of multicast groups to which a switch port can belong.

## Configuration > IPMC > IGMP Snooping > VLAN Configuration

### IGMP Snooping VLAN Configuration

Start from VLAN  with  entries per page.

Delete	VLAN ID	Snooping Enabled	Querier Election	Querier Address	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
Delete		<input type="checkbox"/>	<input checked="" type="checkbox"/>	0.0.0.0	IGMP-Auto	0	2	125	100	10	1

#### Navigating the IGMP Snooping VLAN Table

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
<b>Delete</b>	Check to delete the entry. The designated entry will be deleted during the next save.
<b>VLAN ID</b>	The VLAN ID of the entry.
<b>IGMP Snooping Enabled</b>	Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
<b>Querier Election</b>	Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non- Querier.
<b>Querier Address</b>	Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.
<b>Compatibility</b>	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 <b>IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3</b> , default compatibility value is IGMP-Auto.
<b>PRI</b>	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 <b>0</b> (best effort) to <b>7</b> (highest), default interface priority value is 0.
<b>RV</b>	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is <b>1</b> to <b>255</b> , default robustness variable value is 2.
<b>QI</b>	Query Interval.

	<p>The Query Interval is the interval between General Queries sent by the Querier. The allowed range is <b>1</b> to <b>31744</b> seconds, default query interval is 125 seconds.</p>
<b>QRI</b>	<p>Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is <b>0</b> to <b>31744</b> in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).</p>
<b>LLQI (LMQI for IGMP)</b>	<p>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 <b>0</b> to <b>31744</b> in tenths of seconds, default last member query interval is 10 in tenths of seconds (1 second).</p>
<b>URI</b>	<p>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 <b>0</b> to <b>31744</b> seconds, default unsolicited report interval is 1 second.</p>

## Configuration > IPMC > IGMP Snooping > Port Filtering Profile

### IGMP Snooping Port Filtering Profile Configuration

Port	Filtering Profile
1	 - ▾
2	 - ▾
3	 - ▾
4	 - ▾
5	 - ▾
6	 - ▾
7	 - ▾
8	 - ▾
9	 - ▾
10	 - ▾
11	 - ▾
12	 - ▾
13	 - ▾
14	 - ▾
15	 - ▾
16	 - ▾
17	 - ▾
18	 - ▾
19	 - ▾
20	 - ▾
21	 - ▾
22	 - ▾
23	 - ▾
24	 - ▾
25	 - ▾
26	 - ▾
27	 - ▾
28	 - ▾
29	 - ▾
30	 - ▾
31	 - ▾
32	 - ▾
33	 - ▾

Save Reset

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.

## Configuration > IPMC > MLD Snooping > Basic Configuration

### MLD Snooping Configuration

Global Configuration	
Snooping Enabled	<input type="checkbox"/>
Unregistered IPMCv6 Flooding Enabled	<input checked="" type="checkbox"/>
MLD SSM Range	ff3e:: / 96
Leave Proxy Enabled	<input type="checkbox"/>
Proxy Enabled	<input type="checkbox"/>

#### Global Configuration

Setting	Description
<b>Snooping Enabled</b>	Enable the Global MLD Snooping.
<b>Unregistered IPMCv6 Flooding Enabled</b>	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.
<b>MLD SSM Range</b>	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers 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.
<b>Leave Proxy Enabled</b>	Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
<b>Proxy Enabled</b>	Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

## Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	<input type="checkbox"/>	<input type="checkbox"/>	<> ▾
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
9	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
10	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
11	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
12	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
13	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
14	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
15	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
16	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
17	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
18	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
19	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
20	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
21	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
22	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
23	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
24	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
25	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
26	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
27	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
28	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
29	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
30	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
31	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
32	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
33	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾

Setting	Description
<b>Router Port</b>	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.
<b>Fast Leave</b>	Enable the fast leave on the port.
<b>Throttling</b>	Enable to limit the number of multicast groups to which a switch port can belong.

## Configuration > IPMC > MLD Snooping > VLAN Configuration

### MLD Snooping VLAN Configuration

Start from VLAN  with  entries per page.

Delete	VLAN ID	Snooping Enabled	Querier Election	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
Delete		<input type="checkbox"/>	<input checked="" type="checkbox"/>	MLD-Auto	0	2	125	100	10	1

#### Navigating the MLD Snooping VLAN Table

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
<b>Delete</b>	Check to delete the entry. The designated entry will be deleted during the next save.
<b>VLAN ID</b>	The VLAN ID of the entry.
<b>Snooping Enabled</b>	Enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected for MLD Snooping.
<b>Querier Election</b>	Enable to join MLD Querier election in the VLAN. Disable to act as a MLD Non- Querier.
<b>Compatibility</b>	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 <b>MLD-Auto, Forced MLDv1, Forced MLDv2</b> , default compatibility value is MLD-Auto.
<b>PRI</b>	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 <b>0</b> (best effort) to <b>7</b> (highest), default interface priority value is 0.
<b>RV</b>	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a link. The allowed range is <b>1</b> to <b>255</b> , default robustness variable value is 2.
<b>QI</b>	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is <b>1</b> to <b>31744</b> seconds, default query interval is 125 seconds.
<b>QRI</b>	Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is <b>0</b> to <b>31744</b> in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).
<b>LLQI</b>	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

	<p>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.</p> <p>The allowed range is <b>0</b> to <b>31744</b> in tenths of seconds, default last listener query interval is 10 in tenths of seconds (1 second).</p>
<b>URI</b>	<p>Unsolicited Report Interval.</p> <p>The Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address.</p> <p>The allowed range is <b>0</b> to <b>31744</b> seconds, default unsolicited report interval is 1 second.</p>

## Configuration > IPMC > MLD Snooping > Port Filtering Profile

### MLD Snooping Port Filtering Profile Configuration

Port	Filtering Profile
1	 - ▾
2	 - ▾
3	 - ▾
4	 - ▾
5	 - ▾
6	 - ▾
7	 - ▾
8	 - ▾
9	 - ▾
10	 - ▾
11	 - ▾
12	 - ▾
13	 - ▾
14	 - ▾
15	 - ▾
16	 - ▾
17	 - ▾
18	 - ▾
19	 - ▾
20	 - ▾
21	 - ▾
22	 - ▾
23	 - ▾
24	 - ▾
25	 - ▾
26	 - ▾
27	 - ▾
28	 - ▾
29	 - ▾
30	 - ▾
31	 - ▾
32	 - ▾
33	 - ▾

Save Reset

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.
	List the rules associated with the designated profile.

Profile  
Management  
Button

## Configuration > LLDP > LLDP

### LLDP Configuration

#### LLDP Parameters

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

#### 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 <b>Tx Interval</b> 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 time the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to <b>Tx Hold</b> multiplied by <b>Tx Interval</b> 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 <b>Tx Delay</b> seconds. <b>Tx Delay</b> cannot be larger than 1/4 of the <b>Tx Interval</b> value. Valid values are restricted to 1 - 8192 seconds.	2

#### Tx Reinit

Setting	Description	Factory Default
---------	-------------	-----------------

1 ~ 10	<p>When a 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. <b>Tx Reinit</b> controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.</p>	2
--------	---	---

### LLDP Interface Configuration

Interface	Mode	CDP aware	Optional TLVs				
			Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/1	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/2	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/3	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/4	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/5	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/6	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/7	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/8	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/9	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/10	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/11	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/12	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/13	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/14	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/15	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/16	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/17	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/18	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/19	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/20	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/21	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/22	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/23	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/24	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/25	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/26	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/27	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/28	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
10GigabitEthernet 1/1	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
10GigabitEthernet 1/2	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
10GigabitEthernet 1/3	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
10GigabitEthernet 1/4	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/29	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>				

Setting	Description
<b>Interface</b>	The switch interface name of the logical LLDP interface.
<b>Mode</b>	<p>Select LLDP mode.</p> <p><b>Rx only:</b> The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.</p> <p><b>Tx only:</b> The switch will drop LLDP information received from neighbors, but will send out LLDP information.</p> <p><b>Disabled:</b> The switch will not send out LLDP information, and will drop LLDP information received from neighbors.</p> <p><b>Enabled:</b> The switch will send out LLDP information, and will analyze LLDP information received from neighbors.</p>
<b>CDP Aware</b>	<p>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.</p> <p>Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table as shown below.</p> <p>CDP TLV Device ID is mapped to the LLDP Chassis ID field.</p> <p>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.</p> <p>CDP TLV Port ID is mapped to the LLDP Port ID field.</p> <p>CDP TLV Version and Platform is mapped to the LLDP System Description field.</p> <p>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.</p> <p>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.</p> <p><b>NOTE:</b> When CDP awareness on an interface is disabled the CDP information isn't removed immediately, but gets removed when the hold time is exceeded.</p>
<b>Port Descr</b>	Optional TLV: When checked the port description is included in LLDP information transmitted.
<b>Sys Name</b>	Optional TLV: When checked the system name is included in LLDP information transmitted.
<b>Sys Descr</b>	Optional TLV: When checked the system description is included in LLDP information transmitted.
<b>Sys Capa</b>	Optional TLV: When checked the system capability is included in LLDP information transmitted.
<b>Mgmt Addr</b>	Optional TLV: When checked the management address is included in LLDP information transmitted.

## Configuration > LLDP > LLDP-MED

### LLDP-MED Configuration

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

#### *Fast start repeat count*

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 LLDPDU 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 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.

Interface	Capabilities	Policies	Location
*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/12	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/13	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/14	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/15	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/17	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/19	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/20	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/21	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/22	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/23	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/24	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/25	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/26	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/27	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/28	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10GigabitEthernet 1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10GigabitEthernet 1/2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10GigabitEthernet 1/3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10GigabitEthernet 1/4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/29	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Setting	Description
<b>Interface</b>	The interface name to which the configuration applies.
<b>Capabilities</b>	When checked the switch's capabilities is included in LLDP-MED information transmitted.

<b>Policies</b>	When checked the configured policies for the interface is included in LLDP-MED information transmitted.
<b>Location</b>	When checked the configured location information for the switch is included in LLDP-MED information transmitted.
<b>PoE</b>	When checked the configured PoE (Power Over Ethernet) information for the interface is included in LLDP-MED information transmitted.

### Coordinates Location

Latitude	0	°	North	▼	Longitude	0	°	East	▼	Altitude	0	Meters	▼	Map Datum	WGS84	▼
----------	---	---	-------	---	-----------	---	---	------	---	----------	---	--------	---	-----------	-------	---

Setting	Description
<b>Latitude</b>	<b>Latitude</b> SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either <b>North</b> of the equator or <b>South</b> of the equator.
<b>Longitude</b>	<b>Longitude</b> SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either <b>East</b> of the prime meridian or <b>West</b> of the prime meridian.
<b>Altitude</b>	<p><b>Altitude</b> SHOULD be normalized to within -2097151.9 to 2097151.9 with a maximum of 1 digits.</p> <p>It is possible to select between two altitude types (floors or meters).</p> <ul style="list-style-type: none"> <li>• <b>Meters:</b> Representing meters of Altitude defined by the vertical datum specified.</li> <li>• <b>Floors:</b> 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.</li> </ul>
<b>Map Datum</b>	<p>The <b>Map Datum</b> is used for the coordinates given in these options:</p> <ul style="list-style-type: none"> <li>• <b>WGS84:</b> (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.</li> <li>• <b>NAD83/NAVD88:</b> 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).</li> <li>• <b>NAD83/MLLW:</b> 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.</li> </ul>

### 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.

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

Setting	Description
<b>Country code</b>	The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.
<b>State</b>	National subdivisions (state, canton, region, province, prefecture).
<b>County</b>	County, parish, gun (Japan), district.
<b>City</b>	City, township, shi (Japan) - Example: Copenhagen.
<b>City district</b>	City division, borough, city district, ward, chou (Japan).
<b>Block (Neighborhood)</b>	Neighborhood, block.
<b>Street</b>	Street - Example: Poppelvej.
<b>Leading street direction</b>	Leading street direction - Example: N.
<b>Trailing street suffix</b>	Trailing street suffix - Example: SW.
<b>Street suffix</b>	Street suffix - Example: Ave, Platz.
<b>House no.</b>	House number - Example: 21.
<b>House no. suffix</b>	House number suffix - Example: A, 1/2.
<b>Landmark</b>	Landmark or vanity address - Example: Columbia University.
<b>Additional location info</b>	Additional location info - Example: South Wing.
<b>Name</b>	Name (residence and office occupant) - Example: Flemming Jahn.
<b>Zip code</b>	Postal/zip code - Example: 2791.
<b>Building</b>	Building (structure) - Example: Low Library.
<b>Apartment</b>	(Apartment, suite) - Example: Apt 42.
<b>Floor</b>	Floor - Example: 4.
<b>Room no.</b>	Room number - Example: 450F.
<b>Place type</b>	Place type - Example: Office.
<b>Postal community name</b>	Postal community name - Example: Leonia.
<b>P.O. Box</b>	Post office box (P.O. BOX) - Example: 12345.
<b>Additional code</b>	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.

**Emergency Call Service**

## 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.

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
No entries present						

[Add New Policy](#)

Setting	Description
<b>Delete</b>	Check to delete the policy. It will be deleted during the next save.
<b>Policy ID</b>	ID for the policy. This is auto generated and shall be used when selecting the policies that shall be mapped to the specific interfaces.
<b>Application Type</b>	Intended use of the application types: <ol style="list-style-type: none"> <li>1. <b>Voice</b> - 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.</li> </ol>

	<ol style="list-style-type: none"> <li>2. <b>Voice Signaling (conditional)</b> - 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.</li> <li>3. <b>Guest Voice</b> - 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.</li> <li>4. <b>Guest Voice Signaling (conditional)</b> - 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.</li> <li>5. <b>Softphone Voice</b> - 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.</li> <li>6. <b>Video Conferencing</b> - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.</li> <li>7. <b>Streaming Video</b> - 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.</li> <li>8. <b>Video Signaling (conditional)</b> - 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.</li> </ol>
<b>Tag</b>	<p><b>Tag</b> indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN.</p> <p><b>Untagged</b> 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.</p> <p><b>Tagged</b> 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.</p>
<b>VLAN ID</b>	VLAN identifier (VID) for the interface as defined in IEEE 802.1Q-2003.
<b>L2 Priority</b>	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.
<b>DSCP</b>	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.
<b>Adding a new policy</b>	Click " <b>Add New Policy</b> " 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

### ***Policies Interface Configuration***

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

<b>Setting</b>	<b>Description</b>
<b>Interface</b>	The interface name to which the configuration applies.
<b>Policy Id</b>	The set of policies that shall apply to a given interface. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

## Configuration > MAC Table

### Aging Configuration

Disable Automatic Aging	<input type="checkbox"/>
Aging Time	<input type="text" value="300"/> seconds

Disable the automatic aging of dynamic entries by checking **Disable Automatic Aging**.

Setting	Description	Factory Default
10~1000000	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.	300

### MAC Table Learning

	Port Members																																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
Auto	<input checked="" type="radio"/>																																
Disable	<input type="radio"/>																																
Secure	<input type="radio"/>																																

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

### Static MAC Table Configuration

Delete	VLAN ID	MAC Address	Port Members																																
Delete	1	00-00-00-00-00-00	<input type="checkbox"/>																																

[Add New Static Entry](#)

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

The MAC table is sorted first by VLAN ID and then by MAC address.

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

<b>MAC Address</b>	The MAC Address of the entry
<b>Port Members</b>	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
<b>Adding a New Static Entry</b>	Click <b>Add a New Static Entry</b> to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".

## Configuration > 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

<b>Allowed Access VLANs</b>	1
<b>Ethertype for Custom S-ports</b>	88A8

Setting	Description
<b>Allowed Access VLANs</b>	<p>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.</p> <p>The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300:  <b>1,10-13,200,300</b>. Spaces are allowed in between the delimiters.</p>
<b>Ethertype for Custom S-ports</b>	<p>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.</p>

### Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	<input checked="" type="checkbox"/>	<>	<>	1	
1	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
7	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
8	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
9	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
11	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
12	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
13	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
14	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
15	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
16	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
17	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
18	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
19	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
20	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
21	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
22	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
23	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
24	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
25	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
26	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
27	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
28	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
29	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
30	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
31	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
32	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
33	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	

Setting	Description
<b>Port</b>	This is the logical port number of this row.
<b>Mode</b>	<p>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.</p> <p><b>Access:</b> 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:</p> <ul style="list-style-type: none"> <li>● Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1</li> <li>● Accepts untagged and C-tagged frames</li> <li>● Discards all frames not classified to the Access VLAN</li> <li>● On egress all frames are transmitted untagged</li> </ul> <p><b>Trunk:</b> Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics:</p> <ul style="list-style-type: none"> <li>● By default, a trunk port is member of all VLANs (1-4095)</li> <li>● The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs</li> <li>● Frames classified to a VLAN that the port is not a member of are discarded</li> <li>● 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</li> <li>● Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress</li> </ul> <p><b>Hybrid:</b> 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:</p> <ul style="list-style-type: none"> <li>● Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware</li> <li>● Ingress filtering can be controlled</li> <li>● Ingress acceptance of frames and configuration of egress tagging can be configured independently</li> </ul>

<b>Port VLAN</b>	<p>Determines the ports VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4095, default being 1.</p> <p>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).</p> <p>On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN.</p> <p>The Port VLAN is called an “Access VLAN” for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.</p>
<b>Port Type</b>	<p>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.</p> <p><b>Unaware:</b> 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.</p> <p><b>C-Port:</b> 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.</p> <p><b>S-Port:</b> 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.</p> <p><b>S-Custom-Port:</b> 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.</p>
<b>Ingress Filtering</b>	<p>Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled.</p> <p>If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded.</p> <p>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.</p>

<b>Ingress Acceptance</b>	<p>Hybrid ports allow for changing the type of frames that are accepted on ingress.</p> <p><b>Tagged and Untagged:</b> Both tagged and untagged frames are accepted.</p> <p><b>Tagged Only:</b> Only frames tagged with the corresponding Port Type tag are accepted on ingress.</p> <p><b>Untagged Only:</b> Only untagged frames are accepted on ingress.</p>
<b>Egress Tagging</b>	<p>Ports in Trunk and Hybrid mode may control the tagging of frames on egress.</p> <p><b>Untag Port VLAN:</b> Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.</p> <p><b>Tag All:</b> All frames, whether classified to the Port VLAN or not, are transmitted with a tag.</p> <p><b>Untag All:</b> 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.</p>
<b>Allowed VLANs</b>	<p>Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN.</p> <p>The field's syntax is identical to the syntax used in the Enabled VLANs field. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to <b>1-4095</b>.</p> <p>The field may be left empty, which means that the port will not become member of any VLANs.</p>
<b>Forbidden VLANs</b>	<p>A port may be configured to never become 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.</p> <p>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.</p> <p>By default, the field is left blank, which means that the port may become a member of all possible VLANs.</p>

## Configuration > Private VLANs > Membership

### Private VLAN Membership Configuration

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.

		Port Members																																	
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>																																	

[Add New Private VLAN](#)

Setting	Description
<b>Delete</b>	To delete a private VLAN entry, check this box. The entry will be deleted during the next save.
<b>Private VLAN ID</b>	Indicates the ID of this particular private VLAN.
<b>Port Members</b>	A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

## Configuration > Private VLANs > Port Isolation

### Port Isolation Configuration

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																																	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	
<input type="checkbox"/>																																	

### Port Number

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

## Configuration > VCL > MAC-based VLAN

### MAC-Based VLAN Membership Configuration

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.

Delete	MAC Address	VLAN ID	Port Members																															
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Currently no entries present																																		

[Add New Entry](#)

Setting	Description
<b>Delete</b>	To delete a MAC to VLAN ID mapping entry, check this box and press save. The entry will be deleted in the stack.
<b>MAC Address</b>	Indicates the MAC address of the mapping.
<b>VLAN ID</b>	Indicates the VLAN ID the above MAC will be mapped to.
<b>Port Members</b>	A row of check boxes 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.

## Configuration > VCL > Protocol-based VLAN > Protocol to Group

### Protocol to Group Mapping Table

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.

Delete	Frame Type	Value	Group Name
<input type="checkbox"/>	Ethernet ▼	Etype: 0x0800	

Setting	Description
<b>Delete</b>	To delete a Protocol to Group Name map entry, check this box. The entry will be deleted from the switch during the next Save.
<b>Frame Type</b>	<p>Frame Type can have one of the following values:</p> <ul style="list-style-type: none"> <li>• <b>Ethernet</b></li> <li>• <b>LLC</b></li> <li>• <b>SNAP</b></li> </ul> <p><b>NOTE:</b> When changing the Frame type field, the valid value of the following text field will vary depending on the new frame type you selected.</p>
<b>Value</b>	<p>Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu.</p> <p>Below are the criteria for the three different Frame Types:</p> <ul style="list-style-type: none"> <li>• <b>Ethernet:</b> Value in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype range between 0x0600 and 0xffff</li> <li>• <b>LLC:</b> Valid value in this case is comprised of two different sub-values. <ul style="list-style-type: none"> <li>a. <b>DSAP:</b> 1-byte long string (0x00-0xff)</li> <li>b. <b>SSAP:</b> 1-byte long string (0x00-0xff)</li> </ul> </li> <li>• <b>SNAP:</b> Valid value in this case is also comprised of two different sub-values. <ul style="list-style-type: none"> <li>a. <b>OUI:</b> 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.</li> <li>b. <b>PID:</b> 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 etype (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.</li> </ul> </li> </ul>

**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.

## Configuration > VCL > Protocol-based VLAN > Group to VLAN

### Group Name to VLAN mapping Table

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

Delete	Group Name	VLAN ID	Port Members																															
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Currently no entries present in the switch																																		

Setting	Description
<b>Delete</b>	To delete a Group Name to VLAN mapping, check this box. The entry will be deleted from the switch during the next Save.
<b>Group Name</b>	A valid Group Name is a string, at the 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).
<b>VLAN ID</b>	Indicates the VLAN ID to which the Group Name will be mapped. A valid VLAN ID ranges from 1 to 4095.
<b>Port Members</b>	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.

#### Delete Button

The Delete button can be used to undo the addition of a new entry. The maximum possible Group to VLAN mappings are limited to 256.



## Configuration > 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.

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

Setting	Description
<b>Mode</b>	Indicates the Voice VLAN mode operation. The MSTP feature must be disabled before enabling Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are: <b>Enabled:</b> Enable Voice VLAN mode operation. <b>Disabled:</b> Disable Voice VLAN mode operation.
<b>VLAN ID</b>	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 <b>1</b> to <b>4095</b> .
<b>Aging Time</b>	Indicates the Voice VLAN secure learning aging time. The allowed range is <b>10</b> to <b>10000000</b> 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.
<b>Traffic Class</b>	Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply to this class.
<b>Port Mode</b>	Indicates the Voice VLAN port mode. Possible port modes are: <b>Disabled:</b> Disjoin from Voice VLAN. <b>Auto:</b> Enable auto detect mode. It detects whether there is a VoIP phone attached to the specific port and configures the Voice VLAN members automatically. <b>Forced:</b> Force join to Voice VLAN.
<b>Port Security</b>	Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are: <b>Enabled:</b> Enable Voice VLAN security mode operation. <b>Disabled:</b> Disable Voice VLAN security mode operation.
<b>Port Discovery Protocol</b>	Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process. Possible discovery protocols are: <b>OUI:</b> Detect telephony device by OUI address. <b>LLDP:</b> Detect telephony device by LLDP. <b>Both:</b> Both OUI and LLDP.

## Configuration > Voice VLAN > OUI

### Voice VLAN OUI Configuration

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

Delete	Telephony OUI	Description
<input type="checkbox"/>	00-01-e3	Siemens AG phones
<input type="checkbox"/>	00-03-6b	Cisco phones
<input type="checkbox"/>	00-0f-e2	H3C phones
<input type="checkbox"/>	00-60-b9	Philips and NEC AG phones
<input type="checkbox"/>	00-d0-1e	Pingtel phones
<input type="checkbox"/>	00-e0-75	Polycom phones
<input type="checkbox"/>	00-e0-bb	3Com phones

Setting	Description
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>Telephony OUI</b>	A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).
<b>Description</b>	The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.

## Configuration > QoS > Port Classification

### QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	WRED Group
*	<> v	<> v	<> v	<> v		<input type="checkbox"/>	<> v
1	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
2	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
3	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
4	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
5	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
6	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
7	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
8	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
9	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
10	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
11	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
12	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
13	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
14	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
15	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
16	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
17	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
18	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
19	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
20	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
21	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
22	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
23	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
24	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
25	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
26	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
27	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
28	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
29	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
30	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
31	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
32	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v
33	0 v	0 v	0 v	0 v	<a href="#">Disabled</a>	<input type="checkbox"/>	1 v

Save Reset

Setting	Description
<b>Port</b>	The port number for which the configuration below applies.
<b>CoS</b>	<p>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. <b>Note:</b> If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.</p>
<b>DPL</b>	<p>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.</p>
<b>PCP</b>	<p>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.</p>
<b>DEI</b>	<p>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.</p>
<b>Tag Class.</b>	<p>Shows the classification mode for tagged frames on this port.</p> <ul style="list-style-type: none"> <li>● <b>Disabled:</b> Use default CoS and DPL for tagged frames.</li> <li>● <b>Enabled:</b> Use mapped versions of PCP and DEI for tagged frames.</li> </ul> <p>Click on the mode in order to configure the mode and/or mapping. <b>NOTE:</b> 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.</p>
<b>DSCP Based</b>	Click to Enable DSCP Based QoS Ingress Port Classification.
<b>WRED Group</b>	Controls the WRED group membership.

## QoS Ingress Port Tag Classification Port n

The classification mode for tagged frames are configured on this page.

### Tagged Frames Settings

#### Tagged Frames Settings

Tag Classification

Setting	Description	Factory Default
<b>Enabled</b>	Use mapped versions of PCP and DEI for tagged frames.	Disabled
<b>Disabled</b>	Use default QoS class and Drop Precedence Level for tagged frames.	

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

Controls the mapping of the classified (PCP, DEI) to (QoS class, DP level) values when Tag Classification is set to **Enabled**.

PCP	DEI	QoS class	DP level
*	*	<> ▾	<> ▾
0	0	1 ▾	0 ▾
0	1	1 ▾	1 ▾
1	0	0 ▾	0 ▾
1	1	0 ▾	1 ▾
2	0	2 ▾	0 ▾
2	1	2 ▾	1 ▾
3	0	3 ▾	0 ▾
3	1	3 ▾	1 ▾
4	0	4 ▾	0 ▾
4	1	4 ▾	1 ▾
5	0	5 ▾	0 ▾
5	1	5 ▾	1 ▾
6	0	6 ▾	0 ▾
6	1	6 ▾	1 ▾
7	0	7 ▾	0 ▾
7	1	7 ▾	1 ▾

Save Reset Cancel

## Configuration > QoS > Port Policing

### QoS Ingress Port Policers

Port	Enable	Rate	Unit	Flow Control
*	<input type="checkbox"/>	500	<>	<input type="checkbox"/>
1	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
2	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
3	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
4	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
5	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
6	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
7	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
8	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
9	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
10	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
11	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
12	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
13	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
14	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
15	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
16	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
17	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
18	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
19	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
20	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
21	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
22	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
23	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
24	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
25	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
26	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
27	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
28	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
29	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
30	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
31	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
32	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
33	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>

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 10-13128147 when "Unit" is kbps or fps, and 1-13128 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.

**Configuration > QoS > Queue Policing****QoS Ingress Queue Policers**

Port	Queue 0 Enable	Queue 1 Enable	Queue 2 Enable	Queue 3 Enable	Queue 4 Enable	Queue 5 Enable	Queue 6 Enable	Queue 7 Enable
*	<input type="checkbox"/>							
1	<input type="checkbox"/>							
2	<input type="checkbox"/>							
3	<input type="checkbox"/>							
4	<input type="checkbox"/>							
5	<input type="checkbox"/>							
6	<input type="checkbox"/>							
7	<input type="checkbox"/>							
8	<input type="checkbox"/>							
9	<input type="checkbox"/>							
10	<input type="checkbox"/>							
11	<input type="checkbox"/>							
12	<input type="checkbox"/>							
13	<input type="checkbox"/>							
14	<input type="checkbox"/>							
15	<input type="checkbox"/>							
16	<input type="checkbox"/>							
17	<input type="checkbox"/>							
18	<input type="checkbox"/>							
19	<input type="checkbox"/>							
20	<input type="checkbox"/>							
21	<input type="checkbox"/>							
22	<input type="checkbox"/>							
23	<input type="checkbox"/>							
24	<input type="checkbox"/>							
25	<input type="checkbox"/>							
26	<input type="checkbox"/>							
27	<input type="checkbox"/>							
28	<input type="checkbox"/>							
29	<input type="checkbox"/>							
30	<input type="checkbox"/>							
31	<input type="checkbox"/>							
32	<input type="checkbox"/>							
33	<input type="checkbox"/>							

Setting	Description
<b>Port</b>	The port number for which the configuration below applies.
<b>Enable</b>	Enable or disable the queue policer for this switch port.
<b>Rate</b>	Controls the rate for the queue policer. This value is restricted to 25-13128147 when "Unit" is kbps, and 1-13128 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.

<b>Unit</b>	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.
-------------	--

## Configuration > QoS > Port Scheduler

### QoS Egress Port Schedulers

Port	Mode	Weight							
		Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
<a href="#">1</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">2</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">3</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">4</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">5</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">6</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">7</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">8</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">9</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">10</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">11</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">12</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">13</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">14</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">15</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">16</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">17</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">18</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">19</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">20</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">21</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">22</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">23</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">24</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">25</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">26</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">27</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">28</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">29</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">30</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">31</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">32</a>	Strict Priority	-	-	-	-	-	-	-	-
<a href="#">33</a>	Strict Priority	-	-	-	-	-	-	-	-

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



## Configuration > QoS > Port Shaping

### QoS Egress Port Shapers

Port	Shapers								Port
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	
<a href="#">1</a>	-	-	-	-	-	-	-	-	-
<a href="#">2</a>	-	-	-	-	-	-	-	-	-
<a href="#">3</a>	-	-	-	-	-	-	-	-	-
<a href="#">4</a>	-	-	-	-	-	-	-	-	-
<a href="#">5</a>	-	-	-	-	-	-	-	-	-
<a href="#">6</a>	-	-	-	-	-	-	-	-	-
<a href="#">7</a>	-	-	-	-	-	-	-	-	-
<a href="#">8</a>	-	-	-	-	-	-	-	-	-
<a href="#">9</a>	-	-	-	-	-	-	-	-	-
<a href="#">10</a>	-	-	-	-	-	-	-	-	-
<a href="#">11</a>	-	-	-	-	-	-	-	-	-
<a href="#">12</a>	-	-	-	-	-	-	-	-	-
<a href="#">13</a>	-	-	-	-	-	-	-	-	-
<a href="#">14</a>	-	-	-	-	-	-	-	-	-
<a href="#">15</a>	-	-	-	-	-	-	-	-	-
<a href="#">16</a>	-	-	-	-	-	-	-	-	-
<a href="#">17</a>	-	-	-	-	-	-	-	-	-
<a href="#">18</a>	-	-	-	-	-	-	-	-	-
<a href="#">19</a>	-	-	-	-	-	-	-	-	-
<a href="#">20</a>	-	-	-	-	-	-	-	-	-
<a href="#">21</a>	-	-	-	-	-	-	-	-	-
<a href="#">22</a>	-	-	-	-	-	-	-	-	-
<a href="#">23</a>	-	-	-	-	-	-	-	-	-
<a href="#">24</a>	-	-	-	-	-	-	-	-	-
<a href="#">25</a>	-	-	-	-	-	-	-	-	-
<a href="#">26</a>	-	-	-	-	-	-	-	-	-
<a href="#">27</a>	-	-	-	-	-	-	-	-	-
<a href="#">28</a>	-	-	-	-	-	-	-	-	-
<a href="#">29</a>	-	-	-	-	-	-	-	-	-
<a href="#">30</a>	-	-	-	-	-	-	-	-	-
<a href="#">31</a>	-	-	-	-	-	-	-	-	-
<a href="#">32</a>	-	-	-	-	-	-	-	-	-
<a href="#">33</a>	-	-	-	-	-	-	-	-	-

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".

## Configuration > QoS > Port Tag Remarking

### QoS Egress Port Tag Remarking

Port	Mode
<a href="#">1</a>	Classified
<a href="#">2</a>	Classified
<a href="#">3</a>	Classified
<a href="#">4</a>	Classified
<a href="#">5</a>	Classified
<a href="#">6</a>	Classified
<a href="#">7</a>	Classified
<a href="#">8</a>	Classified
<a href="#">9</a>	Classified
<a href="#">10</a>	Classified
<a href="#">11</a>	Classified
<a href="#">12</a>	Classified
<a href="#">13</a>	Classified
<a href="#">14</a>	Classified
<a href="#">15</a>	Classified
<a href="#">16</a>	Classified
<a href="#">17</a>	Classified
<a href="#">18</a>	Classified
<a href="#">19</a>	Classified
<a href="#">20</a>	Classified
<a href="#">21</a>	Classified
<a href="#">22</a>	Classified
<a href="#">23</a>	Classified
<a href="#">24</a>	Classified
<a href="#">25</a>	Classified
<a href="#">26</a>	Classified
<a href="#">27</a>	Classified
<a href="#">28</a>	Classified
<a href="#">29</a>	Classified
<a href="#">30</a>	Classified
<a href="#">31</a>	Classified
<a href="#">32</a>	Classified
<a href="#">33</a>	Classified

Setting	Description
<b>Port</b>	The logical port for the settings contained in the same row. Click on the port number in order to configure tag remarking.
<b>Mode</b>	Shows the tag remarking mode for this port. <ul style="list-style-type: none"> <li>● <b>Classified:</b> Use classified PCP/DEI values.</li> <li>● <b>Default:</b> Use default PCP/DEI values.</li> <li>● <b>Mapped:</b> Use mapped versions of QoS class and DP level.</li> </ul>

## Configuration > QoS > Port DSCP

### QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	<input type="checkbox"/>	<> ▾	<> ▾
1	<input type="checkbox"/>	Disable ▾	Disable ▾
2	<input type="checkbox"/>	Disable ▾	Disable ▾
3	<input type="checkbox"/>	Disable ▾	Disable ▾
4	<input type="checkbox"/>	Disable ▾	Disable ▾
5	<input type="checkbox"/>	Disable ▾	Disable ▾
6	<input type="checkbox"/>	Disable ▾	Disable ▾
7	<input type="checkbox"/>	Disable ▾	Disable ▾
8	<input type="checkbox"/>	Disable ▾	Disable ▾
9	<input type="checkbox"/>	Disable ▾	Disable ▾
10	<input type="checkbox"/>	Disable ▾	Disable ▾
11	<input type="checkbox"/>	Disable ▾	Disable ▾
12	<input type="checkbox"/>	Disable ▾	Disable ▾
13	<input type="checkbox"/>	Disable ▾	Disable ▾
14	<input type="checkbox"/>	Disable ▾	Disable ▾
15	<input type="checkbox"/>	Disable ▾	Disable ▾
16	<input type="checkbox"/>	Disable ▾	Disable ▾
17	<input type="checkbox"/>	Disable ▾	Disable ▾
18	<input type="checkbox"/>	Disable ▾	Disable ▾
19	<input type="checkbox"/>	Disable ▾	Disable ▾
20	<input type="checkbox"/>	Disable ▾	Disable ▾
21	<input type="checkbox"/>	Disable ▾	Disable ▾
22	<input type="checkbox"/>	Disable ▾	Disable ▾
23	<input type="checkbox"/>	Disable ▾	Disable ▾
24	<input type="checkbox"/>	Disable ▾	Disable ▾
25	<input type="checkbox"/>	Disable ▾	Disable ▾
26	<input type="checkbox"/>	Disable ▾	Disable ▾
27	<input type="checkbox"/>	Disable ▾	Disable ▾
28	<input type="checkbox"/>	Disable ▾	Disable ▾
29	<input type="checkbox"/>	Disable ▾	Disable ▾
30	<input type="checkbox"/>	Disable ▾	Disable ▾
31	<input type="checkbox"/>	Disable ▾	Disable ▾
32	<input type="checkbox"/>	Disable ▾	Disable ▾
33	<input type="checkbox"/>	Disable ▾	Disable ▾

Save Reset

Setting	Description
Port	The Port column shows the list of ports for which you can configure dscp ingress and egress settings.
Ingress	<b>Translate:</b> To Enable the Ingress Translation click the checkbox. <b>Classify:</b> Classification for a port have 4 different values. <ol style="list-style-type: none"><li>1. <b>Disable:</b> No Ingress DSCP Classification.</li><li>2. <b>DSCP=0:</b> Classify if incoming (or translated if enabled) DSCP is 0.</li><li>3. <b>Selected:</b> Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.</li><li>4. <b>All:</b> Classify all DSCP.</li></ol>
Egress	<b>Disable:</b> No Egress rewrite. <b>Enable:</b> Rewrite enabled without remapping. <b>Remap:</b> DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.

## Configuration > QoS > DSCP-Based QoS

### DSCP-based QoS Ingress Classification

DSCP	Trust	QoS Class	DPL
*	<input type="checkbox"/>	<> ▾	<> ▾
0 (BE)	<input type="checkbox"/>	0 ▾	0 ▾
1	<input type="checkbox"/>	0 ▾	0 ▾
2	<input type="checkbox"/>	0 ▾	0 ▾
3	<input type="checkbox"/>	0 ▾	0 ▾
4	<input type="checkbox"/>	0 ▾	0 ▾
5	<input type="checkbox"/>	0 ▾	0 ▾
6	<input type="checkbox"/>	0 ▾	0 ▾
7	<input type="checkbox"/>	0 ▾	0 ▾
8 (CS1)	<input type="checkbox"/>	0 ▾	0 ▾
9	<input type="checkbox"/>	0 ▾	0 ▾
10 (AF11)	<input type="checkbox"/>	0 ▾	0 ▾
• • •			
59	<input type="checkbox"/>	0 ▾	0 ▾
60	<input type="checkbox"/>	0 ▾	0 ▾
61	<input type="checkbox"/>	0 ▾	0 ▾
62	<input type="checkbox"/>	0 ▾	0 ▾
63	<input type="checkbox"/>	0 ▾	0 ▾

Setting	Description
<b>DSCP</b>	Maximum number of supported DSCP values are 64.
<b>Trust</b>	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.
<b>QoS Class</b>	QoS class value can be any of (0-7)
<b>DPL</b>	Drop Precedence Level (0-3)

## Configuration > QoS > DSCP Translation

### DSCP Translation

DSCP	Ingress		Egress
	Translate	Classify	Remap
*	<> ▾	<input type="checkbox"/>	<> ▾
0 (BE)	0 (BE) ▾	<input type="checkbox"/>	0 (BE) ▾
1	1 ▾	<input type="checkbox"/>	1 ▾
2	2 ▾	<input type="checkbox"/>	2 ▾
3	3 ▾	<input type="checkbox"/>	3 ▾
4	4 ▾	<input type="checkbox"/>	4 ▾
5	5 ▾	<input type="checkbox"/>	5 ▾
6	6 ▾	<input type="checkbox"/>	6 ▾
7	7 ▾	<input type="checkbox"/>	7 ▾
8 (CS1)	8 (CS1) ▾	<input type="checkbox"/>	8 (CS1) ▾
9	9 ▾	<input type="checkbox"/>	9 ▾
10 (AF11)	10 (AF11) ▾	<input type="checkbox"/>	10 (AF11) ▾
• • •			
57	57 ▾	<input type="checkbox"/>	57 ▾
58	58 ▾	<input type="checkbox"/>	58 ▾
59	59 ▾	<input type="checkbox"/>	59 ▾
60	60 ▾	<input type="checkbox"/>	60 ▾
61	61 ▾	<input type="checkbox"/>	61 ▾
62	62 ▾	<input type="checkbox"/>	62 ▾
63	63 ▾	<input type="checkbox"/>	63 ▾

Save Reset

Setting	Description
<b>DSCP</b>	Maximum number of supported DSCP values is 64 and valid DSCP values range from 0 to 63.
<b>Ingress</b>	Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. <ul style="list-style-type: none"> <li>• <b>Translate:</b> DSCP at Ingress side can be translated to any of (0-63) DSCP values.</li> <li>• <b>Classify:</b> Click to enable Classification at Ingress side.</li> </ul>
<b>Egress</b>	<ul style="list-style-type: none"> <li>• <b>Remap:</b> Select the DSCP value from the select menu to which you want to remap. DSCP value ranges from 0 to 63.</li> </ul>

## Configuration > QoS > DSCP Classification

### DSCP Classification

QoS Class	DSCP DP0	DSCP DP1	DSCP DP2	DSCP DP3
*	<> ▼	<> ▼	<> ▼	<> ▼
0	0 (BE) ▼	0 (BE) ▼	0 (BE) ▼	0 (BE) ▼
1	0 (BE) ▼	0 (BE) ▼	0 (BE) ▼	0 (BE) ▼
2	0 (BE) ▼	0 (BE) ▼	0 (BE) ▼	0 (BE) ▼
3	0 (BE) ▼	0 (BE) ▼	0 (BE) ▼	0 (BE) ▼
4	0 (BE) ▼	0 (BE) ▼	0 (BE) ▼	0 (BE) ▼
5	0 (BE) ▼	0 (BE) ▼	0 (BE) ▼	0 (BE) ▼
6	0 (BE) ▼	0 (BE) ▼	0 (BE) ▼	0 (BE) ▼
7	0 (BE) ▼	0 (BE) ▼	0 (BE) ▼	0 (BE) ▼

Save Reset

Setting	Description
<b>QoS Class</b>	Actual QoS class.
<b>DSCP DP0</b>	Select the classified DSCP value (0-63) for Drop Precedence Level 0.
<b>DSCP DP1</b>	Select the classified DSCP value (0-63) for Drop Precedence Level 1.
<b>DSCP DP2</b>	Select the classified DSCP value (0-63) for Drop Precedence Level 2.
<b>DSCP DP3</b>	Select the classified DSCP value (0-63) for Drop Precedence Level 3.

## Configuration > QoS > QoS Control List

### QoS Control List Configuration

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.

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action						
									CoS	DPL	DSCP	PCP	DEI	Policy	
1	Any	Any	Any	Any	Any	Any	Any	Any	0	Default	Default	Default	Default	Default	

You can modify each QCE (QoS Control Entry) in the table using the following buttons:

- : Inserts a new QCE before the current row.
- : Edits the QCE.
- : Moves the QCE up the list.
- : Moves the QCE down the list.
- : Deletes the QCE.
- : The lowest plus sign adds a new entry at the bottom of the QCE listings.

Setting	Description
<b>QCE</b>	Indicates the QCE id.
<b>Port</b>	Indicates the list of ports configured with the QCE or 'Any'.
<b>DMAC</b>	Indicates the destination MAC address. Possible values are: <ul style="list-style-type: none"> <li>● <b>Any</b>: Match any DMAC.</li> <li>● <b>Unicast</b>: Match unicast DMAC.</li> <li>● <b>Multicast</b>: Match multicast DMAC.</li> <li>● <b>Broadcast</b>: Match broadcast DMAC.</li> <li>● <b>&lt;MAC&gt;</b>: Match specific DMAC.</li> </ul> The default value is 'Any'.
<b>SMAC</b>	Match specific source MAC address or 'Any'. If a port is configured to match on destination addresses, this field indicates the DMAC.
<b>Tag Type</b>	Indicates tag type. Possible values are: <ul style="list-style-type: none"> <li>● <b>Any</b>: Match tagged and untagged frames.</li> <li>● <b>Untagged</b>: Match untagged frames.</li> <li>● <b>Tagged</b>: Match tagged frames.</li> <li>● <b>C-Tagged</b>: Match C-tagged frames.</li> <li>● <b>S-Tagged</b>: Match S-tagged frames.</li> </ul> The default value is 'Any'.
<b>VID</b>	Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'
<b>PCP</b>	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'.



## Port Members

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

## Key Parameters

Setting	Description
<b>DMAC</b>	Destination MAC address: Possible values are <b>Unicast, Multicast, Broadcast , Specific (xx-xx-xx-xx-xx-xx)</b> , or <b>Any</b> .
<b>SMAC</b>	Source MAC address: <b>xx-xx-xx-xx-xx-xx</b> or <b>Any</b> .
<b>Tag</b>	Value of Tag field can be <b>Untagged, Tagged, C-Tagged, S-Tagged</b> or <b>Any</b> .
<b>VID</b>	Valid value of VLAN ID can be any value in the range <b>1-4095</b> or <b>Any</b> ; user can enter either a specific value or a range of VIDs.
<b>PCP</b>	Valid value PCP are specific ( <b>0, 1, 2, 3, 4, 5, 6, 7</b> ) or range ( <b>0-1, 2-3, 4-5, 6-7, 0-3, 4-7</b> ) or <b>Any</b> .
<b>DEI</b>	Valid value of DEI can be <b>0, 1</b> or <b>Any</b> .
<b>Inner Tag</b>	Value of Inner Tag field can be <b>Untagged, Tagged, C-Tagged, S-Tagged</b> or <b>Any</b> .
<b>Inner Tag VID</b>	Valid value of Inner VLAN ID can be any value in the range <b>1-4095</b> or <b>Any</b> ; user can enter either a specific value or a range of VIDs.
<b>Inner PCP</b>	Valid value of Inner PCP are specific ( <b>0, 1, 2, 3, 4, 5, 6, 7</b> ) or range ( <b>0-1, 2-3, 4-5, 6-7, 0-3, 4-7</b> ) or <b>Any</b> .
<b>Inner DEI</b>	Valid value of Inner DEI can be <b>0, 1</b> , or <b>Any</b> .
<b>Frame Type</b>	Frame Type can have any of the following. <ol style="list-style-type: none"> <li>1. <b>Any</b></li> <li>2. <b>EtherType</b></li> <li>3. <b>LLC</b></li> <li>4. <b>SNAP</b></li> <li>5. <b>IPv4</b></li> <li>6. <b>IPv6</b></li> </ol>

### 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: <b>(0-7)</b> or <b>Default</b> .
DP	Drop Precedence Level: <b>(0-1)</b> or <b>Default</b> .
DSCP	DS1CP: <b>(0-63, BE, CS1-CS7, EF or AF11-AF43)</b> or <b>Default</b> .
PCP	PCP: <b>(0-7)</b> or <b>Default</b> . Note: PCP and DEI cannot be set individually.
DEI	DEI: <b>(0-1)</b> or <b>Default</b> .
Policy	ACL Policy number: <b>(0-255)</b> or <b>Default</b> (empty field).

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

## Configuration > QoS > Storm Policing

### Global Storm Policer Configuration

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.

Frame Type	Enable	Rate	Unit
Unicast	<input type="checkbox"/>	10	fps ▼
Multicast	<input type="checkbox"/>	10	fps ▼
Broadcast	<input type="checkbox"/>	10	fps ▼

Setting	Description
<b>Frame Type</b>	The frame type for which the configuration below applies.
<b>Enable</b>	Enable or disable the global storm policer for the given frame type.
<b>Rate</b>	Controls the rate for the global storm policer. This value is restricted to 10-13128147 when "Unit" is fps or kbps, and 1-13128 when "Unit" is kfps or Mbps. The rate is internally rounded up to the nearest value supported by the global storm policer.
<b>Unit</b>	Controls the unit of measure for the global storm policer rate fps, kfps, kbps or Mbps.

Port	Unicast Frames			Broadcast Frames			Unknown Frames		
	Enable	Rate	Unit	Enable	Rate	Unit	Enable	Rate	Unit
*	<input type="checkbox"/>	500	<> ▾	<input type="checkbox"/>	500	<> ▾	<input type="checkbox"/>	500	<> ▾
1	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
2	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
3	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
4	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
5	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
6	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
7	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
8	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
9	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
10	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
11	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
12	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
13	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
14	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
15	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
16	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
17	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
18	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
19	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
20	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
21	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
22	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
23	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
24	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
25	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
26	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
27	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
28	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
29	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
30	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
31	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
32	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾
33	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>	500	kpbs ▾

Setting	Description
Port	The port number for which the configuration below applies.
Enable	Enable or disable the storm policer for this switch port.
Rate	Controls the rate for the port storm policer. This value is restricted to 10-13128147 when "Unit" is fps or kbps, and 1-13128 when "Unit" is kfps or Mbps. The rate is internally rounded up to the nearest value supported by the port storm policer.
Unit	Controls the unit of measure for the port storm policer rate as fps, kfps, kbps or Mbps.



## Configuration > QoS > WRED

### QoS Weighted Random Early Detection Configuration

Through different RED configuration for the queues (QoS classes) it is possible to obtain Weighted Random Early Detection (WRED) operation between queues.

The settings are global for all ports in the switch.

Group	Queue	DPL	Enable	Min	Max	Max Unit
1	0	1	<input type="checkbox"/>	0	50	Drop Probability ▼
1	0	2	<input type="checkbox"/>	0	50	Drop Probability ▼
1	0	3	<input type="checkbox"/>	0	50	Drop Probability ▼
1	1	1	<input type="checkbox"/>	0	50	Drop Probability ▼
1	1	2	<input type="checkbox"/>	0	50	Drop Probability ▼
1	1	3	<input type="checkbox"/>	0	50	Drop Probability ▼
1	2	1	<input type="checkbox"/>	0	50	Drop Probability ▼
1	2	2	<input type="checkbox"/>	0	50	Drop Probability ▼
1	2	3	<input type="checkbox"/>	0	50	Drop Probability ▼
1	3	1	<input type="checkbox"/>	0	50	Drop Probability ▼
1	3	2	<input type="checkbox"/>	0	50	Drop Probability ▼
1	3	3	<input type="checkbox"/>	0	50	Drop Probability ▼
1	4	1	<input type="checkbox"/>	0	50	Drop Probability ▼
1	4	2	<input type="checkbox"/>	0	50	Drop Probability ▼
1	4	3	<input type="checkbox"/>	0	50	Drop Probability ▼
•						
•						
•						
3	5	1	<input type="checkbox"/>	0	50	Drop Probability ▼
3	5	2	<input type="checkbox"/>	0	50	Drop Probability ▼
3	5	3	<input type="checkbox"/>	0	50	Drop Probability ▼
3	6	1	<input type="checkbox"/>	0	50	Drop Probability ▼
3	6	2	<input type="checkbox"/>	0	50	Drop Probability ▼
3	6	3	<input type="checkbox"/>	0	50	Drop Probability ▼
3	7	1	<input type="checkbox"/>	0	50	Drop Probability ▼
3	7	2	<input type="checkbox"/>	0	50	Drop Probability ▼
3	7	3	<input type="checkbox"/>	0	50	Drop Probability ▼

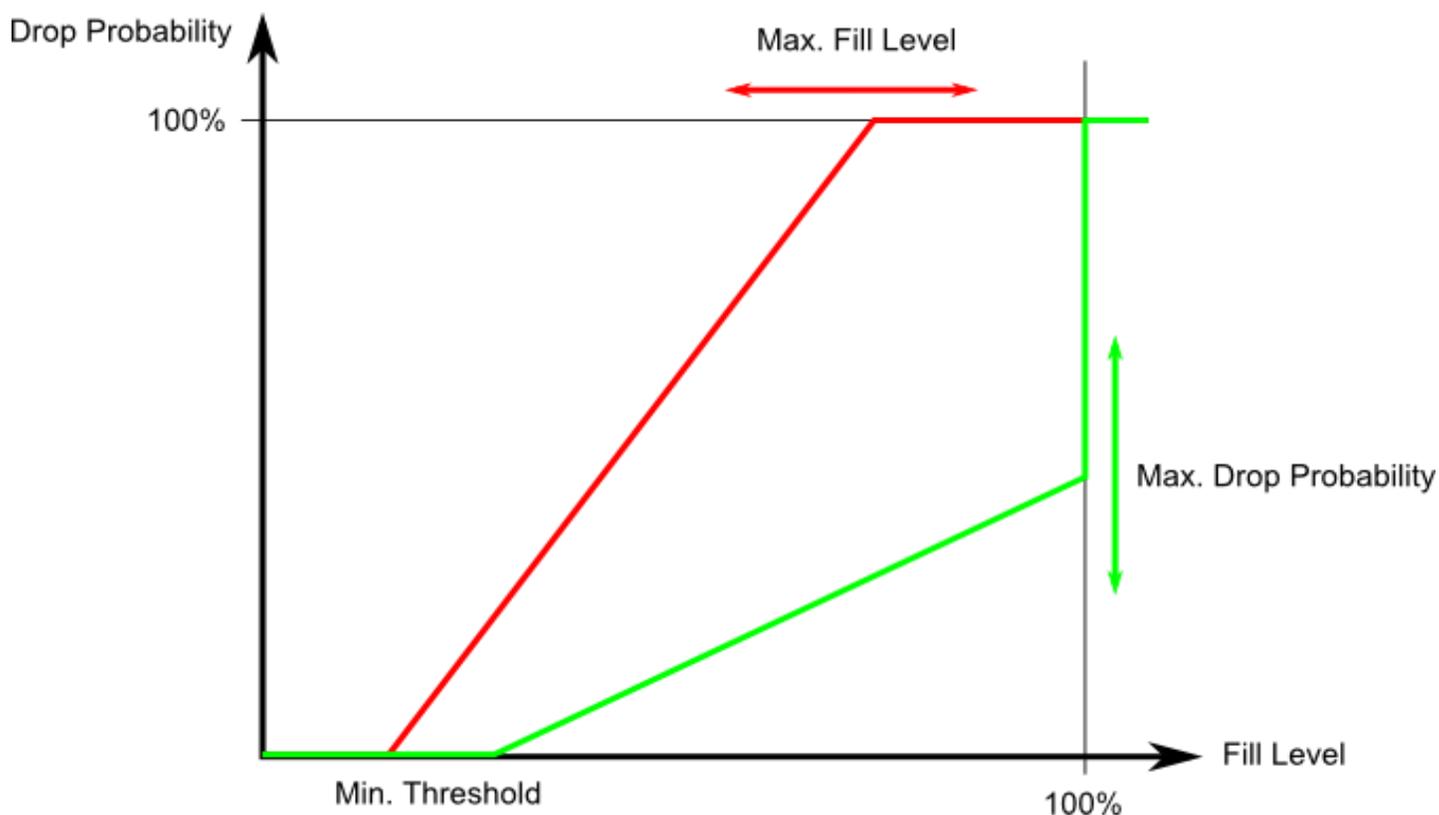
Save Reset

Setting	Description
<b>Group</b>	The WRED group number for which the configuration below applies.
<b>Queue</b>	The queue number (QoS class) for which the configuration below applies.
<b>DPL</b>	The Drop Precedence Level for which the configuration below applies.
<b>Enable</b>	Controls whether RED is enabled for this entry.

<b>Min</b>	Controls the lower RED fill level threshold. If the queue filling level is below this threshold, the drop probability is zero. This value is restricted to 0-100%.
<b>Max</b>	Controls the upper RED drop probability or fill level threshold for frames marked with Drop Precedence Level > 0 (yellow frames). This value is restricted to 1-100%.
<b>Max Unit</b>	Selects the unit for Max. <b>Drop Probability:</b> Max controls the drop probability just below 100% fill level. <b>Fill Level:</b> Max controls the fill level where drop probability reaches 100%.

## RED Drop Probability Function

The following illustration shows the drop probability versus fill level function with associated parameters.



Min is the fill level where the queue randomly start dropping frames marked with Drop Precedence Level > 0 (yellow frames).

If Max Unit is 'Drop Probability' (the green line), Max controls the drop probability when the fill level is just below 100%.

If Max Unit is 'Fill Level' (the red line), Max controls the fill level where drop probability reaches 100%. This configuration makes it possible to reserve a portion of the queue exclusively for frames marked with Drop Precedence Level 0 (green frames). The reserved portion is calculated as  $(100 - \text{Max}) \%$ . Frames marked with Drop Precedence Level 0 (green frames) are never dropped.

The drop probability for frames increases linearly from zero (at Min average queue filling level) to Max Drop Probability or Fill Level.

## Configuration > Mirroring

### Mirroring & Remote Mirroring Configuration

Mirroring is a feature for switched port analyzer. 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 extend function of Mirroring. It can extend the destination port in other switch. 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.

Mode	Disabled	▼
Type	Mirror	▼
VLAN ID	200	
Reflector Port	Port 25	▼

Setting	Description
<b>Session</b>	Select session id to configure.
<b>Mode</b>	To Enabled/Disabled the mirror or Remote Mirroring function.
<b>Type</b>	<p>Select switch type.</p> <ul style="list-style-type: none"> <li>● <b>Mirror:</b> The switch is running on mirror mode. The source port(s) and destination port are located on this switch.</li> <li>● <b>Source:</b> The switch is a source node for monitor flow. The source port(s), reflector port are located on this switch.</li> <li>● <b>Intermediate:</b> The switch is a forwarding node for monitor flow and the switch is an option node. The object is to forward traffic from source switch to destination switch. The intermediate ports are located on this switch.</li> <li>● <b>Destination:</b> The switch is an end node for monitor flow. The destination port(s) is located on this switch.</li> </ul>
<b>VLAN ID</b>	The VLAN ID points out where the monitor packet will copy to. The default VLAN ID is 200.
<b>Reflector Port</b>	<p>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.</p> <p>In the stacking mode, you need to select switch ID to select the correct device. If you shut down a port, it cannot be a candidate for reflector port.</p> <p>If you shut down the port which is a reflector port, the remote mirror function cannot work.</p> <p><b>Note1:</b> The reflector port needs to select only on Source switch type.</p> <p><b>Note2:</b> The reflector port needs to disable MAC Table learning and STP.</p> <p><b>Note3:</b> The reflector port only supports on pure copper ports.</p>

### Source VLAN(s) Configuration

The switch can supports VLAN-based Mirroring. If you want to monitor some VLANs on the switch, you can set the selected VLANs on this field.

Source VLANs	
--------------	--

**NOTE:** The Mirroring session shall have either ports or VLANs as sources, but not both.

## Port Configuration

Port	Source	Intermediate	Destination
1	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
2	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
3	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
4	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
5	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
6	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
7	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
8	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
9	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
10	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
11	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
12	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
13	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
14	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
15	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
16	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
17	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
18	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
19	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
20	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
21	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
22	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
23	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
24	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
25	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
26	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
27	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
28	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
29	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
30	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
31	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
32	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>
33	Disabled ▼	<input type="checkbox"/>	<input type="checkbox"/>

<b>Setting</b>	<b>Description</b>
----------------	--------------------

<b>Port</b>	The logical port for the settings contained in the same row.
<b>Source</b>	<p>Select mirror mode.</p> <ul style="list-style-type: none"> <li>• <b>Disabled:</b> Neither frames transmitted nor frames received are mirrored.</li> <li>• <b>Both:</b> Frames received and frames transmitted are mirrored on the Destination port.</li> <li>• <b>Rx only:</b> Frames received on this port are mirrored on the Destination port. Frames transmitted are not mirrored.</li> <li>• <b>Tx only:</b> Frames transmitted on this port are mirrored on the Destination port. Frames received are not mirrored.</li> </ul>
<b>Intermediate</b>	<p>Select intermediate port. This checkbox is designed for Remote Mirroring. The intermediate port is a switched port to connect to other switch.</p> <p><b>Note:</b> The intermediate port needs to disable MAC Table learning.</p>
<b>Destination</b>	<p>Select destination port. This checkbox is designed for mirror or Remote Mirroring. The destination port is a switched port that you receive a copy of traffic from the source port.</p> <p><b>Note1:</b> On mirror mode, the device only supports one destination port. <b>Note2:</b> The destination port needs to disable MAC Table learning.</p>

## Configuration Guideline for All Features

When the switch is running on Remote Mirroring mode, the administrator also needs to check whether or not other features are enabled or disabled.

For example, the administrator is not disabled the MSTP on reflector port. All monitor traffic will be blocked on reflector port.

All recommended settings are described as follows.

	Impact	Source Port	Reflector Port	Intermediate Port	Destination Port	Remote Mirroring VLAN
<b>arp_inspection</b>	High		* disabled	* disabled		
<b>acl</b>	Critical		* disabled	* disabled	* disabled	
<b>dhcp_relay</b>	High		* disabled	* disabled		
<b>dhcp_snooping</b>	High		* disabled	* disabled		
<b>ip_source_guard</b>	Critical		* disabled	* disabled	* disabled	
<b>ipmc/igmpsnp</b>	Critical					un-conflict
<b>ipmc/mlidsnp</b>	Critical					un-conflict
<b>lACP</b>	Low				o disabled	
<b>lldp</b>	Low				o disabled	
<b>mac learning</b>	Critical		* disabled	* disabled	* disabled	
<b>mstp</b>	Critical		* disabled		o disabled	
<b>mvr</b>	Critical					un-conflict
<b>nas</b>	Critical		* authorized	* authorized	* authorized	

<b>psec</b>	Critical		* disabled	* disabled	* disabled	
<b>qos</b>	Critical		* unlimited	* unlimited	* unlimited	
<b>upnp</b>	Low				o disabled	
<b>mac-based vlan</b>	Critical		* disabled	* disabled		
<b>protocol-based vlan</b>	Critical		* disabled	* disabled		
<b>vlan_translation</b>	Critical		* disabled	* disabled	* disabled	
<b>voice_vlan</b>	Critical		* disabled	* disabled		
<b>mrp</b>	Low				o disabled	
<b>mvrp</b>	Low				o disabled	

**Note:**

\* -- must

o -- optional

Impact: Critical/High/Low

Critical 5 packets -&gt; 0 packet

High 5 packets -&gt; 4 packets

Low 5 packets -&gt; 6 packets

## Configuration > UPnP

Mode	Disabled ▾
TTL	4
Advertising Duration	100

Save Reset

Setting	Description
<b>Mode</b>	<p>Indicates the UPnP operation mode. Possible modes are:</p> <p><b>Enabled:</b> Enable UPnP mode operation.</p> <p><b>Disabled:</b> Disable UPnP mode operation.</p> <p>When the mode is enabled, two ACEs are added automatically to trap UPnP related packets to CPU. The ACEs are automatically removed when the mode is disabled.</p>
<b>TTL</b>	<p>The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range 1 to 255.</p>
<b>Advertising Duration</b>	<p>The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range 100 to 86400.</p>

## Configuration > GVRP > Global config

### GVRP Configuration

Enable GVRP

Parameter	Value
Join-time:	20
Leave-time:	60
LeaveAll-time:	1000
Max VLANs:	20

Save

#### Enable GVRP

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

## Configuration > GVRP > Port config

### GVRP Port Configuration

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

Port	Mode
*	<> ▼
1	Disabled ▼
2	Disabled ▼
3	Disabled ▼
4	Disabled ▼
5	Disabled ▼
6	Disabled ▼
7	Disabled ▼
8	Disabled ▼
9	Disabled ▼
10	Disabled ▼
11	Disabled ▼
12	Disabled ▼
13	Disabled ▼
14	Disabled ▼
15	Disabled ▼
16	Disabled ▼
17	Disabled ▼
18	Disabled ▼
19	Disabled ▼
20	Disabled ▼
21	Disabled ▼
22	Disabled ▼
23	Disabled ▼
24	Disabled ▼
25	Disabled ▼
26	Disabled ▼
27	Disabled ▼
28	Disabled ▼
29	Disabled ▼
30	Disabled ▼
31	Disabled ▼
32	Disabled ▼
33	Disabled ▼

Save Reset

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



## Configuration > sFlow

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	127.0.0.1
------------	-----------

#### 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	<none>	Release
IP Address/Hostname	0.0.0.0	
UDP Port	6343	
Timeout	0	seconds
Max. Datagram Size	1400	bytes

#### 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 **Configured 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 disable 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
<b>port number</b>	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
<b>0 ~ 2147483647</b>	The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings. Valid range is 0 to 2147483647 seconds.	0

### Max. Datagram Size

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

## Port Configuration

Port	Flow Sampler			Counter Poller	
	Enabled	Sampling Rate	Max. Header	Enabled	Interval
*	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
1	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
2	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
3	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
4	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
5	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
6	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
7	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
8	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
9	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
10	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
11	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
12	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
13	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
14	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
15	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
16	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
17	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
18	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
19	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
20	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
21	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
22	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
23	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
24	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
25	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
26	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
27	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
28	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
29	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
30	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
31	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
32	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
33	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0

Setting	Description
Port	The port number for which the configuration below applies.
Flow Sampler Enabled	Enables/disables flow sampling on this port.

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

## Configuration > UDLD

Port	UDLD mode	Message Interval
*	<>	7
1	Disable	7
2	Disable	7
3	Disable	7
4	Disable	7
5	Disable	7
6	Disable	7
7	Disable	7
8	Disable	7
9	Disable	7
10	Disable	7
11	Disable	7
12	Disable	7
13	Disable	7
14	Disable	7
15	Disable	7
16	Disable	7
17	Disable	7
18	Disable	7
19	Disable	7
20	Disable	7
21	Disable	7
22	Disable	7
23	Disable	7
24	Disable	7
25	Disable	7
26	Disable	7
27	Disable	7
28	Disable	7
29	Disable	7
30	Disable	7
31	Disable	7
32	Disable	7
33	Disable	7

Setting	Description
Port	The port number of the switch
UDLD Mode	Configures the UDLD mode on a port. Valid values are Disable, Normal and Aggressive. Default mode is Disable.

	<p><b>Disable:</b> In disabled mode, UDLD functionality doesn't exist on port.</p> <p>Normal</p> <p><b>Normal:</b> In normal mode, if the link state of the port was determined to be unidirectional, it will not affect the port state.</p> <p><b>Aggressive:</b> In aggressive mode, unidirectional detected ports will get shutdown. To bring back the ports up, need to disable UDLD on that port.</p>
<b>Message Interval</b>	Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is from 7 to 90 seconds (Default value is 7 seconds) (Currently default time interval is supported, due to lack of detailed information in RFC 5171).

# Diagnostics

## Diagnostics > Ping/Ping6

### ICMP Ping

IP Address	<input type="text" value="0.0.0.0"/>
Ping Length	<input type="text" value="56"/>
Ping Count	<input type="text" value="5"/>
Ping Interval	<input type="text" value="1"/>

### ICMPv6 Ping

IP Address	<input type="text" value="0:0:0:0:0:0:0:0"/>
Ping Length	<input type="text" value="56"/>
Ping Count	<input type="text" value="5"/>
Ping Interval	<input type="text" value="1"/>
Egress Interface	<input type="text"/>

Setting	Description
IP Address	The destination IP Address.
Ping Length	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
Ping Count	The count of the ICMP packet. Values range from 1 time to 60 times.
Ping Interval	The interval of the ICMP packet. Values range from 0 second to 30 seconds.
Egress Interface (Only for IPv6)	<p>The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes.</p> <p>The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid.</p> <p>When the egress interface is not given, PING6 finds the best match interface for destination.</p> <p>Do not specify egress interface for loopback address.</p> <p>Do specify egress interface for link-local or multicast address.</p>

### Ping

After you press the **Start** button, ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The amount of data received inside of an IP packet of type ICMP ECHO\_REPLY will always be 8 bytes more than the requested data space (the ICMP header). The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

```
PING server 10.10.132.20, 56 bytes of data.  
64 bytes from 10.10.132.20: icmp_seq=0, time=0ms  
64 bytes from 10.10.132.20: icmp_seq=1, time=0ms  
64 bytes from 10.10.132.20: icmp_seq=2, time=0ms  
64 bytes from 10.10.132.20: icmp_seq=3, time=0ms  
64 bytes from 10.10.132.20: icmp_seq=4, time=0ms  
Sent 5 packets, received 5 OK, 0 bad
```

### **Ping6**

After you press the **Start** , ICMPv6 packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

```
PING6 server ff02::2, 56 bytes of data.  
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=0, time=10ms  
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=0, time=10ms  
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=1, time=0ms  
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=1, time=0ms  
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=2, time=0ms  
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=2, time=0ms  
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=3, time=0ms  
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=3, time=0ms  
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=4, time=0ms  
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=4, time=0ms  
Sent 5 packets, received 10 OK, 0 bad
```

You can configure the following properties of the issued ICMP packets:

## Diagnostics > VeriPHY

### Port

Port  ▾

Setting	Description
Port	The port where you are requesting VeriPHY Cable Diagnostics

### Cable Status

Cable Status								
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
25	--	--	--	--	--	--	--	--
26	--	--	--	--	--	--	--	--
27	--	--	--	--	--	--	--	--
28	--	--	--	--	--	--	--	--
33	--	--	--	--	--	--	--	--

Setting	Description
Port	Port Number
Pair	<p>The status of the cable pair.</p> <p><b>OK</b> - Correctly terminated pair</p> <p><b>Open</b> - Open pair</p> <p><b>Short</b> - Shorted pair</p> <p><b>Short A</b> - Cross-pair short to pair A</p> <p><b>Short B</b> - Cross-pair short to pair B</p> <p><b>Short C</b> - Cross-pair short to pair C</p> <p><b>Short D</b> - Cross-pair short to pair D</p> <p><b>Cross A</b> - Abnormal cross-pair coupling with pair A</p> <p><b>Cross B</b> - Abnormal cross-pair coupling with pair B</p> <p><b>Cross C</b> - Abnormal cross-pair coupling with pair C</p> <p><b>Cross D</b> - Abnormal cross-pair coupling with pair D</p>
Length	The length (in meters) of the cable pair. The resolution is 3 meters

# Maintenance

---

## Maintenance > Restart Device

### Restart Device

You can restart the switch on this page. After restart, the switch will boot normally.

Click **Yes** to restart device.

Click **No** to return to the Port State page without restarting.

**Are you sure you want to perform a Restart?**

## Maintenance > Factory Defaults

### 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 Port State page without resetting the configuration.

#### Factory Defaults

**Are you sure you want to reset the configuration to  
Factory Defaults?**

## Maintenance > Software > Upload

### Software Upload

This page facilitates an update of the firmware controlling the switch. Click **Choose File** to the location of a software image and click **Upload**.

After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch restarts.

#### Software Upload

File Source	Parameters
<input type="radio"/> Local	<input type="text"/>
<input type="radio"/> USB	<input type="text"/>



#### **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.

## Maintenance > Software > Image Select

### Software Image Selection

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

Active Image	
Image	LMX-3228G-10G-SFP.dat
Version	"V1.010"
Date	2022-02-23T15:47:13+08:00

Alternate Image	
Image	LMX-3228G-10G-SFP.dat
Version	"V1.010"
Date	2022-02-23T13:29:36+08:00

**NOTE:** 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. 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. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

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.

## Maintenance > Configuration > Save startup-config

### Save Running Configuration to startup-config

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

Please note: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

Save Configuration

## Maintenance > Configuration > Download

### Download 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.

Select configuration file to save.

Please note: running-config may take a while to prepare for download.

File Name
<input type="radio"/> running-config
<input type="radio"/> default-config
<input type="radio"/> startup-config

Download Configuration

- **running-config:** A virtual file that represents the currently active configuration on the switch. This file is volatile.
- **default-config:** A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.
- **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.
- Up to 31 other files, typically used for configuration backups or alternative configurations.

## Maintenance > Configuration > Upload

### Upload Configuration

#### File To Upload

No file chosen

#### Destination File

File Name	Parameters
<input type="radio"/> running-config	<input checked="" type="radio"/> Replace <input type="radio"/> Merge
<input type="radio"/> startup-config	
<input type="radio"/> Create new file	

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.

Select the file to upload, select the destination file on the target, then click **Upload Configuration**.

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.

## Maintenance > Configuration > Activate

### Activate Configuration

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

Select the file to activate and click Activate Configuration. This will initiate the process of completely replacing the existing configuration with that of the selected file.

Select configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

Please note: The activated configuration file will not be saved to startup-config automatically.

File Name
<input type="radio"/> default-config
<input type="radio"/> startup-config

Activate Configuration

## Maintenance > Configuration > Delete

### Delete Configuration File

It is possible to delete any of the writable files stored in flash, including startup-config. If this is done and the switch is rebooted without a prior Save operation, this effectively resets the switch to default configuration.

Select configuration file to delete

File Name
<input type="radio"/> startup-config

Delete Configuration File