

User's Guide

TRENDNET®



14-Port Gigabit Managed Layer 2 SFP Switch with 2 Shared RJ-45 Ports

TL2-FG142

Contents	
1. Introduction.....	1
1.1 Introduction of the management functions	1
1.2 General Features	2
1.3 Layer-2 Switching	3
1.4 Multicast	3
1.5 Carrier Ethernet	3
1.6 Quality of Service	3
1.7 Security	3
1.8 Standard References	3
1.9 Front Panel LEDs Indicators	4
1.10 Rear Panel Connectors	4
2. Hardware Installation	5
2.1 Unpacking	5
2.2 Switch Installation	5
2.3 Adding Module	5
3. Console	5
3.1 Console Setup	5
3.2 Login	6
4. Configuring with WEB	6
4.1 Login	7
4.2 Web Menus	7
4.3 Configuration	8
4.3.1 System	8
4.3.1.1 Information.....	8
4.3.1.2 IP	8
4.3.1.3 NTP	10
4.3.1.4 Time	10
4.3.1.5 Log	12
4.3.2 Green Ethernet.....	12
4.3.2.1 Port Power Savings.....	12
4.3.3 Port.....	13
4.3.4 DHCP	15
4.3.4.1 Server-Mode.....	15
4.3.4.2 Server-Excluded IP.....	15
4.3.4.3 Server-pool	16
4.3.4.4 Snooping	16
4.3.4.5 Relay	17
4.3.5 Security	17
4.3.5.1 User	17
4.3.5.2 Privilege Levels.....	18
4.3.5.3 Authentication Method Configuration.....	19
4.3.5.4 SSH Configuration.....	19
4.3.5.5 HTTPS Configuration.....	20
4.3.5.6 Access Management Configuration	20
4.3.5.7 Limit Control.....	21
4.3.5.8 NAS.....	22
4.3.6 SNMP	25
4.3.6.1 System	25
4.3.6.2 Trap	26
4.3.6.3 Community	27
4.3.6.4 User	27
4.3.6.5 Group	28
4.3.6.6 View	29
4.3.6.7 Access	29
4.3.7 RMON.....	30
4.3.7.1 Statistics	30
4.3.7.2 History	30
4.3.7.3 Alarm	30
4.3.7.4 Event	31
4.3.8 ACL	32
4.3.8.1 Ports.....	32
4.3.8.2 Rate Limiters.....	33
4.3.8.3 Access Control List.....	34
4.3.9 IP Source Guard.....	37
4.3.9.1 IP Source Guard Configuration.....	37

4.3.9.2 IP Static Table.....	37	4.3.22 MAC Table.....	66
4.3.10 ARP Inspection.....	38	4.3.23 VLAN Translation.....	67
4.3.10.1 Port Configuration.....	38	4.3.23.1 Port to Group Mapping.....	67
4.3.10.2 VLAN Mode Configuration.....	39	4.3.23.2 VID Translation Mapping.....	68
4.3.10.3 Static ARP Inspection Table.....	39	4.3.24 VLANs.....	69
4.3.10.4 Dynamic ARP Inspection Table.....	40	4.3.25 Private VLANs.....	72
4.3.11 AAA.....	40	4.3.25.1 Private VLAN Membership.....	72
4.3.11.1 RADIUS Server Configuration.....	40	4.3.25.2 Port Isolation.....	72
4.3.11.2 TACACS+ Server Configuration.....	41	4.3.26 VCL.....	73
4.3.12 Aggregation.....	42	4.3.26.1 MAC-based VLAN.....	73
4.3.12.1 Static.....	42	4.3.26.2 Protocol-based VLAN.....	73
4.3.12.2 LACP.....	43	4.3.26.3 IP Subnet-based VLAN.....	75
4.3.13 Link OAM.....	44	4.3.27 Voice VLAN.....	76
4.3.13.1 Port Settings.....	44	4.3.27.1 Configuration.....	76
4.3.13.2 Event Settings.....	45	4.3.27.2 OUI.....	77
4.3.14 Loop Protection.....	46	4.3.28 Ethernet Services.....	77
4.3.15 Spanning Tree.....	47	4.3.28.1 Port.....	77
4.3.15.1 Bridge Setting.....	47	4.3.28.2 Bandwidth Profiles.....	78
4.3.15.2 MSTI Mapping.....	48	4.3.28.3 EVCs.....	79
4.3.15.3 MSTI Priorities.....	49	4.3.28.4 ECEs.....	80
4.3.15.4 CIST Ports.....	49	4.3.29 QoS.....	81
4.3.15.5 MSTI Ports.....	50	4.3.29.1 Port Classification.....	81
4.3.16 IPMC Profile.....	51	4.3.29.2 Port Policing.....	82
4.3.16.1 Profile Table.....	51	4.3.29.3 Queue Policing.....	83
4.3.16.2 Address Entry.....	52	4.3.29.4 Port Scheduler.....	84
4.3.17 MVR.....	52	4.3.29.5 Port Shaping.....	85
4.3.18 IPMC.....	55	4.3.29.6 Port Tag Remarking.....	86
4.3.18.1 IGMP Snooping-Base Cfg.....	55	4.3.29.7 Port DSCP.....	88
4.3.18.2 IGMP Snooping-VLAN Cfg.....	55	4.3.29.8 DSCP-Based QoS.....	88
4.3.18.3 IGMP Snooping- Port Filtering Profile.....	57	4.3.29.9 DSCP Translation.....	89
4.3.18.3 MLD Snooping- Base Cfg.....	57	4.3.29.10 DSCP Classification.....	90
4.3.18.4 MLD Snooping- VLAN Cfg.....	58	4.3.29.11 QoS Control List.....	90
4.3.18.4 MLD Snooping- Port Filter profile.....	60	4.3.29.12 Storm Control.....	93
4.3.19 LLDP.....	60	4.3.30 Mirror.....	94
4.3.19.1 LLDP Configuration.....	60	4.3.31 sFlow.....	94
4.3.19.2 LLDP-MED.....	62		
4.3.20 EPS.....	65	5. Monitor..... 96	
4.3.21 MEP.....	66	5.1 System.....	96

5.1.1 Information.....	96	5.8 Spanning Tree	108
5.1.2 CPU Load	97	5.8.1 Bridge Status.....	108
5.1.3 IP Status.....	97	5.8.2 Port Status.....	108
5.1.4 Log	98	5.8.3 Port Statistics.....	108
5.1.5 Detailed Log	98	5.9 MVR	108
5.2 Green Ethernet.....	98	5.9.1 Statistics.....	108
5.2.1 Port Power Savings.....	98	5.9.2 MVR Channel Groups	109
5.3 Ports.....	99	5.9.3 MVR SFM Information	109
5.3.1 State	99	5.10 IPMC.....	109
5.3.2 Port Statistics Overview.....	99	5.10.1 IGMP Status	109
5.3.3 QoS Statistics	99	5.10.2 IGMP Group Information	109
5.3.4 QCL Status	100	5.10.3 IGMP SFM Information.....	109
5.3.5 Detailed Port Statistics.....	100	5.10.4 MLD Status.....	110
5.3.6 DDMI	101	5.10.5 MLD group Information.....	110
5.4 Link OAM	101	5.10.6 MLD SFM Information.....	110
5.4.1 Statistics.....	101	5.11 LLDP	110
5.4.2 Port status.....	102	5.11.1 Neighbours.....	110
5.4.3 Event Status	102	5.11.2 LLDP-MED Neighbour Information.....	110
5.5 Security	102	5.11.3 EEE	110
5.5.1 Access Management Statistics	102	5.11.4 Port Statistics.....	111
5.5.2 Port Security - Switch.....	103	5.12 Ethernet Services	111
5.5.3 Port Security - Port.....	104	5.12.1 EVC Statistics	111
5.5.4 NAS - Switch.....	104	5.13 MAC Table	111
5.5.5 NAS - Port.....	105	5.14 VLANs	111
5.5.6 ACL Status.....	105	5.14.1 VLAN Membership.....	111
5.5.7 ARP inspection.....	105	5.14.2 VLAN Port	111
5.5.8 IP Source Guard.....	105	5.15 VCL.....	112
5.5.9 AAA Radius.....	106	5.15.1 MAC-Based VLAN.....	112
5.5.10 AAA Overview	106	5.16 sFlow	112
5.5.11 ROM Statistics	106		
5.5.12 ROM History.....	107	6. Diagnostics..... 112	
5.5.13 ROM Alarm	107	6.1 Ping.....	112
5.5.14 ROM Event	107	6.2 Link OAM	113
5.6 LACP	107	6.2.1 MIB Retrieval	113
5.6.1 System Status	107	6.3 Ping6.....	113
5.6.2 LACP Status	107	6.4 VeriPHY	114
5.6.3 LACP Statistics	108		
5.7 Loop Protection	108		

- 7. Maintenance..... 115**
 - 7.1 Restart Device..... 115
 - 7.2 Factory Default..... 115
 - 7.3 Software..... 115
 - 7.3.1 Upload..... 115
 - 7.3.2 Image Select..... 115
 - 7.4 Configuration 116
 - 7.4.1 Save startup-config..... 116
 - 7.4.2 Download 116
 - 7.4.3 Upload..... 117
 - 7.4.4 Activate..... 117
 - 7.4.5 Delete..... 117
- Technical Specifications 119**
- Troubleshooting 123**
- Appendix..... 124**

1. Introduction

TL2-FG142 supports 14 fiber ports SFP type with 100/1000M bps and 2 RJ-45 Copper port with adaptive 10/100/1000M bps.



1.1 Introduction of the management functions

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

1. VLAN (Virtual LAN)

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

2. Trunk

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

Notes: About redundant application

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

3. Spanning Tree Protocol / Rapid Spanning Tree Protocol

Spanning tree is a protocol to prevent network loop in network topology. If network loop happens, it will cause switches in the network unstable because more and more traffic will loop in the network. If network loop happens, spanning tree protocol will block one connection in the loop automatically. But it will also cause a period of delay (30 seconds for STP and shorter time for RSTP) if any network connection is changed because of the network topology detection operation of the protocol.

Because there could be more than one switch in the network, users can configure this function for their network spanning tree application.

4. Port Mirror

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

5. QoS

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

6. Static Mac ID in ARL table

The switch can learn the Mac address from user's packets and keep these Mac address in the ARL table for store-and-forward table lookup operation. But these Mac addresses will be deleted from ARL table after some time when users do not send any packets to the switch. This operation is called aging and the time is called aging time. It is about 5 minutes normally (it could be changed by users.) If users want to keep a Mac address always in ARL table on some port, they can assign the Mac address to ARL table. These Mac ID are called Static Mac address. This switch supports static Mac address assignment. The static Mac address assignment will also limit the Mac address could be

used on the assigned port only with the port security configuration function. For example, assigning "00-00-e2-11-22-33" to Port 5 will always keep this Mac ID alive on Port 5 but also limit this Mac address could work on Port 5 only.

Note: About Static Mac Address Filter-in (port binding) function

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

7. Dynamic Mac ID Number Limit

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

8. IEEE 802.1x Port Security Function

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

9. Rate Control

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

10. IP Multicast with IGMP Snooping

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

11. MVR (Multicast VLAN Registration)

VLAN function will isolate traffic between VLAN groups. But it will also isolate IP multicast traffic for subscribers in different VLANs. The MVR function allows one

multicast VLAN to be shared by subscribers in different VLANs. That can reduce the multicast traffic for VLANs.

12. IP Source Guard

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

13. ACL (Access Control List)

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

14. LLDP (Link Layer Discover Protocol)

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

15. Software Backup/Update

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

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

1.2 General Features

- All 1G Ethernet ports are tri-speed 10/100/1000 Mbps ports for RJ-45 port
- Fully non-blocking wire-speed switching performance for all frame sizes
- Eight priorities and eight queues per port
- Dual leaky bucket policing per queue and per port
- DWRR scheduler/shaper per queue and per port with a mix of strict and weighted queues

- 256 TCAM-based egress tagging entries
- Up to 256 TCAM-based classification entries for Quality of Service (QoS) and VLAN membership
- Up to 512 host identity entries for source IP guarding
- Energy Efficient Ethernet (IEEE 802.3az) is supported by both the switch core and the internal copper PHYs

1.3 Layer-2 Switching

- 8,192 MAC addresses
- 4,096 VLANs (IEEE 802.1Q)
- Push/pop/translate up to two VLAN tags; translation on ingress and/or on egress
- Up to 256 QoS and VLAN TCAM entries
- 256 VLAN egress tagging TCAM entries
- Link aggregation (IEEE 802.3ad)
- Independent and shared VLAN learning
- Provider Bridging (VLAN Q-in-Q) support (IEEE 802.1ad)
- Rapid Spanning Tree Protocol support (IEEE 802.1w)
- Multiple Spanning Tree Protocol support (IEEE 802.1s)
- Jumbo frame support up to 9.6 kilobytes with programmable MTU per port

1.4 Multicast

- 8K IPv4/IPv6 multicast groups
- Internet Group Management Protocol version 2 (IGMPv2) support
- Internet Group Management Protocol version 3 (IGMPv3) support with source specific multicast forwarding

1.5 Carrier Ethernet

- Provider Bridge (Q-in-Q) switch 8K MACs, 4K VLANs
- Per port per queue Dual Leaky Bucket Service Policers with PCP or DSCP remarking per Service Point
- Statistics and Tagging options per Service Point

- OAM hardware for generating CCM messages, CCM checking is done by software
- Software for OAM and protection switching

1.6 Quality of Service

- Eight QoS queues per port with strict or deficit weighted round-robin scheduling (DWRR)
- 256 QoS and VLAN TCAM entries
- DSCP translation, both ingress and/or egress
- DSCP remarking based on QoS class and drop precedence level
- VLAN (PCP, DEI, and VID) translation, both ingress and egress
- PCP and DEI remarking based on QoS class and drop precedence level
- Per-queue and per-port policing and shaping, programmable in steps of 100 kbps
- Per-flow policing through TCAM-based pattern matching, up to 256 policers
- Full-duplex flow control (IEEE 802.3X) and half-duplex backpressure, symmetric and asymmetric

1.7 Security

- Generic storm controllers for flooded broadcast, flooded multicast, and flooded unicast traffic
- Port-based and MAC-based access control (IEEE 802.1X)
- Per-port ingress and egress mirroring

1.8 Standard References

This switch uses the following industry references.

Document	Title	Revision
IEEE		
IEEE 802.1ad	802.1Q Amendment 4: Provider Bridges	-2005
IEEE P802.1ag	802.1Q Amendment 5: Connectivity Fault Management (CFM)	Evolving
IEEE 802.1D	Media Access Control (MAC) Bridges	-2004
IEEE 802.1Q	Virtual Bridged Local Area Networks	-2005
IEEE 802.3	Local and metropolitan area networks — Specific requirements Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications	-2008

IEEE 802.3az	Standard for Information Technology – Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications - Amendment: Media Access Control Parameters, Physical Layers and Management Parameters for Energy-Efficient Ethernet	-2010
IEEE 1588	Precision Clock Synchronization Protocol for Networked Measurement and Control Systems	-2008
MEF		
MEF-9	Abstract Test Suite for Ethernet Services at the UNI	October 2004
MEF-10.1	Ethernet Services Attributes Phase 2	November 2006
MEF-14	Abstract Test Suite for Traffic Management Phase 1	November 2005
MEF-16	Ethernet Local Management Interface (E-LMI)	January 2006
ITU-T		
Y.1731	OAM Functions and Mechanisms for Ethernet Based Networks	5/22/2006
G.8261	Timing and Synchronization Aspects in Packet Networks	12/14/2006
IETF		
RFC-2236	Internet Group Management Protocol, Version 2 (IGMPv2)	November 1997
RFC-2710	Multicast Listener Discovery for IPv6 (MLDv1)	October 1999
RFC-2819	Remote Network Monitoring (RMON) MIB	May 2000
RFC-2863	The Interfaces Group MIB	June 2000
RFC-3376	Internet Group Management Protocol, Version 3 (IGMPv3)	October 2002

RFC-3635	Definitions of Managed Objects for Ethernet-like Interface Types	September 2003
Other		
ENG-46158	Cisco Serial GMII (SGMII) Specification	1.7
EDCS-540123	Cisco QSGMII Specification	1.3
JESD79	DDR2 SDRAM Specification	2B

1.9 Front Panel LEDs Indicators

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

LED	Color	State	Indication
Power	Green	ON	-Power on
		OFF	- Power off
Run	Green	OFF	- System failed
		Blinking	-System is ready
Fiber(Link)	Green	ON	-Connection (or link) at 1000Mbps
	Amber	ON	-Connection (or link) at 100Mbps
		OFF	-Disconnection
		Blinking	-Sending & Receiving data

1.10 Rear Panel Connectors

The rear panel is provided the power connector.

2. Hardware Installation

This chapter provides unpacking and installation information for the Switch

2.1 Unpacking

Open the shipping carton and carefully unpack its contents. Please consult the packing list located in the User Manual to make sure all items are present and undamaged. If any item is missing or damaged, please contact your local reseller for replacement.

- One Gigabit Management Switch
- One AC power cord (*for AC power model only)
- One console cable
- This user's manual

If any item is found missing or damaged, please contact the local reseller for replacement.

2.2 Switch Installation

For safe switch installation and operation, it is recommended that you:

- Visually inspect the power cord to see that it is secured fully to the AC power connector.
- Make sure that there is proper heat dissipation and adequate ventilation around the switch.
- Do not place heavy objects on the switch

Desktop Installation

When installing the switch on a desktop, make sure that there is enough ventilation space between the device and the objects around it.

Rack Installation

The switch can be mounted in an EIA standard size 19-inch rack, which can be placed in a wiring closet with other equipment. To install, attach the mounting brackets to the switch's side panels (one on each side) and secure them with the screws provided (please note that these brackets are not designed for palm size switches).

Then, use the screws provided with the equipment rack to mount the switch in the rack.

Please be aware of following safety instructions when installing:

1. Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the

equipment in an environment compatible with the maximum ambient temperature specified by the manufacturer.

2. Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
3. Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
4. Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit, and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

2.3 Adding Module

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

3. Console

The TC-224T Switch allows hyper terminal to perform configuration and monitoring by using the Command Line Interface (CLI) via console port or telnet.

3.1 Console Setup

Step 1: Connect computer to the device through the console port.

Step 2: Open the terminal emulator software (like Hyper-Terminal on Microsoft Windows machine, or "Minicom" on Linux machine), then select the proper COM port for the connection. Set the terminal and port to the following parameters:

- Terminal Mode: VT-100
- Baud rate : 115200 bps
- Data bits : 8
- Parity : None

- Stop bits : 1
- Flow Control : None

Turning on the switch, then after few seconds of machine initialization, the system management terminal will display the login screen as show below.

3.2 Login

```

Serial-COM4 - SecureCRT
File Edit View Options Transfer Script Tools Help
Serial-COM4
+
RedBoot(tm) version V1.16 - built 15:42:57, Nov 18 2013

== Executing boot script in 3.000 seconds - enter ^C to abort
RedBoot> fis load -d managed
Image loaded from 0x80040000-0x80a59048
RedBoot> go

press ENTER to get started

Username: admin
Password:
#
Ready Serial: COM4 13, 3 24 Rows, 80 Cols VT100 NUM

```

- Enter “**admin**” for the switch.
- Without the Password .
- You can see “**#**”.

If you want to set IP address of switch, you can enter configuration mode to setup the IP address as the below.

```

Serial-COM4 - SecureCRT
File Edit View Options Transfer Script Tools Help
Serial-COM4
+
RedBoot(tm) version V1.16 - built 15:42:57, Nov 18 2013

== Executing boot script in 3.000 seconds - enter ^C to abort
RedBoot> fis load -d managed
Image loaded from 0x80040000-0x80a59048
RedBoot> go

press ENTER to get started

Username: admin
Password:
#
co
configure copy
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# ip address 192.168.1.240 255.255.255.0
(config-if-vlan)#
Ready Serial: COM4 18, 19 24 Rows, 80 Cols VT100 NUM

```

- # configureterminal
- (config)# interface vlan 1
- (config-if-vlan)# ip address 192.168.1.240 255.255.255.0
- (config-if-vlan)#

4. Configuring with WEB

You are able to manage the switch with Http Web Browser. The default IP settings is 192.168.0.1 and Net Mask 255.255.255.0. The default Gateway is 0.0.0.0. Before http connection, IP address configuration of the switch should be changed first.

1. Please follow the instruction in Section 3.1 to complete the console connection.
2. Login with “admin” (password is also none by default.)
3. Use “show” command to check IP address of the switch first.
4. Enter “show running-config interface vlan 1” command, and the prompt will show the IP address of the switch as the below.

```
# show running-config interface vlan 1
Building configuration...
interface vlan 1
ip address 192.168.0.1 255.255.255.0
end
#.
```

5. If IP address needs to be changed, please login to the configuration mode as the below steps...

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# ip address 192.168.1.240 255.255.255.0
(config-if-vlan)#
```

After IP address configuration done and the switch is connected to network, you are able to start Http connection by entering IP address of the switch in the web browser as the below section.

4.1 Login

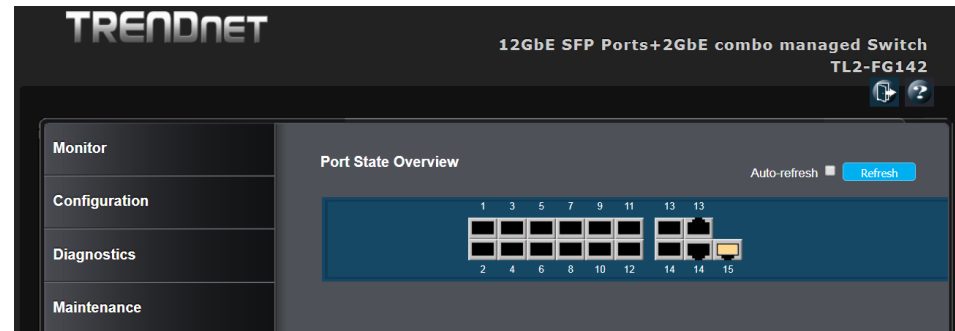
When connected, the Switch has the following pre-configured switch IP addresses "192.168.10.200" as shown below.



To access the Web Utility,

- Configure your PC to the same network segment as the switch. For example, you could set the PC to IP address **192.168.10.x** with a subnet mask of 255.255.255.0.
- Connect the PC to any of LAN port designated 1 to 24 on the Front Panel.
- Open the Web browser.
- Enter the IP address of the GSHDSL in the address field of the browser as example: **http://192.168.10.200** and then press <Enter> to connect.
- There is a default User Name "admin" for the GSHDSL.
- Without password.

Then the management home page will be showed as the below.



4.2 Web Menus

This section introduces how to use web browser to manage the switch. There are 3 areas of the web-based management screen.

Left part of the management screen is a function list. Users can select one of them for status monitoring or switch configuration.

There are four operation groups in the function list.

1. Configuration: provide configure switch.
2. Monitor: get the function status and statistics of the switch.
3. Diagnostics: provide some tools for testing the switch
4. Maintenance: provide the maintenance features, for example firmware upgrade, configuration backup/restore, system reset,...

Middle part of the management screen is the main operation area for each function.

There are two icons logout and help menu at the **Right part of the management screen**.



Logout icon, click to exit the switch.



Help icon, click to get the on-line help menus

4.3 Configuration

The features and functions of the Switch can be configured for optimum use through the Web-based Management Utility.

4.3.1 System

The System Setting allows the user to configure the IP address and the basic system information of the Switch.

4.3.1.1 Information

The switch system information is provided here. In this menu, user can setup the system contact, system name and system location, as below figure.

Items	Description
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-Z a-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character.

	And the first or last character must not be a minus sign. The allowed string length is 0 to 255.
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.

Button



Click to save changes.



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

4.3.1.2 IP

Configure IP basic settings, control IP interfaces and IP routes, as below figure. The maximum number of interfaces supported is 8 and the maximum number of routes is 32.

IP Configuration

Items	Description
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. The following modes are supported: From any DHCP interfaces. The first DNS server offered from a DHCP lease to a DHCP-enabled interface will be used. No DNS server. No DNS server will be used. Configured. Explicitly provide the IP address of the DNS Server in dotted decimal notation. From this DHCP interface. Specify from which DHCP-enabled interface a provided DNS server should be preferred.
DNS Proxy	When DNS proxy is enabled, system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network.

IP Interface

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

Fallback Timeout	DHCP protocol. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.
IPv4 DHCP Fallback Timeout	The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds.
IPv4 DHCP Current Lease	For DHCP interfaces with an active lease, this column show the current interface address, as provided by the DHCP server.
IPv4 Address	The IPv4 address of the interface in dotted decimal notation. If DHCP is enabled, this field is not used. The field may also be left blank if IPv4 operation on the interface is not desired.
IPv4 Mask	The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for a IPv4 address. If DHCP is enabled, this field is not used. The field may also be left blank if IPv4 operation on the interface is not desired.
IPv6 Address	The IPv6 address of the interface. A IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::215:c5ff:fe03:4dc7. The symbol :: is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, ::192.1.2.34. The field may be left blank if IPv6 operation on the interface is not desired.
IPv6 Mask	The IPv6 network mask, in number of bits (prefix length). Valid values are between 1 and 128 bits for a IPv6 address. The field may be left blank if IPv6 operation on the interface is not desired.

Button

Add Interface

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

IP Routes

Items	Description
Delete	Select this option to delete an existing IP route.
Mask Length	The destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bits respectively 128 for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything).
Gateway	The IP address of the IP gateway. Valid format is dotted decimal notation or a valid IPv6 notation. Gateway and Network must be of the same type.
Next Hop VLAN (Only for IPv6)	The VLAN ID (VID) of the specific IPv6 interface associated with the gateway. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid. If the IPv6 gateway address is link-local, it must specify the next hop VLAN for the gateway. If the IPv6 gateway address is not link-local, system ignores the next hop VLAN for the gateway.

Button

Add Interface

Click to add a new IP route. A maximum of 32 routes is supported.

Save

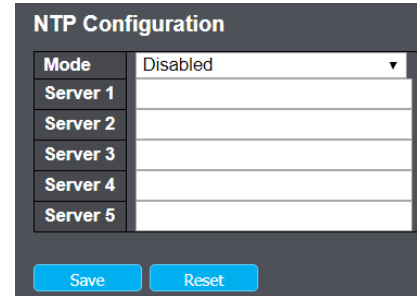
Click to save changes.

Reset

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

4.3.1.3 NTP

NTP is an acronym for Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer. Configure NTP on this page.



Items	Description
Mode	Indicates the NTP mode operation. Possible modes are: Enabled: Enable NTP client mode operation. Disabled: Disable NTP client mode operation.
Server #	Provide the IPv4 or IPv6 address of a NTP server. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, ':::192.1.2.34'.

Button

Save

Click to save changes.

Reset

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

4.3.1.4 Time

This page allows you to configure the Time Zone.

Time Zone Configuration

Time Zone Configuration

Time Zone: None (dropdown menu)

Acronym: (0 - 16 characters)

Daylight Saving Time Configuration

Daylight Saving Time Mode

Daylight Saving Time: Disabled (dropdown menu)

Start Time settings

Month: Jan (dropdown menu)

Date: 1 (dropdown menu)

Year: 2000 (dropdown menu)

Hours: 0 (dropdown menu)

Minutes: 0 (dropdown menu)

End Time settings

Month: Jan (dropdown menu)

Date: 1 (dropdown menu)

Year: 2000 (dropdown menu)

Hours: 0 (dropdown menu)

Minutes: 0 (dropdown menu)

Offset settings

Offset: 1 (1 - 1440) Minutes

Save Reset

[Time Zone Configuration](#)

Items	Description
Time Zone	Lists various Time Zones worldwide. Select appropriate Time Zone from the drop down and click Save to set..
Acronym	User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range : Up to 16 characters)

[Daylight Saving Time Configuration](#)

This page is used to setup Daylight Saving Time Configuration

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

[Start time settings](#)

Items	Description
Week	Select the starting week number.
Day	Select the starting day.
Month	Select the starting month.
Hours	Select the starting hour.
Minutes	Select the starting minute.

[End time settings](#)

Items	Description
Week	Select the ending week number.
Day	Select the ending day.
Month	Select the ending month.
Hours	Select the ending hour.
Minutes	Select the ending minute.

[Offset settings](#)

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

[Button](#)

Save

Click to save changes.

Reset

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

4.3.1.5 Log

Configure System Log on this page.

System Log Configuration

Server Mode	Disabled ▾
Server Address	<input style="width: 100%;" type="text"/>
Syslog Level	Info ▾

Save
Reset

Items	Description
Server Mode	Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are: Enabled: Enable server mode operation. Disabled: Disables server mode operation.
Server Address	Indicates the IPv4 host address of syslog server. If the switch provide DNS feature, it also can be a host name.
Syslog Level	Indicates what kind of message will send to syslog server. Possible modes are: Info: Send information, warnings and errors. Warning: Send warnings and errors. Error: Send errors.

Button

Save

Click to save changes.

Reset

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

4.3.2 Green Ethernet

Green Ethernet is a feature that reduces energy consumption on the switch. This way, the switch is more environmentally friendly, and your costs to run the switch are reduced. This section explains how to configure Green Ethernet on the Managed Switch.

4.3.2.1 Port Power Savings

Before introduce this feature, let us talk about EEE.

What is EEE?

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

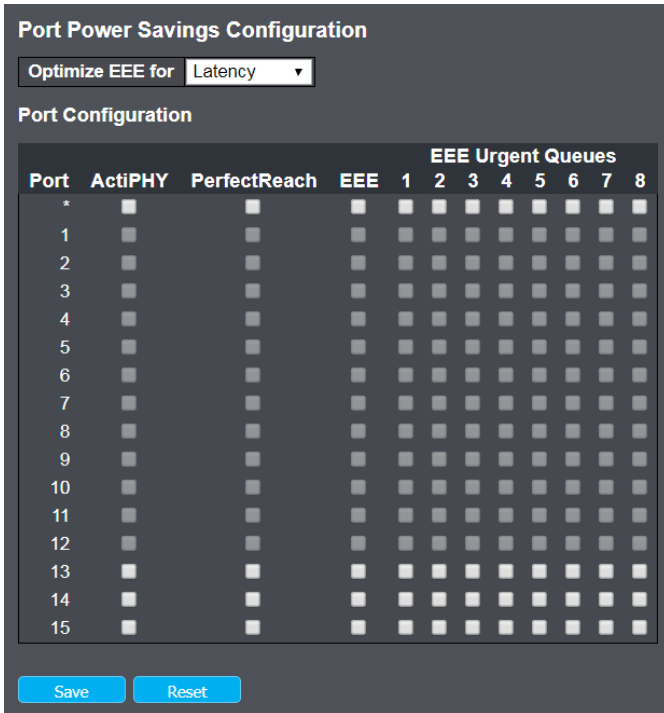
EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted all circuits are powered up. The time it takes to power up the circuits is named wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree 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.

This page allows the user to configure the port power savings features.



Port Power Savings Configuration

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

Port Configuration

Items	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 power up for short moment in order to determine if cable is inserted.

Perfect Reach	Cable length power savings enabled. Perfect Reach works by determining the cable length and lowering the power for ports with short cables.
EEE	Controls whether EEE is enabled for this switch port. For maximizing power savings, the circuit isn't started at once transmit data is ready for a port, but is instead queued until a burst of data is ready to be transmitted. This will give some traffic latency. If desired it is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.
EEE Urgent Queues	Queues set will activate transmission of frames as soon as data is available. Otherwise the queue will postpone transmission until a burst of frames can be transmitted.

Button



Click to save changes.



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

4.3.3 Port

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

Port Configuration Refresh

Port	Link	Current	Speed		Flow Control		Maximum Frame Size	Excessive Collision Mode
			Configured	Current Rx	Current Tx	Configured		
*			<>				9600	<>
1	Down	Down	Auto	X	X		9600	
2	Down	Down	Auto	X	X		9600	
3	Down	Down	Auto	X	X		9600	
4	Down	Down	Auto	X	X		9600	
5	Down	Down	Auto	X	X		9600	
6	Down	Down	Auto	X	X		9600	
7	Down	Down	Auto	X	X		9600	
8	Down	Down	Auto	X	X		9600	
9	Down	Down	Auto	X	X		9600	
10	Down	Down	Auto	X	X		9600	
11	Down	Down	Auto	X	X		9600	
12	Down	Down	Auto	X	X		9600	
13	Down	Down	Auto	X	X		9600	Discard
14	Down	Down	Auto	X	X		9600	Discard
15	100fdx	Up	Auto	X	X		9600	Discard

Save Reset

Port Configuration

Items	Description
Port	This is the logical port number for this row.
Link	The current link state is displayed graphically. Green indicates the link is up and red that it is down.
Current	Provides the current link speed of the port.
Configured	<p>Selects any available link speed for the given switch port. Only speeds supported by the specific port is shown. Possible speeds are:</p> <p>Disabled - Disables the switch port operation.</p> <p>Auto - Port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner.</p> <p>10Mbps HDX - Forces the cu port in 10Mbps half duplex mode.</p> <p>10Mbps FDX - Forces the cu port in 10Mbps full duplex mode.</p> <p>100Mbps HDX - Forces the cu port in 100Mbps half duplex mode.</p> <p>100Mbps FDX - Forces the cu port in 100Mbps full duplex mode.</p> <p>1Gbps FDX - Forces the port in 1Gbps full duplex</p>

	<p>2.5Gbps FDX - Forces the Serdes port in 2.5Gbps full duplex mode.</p> <p>SFP_Auto_AMS - Automatically determines the speed of the SFP. Note: There is no standardized way to do SFP auto detect, so here it is done by reading the SFP rom. Due to the missing standardized way of doing SFP auto detect some SFPs might not be detectable. The port is set in AMS mode. Cu port is set in Auto mode.</p> <p>100-FX - SFP port in 100-FX speed. Cu port disabled.</p> <p>100-FX_AMS - Port in AMS mode. SFP port in 100-FX speed. Cu port in Auto mode.</p> <p>1000-X - SFP port in 1000-X speed. Cu port disabled.</p> <p>1000-X_AMS - Port in AMS mode. SFP port in 1000-X speed. Cu port in Auto mode.</p> <p>Ports in AMS mode with 1000-X speed has Cu port preferred.</p> <p>Ports in AMS mode with 1000-X speed has fiber port preferred.</p> <p>Ports in AMS mode with 100-FX speed has fiber port preferred.</p>
Flow Control Configured	<p>When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner.</p> <p>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.</p> <p>Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.</p>
Maximum Frame Size	Enter the maximum frame size allowed for the switch port, including FCS.
Excessive Collision Mode	<p>Configure port transmit collision behavior.</p> <p>Discard: Discard frame after 16 collisions (default).</p> <p>Restart: Restart back off algorithm after 16 collisions.</p>

Button

Save Click to save changes.

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

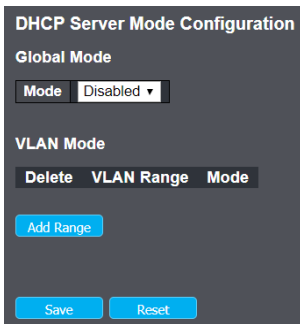
Refresh Click to refresh the page. Any changes made locally will be undone.

4.3.4 DHCP

DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

4.3.4.1 Server-Mode

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.

Items	Description
Mode	Configure the operation mode per system. Possible modes are: Enabled: Enable DHCP server per system. Disabled: Disable DHCP server pre system.

VLAN Mode

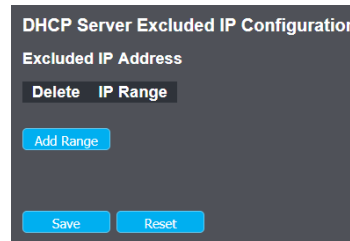
Configure operation mode to enable/disable DHCP server per VLAN.

Items	Description
-------	-------------

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 existed 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	Indicate the the operation mode per VLAN. Possible modes are: Enabled: Enable DHCP server per VLAN. Disabled: Disable DHCP server pre VLAN.

4.3.4.2 Server-Excluded IP

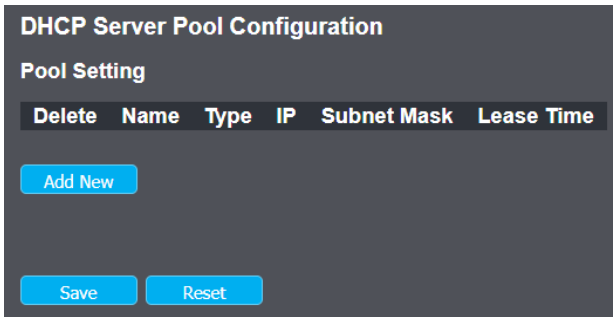
This page configures excluded IP addresses. DHCP server will not allocate these excluded IP addresses to DHCP client.



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

4.3.4.3 Server-pool

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



Add or delete pools.

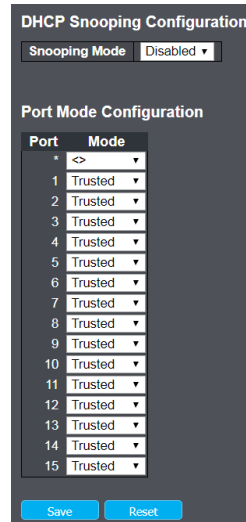
Adding a pool and giving a name is to create a new pool with "default" configuration. If you want to configure all settings including type, IP subnet mask and lease time, you can click the pool name to go into the configuration page.

Items	Description
Name	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.
Type	Display which type of the pool is. Network: the pool defines a pool of IP addresses to service more than one DHCP client. Host: the pool services for a specific DHCP client identified by client identifier or hardware address. If "-" is displayed, it means not defined.
IP	Display network number of the DHCP address pool. If "-" is displayed, it means not defined.
Subnet Mask	Display subnet mask of the DHCP address pool. If "-" is displayed, it means not defined

Lease Time	Display lease time of the pool.
------------	---------------------------------

4.3.4.4 Snooping

Configure DHCP Snooping on this page.



Items	Description
Snooping Mode	Indicates the DHCP snooping mode operation. Possible modes are: 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: Disable DHCP snooping mode operation.
Port Mode Configuration	Indicates the DHCP snooping port mode. Possible port modes are: Trusted: Configures the port as trusted source of the DHCP messages. Untrusted: Configures the port as untrusted source of the DHCP messages.

4.3.4.5 Relay

A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain. It stores the incoming interface IP address in the GIADDR field of the DHCP packet. The DHCP server can use the value of GIADDR field to determine the assigned subnet. For such condition, please make sure the switch configuration of VLAN interface IP address and PVID(Port VLAN ID) correctly.

The screenshot shows a configuration window titled "DHCP Relay Configuration". It contains four rows of settings, each with a label and a dropdown menu:

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

At the bottom of the window are two buttons: "Save" and "Reset".

Items	Description
Relay Mode	Indicates the DHCP relay mode operation. Possible modes are: Enabled: Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations. Disabled: Disable DHCP relay mode operation. Relay Server
Relay Server	Indicates the DHCP relay server IP address.
Relay Information Mode	Indicates the DHCP relay information mode option operation. The option 82 circuit ID format as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID (in standalone device it always equal 0, in stackable device it means switch ID), and the last two characters are the port number. For example, "00030108" means the DHCP message receive from VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal the switch MAC address.

	<p>Possible modes are:</p> <p>Enabled: Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.</p> <p>Disabled: Disable DHCP relay information mode operation.</p>
Relay Information Policy	<p>Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' policy is invalid when relay information mode is disabled. Possible policies are:</p> <p>Replace: Replace the original relay information when a DHCP message that already contains it is received.</p> <p>Keep: Keep the original relay information when a DHCP message that already contains it is received.</p> <p>Drop: Drop the package when a DHCP message that already contains relay information is received.</p>

4.3.5 Security

There are several security features that have been embedded in switch software. There are switch, network and AAA.

4.3.5.1 User

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.

The screenshot shows a configuration window titled "Users Configuration". It contains a table with two columns: "User Name" and "Privilege Level".

User Name	Privilege Level
admin	15

Below the table is an "Add User" button.

The displayed values for each user are:

Items	Description
-------	-------------

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

Button

Add New User

Click to add a new user.

4.3.5.2 Privilege Levels

This page provides an overview of the privilege levels.

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
Dhcp_Client	5	10	5	10
Diagnostics	5	10	5	10
EEE	5	10	5	10
EPS	5	10	5	10
ERPS	5	10	5	10
ETH_LINK_OAM	5	10	5	10
EVC	5	10	5	10
Fan_Control	5	10	5	10
Green_Ethernet	5	10	5	10
IP2	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
Maintenance	15	15	15	15
MEP	5	10	5	10
Mirroring	5	10	5	10
MVR	5	10	5	10
NTP	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10
QoS	5	10	5	10
RFC2544	5	10	5	10
RPC	5	10	5	10
Security	5	10	5	10
sFlow	5	10	5	10
Spanning_Tree	5	10	5	10
System	5	10	1	10
Timer	5	10	5	10
VCL	5	10	5	10
VLAN_Translation	5	10	5	10
VLANs	5	10	5	10
Voice_VLAN	5	10	5	10
XXRP	5	10	5	10

Save Reset

Items	Description
Group Name	The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of

	<p>them contains more than one. The following description defines these privilege level groups in details:</p> <p>System: Contact, Name, Location, Timezone, Daylight Saving Time, Log.</p> <p>Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard.</p> <p>IP: Everything except 'ping'.</p> <p>Port: Everything except 'VeriPHY'.</p> <p>Diagnostics: 'ping' and 'VeriPHY'.</p> <p>Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.</p> <p>Debug: Only present in CLI.</p>
Privilege Levels	<p>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 same or greater than the authorization Privilege level to have the access to that group.</p>

Button



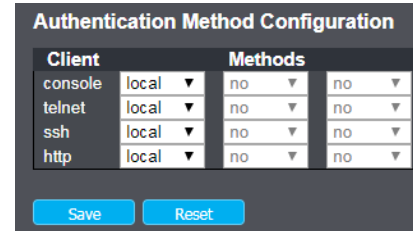
Click to save changes.



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

4.3.5.3 Authentication Method Configuration

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



The table has one row for each client type and a number of columns, which are:

Items	Description
Client	The management client for which the configuration below applies.
Methods	<p>Method can be set to one of the following values:</p> <p>no: Authentication is disabled and login is not possible.</p> <p>local: Use the local user database on the switch for authentication.</p> <p>radius: Use remote RADIUS server(s) for authentication.</p> <p>tacacs+: Use remote TACACS+ server(s) for authentication.</p> <p>Methods that involves remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.</p>

Button



Click to save changes.



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

4.3.5.4 SSH Configuration

Configure SSH on this page.

SSH Configuration

Mode

Items	Description
Mode	Indicates the SSH mode operation. Possible modes are: Enabled: Enable SSH mode operation. Disabled: Disable SSH mode operation.

Button

Click to save changes.

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

4.3.5.5 HTTPS Configuration

Configure HTTPS on this page.

HTTPS Configuration

Mode

Automatic Redirect

Items	Description
Mode	Indicates the HTTPS mode operation. When the current connection is HTTPS, to apply HTTPS disabled mode operation will automatically redirect web browser to an HTTP connection. Possible modes are: Enabled: Enable HTTPS mode operation. Disabled: Disable HTTPS mode operation.
Automatic Redirect	Indicates the HTTPS redirect mode operation. It only significant if HTTPS mode "Enabled" is selected. Automatically redirects web browser to an

	HTTPS connection when both HTTPS mode and Automatic Redirect are enabled. Possible modes are: Enabled: Enable HTTPS redirect mode operation. Disabled: Disable HTTPS redirect mode operation.
--	---

Button

Click to save changes.

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

4.3.5.6 Access Management Configuration

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

Access Management Configuration

Mode

Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
<input type="button" value="Add Entry"/>						

Items	Description
Mode	Indicates the access management mode operation. Possible modes are: Enabled: Enable access management mode operation. Disabled: Disable access management mode operation.
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.

Button

Add New Entry

Click to add a new access management entry.

Save

Click to save changes.

Reset

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

4.3.5.7 Limit Control

This page allows you to configure the Port Security Limit Control system and port settings.

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

Items	Description
Mode	Indicates if Limit Control is globally enabled or disabled on the switch. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.
Aging Enabled	If checked, secured MAC addresses are subject to aging as discussed under Aging Period.
Aging Period	If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying 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.

The Aging Period can be set to a number between 10 and 10,000,000 seconds.

To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the correspon

Port Configuration

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

Items	Description
Port	The port number to which the configuration below applies.
Mode	Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.
Limit	The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken. The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.
Action	If Limit is reached, the switch can take one of the following actions: None: Do not allow more than Limit MAC addresses on the port, but take no further action.

Trap: If Limit + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded.

Shutdown: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:

- 1) Boot the switch,
- 2) Disable and re-enable Limit Control on the port or the switch,
- 3) Click the Reopen button.

Trap & Shutdown: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.

State	This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values: Disabled: Limit Control is either globally disabled or disabled on the port. Ready: The limit is not yet reached. This can be shown for all actions. Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if Action is set to None or Trap. Shutdown: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown.
Re-open Button	If a port is 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.

4.3.5.8NAS

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

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

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

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

Network Access Server Configuration Refresh

System Configuration

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

Port Configuration

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

Save
Reset

System Configuration

Items	Description
Mode	Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.
Reauthentication Enabled	<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>
Reauthentication Period	Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.
EAPOL Timeout	<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>
Aging Period	<p>This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:</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>
Hold Time	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:

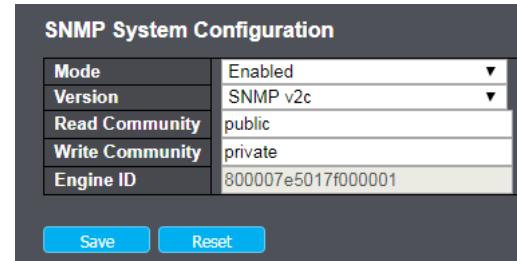
	<ul style="list-style-type: none"> • Single 802.1X • Multi 802.1X • MAC-Based Auth. <p>If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration→Security→AAA" page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication.</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>
RADIUS-Assigned QoS Enabled	<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>
RADIUS-Assigned VLAN Enabled	<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 RADIUS-Assigned VLAN Enabled 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.</p>

	When unchecked, RADIUS-server assigned VLAN is disabled on all ports.
Guest VLAN Enabled	<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 "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.</p>
Guest VLAN ID	<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>
Max. Reauth. Count	<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>
Allow Guest VLAN if EAPOL Seen	<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>

4.3.6 SNMP

4.3.6.1 System

Configure SNMP on this page.



Items	Description
Mode	<p>Indicates the SNMP mode operation. Possible modes are:</p> <p>Enabled: Enable SNMP mode operation.</p> <p>Disabled: Disable SNMP mode operation.</p>
Version	<p>Indicates the SNMP supported version. Possible versions are:</p> <p>SNMP v1: Set SNMP supported version 1.</p> <p>SNMP v2c: Set SNMP supported version 2c.</p> <p>SNMP v3: Set SNMP supported version 3.</p>
Read Community	<p>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.</p> <p>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.</p>
Write Community	<p>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.</p> <p>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</p>

	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 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.

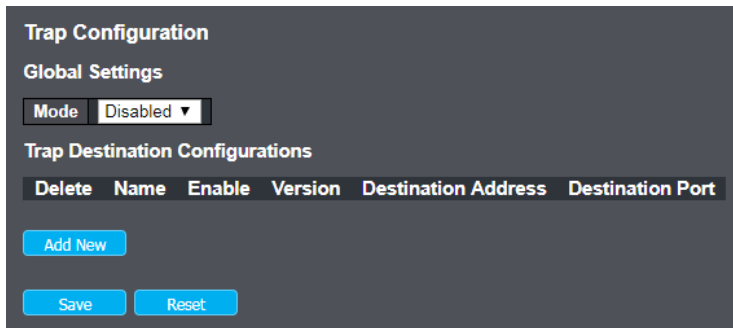
Button

Click to save changes.

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

4.3.6.2 Trap

Configure SNMP trap on this page.



Global Settings

Items	Description
Mode	Indicates the SNMP trap mode operation. Possible modes are: Enabled: Enable SNMP trap mode operation. Disabled: Disable SNMP trap mode operation.

Trap Destination Configurations

Configure trap destinations on this page.

Items	Description
Name	Indicates the trap Configuration's name. Indicates the trap destination's name.
Enable	Indicates the trap destination mode operation. Possible modes are: Enabled: Enable SNMP trap mode operation. Disabled: Disable SNMP trap mode operation.
Version	Indicates the SNMP trap supported version. Possible versions are: SNMPv1: Set SNMP trap supported version 1. SNMPv2c: Set SNMP trap supported version 2c. SNMPv3: Set SNMP trap supported version 3.
Trap Community	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.
Destination Address	Indicates the SNMP trap destination address. It allow 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.

Button

Add New Entry Click to add a new access management entry.

Save Click to save changes.

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

4.3.6.3 Communit

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

SNMPv3 Community Configuration

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
Save
Reset

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

Button

Add New Entry Click to add a new access management entry.

Save Click to save changes.

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

4.3.6.4 User

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

SNMPv3 User Configuration

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

Add New
Save
Reset

Items	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Engine ID	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with 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 usm User Engine ID and usm User Name are the entry's keys. In a simple agent, usm User Engine ID is always that agent's own snmp Engine ID value. The value can also take the value of the snmp Engine ID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user.
User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Security Level	Indicates the security model that this entry should belong to. Possible security models are: NoAuth, NoPriv: No authentication and no privacy. Auth, NoPriv: Authentication and no privacy. Auth, Priv: Authentication and privacy.

	The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.
Authentication Protocol	<p>Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:</p> <p>None: No authentication protocol.</p> <p>MD5: An optional flag to indicate that this user uses MD5 authentication protocol.</p> <p>SHA: An optional flag to indicate that this user uses SHA authentication protocol.</p> <p>The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.</p>
Authentication Password	<p>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.</p> <p>Privacy Protocol</p> <p>Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:</p> <p>None: No privacy protocol.</p> <p>DES: An optional flag to indicate that this user uses DES authentication protocol.</p> <p>AES: An optional flag to indicate that this user uses AES authentication protocol.</p>
Privacy Password	A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.

Button

Click to add a new access management entry.

Click to save changes.

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

4.3.6.5 Group

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

SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
<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

Items	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Security Model	<p>Indicates the security model that this entry should belong to. Possible security models are:</p> <p>v1: Reserved for SNMPv1.</p> <p>v2c: Reserved for SNMPv2c.</p> <p>usm: User-based Security Model (USM).</p>
Security Name	A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Button

Click to add a new access management entry.

Click to save changes.

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

4.3.6.6 View

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

Items	Description
Delete	Check to delete the entry. It will be deleted during the next save.
View Name	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
View Type	Indicates the view type that this entry should belong to. Possible view types are: included: An optional flag to indicate that this view subtree should be included. excluded: An optional flag to indicate that this view subtree should be excluded. In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and it's OID subtree should overstep the 'excluded' view entry.
OID Subtree	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

Button

Add New Entry

Click to add a new access management entry.

Save

Click to save changes.

Reset

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

4.3.6.7 Access

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

Items	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: any: Any security model accepted(v1 v2c usm). v1: Reserved for SNMPv1. v2c: Reserved for SNMPv2c. usm: User-based Security Model (USM).
Security Level	Indicates the security model that this entry should belong to. Possible security models are: NoAuth, NoPriv: No authentication and no privacy. Auth, NoPriv: Authentication and no privacy. Auth, Priv: Authentication and privacy.
Read View Name	The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Write View Name	The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
-----------------	--

Button

Add New Entry

Click to add a new access management entry.

Save

Click to save changes.

Reset

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

4.3.7 RMON

4.3.7.1 Statistics

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

Items	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Data Source	Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005

Button

Add New Entry

Click to add a new access management entry.

Save

Click to save changes.

Reset

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

4.3.7.2 History

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

Items	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Data Source	Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005
Interval	Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.
Buckets	Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600, default value is 50.
Buckets Granted	The number of data shall be saved in the RMON.

Button

Add New Entry

Click to add a new access management entry.

Save

Click to save changes.

Reset

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

4.3.7.3 Alarm

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

Items	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Interval	Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^31-1.
Variable	Indicates the particular variable to be sampled, the possible variables are: InOctets: The total number of octets received on the interface, including framing characters. InUcastPkts: The number of uni-cast packets delivered to a higher-layer protocol. InNUcastPkts: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol. InDiscards: The number of inbound packets that are discarded even the packets are normal. InErrors: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. InUnknownProtos: the number of the inbound packets that were discarded because of the unknown or un-support protocol. OutOctets: The number of octets transmitted out of the interface , including framing characters. OutUcastPkts: The number of uni-cast packets that request to transmit. OutNUcastPkts: The number of broad-cast and multi-cast packets that request to transmit. OutDiscards: The number of outbound packets that are discarded event the packets is normal. OutErrors: The The number of outbound packets that could not be transmitted because of errors. OutQlen: The length of the output packet queue (in packets).
Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: Absolute: Get the sample directly.

	Delta: Calculate the difference between samples (default).
Value	The value of the statistic during the last sampling period.
Startup Alarm	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: RisingTrigger alarm when the first value is larger than the rising threshold. FallingTrigger alarm when the first value is less than the falling threshold. RisingOrFallingTrigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).
Rising Threshold	Rising threshold value (-2147483648-2147483647).
Rising Index	Rising event index (1-65535).
Falling Threshold	Falling threshold value (-2147483648-2147483647)
Falling Index	Falling event index (1-65535).

Button

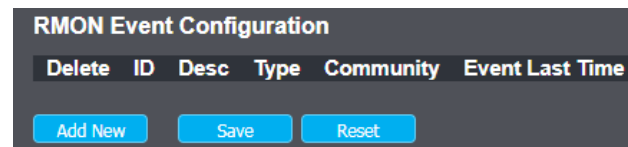
Click to add a new access management entry.

Click to save changes.

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

4.3.7.4 Event

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



Items	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.

Desc	Indicates this event, the string length is from 0 to 127, default is a null string.
Type	Indicates the notification of the event, the possible types are: none: The total number of octets received on the interface, including framing characters. log: The number of uni-cast packets delivered to a higher-layer protocol. snmptrap: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol. logandtrap: The number of inbound packets that are discarded even the packets are normal.
Community	Specify the community when trap is sent, the string length is from 0 to 127, default is "public".
Event Last Time	Indicates the value of sysUpTime at the time this event entry last generated an event.

Button

Add New Entry

Click to add a new access management entry.

Save

Click to save changes.

Reset

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

4.3.8 ACL

4.3.8.1 Ports

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.

Items	Description
Port	The logical port for the settings contained in the same row.
Policy ID	Select the policy to apply to this port. The allowed values are 0 through 255. The default value is 0.
Action	Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".
Rate Limiter ID	Select which rate limiter to apply on this port. The allowed values are Disabled or the values 1 through 16. The default value is "Disabled".

EVC Policer	Select whether EVC policer is enabled or disabled. The default value is "Disabled".
EVC Policer ID	Select which EVC policer ID to apply on this port. The allowed values are Disabled or the values 1 through 256.
Port Redirect	Select which port frames are redirected on. The allowed values are Disabled or a specific port number and it can't be set when action is permitted. The default value is "Disabled".
Mirror	Specify the mirror operation of this port. The allowed values are: Enabled: Frames received on the port are mirrored. Disabled: Frames received on the port are not mirrored. The default value is "Disabled".
Logging	Specify the logging operation of this port. The allowed values are: Enabled: Frames received on the port are stored in the System Log. Disabled: Frames received on the port are not logged. The default value is "Disabled". Please note that the System Log memory size and logging rate is limited.
Shutdown	Specify the port shut down operation of this port. The allowed values are: Enabled: If a frame is received on the port, the port will be disabled. Disabled: Port shut down is disabled. The default value is "Disabled".
State	Specify the port state of this port. The allowed values are: Enabled: To reopen ports by changing the volatile port configuration of the ACL user module. Disabled: To close ports by changing the volatile port configuration of the ACL user module. The default value is "Enabled".
Counter	Counts the number of frames that match this ACE.

Button



Click to save changes.



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



Click to refresh the page. Note that non-committed changes will be lost.



Click to clear the counters.

4.3.8.2 Rate Limiters

Configure the rate limiter for the ACL of the switch.

ACL Rate Limiter Configuration

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

Items	Description
Rate Limiter ID	The rate limiter ID for the settings contained in the same row.
Rate	The allowed values are: 0-3276700 in pps or 0, 100, 200, 300, ..., 1000000 in kbps.

Action	Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".
Unit	Specify the rate unit. The allowed values are: pps: packets per second. kbps: Kbits per second.

Button



Click to save changes.



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







4.3.8.3 Access Control List

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 256 on each switch.

Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed and the priority is highest.

Items	Description
Ingress Port	Indicates the ingress port of the ACE. Possible values are: All: The ACE will match all ingress port. Port: The ACE will match a specific ingress port.
Policy / Bitmask	Indicates the policy number and bitmask of the ACE.
Frame Type	Indicates the frame type of the ACE. Possible values are: Any: The ACE will match any frame type.

	<p>EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.</p> <p>ARP: The ACE will match ARP/RARP frames.</p> <p>IPv4: The ACE will match all IPv4 frames.</p> <p>IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol.</p> <p>IPv4/UDP: The ACE will match IPv4 frames with UDP protocol.</p> <p>IPv4/TCP: The ACE will match IPv4 frames with TCP protocol.</p> <p>IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.</p> <p>IPv6: The ACE will match all IPv6 standard frames.</p>
Action	<p>Indicates the forwarding action of the ACE.</p> <p>Permit: Frames matching the ACE may be forwarded and learned.</p> <p>Deny: Frames matching the ACE are dropped.</p> <p>Filter: Frames matching the ACE are filtered.</p>
Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.
Port Redirect	Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.
Mirror	<p>Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are:</p> <p>Enabled: Frames received on the port are mirrored.</p> <p>Disabled: Frames received on the port are not mirrored.</p> <p>The default value is "Disabled".</p>
Counter	The counter indicates the number of times the ACE was hit by a frame.
Modification Buttons	<p>You can modify each ACE (Access Control Entry) in the table using the following buttons:</p> <p>Add: Inserts a new ACE before the current row.</p> <p>Edit: Edits the ACE row.</p> <p>Up: Moves the ACE up the list.</p>

	Down: Moves the ACE down the list.
	Delete: Deletes the ACE.
	Add: The lowest plus sign adds a new entry at the bottom of the ACE listings.
	
	
	

Button

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

Refresh Click to refresh the page; any changes made locally will be undone.

Clear Click to clear the counters.

Remove All Click to remove all ACEs.

ACE Configuration

Configure an ACE (Access Control Entry) on this page.

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.

ACE Configuration

Ingress Port	All Port 1 Port 2 Port 3 Port 4	Action	Permit
Policy Filter	Any	Rate Limiter	Disabled
Frame Type	Any	EVC Policer	Disabled
		Mirror	Disabled
		Logging	Disabled
		Shutdown	Disabled
		Counter	0

VLAN Parameters

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

Items	Description
Ingress Port	Select the ingress port for which this ACE applies. All: The ACE applies to all port. Port n: The ACE applies to this port number, where n is the number of the switch port.
Policy Filter	Specify the policy number filter for this ACE. Any: No policy filter is specified. (policy filter status is "don't-care".) Specific: If you want to filter a specific policy with this ACE, choose this value. Two field for entering an policy value and bitmask appears. Policy Value When "Specific" is selected for the policy filter, you can enter a specific policy value. The allowed range is 0 to 255. Policy Bitmask When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is 0x0 to 0xff.
Frame Type	Select the frame type for this ACE. These frame types are mutually exclusive.

	<p>Any: Any frame can match this ACE.</p> <p>Ethernet Type: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal).</p> <p>ARP: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type.</p> <p>IPv4: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type.</p> <p>IPv6: Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with Ethernet type.</p>
Action	<p>Specify the action to take with a frame that hits this ACE.</p> <p>Permit: The frame that hits this ACE is granted permission for the ACE operation.</p> <p>Deny: The frame that hits this ACE is dropped.</p> <p>Filter: Frames matching the ACE are filtered.</p>
Rate Limiter	Specify the rate limiter in number of base units. The allowed range is 1 to 16. Disabled indicates that the rate limiter operation is disabled.
EVC Policer	<p>Select whether EVC policer is enabled or disabled. The default value is "Disabled".</p> <p>EVC Policer ID</p> <p>Select which EVC policer ID to apply on this ACE. The allowed values are Disabled or the values 1 through 256.</p> <p>Port Redirect</p> <p>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.</p>
Mirror	<p>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. The allowed values are:</p> <p>Enabled: Frames received on the port are mirrored.</p> <p>Disabled: Frames received on the port are not mirrored.</p>

	The default value is "Disabled".
Logging	<p>Specify the logging operation of the ACE. The allowed values are:</p> <p>Enabled: Frames matching the ACE are stored in the System Log.</p> <p>Disabled: Frames matching the ACE are not logged.</p> <p>Please note that the System Log memory size and logging rate is limited.</p>
Shutdown	<p>Specify the port shut down operation of the ACE. The allowed values are:</p> <p>Enabled: If a frame matches the ACE, the ingress port will be disabled.</p> <p>Disabled: Port shut down is disabled for the ACE.</p>
Counter	The counter indicates the number of times the ACE was hit by a frame.

VLAN Parameters

Items	Description
802.1Q Tagged	<p>Specify whether frames can hit the action according to the 802.1Q tagged. The allowed values are:</p> <p>Any: Any value is allowed ("don't-care").</p> <p>Enabled: Tagged frame only.</p> <p>Disabled: Untagged frame only.</p> <p>The default value is "Any".</p>
VLAN ID Filter	<p>Specify the VLAN ID filter for this ACE.</p> <p>Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".)</p> <p>Specific: If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.</p> <p>VLAN ID</p> <p>When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.</p>
Tag Priority	Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7 or range 0-1, 2-3, 4-5, 6-7, 0-3 and 4-7. The value Any means that no tag priority is specified (tag priority is "don't-care").

Button

Click to save changes.

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

Return to the previous page.

4.3.9 IP Source Guard

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

4.3.9.1 IP Source Guard Configuration

This page provides IP Source Guard related configuration.

IP Source Guard Configuration

Mode: ▼

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 ▼

Mode of IP Source Guard Configuration

Items	Description
Mode	Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.

Port Mode Configuration

Items	Description
Mode	Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.
Max Dynamic Clients	Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port.

Button

Click to save changes.

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

Click to translate all dynamic entries to static entries.

4.3.9.2 IP Static Table

This page provides Static IP Source guard configuration.

Static IP Source Guard Table

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

Items	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.

Button

Save

Click to save changes.

Reset

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

Translate dynamic to static

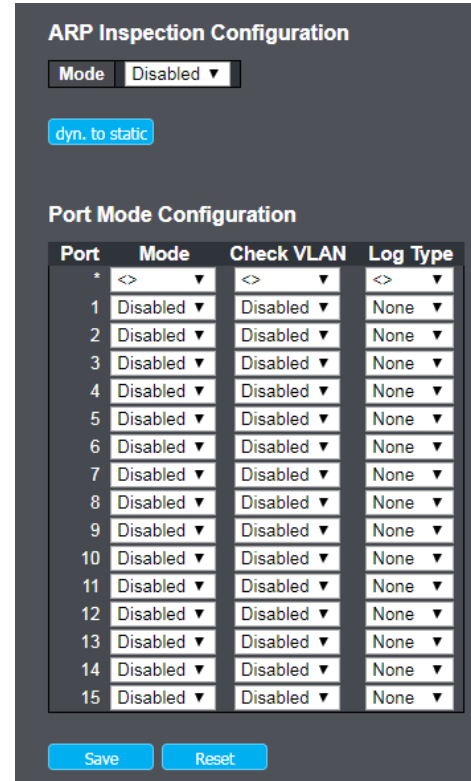
Click to translate all dynamic entries to static entries.

4.3.10 ARP Inspection

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

4.3.10.1 Port Configuration

This page provides ARP Inspection related configuration.



ARP Inspection Configuration

Items	Description
Mode	Enable the Global ARP Inspection or disable the Global ARP Inspection.

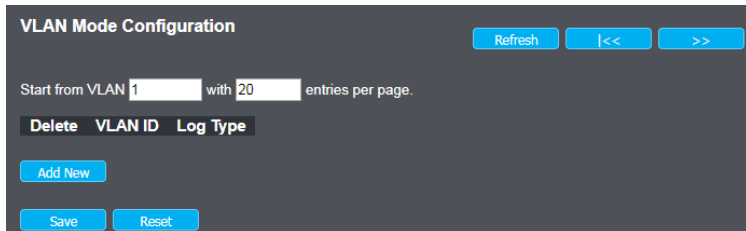
Port Mode Configuration

Items	Description
Mode	Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Possible modes are: Enabled: Enable ARP Inspection operation.

	Disabled: Disable ARP Inspection operation.
Check VLAN	<p>If you want to inspect the VLAN configuration, you have to enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of "Check VLAN" are:</p> <p>Enabled: Enable check VLAN operation.</p> <p>Disabled: Disable check VLAN operation.</p>
Log Type	<p>Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. There are four log types and possible types are:</p> <p>None: Log nothing.</p> <p>Deny: Log denied entries.</p> <p>Permit: Log permitted entries.</p> <p>ALL: Log all entries.</p>

4.3.10.2 VLAN Mode Configuration

This page provides ARP Inspection related 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.

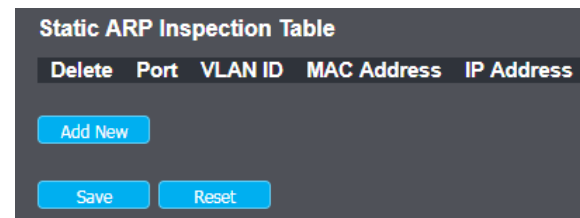
The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the Refresh button will update the displayed table starting from that or the closest next VLAN Table match. The >> will use the next entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the warning message is shown in the displayed table. Use the |<< button to start over.

Items	Description
VLAN ID	<p>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.</p> <p>Possible types are:</p>
Log Type	<p>None: Log nothing.</p> <p>Deny: Log denied entries.</p> <p>Permit: Log permitted entries.</p> <p>ALL: Log all entries.</p>

Button

- Click to add a new VLAN to the ARP Inspection VLAN table.
- Click to save changes.
- Click to undo any changes made locally and revert to previously saved values.

4.3.10.3 Static ARP Inspection Table



Items	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.

Button

Add New Entry Click to add a new VLAN to the ARP Inspection VLAN table.

Save Click to save changes.

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

4.3.10.4 Dynamic ARP Inspection Table

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

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. Clicking the Refresh button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the <<< button to start over

Items	Description
Port	Switch Port Number for which the entries are displayed.
VLAN ID	VLAN-ID in which the ARP traffic is permitted.
VLAN ID	The vlan id for the settings.
MAC Address	User MAC address of the entry.
IP Address	User IP address of the entry.
Translate to static	Select the checkbox to translate the entry to static entry.

Button

Save Click to save changes.

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

4.3.11 AAA

4.3.11.1 RADIUS Server Configuration

This page allows you to configure the RADIUS servers.

Global Configuration

These settings are common for all of the RADIUS servers.

Items	Description
Timeout	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.
Retransmit	Retransmit is the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.
Deatime	Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.
Key	The secret key - up to 63 characters long - shared between the RADIUS server and the switch..
NAS-IP-Address (Attribute 4)	The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.
NAS-IPv6-Address (Attribute 95)	The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.
NAS-Identifier (Attribute 32)	The identifier - up to 255 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.

Server Configuration

The table has one row for each RADIUS server and a number of columns, which are:

Items	Description
-------	-------------

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

Button

Click Add New Server 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.

Click to save changes.

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

4.3.11.2 TACACS+ Server Configuration

This page allows you to configure the TACACS+ servers.

TACACS+ Server Configuration

Global Configuration

Timeout	5	seconds
Deadtime	0	minutes
Key	<input type="text"/>	

Server Configuration

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

Global Configuration

These settings are common for all of the TACACS+ servers.

Items	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, which are:

Items	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.

Button

Click Add New Server 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.

Click to save changes.

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

4.3.12 Aggregation

Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

4.3.12.1 Static

This page is used to configure the Aggregation hash mode and the aggregation group.

Aggregation Mode Configuration

Hash Code Contributors

Source MAC Address

Destination MAC Address

IP Address

TCP/UDP Port Number

Aggregation Group Configuration

Group ID	Port Members														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Normal	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
7	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Save
Reset

Hash Code Contributors

Items	Description
Source MAC Address	The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC
Destination MAC Address	The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled.
IP Address	The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled
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. By default, TCP/UDP Port Number is enabled.

Aggregation Group Configuration

Items	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.

Button

Save

Click to save changes.

Reset

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

4.3.12.2 LACP

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

Items	Description
Port	The switch port number.
LACP Enabled	Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner.
Key	The Key value incurred by the port, range 1-65535. The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.
Role	The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).

Timeout	The Timeout controls the period between BPDUs transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.
Prio	The Prio controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.

Button

Click to save changes.

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

4.3.13 Link OAM

OAM is an acronym for Operation Administration and Maintenance.

It is a protocol described in ITU-T Y.1731 used to implement carrier Ethernet functionality. MEP functionality like CC and RDI is based on this.

4.3.13.1 Port Settings

This page allows the user to inspect the current Link OAM port configurations, and change them as well.

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

Items	Description
Port	The switch port number.
OAM Enabled	Controls whether Link OAM is enabled on this switch port. Enabling Link OAM provides the network operators the ability to monitor the health of the network and quickly determine the location of failing links or fault conditions.
OAM Mode	Configures the OAM Mode as Active or Passive. The default mode is Passive.
Active mode	DTE's configured in Active mode initiate the exchange of Information OAMPDUs as defined by the Discovery process. Once the Discovery process completes, Active DTE's are permitted to send any OAMPDU while connected to a remote OAM peer entity in Active mode. Active DTE's operate in a limited respect if the remote OAM entity is operating

	in Passive mode. Active devices should not respond to OAM remote loopback commands and variable requests from a Passive peer.
Passive mode	DTE's configured in Passive mode do not initiate the Discovery process. Passive DTE's react to the initiation of the Discovery process by the remote DTE. This eliminates the possibility of passive to passive links. Passive DTE's shall not send Variable Request or Loopback Control OAMPDUs.
Loopback Support	Controls whether the loopback support is enabled for the switch port. Link OAM remote loopback can be used for fault localization and link performance testing. Enabling the loopback support will allow the DTE to execute the remote loopback command that helps in the fault detection.
Link Monitor Support	Controls whether the Link Monitor support is enabled for the switch port. On enabling the Link Monitor support, the DTE supports event notification that permits the inclusion of diagnostic information.
MIB Retrieval Support	Controls whether the MIB Retrieval Support is enabled for the switch port. On enabling the MIB retrieval support, the DTE supports polling of various Link OAM based MIB variables' contents.
Loopback Operation	If the Loopback support is enabled, enabling this field will start a loopback operation for the port.

Button

Save

Click to save changes.

Reset

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

4.3.13.2 Event Settings

This page allows the user to inspect the current Link OAM Link Event configurations, and change them as well.

Link Event Configuration for Port 1 Port 1 ▼

Event Name	Error Window	Error Threshold
Error Frame Event	1	1
Symbol Period Error Event	1	1
Seconds Summary Event	60	1

Save
Reset

Items	Description
Port	The switch port number.
Event Name	Name of the Link Event which is being configured.
Error Window	Represents the window period in the order of 1 sec for the observation of various link events.
Error Threshold	Represents the threshold value for the window period for the appropriate Link event so as to notify the peer of this error.
Error Frame Event	The Errored Frame Event counts the number of errored frames detected during the specified period. The period is specified by a time interval (Window in order of 1 sec). This event is generated if the errored frame count is equal to or greater than the specified threshold for that period (Period Threshold). Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Error Frame Event' must be an integer value between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-0xffffffff and its default value is '0'.
Symbol Period Error Event	The Errored Symbol Period Event counts the number of symbol errors that occurred during the specified period. The period is specified by the number of symbols that can be received in a time interval on the underlying physical layer. This event is generated if the symbol error count is equal to or greater than the specified threshold for that period. Error Window for 'Symbol Period Error Event' must be an integer value between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-0xffffffff and its default value is '0'.
Seconds Summary Event	The Errored Frame Seconds Summary Event TLV counts the number of errored frame seconds that occurred during the specified period. The period is specified by a time interval. This event is generated if the number of errored frame seconds is equal to or greater than the

specified threshold for that period. An errored frame second is a one second interval wherein at least one frame error was detected. Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Seconds Summary Event' must be an integer value between 10-900 and its default value is '60'. Whereas Error Threshold must be between 0-0xffff and its default value is '1'.

Button

Save

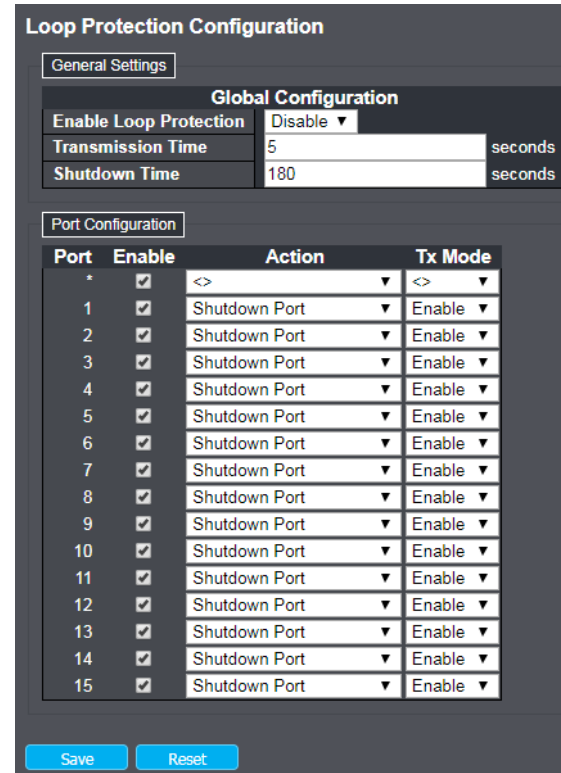
Click to save changes.

Reset

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

4.3.14 Loop Protection

This page allows the user to inspect the current Loop Protection configurations, and possibly change them as well.



General Settings

Items	Description
Enable Loop Protection	Controls whether loop protections is enabled (as a whole).
Transmission Time	The interval between each loop protection PDU sent on each port. valid values are 1 to 10 seconds.
Shutdown Time	The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart).

Port Configuration

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

Button

Save

Click to save changes.

Reset

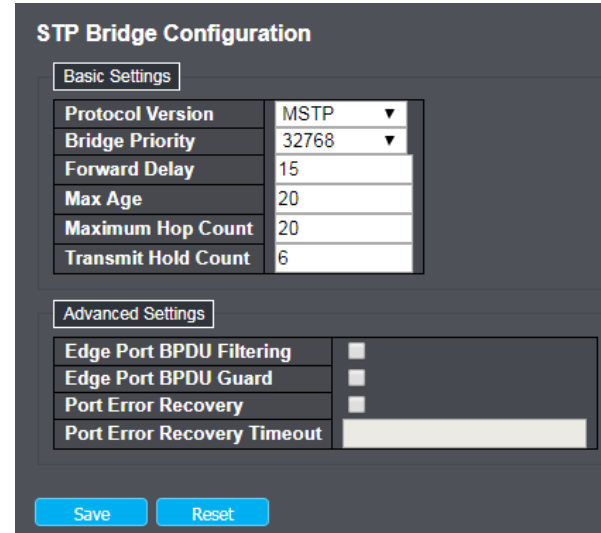
Click to undo any changes made locally and revert to previously saved values.

4.3.15 Spanning Tree

The Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for Ethernet networks. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. Spanning tree also allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling or disabling of these backup links.

4.3.15.1 Bridge Setting

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



Basic Settings

Items	Description
Protocol Version	The MSTP / RSTP / STP protocol version setting. Valid values are STP, RSTP and MSTP.
Bridge Priority	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.
Forward Delay	The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.
Max Age	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and Max Age must be $\leq (FwdDelay-1)*2$.
Maximum Hop Count	This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many

	bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.
Transmit Hold Count	The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.

Advanced Settings

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

Button



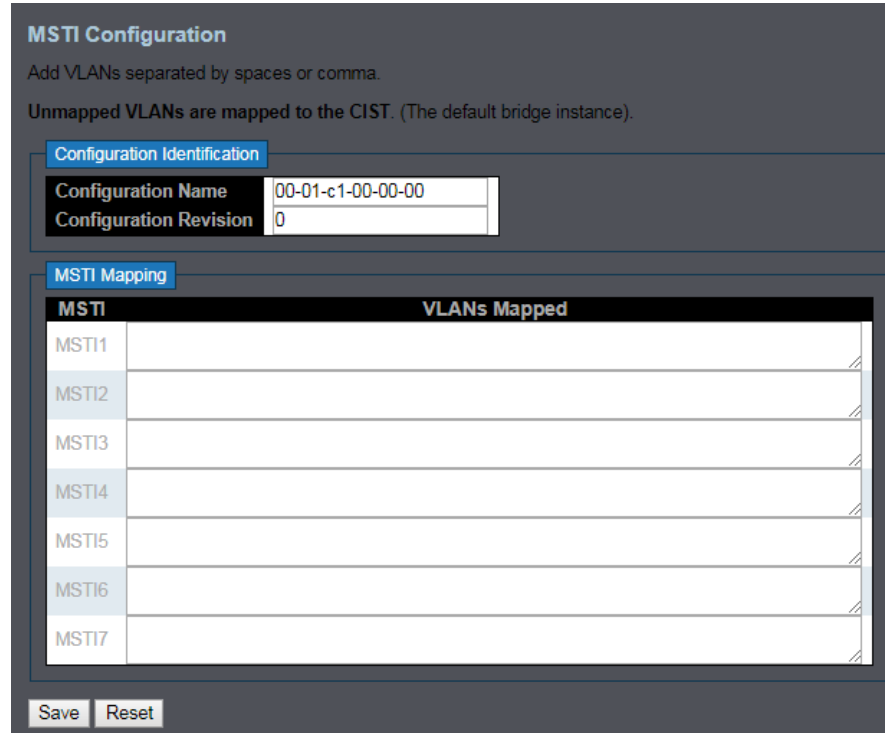
Click to save changes.



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

4.3.15.2 MSTI Mapping

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.



Configuration Identification

Items	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 Mapping

Items	Description
-------	-------------

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

Button

Click to save changes.

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

4.3.15.3 MSTI Priorities

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

MSTI Configuration

MSTI Priority Configuration

MSTI	Priority
*	<>
CIST	32768
MSTI1	32768
MSTI2	32768
MSTI3	32768
MSTI4	32768
MSTI5	32768
MSTI6	32768
MSTI7	32768

Items	Description
-------	-------------

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

Button

Click to save changes.

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

4.3.15.4 CIST Ports

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

STP CIST Port Configuration

CIST Aggregated Port Configuration

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

CIST Normal Port Configuration

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
*	<input checked="" type="checkbox"/>	<>	<>	<>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
2	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
3	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
4	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
5	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
6	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
7	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
8	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
9	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
10	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
11	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
12	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
13	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
14	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
15	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto

This page contains settings for physical and aggregated ports.

Items	Description
Port	The switch port number of the logical STP port.
STP Enabled	Controls whether STP is enabled on this switch port.
Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
operEdge (state flag)	Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having operEdge true) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status.
AdminEdge	Controls whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized).
AutoEdge	Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.
Restricted Role	If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.

Restricted TCN	If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently
BPDU Guard	If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not effect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.
Point-to-Point	Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

Button



Click to save changes.



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

4.3.15.5 MSTI Ports

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

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.

MST1 MSTI Port Configuration

MSTI Aggregated Ports Configuration

Port	Path Cost	Priority
-	Auto	128

MSTI Normal Ports Configuration

Port	Path Cost	Priority
*	<>	<>
1	Auto	128
2	Auto	128
3	Auto	128
4	Auto	128
5	Auto	128
6	Auto	128
7	Auto	128
8	Auto	128
9	Auto	128
10	Auto	128
11	Auto	128
12	Auto	128
13	Auto	128
14	Auto	128
15	Auto	128

Save Reset

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

Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
----------	--

Button

Save Click to save changes.

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

4.3.16 IPMC Profile

This page provides IPMC Profile related configurations.

4.3.16.1 Profile Table

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

IPMC Profile Configurations

Global Profile Mode Disabled

IPMC Profile Table Setting

Delete	Profile Name	Profile Description	Rule
Add New			
Save		Reset	

System starts to do filtering based on profile settings only when the global profile mode is enabled.

Items	Description
Global Profile Mode	Enable/Disable the Global IPMC Profile.
Delete	Check to delete the entry. The designated entry will be deleted during the next save.

Profile Name	The name used for indexing the profile table. Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.
Profile Description	Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile. No blank or space characters are permitted as part of description. Use "_" or "-" to separate the description sentence.
Rule	When the profile is created, click the edit button to enter the rule setting page of the designated profile. Summary about the designated profile will be shown by clicking the view button. You can manage or inspect the rules of the designated profile by using the following buttons: Navigate: List the rules associated with the designated profile. Edit: Adjust the rules associated with the designated profile.

Button



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



Click to save changes.



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

4.3.16.2 Address Entry

This page provides address range settings used in IPMC profile.

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

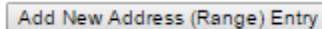
IPMC Profile Address Configuration Refresh

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

Delete	Entry Name	Start Address	End Address
Add Address			
Save Reset			

Items	Description
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
Entry Name	The name used for indexing the address entry table. Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.
Start Address	The starting IPv4/IPv6 Multicast Group Address that will be used as an address range.
End Address	The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.

Button



Click to add new address range. Specify the name and configure the addresses. Click "Save"



Click to save changes.



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

4.3.17 MVR

This page provides MVR related 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. It is allowed to create at maximum 8 MVR VLANs with corresponding channel settings for each Multicast VLAN. There will be totally at maximum 256 group addresses for channel settings.

MVR Configurations

MVR Mode

VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver])

Delete	MVR VID	MVR Name	IGMP Address	Mode	Tagging	Priority	LLQI	Interface Channel Profile
Add MVR								

Immediate Leave Setting

Port	Immediate Leave
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled

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


Items	Description
MVR Mode	<p>Enable/Disable the Global MVR. The designated entry will be deleted during the next save.</p> <p>The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping.</p> <p>It is suggested to enable Unregistered Flooding control when the MVR group table is full.</p>


Delete	Check to delete the entry. The designated entry will be deleted during the next save.
MVR VID	Specify the Multicast VLAN ID. Be Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.
MVR Name	MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 32. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR 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. When the IGMP address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.
Mode	Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode.
Tagging	Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is Tagged.
Priority	Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.
LLQI	Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a seconds. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second.

Interface Channel Profile	When the MVR VLAN is created, select the 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.
Profile Management Button	You can inspect the rules of the designated profile by using the following button: Navigate: List the rules associated with the designated profile.
Port	The logical port for the settings.
Port Role	Configure an MVR port of the designated MVR VLAN as one of the following roles. Inactive: The designated port does not participate MVR operations. Source: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports. Receiver: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages. Be Caution: MVR source ports are not recommended to be overlapped with management VLAN ports. Select the port role by clicking the Role symbol to switch the setting. I indicates Inactive; S indicates Source; R indicates Receiver The default Role is Inactive.
Immediate Leave	Enable the fast leave on the port.

Button

 Click to add new MVR VLAN. Specify the VID and configure the new entry. Click "Save".

 Click to save changes.

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

4.3.18 IPMC

4.3.18.1 IGMP Snooping-Base Cfg

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

This page provides IGMP Snooping related configuration.

Items	Description
Snooping Enabled	Enable the Global IGMP Snooping

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

Port Related Configuration

Items	Description
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	Enable the fast leave on the port.
Throttling	Enable to limit the number of multicast groups to which a switch port can belong.

Button



Click to save changes.



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

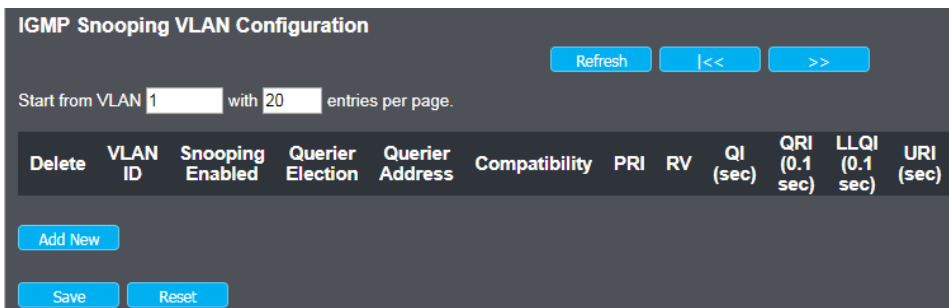
4.3.18.2 IGMP Snooping-VLAN Cfg

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.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the Refresh button will update the displayed table starting from that or the next closest VLAN Table match.

The >> will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the <<< button to start over.



IGMP Snooping VLAN Table Columns

Items	Description
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
VLAN ID	The VLAN ID of the entry.
IGMP Snooping Enabled	Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
Querier Election	Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier
Querier Address	Define the IPv4 address as 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
Compatibility	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto.
PRI	Priority of Interface. It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.
RV	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255, default robustness variable value is 2.
QI	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.
QRI	Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).
LLQI (LMQI for IGMP)	Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds, default last member query interval is 10 in tenths of seconds (1 second)

URI	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.
-----	---

Button

Add New IGMP VLAN

Add New IGMP VLAN : Click to add new IGMP VLAN. Specify the VID and configure the new entry. Click "Save". The specific IGMP VLAN starts working after the corresponding static VLAN is also created

Save

Click to save changes.

Reset

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

4.3.18.3 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	- ▾

Save
Reset

Items	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	You can inspect the rules of the designated profile by using the following button: Navigate: List the rules associated with the designated profile

Button

Save

Click to save changes.

Reset

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

4.3.18.3 MLD Snooping- Base Cfg

MLD is an acronym for Multicast Listener Discovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

This page provides MLD Snooping related configuration.

MLD Snooping Configuration

Global Configuration

Snooping Enabled

Unregistered IPMCv6 Flooding Enabled

MLD SSM Range / 96

Leave Proxy Enabled

Proxy Enabled

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 ▼

Items	Description
Snooping Enabled	Enable the Global MLD Snooping.
Unregistered IPMCv6 Flooding Enabled	Enable unregistered IPMCv6 traffic flooding. The flooding control takes effect only when MLD Snooping is enabled. When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.
MLD SSM Range	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.

Leave Proxy Enabled	Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
Proxy Enabled	Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Port Related Configuration

Items	Description
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	Enable the fast leave on the port.
Throttling	Enable to limit the number of multicast groups to which a switch port can belong.

Button



Click to save changes.



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

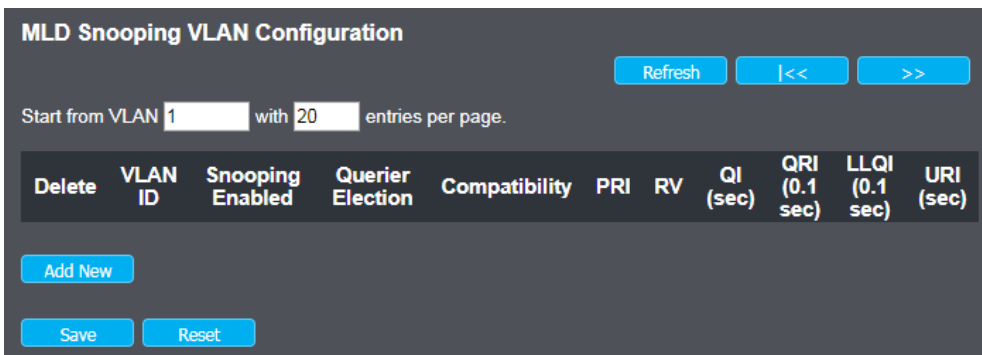
4.3.18.4 MLD Snooping- VLAN Cfg

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.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the Refresh button will update the displayed table starting from that or the next closest VLAN Table match.

The >> will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.



MLD Snooping VLAN Table Columns

Items	Description
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
VLAN ID	The VLAN ID of the entry.
MLD Snooping Enabled	Enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected for MLD Snooping.
Querier Election	Enable to join MLD Querier election in the VLAN. Disable to act as a MLD Non-Querier.
Compatibility	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selection is MLD-Auto, Forced MLDv1, Forced MLDv2, default compatibility value is MLD-Auto.
PRI	Priority of Interface. It indicates the MLD control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.
RV	Robustness Variable.

	<p>The Robustness Variable allows tuning for the expected packet loss on a link.</p> <p>The allowed range is 1 to 255, default robustness variable value is 2.</p>
QI	<p>Query Interval.</p> <p>The Query Interval is the interval between General Queries sent by the Querier.</p> <p>The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.</p>
QRI	<p>Query Response Interval.</p> <p>The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.</p> <p>The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).</p>
LLQI	<p>Last Listener Query Interval.</p> <p>The Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages.</p> <p>The allowed range is 0 to 31744 in tenths of seconds, default last listener query interval is 10 in tenths of seconds (1 second).</p>
URI	<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 0 to 31744 seconds, default unsolicited report interval is 1 second.</p>

Button

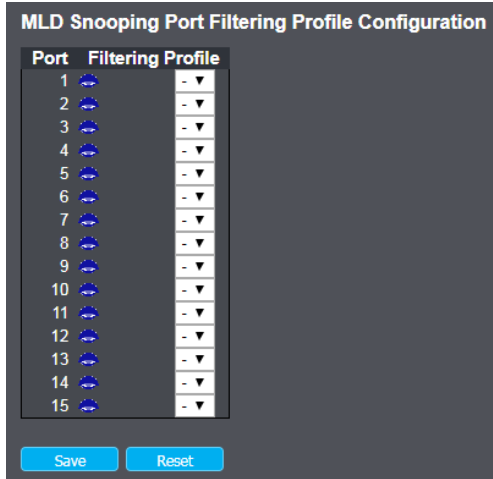


Click to save changes.



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

4.3.18.4 MLD Snooping- Port Filter profile



Items	Description
Port	The logical port for the settings.
Filtering Profile	Select the IPMC Profile as the filtering condition for the specific port. Summary the designated profile will be shown by clicking the view button.
Profile Management Button	You can inspect the rules of the designated profile by using the following button Navigate: List the rules associated with the designated profile

Button



Click to save changes.



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

4.3.19 LLDP

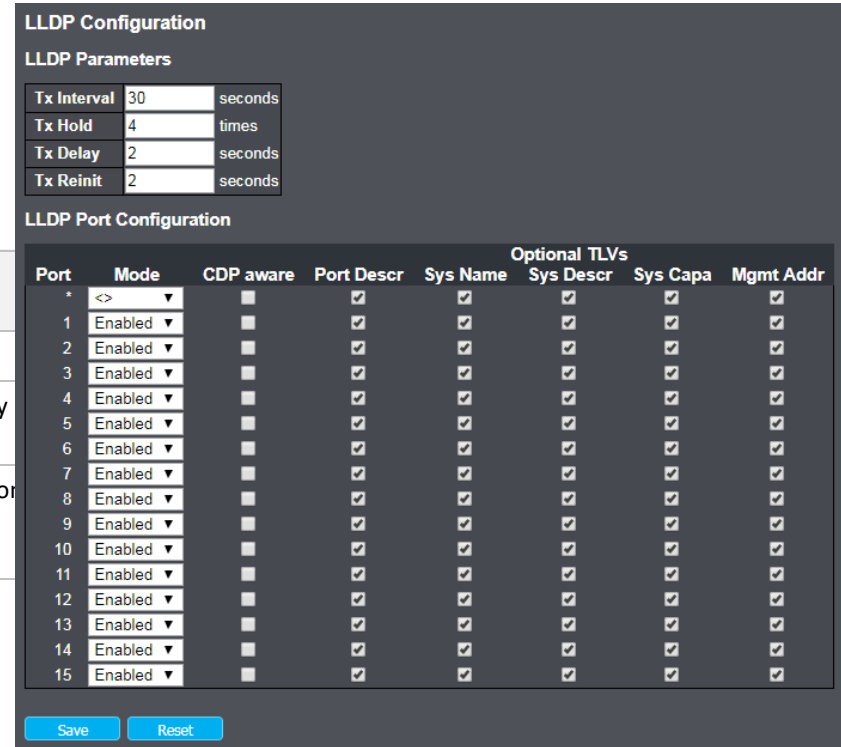
LLDP is an IEEE 802.1ab standard protocol.

The Link Layer Discovery Protocol (LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of

those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

4.3.19.1 LLDP Configuration

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



LLDP Parameters

Items	Description
Tx Interval	The switch periodically transmits LLDP frames to its neighbours for having the network discovery information up-to-date. The interval

	between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5 - 32768 seconds.
Tx Hold	Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2 - 10 times.
Tx Delay	If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value. Valid values are restricted to 1 - 8192 seconds.
Tx Reinit	When a port is disabled, LLDP is disabled or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, signalling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

LLDP Port Configuration

Items	Description
Port	The switch port number of the logical LLDP port.
Mode	<p>Select LLDP mode.</p> <p>Rx only The switch will not send out LLDP information, but LLDP information from neighbour units is analyzed.</p> <p>Tx only The switch will drop LLDP information received from neighbours, but will send out LLDP information.</p> <p>Disabled The switch will not send out LLDP information, and will drop LLDP information received from neighbours.</p> <p>Enabled The switch will send out LLDP information, and will analyze LLDP information received from neighbours.</p>
CDP Aware	<p>Select CDP awareness.</p> <p>The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the port is enabled.</p>

	<p>Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbours' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbours' table as shown below.</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 neighbours 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 neighbours' table.</p> <p>If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbour devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch.</p> <p>Note: When CDP awareness on a port is disabled the CDP information isn't removed immediately, but gets removed when the hold time is exceeded.</p>
Port Descr	Optional TLV: When checked the "port description" is included in LLDP information transmitted.
Sys Name	Optional TLV: When checked the "system name" is included in LLDP information transmitted.
Sys Descr	Optional TLV: When checked the "system description" is included in LLDP information transmitted.
Sys Capa	Optional TLV: When checked the "system capability" is included in LLDP information transmitted.
Mgmt Addr	Optional TLV: When checked the "management address" is included in LLDP information transmitted.

Button



Click to save changes.

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

4.3.19.2 LLDP-MED

LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057). This page allows you to configure the LLDP-MED. This function applies to VoIP devices which support LLDP-MED.

LLDP-MED Configuration

Fast Start Repeat Count

Fast start repeat count

Coordinates Location

Latitude North Longitude East Altitude Meters Map Datum W

Civic Address Location

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"/>

Emergency Call Service

Emergency Call Service

Policies

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

Faststart repeat count

Items	Description
Fast start repeat count	Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in

general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited 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 FastStart interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbour has been detected in order share LLDP-MED information as fast as possible to new neighbours.

Because there is a risk of an LLDP frame being lost during transmission between neighbours, it is recommended to repeat the faststart transmission multiple times to increase the possibility of the neighbours receiving the LLDP frame. With Faststart repeat count it is possible to specify the number of times the faststart 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 FastStart mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links.

Coordinates Location

Items	Description
Latitude	Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either North of the equator or South of the equator.

Longitude	Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.
Altitude	Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters). Meters: Representing meters of Altitude defined by the vertical datum specified. Floors: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.
Map Datum	The Map Datum is used for the coordinates given in these options: WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich. NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW). NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean

Civic Address Location

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

Items	Description
Country code	The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.
State	National subdivisions (state, canton, region, province, prefecture).

County	County, parish, gun (Japan), district.
City	City, township, shi (Japan) - Example: Copenhagen.
City district	City division, borough, city district, ward, chou (Japan).
Block (Neighbourhood)	Neighbourhood, block.
Street	Street - Example: Poppelvej.
Leading street direction	Leading street direction - Example: N.
Trailing street suffix	Trailing street suffix - Example: SW.
Street suffix	Street suffix - Example: Ave, Platz.
House no.	House number - Example: 21.
House no. suffix	House number suffix - Example: A, 1/2.
Landmark	Landmark or vanity address - Example: Columbia University.
Additional location info	Additional location info - Example: South Wing.
Name	Name (residence and office occupant) - Example: Flemming Jahn.
Zip code	Postal/zip code - Example: 2791.
Building	Building (structure) - Example: Low Library.
Apartment	Unit (Apartment, suite) - Example: Apt 42.
Floor	Floor - Example: 4.
Room no.	Room number - Example: 450F.
Place type	Place type - Example: Office.
Postal community name	Postal community name - Example: Leonia.
P.O. Box	Post office box (P.O. BOX) - Example: 12345.

Additional code	Additional code - Example: 1320300003.
Emergency Call Service	Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

Policies

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

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

The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
2. Layer 2 priority value (IEEE 802.1D-2004)
3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

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

1. Voice
2. Guest Voice
3. Softphone Voice
4. Video Conferencing
5. Streaming Video
6. Control / Signalling (conditionally support a separate network policy for the media types above)

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

It should be noted that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise

the multitude of network policies that frequently run on an aggregated link interior to the LAN.

Items	Description
Delete	Check to delete the policy. It will be deleted during the next save.
Policy ID	ID for the policy. This is auto generated and shall be used when selecting the policies that shall be mapped to the specific ports.
Application Type	<p>Intended use of the application types:</p> <ol style="list-style-type: none"> 1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. 2. Voice Signalling (conditional) - for use in network topologies that require a different policy for the voice signalling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy. 3. Guest Voice - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services. 4. Guest Voice Signalling (conditional) - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy. 5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance. 6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.

	<p>7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.</p> <p>8. Video Signalling (conditional) - for use in network topologies that require a separate policy for the video signalling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.</p>
Tag	<p>Tag indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN.</p> <p>Untagged indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance.</p> <p>Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.</p>
VLAN ID	VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003.
L2 Priority	L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004
DSCP	DSCP value to be used to provide Diffserv node behaviour for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475

Button



Click to save changes.



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

4.3.20 EPS

The Ethernet (Linear) Protection Switch instances are configured here.

Ethernet Protection Switching Refresh

Delete	EPS ID	Domain	Architecture	W Flow	P Flow	W SF MEP	P SF MEP	APS MEP	Alarm
--------	--------	--------	--------------	--------	--------	----------	----------	---------	-------

Add New EPS
Save
Reset

Items	Description
Delete	This box is used to mark an EPS for deletion in next Save operation.
EPS ID	The ID of the EPS. Click on the ID of an EPS to enter the configuration page.
Domain	Port: This will create a EPS in the Port Domain. 'W/P Flow' is a Port. Esp: Future use Evc: This will create a EPS in the EVC Domain. 'W/P Flow' is a EVC Mpls: Future use
Architecture	Port: This will create a 1+1 EPS. Port: This will create a 1:1 EPS.
W Flow	The working flow for the EPS - See 'Domain'.
P Flow	The protecting flow for the EPS - See 'Domain'.
W SF MEP	The working Signal Fail reporting MEP.
P SF MEP	The protecting Signal Fail reporting MEP.
APS MEP	The APS PDU handling MEP.
Alarm	There is an active alarm on the EPS.

Button



Click to add a new EPS entry.

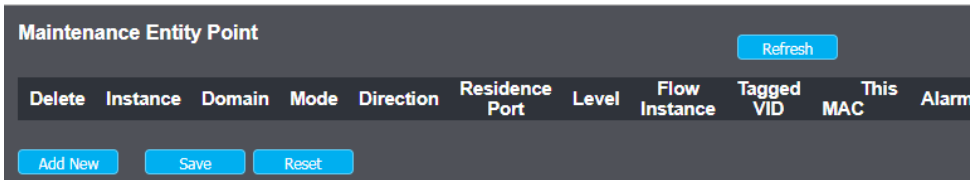


Click to save changes.

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

4.3.21 MEP

The Maintenance Entity Point instances are configured here.



Items	Description
Delete	This box is used to mark an EPS for deletion in next Save operation.
Instance	The ID of the MEP. Click on the ID of a MEP to enter the configuration page.
Domain	Port: This is a MEP in the Port Domain. 'Flow Instance' is a Port. Evc: This is a MEP in the EVC Domain. 'Flow Instance' is a EVC
Mode	MEP: This is a Maintenance Entity End Point. MIP: This is a MaintenanceEntity Intermediate Point.
Direction	Up: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'. Down: This is a Up MEP - monitoring egress OAM and traffic on 'Residence Port'.
Residence Port	The port where MEP is monitoring - see 'Direction'.
Level	The MEG level of this MEP.
Flow Instance	The MEP is related to this flow - See 'Domain'.
Tagged VID	Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.

	EVC MIP: On Serval, this is the Subscriber VID that identify the subscriber flow in this EVC where the MIP is active.
This MAC	The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).
Alarm	There is an active alarm on the MEP.

Button

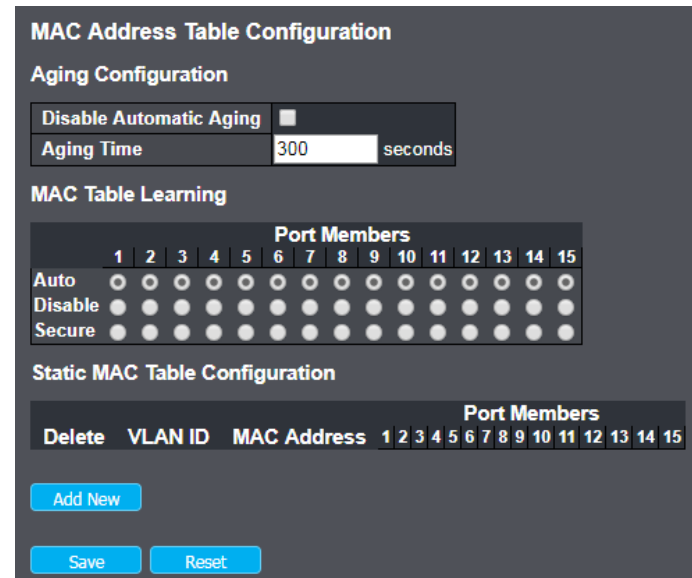
Add New MEP Click to add a new MEP entry.

Save Click to save changes.

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

4.3.22 MAC Table

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



Aging Configuration

Items	Description
-------	-------------

Aging Time	<p>By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.</p> <p>Configure aging time by entering a value here in seconds; for example, Age time seconds.</p> <p>The allowed range is 10 to 1000000 seconds.</p> <p>Disable the automatic aging of dynamic entries by checking Disable automatic aging.</p>
------------	---

MAC Table Learning

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

Each port can do learning based upon the following settings:

Items	Description
Auto	<p>Learning is done automatically as soon as a frame with unknown SMAC is received.</p> <p>Disable No learning is done.</p> <p>Secure Only static MAC entries are learned, all other frames are dropped.</p> <p>Note: Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.</p>

Static MAC Table Configuration

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.

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

VLAN ID	The VLAN ID of the entry.
MAC Address	The MAC address of the entry.
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Button

Click Add New Static Entry 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".

Click to save changes.

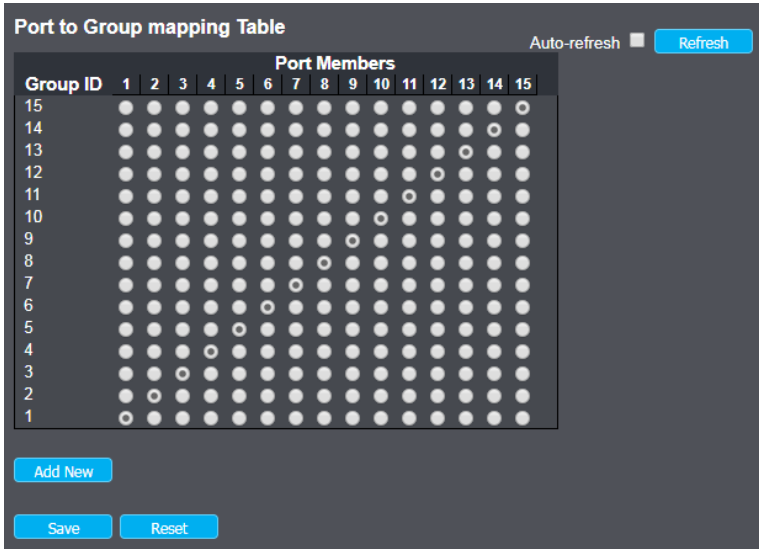
Click to undo any changes made locally and revert to previously saved values.

4.3.23 VLAN Translation

Q-in-Q tunneling and VLAN translation allow service providers to create a Layer 2 Ethernet connection between two customer sites. Providers can segregate different customers' VLAN traffic on a link (for example, if the customers use overlapping VLAN IDs) or bundle different customer VLANs into a single service VLAN. Data centers can use Q-in-Q tunneling and VLAN translation to isolate customer traffic within a single site or to enable customer traffic flows between cloud data centers in different geographic locations.

4.3.23.1 Port to Group Mapping

This page allows you to map set of Port members to a Group ID for all switch ports.



The displayed settings are:

Items	Description
Group ID	A valid Group ID is an integer value form 1 to 26. A set of VLAN Translations are mapped to a group Id. This way a port is mapped to a list of VLAN Translations easily by mapping it to a group. Number of groups in this switch is equal to the number of ports (26) present in this switch. A port can be mapped to any of the groups. Multiple ports can also be mapped to a group with same group Id. Note: By default, each port is mapped to a group with a group Id equal to the port number. For example, port 1 is mapped to the group with ID=1.
Port Members	A row of radio buttons, one radio button for each port is displayed for each Group ID. To include a port in a Group, click the radio button. A port must belong to at least one group. Adding a New Port to Group mapping entry Click Add New Entry to add a new entry in Port to Group Mapping Table. An empty row is added to the table with the Group ID and array of radio buttons, one radio button for each port(click corresponding radio

button to make port to be member of a particular Group). Note that if a VLAN translation is enabled on a management port for management VLAN, it may disrupt the management connectivity in some cases.
Legal values for a VLAN ID are 1 through 4095.
The Delete button can be used to undo the addition of new entry.

Button



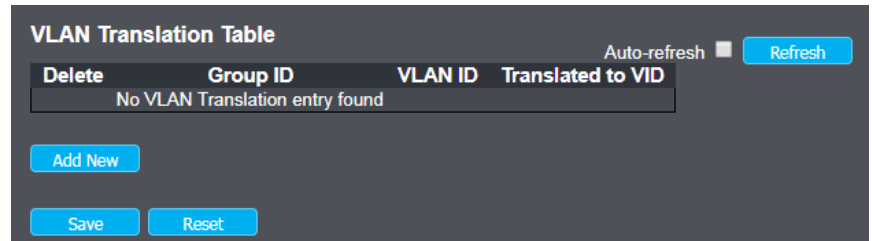
Click to save changes.



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

4.3.23.2 VID Translation Mapping

This page allows you to map VLAN ID to other VLAN ID for a particular Group ID Globally.



The displayed settings are:

Items	Description
Delete	To delete a VLAN Translation Group database entry, check this box. The entry will be deleted on the switch during the next Save
Group ID	A valid Group ID is an integer value from 1 to 26. A set of VLAN Translations are mapped to a group Id. This way a port is mapped to a list of VLAN Translations easily by mapping it to a group. Number of groups in a switch is equal to the number of ports present in this switch. A port can be mapped to any of the groups. Multiple ports can also be mapped to a group with same group Id. Note: By default, each port is mapped to a group with a group Id equal to the port number. For example, port 1 is mapped to the group with ID=1.

VLAN ID	Indicates the ID to which Group ID will be mapped. A valid VLAN ID ranges from 1-4095.
Translated to VLAN ID	Indicates the VID to which VLAN ID of ingress frames will be changed, if VID in incoming frames is same as configured in VLAN ID field preceded by this field on member ports of a particular group to which this entry belongs. Adding a New VLAN Translation entry Click Add New Entry to add a new entry in VLAN Translation table. An empty row is added to the table, the Group ID, VLAN ID and Translated to VID fields can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The Delete button can be used to undo the addition of new entry.

4.3.24 VLANs

VLANs allow network administrators to group hosts together even if the hosts are not on the same network switch. This can greatly simplify network design and deployment, because VLAN membership can be configured through software. Without VLANs, grouping hosts according to their resource needs necessitates the labor of relocating nodes or rewiring data links.

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

Items	Description
Allowed Access VLANs	This field shows the allowed Access VLANs, i.e. it only affects ports configured as Access ports. Ports in other modes are members of all VLANs specified in the Allowed VLANs field. By default, only VLAN 1 is enabled. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.
Ethertype for Custom S-ports	This field specifies the ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.

Port VLAN Configuration

Items	Description
Port	This is the logical port number of this row.
Mode	<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.</p> <p>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.</p> <p>Grayed out fields show the value that the port will get when the mode is applied.</p> <p>Access:</p> <p>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"> Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1 Accepts untagged and C-tagged frames Discards all frames that are not classified to the Access VLAN On egress all frames classified to the Access VLAN are transmitted untagged. Other (dynamically added VLANs) are transmitted tagged <p>Trunk:</p> <p>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"> By default, a trunk port is member of all VLANs (1-4095) The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs Frames classified to a VLAN that the port is not a member of are discarded

	<p>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</p> <p>Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress</p> <p>Hybrid:</p> <p>Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:</p> <ul style="list-style-type: none"> Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware Ingress filtering can be controlled Ingress acceptance of frames and configuration of egress tagging can be configured independently
Port VLAN	<p>Determines the port's 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>
Port Type	<p>Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required.</p> <p>Unaware:</p> <p>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>C-Port:</p>

	<p>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>S-Port: On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag.</p> <p>S-Custom-Port: On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag.</p>
Ingress Filtering	<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>
Ingress Acceptance	<p>Hybrid ports allow for changing the type of frames that are accepted on ingress.</p> <p>Tagged and Untagged Both tagged and untagged frames are accepted.</p> <p>Tagged Only Only tagged frames are accepted on ingress. Untagged frames are discarded.</p>

	<p>Untagged Only Only untagged frames are accepted on ingress. Tagged frames are discarded.</p>
Egress Tagging	<p>Ports in Trunk and Hybrid mode may control the tagging of frames on egress.</p> <p>Untag Port VLAN Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.</p> <p>Tag All All frames, whether classified to the Port VLAN or not, are transmitted with a tag.</p> <p>Untag All All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode.</p>
Allowed VLANs	<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 1-4095.</p> <p>The field may be left empty, which means that the port will not become member of any VLANs.</p>
Forbidden VLANs	<p>A port may be configured to never be member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and 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>

By default, the field is left blank, which means that the port may become a member of all possible VLANs.

Button

Click to save changes.

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

4.3.25 Private VLANs

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

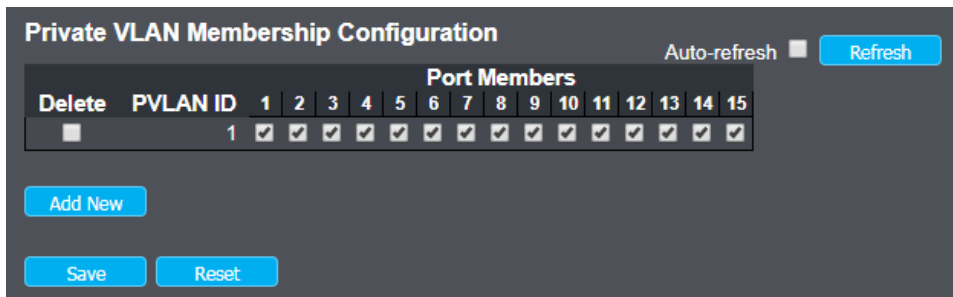
4.3.25.1 Private VLAN Membership

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

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

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

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



Items	Description
Delete	To delete a private VLAN entry, check this box. The entry will be deleted during the next save.

Private VLAN ID	Indicates the ID of this particular private VLAN.
Port Members	<p>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.</p> <p>Adding a New Private VLAN</p> <p>Click Add New Private VLAN to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry, or click "Cancel" to return to the editing and make a correction.</p> <p>The Private VLAN is enabled when you click "Save".</p> <p>The Delete button can be used to undo the addition of new Private VLANs.</p>

Button

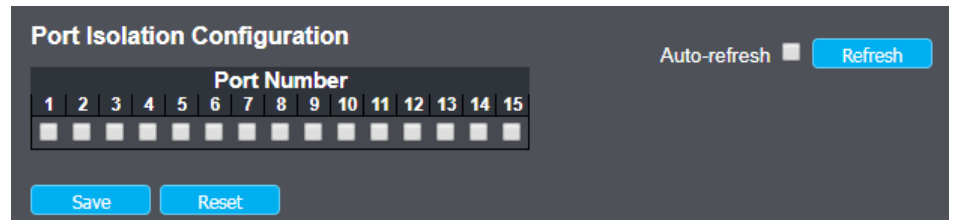
Click to save changes.

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

4.3.25.2 Port Isolation

This page is used for enabling or disabling port isolation on ports in a Private VLAN.

A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.



Items	Description
-------	-------------

Port Members	<p>A check box is provided for each port of a private VLAN.</p> <p>When checked, port isolation is enabled on that port.</p> <p>When unchecked, port isolation is disabled on that port.</p> <p>By default, port isolation is disabled on all ports.</p>
--------------	--

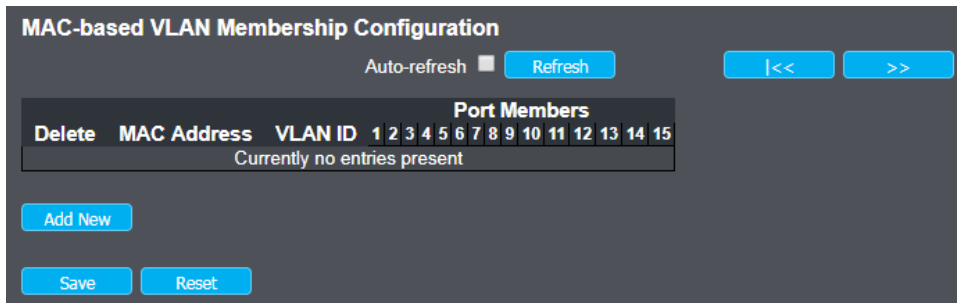
Button

Click to save changes.

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

4.3.26 VCL
4.3.26.1 MAC-based VLAN

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



Items	Description
Delete	To delete a MAC-based VLAN entry, check this box and press save. The entry will be deleted in the stack.
MAC Address	Indicates the MAC address.
VLAN ID	Indicates the VLAN ID.
Port Members	A row of check boxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make sure the

box is unchecked. By default, no ports are members, and all boxes are unchecked.

Adding a New MAC-based VLAN

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

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

. The Delete button can be used to undo the addition of new MAC-based VLANs. The maximum possible MAC-based VLAN entries are limited to 256.

Button

Click to save changes.

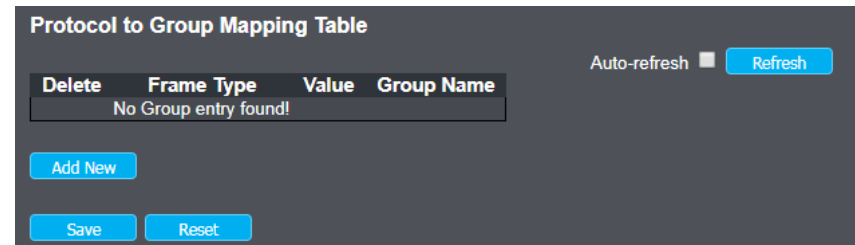
Click to undo any changes made locally and revert to previously saved values.

4.3.26.2 Protocol-based VLAN

In a switch that supports protocol-based VLANs, traffic is handled on the basis of its protocol. Essentially, this segregates or forwards traffic from a port depending on the particular protocol of that traffic; traffic of any other protocol is not forwarded on the port.

4.3.26.2.1 Protocol to Group

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



The displayed settings are:

Items	Description
Delete	To delete a Protocol to Group Name map entry, check this box. The entry will be deleted on the switch during the next Save.
Frame Type	<p>Frame Type can have one of the following values:</p> <ul style="list-style-type: none"> Ethernet LLC SNAP <p>Note: On changing the Frame type field, valid value of the following text field will vary depending on the new frame type you selected.</p>
Value	<p>Valid value that can be entered in this text field depends on the option selected from the the preceding Frame Type selection menu.</p> <p>Below is the criteria for three different Frame Types:</p> <p>For Ethernet: Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff</p> <p>For LLC: Valid value in this case is comprised of two different sub-values.</p> <ul style="list-style-type: none"> a. DSAP: 1-byte long string (0x00-0xff) b. SSAP: 1-byte long string (0x00-0xff) <p>For SNAP: Valid value in this case also is comprised of two different sub-values.</p> <ul style="list-style-type: none"> a. OUI: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff. b. PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. <p>In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.</p>

Group Name	<p>A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers(0-9).</p> <p>Note: special character and underscore(_) are not allowed.</p> <p>Adding a New Group to VLAN mapping entry</p> <p>Click Add New Entry to add a new entry in mapping table. An empty row is added to the table; Frame Type, Value and the Group Name can be configured as needed.</p> <p>The Delete button can be used to undo the addition of new entry. The maximum possible Protocol to Group mappings are limited to 128.</p>
------------	---

Button



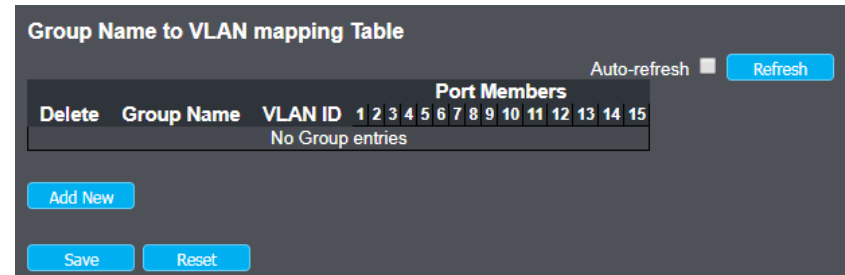
Click to save changes.



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

4.3.26.2.2 Group to VLAN

This page allows you to map a already configured Group Name to a VLAN for the switch.



The displayed settings are:

Items	Description
Delete	To delete a Group Name to VLAN map entry, check this box. The entry will be deleted on the switch during the next Save
Group Name	A valid Group Name is a string at the most 16 characters which consists of a combination of alphabets (a-z or A-Z) and integers(0-9), no special character is allowed. whichever Group name you try map to a VLAN

	must be present in Protocol to Group mapping table and must not be pre-used by any other existing mapping entry on this page.
VLAN ID	<p>Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095.</p> <p>Port Members</p> <p>A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.</p> <p>Adding a New Group to VLAN mapping entry</p> <p>Click Add New Entry to add a new entry in mapping table. An empty row is added to the table, the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095.</p> <p>The Delete button can be used to undo the addition of new entry. The maximum possible Group to VLAN mappings are limited to 64.</p>

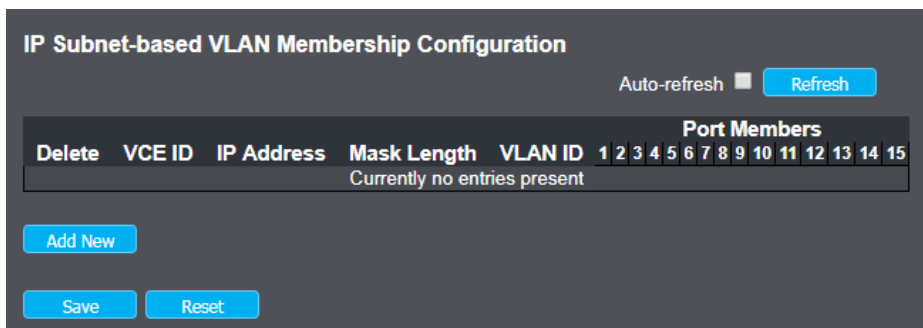
Button

Click to save changes.

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

4.3.26.3 IP Subnet-based VLAN

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



Items	Description
Delete	To delete a IP subnet-based VLAN entry, check this box and press save. The entry will be deleted in the stack.
VCE ID	Indicates the index of the entry. It is user configurable. It's value ranges from 0-128. If a VCE ID is 0, application will auto-generate the VCE ID for that entry. Deletion and lookup of IP subnet-based VLAN are based on VCE ID
IP Address	Indicates the IP address.
Mask Length	Indicates the network mask length.
VLAN ID	Indicates the VLAN ID. VLAN ID can be changed for the existing entries.
Port Members	<p>A row of check boxes for each port is displayed for each IP subnet-based VLAN entry. To include a port in a IP subnet-based VLAN, check the box. To remove or exclude the port from the IP subnet-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.</p> <p>Adding a New IP subnet-based VLAN</p> <p>Click Add New Entry to add a new IP subnet-based VLAN entry. An empty row is added to the table, and the IP subnet-based VLAN entry can be configured as needed. Any IP address/mask can be configured for the IP subnet-based VLAN entry. Legal values for a VLAN ID are 1 through 4095.</p> <p>The IP subnet-based VLAN entry is enabled when you click on "Save". The Delete button can be used to undo the addition of new IP subnet-based VLANs. The maximum possible IP subnet-based VLAN entries are limited to 128.</p>

Button

Click to save changes.

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

4.3.27 Voice VLAN

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

4.3.27.1 Configuration

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

Voice VLAN Configuration

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

Port Configuration

Port	Mode	Security	Discovery Protocol
1	Disabled ▼	Disabled ▼	OUI ▼
2	Disabled ▼	Disabled ▼	OUI ▼
3	Disabled ▼	Disabled ▼	OUI ▼
4	Disabled ▼	Disabled ▼	OUI ▼
5	Disabled ▼	Disabled ▼	OUI ▼
6	Disabled ▼	Disabled ▼	OUI ▼
7	Disabled ▼	Disabled ▼	OUI ▼
8	Disabled ▼	Disabled ▼	OUI ▼
9	Disabled ▼	Disabled ▼	OUI ▼
10	Disabled ▼	Disabled ▼	OUI ▼
11	Disabled ▼	Disabled ▼	OUI ▼
12	Disabled ▼	Disabled ▼	OUI ▼
13	Disabled ▼	Disabled ▼	OUI ▼
14	Disabled ▼	Disabled ▼	OUI ▼
15	Disabled ▼	Disabled ▼	OUI ▼

Save
Reset

Items	Description
-------	-------------

Delete	To delete a IP subnet-based VLAN entry, check this box and press save. The entry will be deleted in the stack.
Mode	Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are: Enabled: Enable Voice VLAN mode operation. Disabled: Disable Voice VLAN mode operation.
VLAN ID	Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID etc. The allowed range is 1 to 4095.
Aging Time	Indicates the Voice VLAN secure learning aging time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval.
Traffic Class	Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.
Port Mode	Indicates the Voice VLAN port mode. Possible port modes are: Disabled: Disjoin from Voice VLAN. Auto: Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically. Forced: Force join to Voice VLAN.
Port Security	Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are: Enabled: Enable Voice VLAN security mode operation. Disabled: Disable Voice VLAN security mode operation.

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

Button

Click to save changes.

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

4.3.27.2 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.

Voice VLAN OUI Table

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

Items	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Telephony OUI	A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).

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

4.3.28 Ethernet Services

4.3.28.1 Port

This page displays current EVC port configurations. The settings can also be configured here.

Port Configuration

Port	DEI Mode	Tag Mode	Address Mode
*	<>	<>	<>
1	Fixed	Outer	Source
2	Fixed	Outer	Source
3	Fixed	Outer	Source
4	Fixed	Outer	Source
5	Fixed	Outer	Source
6	Fixed	Outer	Source
7	Fixed	Outer	Source
8	Fixed	Outer	Source
9	Fixed	Outer	Source
10	Fixed	Outer	Source
11	Fixed	Outer	Source
12	Fixed	Outer	Source
13	Fixed	Outer	Source
14	Fixed	Outer	Source
15	Fixed	Outer	Source

Items	Description
Port	The logical port for the settings contained in the same row.
DEI Mode	The DEI mode for an NNI port determines whether frames transmitted on the port will have the DEI field in the outer tag marked based on the colour of the frame. The allowed values are: Coloured: The DEI is 1 for yellow frames and 0 for green frames. Fixed: The DEI value is determined by ECE rules.

Tag Mode	<p>The tag mode specifying whether the EVC classification must be based on the outer or inner tag. This can be used on NNI ports connected to another service provider, where an outer "tunnel" tag is added together with the inner tag identifying the EVC. The allowed values are:</p> <p>Inner: Enable inner tag in EVC classification.</p> <p>Outer: Enable outer tag in EVC classification.</p>
Address Mode	<p>The IP/MAC address mode specifying whether the EVC classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses. The allowed values are:</p> <p>Source: Enable SMAC/SIP matching.</p> <p>Destination: Enable DMAC/DIP matching.</p>

Button

Save

Click to save changes.

Reset

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

4.3.28.2 Bandwidth Profiles

This page displays current EVC ingress bandwidth profile configurations. These policers may be used to limit the traffic received on UNI ports. The settings can also be configured here.

Bandwidth Profiles Configuration

Refresh |<< << >> >>|

Start from Policer ID 1 with 20 entries per page.

Policer ID	State	Type	Policer Mode	Rate Type	CIR (kbps)	CBS (bytes)	EIR (kbps)	EBS (bytes)
*	<>	<>	<>	<>	0	0	0	0
1	Disabled	MEF	Aware	Data	0	0	0	0
2	Disabled	MEF	Aware	Data	0	0	0	0
3	Disabled	MEF	Aware	Data	0	0	0	0
4	Disabled	MEF	Aware	Data	0	0	0	0
5	Disabled	MEF	Aware	Data	0	0	0	0
6	Disabled	MEF	Aware	Data	0	0	0	0
7	Disabled	MEF	Aware	Data	0	0	0	0
8	Disabled	MEF	Aware	Data	0	0	0	0
9	Disabled	MEF	Aware	Data	0	0	0	0
10	Disabled	MEF	Aware	Data	0	0	0	0
11	Disabled	MEF	Aware	Data	0	0	0	0
12	Disabled	MEF	Aware	Data	0	0	0	0
13	Disabled	MEF	Aware	Data	0	0	0	0
14	Disabled	MEF	Aware	Data	0	0	0	0
15	Disabled	MEF	Aware	Data	0	0	0	0
16	Disabled	MEF	Aware	Data	0	0	0	0
17	Disabled	MEF	Aware	Data	0	0	0	0
18	Disabled	MEF	Aware	Data	0	0	0	0
19	Disabled	MEF	Aware	Data	0	0	0	0
20	Disabled	MEF	Aware	Data	0	0	0	0

Save Reset

Items	Description
Start Policer ID	The start Policer ID for displaying the table entries. The allowed range is from 1 through 256.
Number of Entries	The number of entries per page. The allowed range is from 2 through 256.
Policer ID	The Policer ID is used to identify one of the 256 policers.
State	The administrative state of the bandwidth profile. The allowed values are: Enabled: The bandwidth profile enabled.

	Disabled: The bandwidth profile is disabled.
Policer Mode	The colour mode of the bandwidth profile. The allowed values are: Coupled: Colour-aware mode with coupling enabled. Aware: Colour-aware mode with coupling disabled.
CIR	The Committed Information Rate of the bandwidth profile. The allowed range is from 0 through 10000000 kilobit per second.
CBS	The Committed Burst Size of the bandwidth profile. The allowed range is from 0 through 100000 bytes.
EIR	The Excess Information Rate of the bandwidth profile. The allowed range is from 0 through 10000000 kilobit per second.
EBS	The Excess Burst Size of the bandwidth profile. The allowed range is from 0 through 100000 bytes.

Button



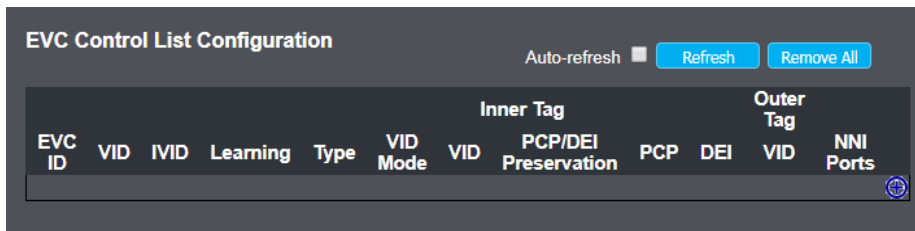
Click to save changes.



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

4.3.28.3 EVCs

This page displays current EVC configurations. On this system, only Provider Bridge based EVCs are supported.



Items	Description
EVC ID	The EVC ID identifies the EVC. The range is from 1 through 128.
VID	The VLAN ID in the PB network. It may be inserted in a C-tag, S-tag or S-custom tag depending on the NNI port VLAN configuration. The range is from 1 through 4095.

IVID	The Internal/classified VLAN ID in the PB network. The range is from 1 through 4095.
Learning	The learning mode for the EVC controls whether source MAC addresses are learned for frames matching the EVC. Learning may be disabled if the EVC only includes two UNI/NNI ports. The possible values are: Enabled: Learning is enabled (MAC addresses are learned). Disabled: Learning is disabled (MAC addresses are not learned).
Inner Tag Type	The inner tag type is used to determine whether an inner tag is inserted in frames forwarded to NNI ports. The possible values are: None: An inner tag is not inserted. C-tag: An inner C-tag is inserted. S-tag: An inner S-tag is inserted. S-custom-tag: An inner tag is inserted and the tag type is determined by the VLAN port configuration of the NNI.
Inner VID Mode	The inner VID Mode affects the VID in the inner and outer tag. The possible values are: Normal: The VID of the two outer tags aren't swapped. Tunnel: The VID of the two outer tags are swapped, so that the VID of the outer tag is taken from the Inner Tag configuration and the VID of the inner tag is the EVC VID. In this mode, the NNI ports are normally configured to do EVC classification based on the inner tag.
Inner Tag VID	The Inner tag VLAN ID. The allowed range is from 0 through 4095.
Inner Tag PCP/DEI Preservation	The inner tag PCP and DEI preservation. The possible values are: Preserved: The inner tag PCP and DEI is preserved. Fixed: The inner tag PCP and DEI is fixed.
Inner Tag PCP	The inner tag PCP value. The allowed range is from 0 through 7.
Inner Tag DEI	The inner tag DEI value. The allowed value is 0 or 1.
Outer Tag VID	The EVC outer tag VID for UNI ports. The allowed range is from 0 through 4095.
NNI Ports	The list of Network to Network Interfaces for the EVC.

Modification Buttons

You can modify each EVC in the table using the following buttons:

Edit: Edits the EVC row.

Delete: Deletes the EVC.

Add: Adds new EVC.

4.3.28.4 ECEs

This page displays current ECE configurations. The settings can also be configured here..

Items	Description
UNI Ports	The list of User Network Interfaces for the ECE.
Tag Type	The tag type for matching the ECE. The possible values are: Any: The ECE will match both tagged and untagged frames.

	Untagged: The ECE will match untagged frames only. C-Tagged: The ECE will match custom tagged frames only. S-Tagged: The ECE will match service tagged frames only. Tagged: The ECE will match tagged frames only.
Frame Type	The frame type for the ECE. The possible values are: Any: The ECE will match any frame type. IPv4: The ECE will match IPv4 frames only. IPv6: The ECE will match IPv6 frames only.
SMAC/DMAC Filter	The source/destination MAC address for matching the ECE. It depends on the port address mode, when port address mode is set to 'Source' then the field is used for source MAC address. Similarly when port address mode is set to 'Destination' then the field is used for destination MAC address. The possible values are: Any: No SMAC/DMAC filter is specified. (SMAC/DMAC filter status is "don't-care"). Specific: If you want to filter a specific SMAC/DMAC value with this ECE, choose this value. A field for entering a specific value appears.
DMAC Type	The destination MAC address for matching the ECE. The possible values are: Any: No destination MAC address is specified. Unicast: Frame must be unicast. Multicast: Frame must be multicast. Broadcast: Frame must be broadcast.
Direction	The EVCs and ECEs are used to setup flows in one or both directions as determined by the ECE Direction parameter. If the ECE is bidirectional, the ingress rules of the NNI ports will be setup to match the traffic being forwarded to NNI ports. The possible values are: Both: Bidirectional. UNI-to-NNI: Unidirectional from UNI to NNI. NNI-to-UNI: Unidirectional from NNI to UNI.
EVC ID Filter	The EVC ID for the ECE. The ECE is only active when mapping to an existing EVC. The possible values are:

	Any: No EVC ID filter is specified. (EVC ID filter status is "don't-care".) Specific: If you want to filter a specific EVC ID with this ECE, choose this value. A field for entering a specific value appears.
EVC ID Value	When "Specific" is selected for the VLAN ID filter, you can enter a specific value. The allowed value is from 1 through 256.
Tag Pop Count	The ingress tag pop count for the ECE. The allowed range is from 0 through 2.
Policy ID	The ACL Policy ID for the ECE for matching ACL rules. The allowed range is from 0 through 255.
Class	The traffic class for the ECE. The allowed range is from 0 through 8 or disabled. Egress Outer Tag
Outer Tag Mode	The outer tag for nni-to-uni direction for the ECE. The possible values are: Enable: Enable outer tag for nni-to-uni direction for the ECE. Disable: Disable outer tag for nni-to-uni direction for the ECE.
Outer Tag PCP/DEI Preservation	The outer tag PCP and DEI preservation for the ECE. The possible values are: Preserved: The outer tag PCP and DEI is preserved. Fixed: The outer tag PCP and DEI is fixed.
Outer Tag PCP	The outer tag PCP value for the ECE. The allowed range is from 0 through 7.
Outer Tag DEI	The outer tag DEI value for the ECE. The allowed value is 0 or 1

Button



Click to save changes.



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

4.3.29 QoS

QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

4.3.29.1 Port Classification

This page allows you to configure the basic QoS Ingress Classification settings for all switch ports.

QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	Address Mode
*	<> ▼	<> ▼	<> ▼	<> ▼		<input type="checkbox"/>	<> ▼
1	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	Source ▼
2	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	Source ▼
3	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	Source ▼
4	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	Source ▼
5	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	Source ▼
6	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	Source ▼
7	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	Source ▼
8	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	Source ▼
9	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	Source ▼
10	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	Source ▼
11	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	Source ▼
12	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	Source ▼
13	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	Source ▼
14	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	Source ▼
15	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>	Source ▼

The displayed settings are:

Items	Description
Port	The port number for which the configuration below applies.
QoS class	Controls the default QoS class.

	<p>All frames are classified to a QoS class. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.</p> <p>If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a QoS class that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default QoS class.</p> <p>The classified QoS class can be overruled by a QCL entry.</p> <p>Note: If the default QoS class has been dynamically changed, then the actual default QoS class is shown in parentheses after the configured default QoS class.</p>
DP level	<p>Controls the default Drop Precedence Level.</p> <p>All frames are classified to a DP level.</p> <p>If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DP level that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DP level.</p> <p>The classified DP level can be overruled by a QCL entry.</p>
PCP	<p>Controls the default PCP value.</p> <p>All frames are classified to a PCP value.</p> <p>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>
DEI	<p>Controls the default DEI value.</p> <p>All frames are classified to a DEI value.</p> <p>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>
Tag Class.	<p>Shows the classification mode for tagged frames on this port.</p> <p>Disabled: Use default QoS class and DP level for tagged frames.</p> <p>Enabled: Use mapped versions of PCP and DEI for tagged frames.</p> <p>Click on the mode in order to configure the mode and/or mapping.</p>

	<p>Note: This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default QoS class and DP level.</p>
DSCP Based	Click to Enable DSCP Based QoS Ingress Port Classification.
QCL Addr	<p>Controls the QCL address matching mode.</p> <p>SMAC/SIP: Match on source MAC and IP addresses in all QCEs on this port.</p> <p>DMAC/DIP: Match on destination MAC and IP addresses in all QCEs on this port.</p>

Button

Save

Click to save changes.

Reset

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

4.3.29.2 Port Policing

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

QoS Ingress Port Policers

Port	Enabled	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"/>

Save Reset

The displayed settings are:

Items	Description
Port	The port number for which the configuration below applies.
Enabled	Controls whether the policer is enabled on this switch port.
Rate	Controls the rate for the policer. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-3300 when the "Unit" is "Mbps" or "kfps".
Unit	Controls the unit of measure for the policer rate as kbps, Mbps, fps or kfps . The default value is "kbps".
Flow Control	If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

Button

Save Click to save changes.

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

4.3.29.3 Queue Policing

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

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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Save Reset

The displayed settings are:

Items	Description
Port	The port number for which the configuration below applies.
Enabled (E)	Controls whether the queue policer is enabled on this switch port.
Rate	Controls the rate for the queue policer. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-3300 when the "Unit" is "Mbps". This field is only shown if at least one of the queue policers are enabled.
Unit	Controls the unit of measure for the queue policer rate as kbps or Mbps. The default value is "kbps".

This field is only shown if at least one of the queue policers are enabled.

Button

Save Click to save changes.

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

4.3.29.4 Port Scheduler

This page provides an overview of QoS Egress Port Schedulers for all switch ports.

QoS Egress Port Schedulers						
Port	Mode	Weight				
		Q0	Q1	Q2	Q3	Q4
1	Strict Priority	-	-	-	-	-
2	Strict Priority	-	-	-	-	-
3	Strict Priority	-	-	-	-	-
4	Strict Priority	-	-	-	-	-
5	Strict Priority	-	-	-	-	-
6	Strict Priority	-	-	-	-	-
7	Strict Priority	-	-	-	-	-
8	Strict Priority	-	-	-	-	-
9	Strict Priority	-	-	-	-	-
10	Strict Priority	-	-	-	-	-
11	Strict Priority	-	-	-	-	-
12	Strict Priority	-	-	-	-	-
13	Strict Priority	-	-	-	-	-
14	Strict Priority	-	-	-	-	-
15	Strict Priority	-	-	-	-	-

The displayed settings are:

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

QoS Egress Port Scheduler and Shapers Configuration

This page allows you to configure the Scheduler and Shapers for a specific port.

The displayed settings are:

Items	Description
Scheduler Mode	Controls whether the scheduler mode is "StrictPriority" or "Weighted" on this switch port.
Queue Shaper Enable	Controls whether the queue shaper is enabled for this queue on this switch port.

Queue Shaper Rate	Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-3300 when the "Unit" is "Mbps".
Queue Shaper Unit	Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".
Queue Shaper Excess	Controls whether the queue is allowed to use excess bandwidth.
Queue Scheduler Weight	Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".
Queue Scheduler Percent	Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".
Port Shaper Enable	Controls whether the port shaper is enabled for this switch port.
Port Shaper Rate	Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-3300 when the "Unit" is "Mbps".
Port Shaper Unit	Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Button



Click to save changes.



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



Click to undo any changes made locally and return to the previous page.

4.3.29.5 Port Shaping

This page provides an overview of QoS Egress Port Shapers for all switch ports.

QoS Egress Port Shapers

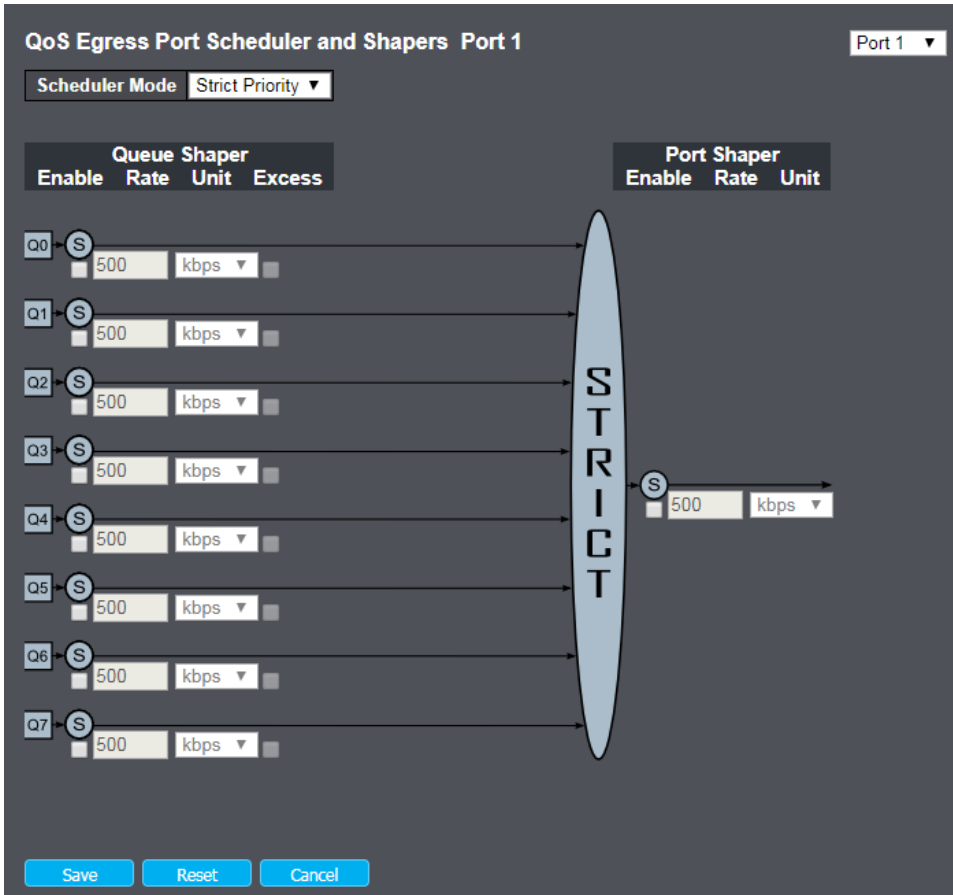
Port	Shapers								Port	
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7		
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
10	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
11	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
12	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
13	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
14	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
15	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

The displayed settings are:

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

[QoS Egress Port Scheduler and Shapers Configuration](#)

This page allows you to configure the Scheduler and Shapers for a specific port.



The displayed settings are:

Items	Description
Scheduler Mode	Controls whether the scheduler mode is "StrictPriority" or "Weighted" on this switch port.
Queue Shaper Enable	Controls whether the queue shaper is enabled for this queue on this switch port.

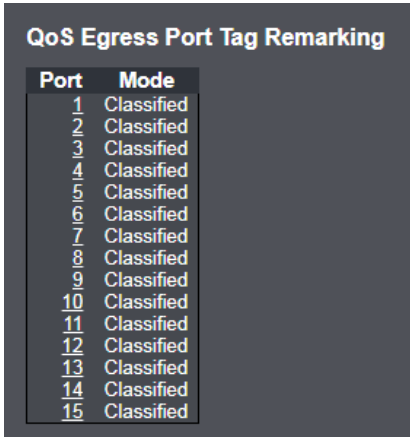
Queue Shaper Rate	Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-3300 when the "Unit" is "Mbps".
Queue Shaper Unit	Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".
Queue Shaper Excess	Controls whether the queue is allowed to use excess bandwidth.
Queue Scheduler Weight	Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".
Queue Scheduler Percent	Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".
Port Shaper Enable	Controls whether the port shaper is enabled for this switch port.
Port Shaper Rate	Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-3300 when the "Unit" is "Mbps".
Port Shaper Unit	Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Button

- Click to save changes.
- Click to undo any changes made locally and revert to previously saved values.
- Click to undo any changes made locally and return to the previous page.

4.3.29.6 Port Tag Remarking

This page provides an overview of QoS Egress Port Tag Remarking for all switch ports.

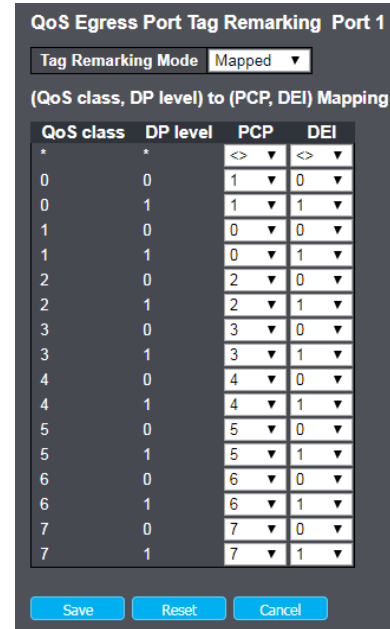


The displayed settings are:

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

[QoS Egress Port Tag Remarking Configuration](#)

The QoS Egress Port Tag Remarking for a specific port are configured on this page.



Items	Description
Mode	Controls the tag remarking mode for this port. Classified: Use classified PCP/DEI values. Default: Use default PCP/DEI values. Mapped: Use mapped versions of QoS class and DP level.
PCP/DEI Configuration	Controls the default PCP and DEI values used when the mode is set to Default.
(QoS class, DP level) to (PCP, DEI) Mapping	Controls the mapping of the classified (QoS class, DP level) to (PCP, DEI) values when the mode is set to Mapped.

Button



Click to save changes.

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

Cancel Click to undo any changes made locally and return to the previous page.

4.3.29.7 Port DSCP

This page allows you to configure the basic QoS Port DSCP Configuration settings for all switch ports.

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

The displayed settings are:

Items	Description
Port	The Port column shows the list of ports for which you can configure dscp ingress and egress settings.
Ingress	In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: 1. Translate

	2. Classify
1. Translate	To Enable the Ingress Translation click the checkbox.
2. Classify	Classification for a port have 4 different values. Disable: No Ingress DSCP Classification. DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0. Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP. All: Classify all DSCP.
Egress	Port Egress Rewriting can be one of - Disable: No Egress rewrite. Enable: Rewrite enabled without remapping. Remap DP Unaware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DPO' table. Remap DP Aware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation->Egress Remap DPO' table or from the 'DSCP Translation->Egress Remap DP1' table.

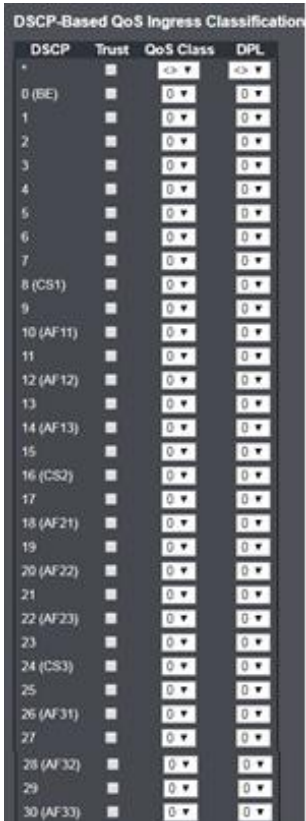
Button

Save Click to save changes.

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

4.3.29.8 DSCP-Based QoS

This page allows you to configure the basic QoS DSCP based QoS Ingress Classification settings for all switches.



The displayed settings are:

Items	Description
DSCP	Maximum number of supported DSCP values are 64.
Trust	Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.
QoS Class	QoS class value can be any of (0-7)
DPL	Drop Precedence Level (0-1)

Button



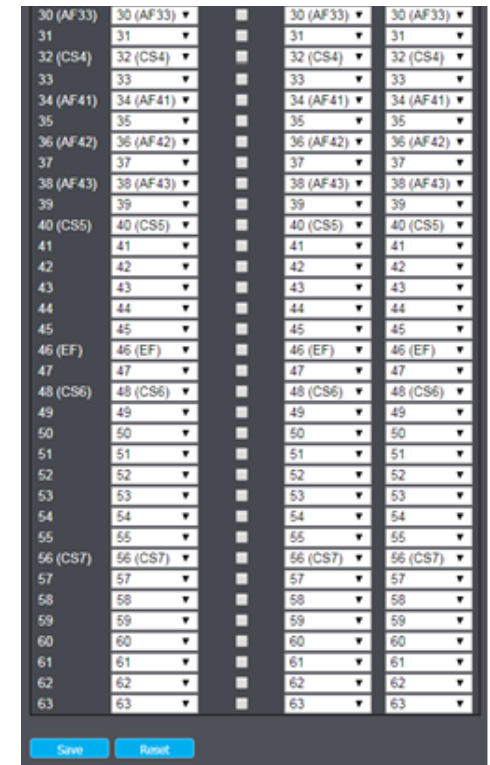
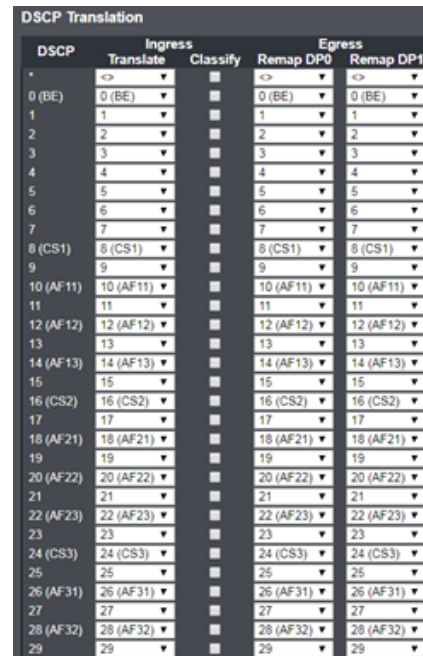
Click to save changes.



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

4.3.29.9 DSCP Translation

This page allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.



The displayed settings are:

Items	Description
DSCP	Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.

Ingress	Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two configuration parameters for DSCP Translation - 1. Translate 2. Classify
1. Translate	DSCP at Ingress side can be translated to any of (0-63) DSCP values.
2. Classify	Click to enable Classification at Ingress side.
Egress	There are the following configurable parameters for Egress side - 1. Remap DP0 Controls the remapping for frames with DP level 0. 2. Remap DP1 Controls the remapping for frames with DP level 1.
1. Remap DP0	Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.
2. Remap DP1	Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

Button



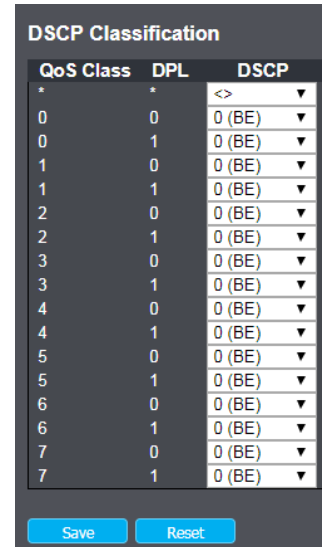
Click to save changes.



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

4.3.29.10 DSCP Classification

This page allows you to configure the mapping of QoS class and Drop Precedence Level to DSCP value.



The displayed settings are:

Items	Description
QoS Class	Actual QoS class.
DPL	Actual Drop Precedence Level.
DSCP	Select the classified DSCP value (0-63).

Button



Click to save changes.



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

4.3.29.11 QoS Control List

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

QoS Control List Configuration

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

Items	Description
QCE#	Indicates the index of QCE.
Port	Indicates the list of ports configured with the QCE.
Frame Type	Indicates the type of frame to look for incoming frames. Possible frame types are: Any: The QCE will match all frame type. Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. LLC: Only (LLC) frames are allowed. SNAP: Only (SNAP) frames are allowed. IPv4: The QCE will match only IPV4 frames. IPv6: The QCE will match only IPV6 frames.
SMAC	Displays the Source MAC address. If a port is configured to match on DMAC/DIP, this field is the Destination MAC address.
DMAC	Specify the type of Destination MAC addresses for incoming frame. Possible values are: Any: All types of Destination MAC addresses are allowed. Unicast: Only Unicast MAC addresses are allowed. Multicast: Only Multicast MAC addresses are allowed. Broadcast: Only Broadcast MAC addresses are allowed. The default value is 'Any'.
VID	Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'

PCP	Priority Code Point: Valid value PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.
DEI	Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'.
Action	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are three action fields: Class, DPL and DSCP. Class: Classified QoS class. DPL: Classified Drop Precedence Level. DSCP: Classified DSCP value.

Modification Buttons

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

Add: Inserts a new QCE before the current row.

Edit: Edits the QCE.

Up: Moves the QCE up the list.

Down: Moves the QCE down the list.

Delete: Deletes the QCE.

Add: The lowest plus sign adds a new entry at the bottom of the QCE listings.

QoS Control List Configuration

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

QCE Configuration

Port Members														
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Key Parameters

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

Action Parameters

CoS	0
DPL	Default
DSCP	Default

Save Reset Cancel

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

Key Parameters

Key configuration is described as below:

Items	Description
Tag	Tag Value of Tag field can be 'Any', 'Untag' or 'Tag'.
VID	VID Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.
PCP	PCP Priority Code Point: Valid value PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.
DEI	DEI Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'.
SMAC	SMAC Source MAC address: xx-xx-xx-xx-xx-xx or 'Any'. If a port is configured to match on

DMAC/DIP	DMAC/DIP, this field is the Destination MAC address.
DMAC Type	DMAC Type Destination MAC type: possible values are unicast(UC), multicast(MC), broadcast(BC) or 'Any'.
Frame Type	<p>Frame Type can have any of the following values:</p> <ul style="list-style-type: none"> Any Ethernet LLC SNAP IPv4 IPv6 <p>Note: All frame types are explained below.</p> <ol style="list-style-type: none"> 1. Any Allow all types of frames. 2. Ethernet Ethernet Type Valid ethernet type can have a value within 0x600-0xFFFF or 'Any' but excluding 0x800(IPv4) and 0x86DD(IPv6), default value is 'Any'. 3. LLC SSAP Address Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'. DSAP Address Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'. Control Valid Control field can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'. 4. SNAP PID Valid PID(a.k.a ethernet type) can have value within 0x00-0xFFFF or 'Any', default value is '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.

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.

IP Fragment IPv4 frame fragmented option: yes|no|any.

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

Items	Description
Class QoS class	Class QoS class: (0-7) or 'Default'.
DPL	DP Valid Drop Precedence Level can be (0-1) or 'Default'.
DSCP	DSCP Valid DSCP value can be (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'.

'Default' means that the default classified value is not modified by this QCE.

Button

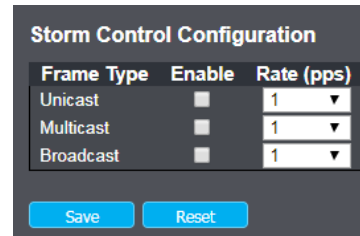
Click to save changes.

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

Click to undo any changes made locally and return to the previous page.

4.3.29.12 Storm Control

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



The configuration indicates the permitted packet rate for unicast, multicast or broadcast traffic across the switch.

Items	Description
Frame Type	The settings in a particular row apply to the frame type listed here: Unicast, Multicast or Broadcast.
Enable	Enable or disable the storm control status for the given frame type.
Rate	The rate unit is packets per second (pps). Valid values are: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K or 1024K.

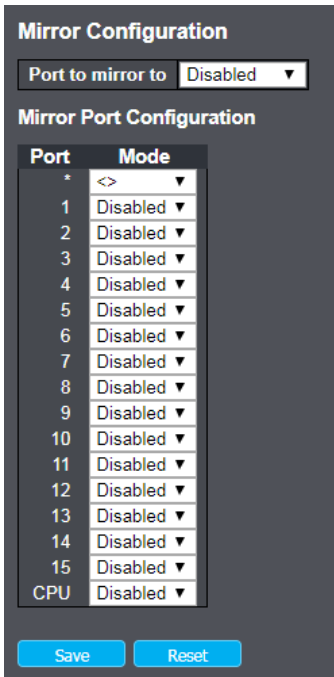
Button

Click to save changes.

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

4.3.30 Mirror

To debug network problems, selected traffic can be copied, or mirrored, on a mirror port where a frame analyzer can be attached to analyze the frame flow.



The traffic to be copied on the mirror port is selected as follows:

All frames received on a given port (also known as ingress or source mirroring).

All frames transmitted on a given port (also known as egress or destination mirroring).

Items	Description
Port to mirror to	Port to mirror also known as the mirror port. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port. Disabled disables mirroring.

Mirror Port Configuration

The following table is used for Rx and Tx enabling.

Items	Description
Port	The logical port for the settings contained in the same row.
Mode	Select mirror mode. Rx only Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored. Tx only Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored. Disabled Neither frames transmitted nor frames received are mirrored. Enabled Frames received and frames transmitted are mirrored on the mirror port.

Note: For a given port, a frame is only transmitted once. It is therefore not possible to mirror mirror port Tx frames. Because of this, mode for the selected mirror port is limited to Disabled or Rx only.

Button



Click to save changes.



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

4.3.31 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 Refresh

Agent Configuration

IP Address

Receiver Configuration

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

Port Configuration

Port	Enabled	Flow Sampler		Counter Poller	
		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

Save Reset

sFlow configuration is not persisted to non-volatile memory, which means that a reboot will disable sFlow sampling.

Agent Configuration

Items	Description
-------	-------------

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.
------------	--

Receiver Configuration

Items	Description
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: <ul style="list-style-type: none"> • 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 disables sFlow sampling. The button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will appear).
IP Address/Hostname	The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.
UDP Port	The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.
Timeout	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.
Max. Datagram Size	The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids

fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes.

Port Configuration

Items	Description
Port	The port number for which the configuration below applies.
Flow Sampler Enabled	Enables/disables flow sampling on this port.
Flow Sampler Sampling Rate	The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port. Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field.
Flow Sampler Max. Header	The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes. If the maximum datagram size does not take into account the maximum header size, samples may be dropped.
Counter Poller Enabled	Enables/disables counter polling on this port.
Counter Poller Interval	With counter polling enabled, this specifies the interval - in seconds - between counter poller samples.

Button

Click to save changes.

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

5. Monitor

5.1 System

5.1.1 Information

The switch system information is provided here.

System Information

System	
Contact Name	
Location	
Hardware	
MAC Address	00-01-c1-00-00-27
Time	
System Date	1970-01-01T00:49:26+00:00
System Uptime	0d 00:49:26
Software	
Software Version	1.2.0.18
Software Date	2018-08-04T05:19:21+08:00
Acknowledgments	Details

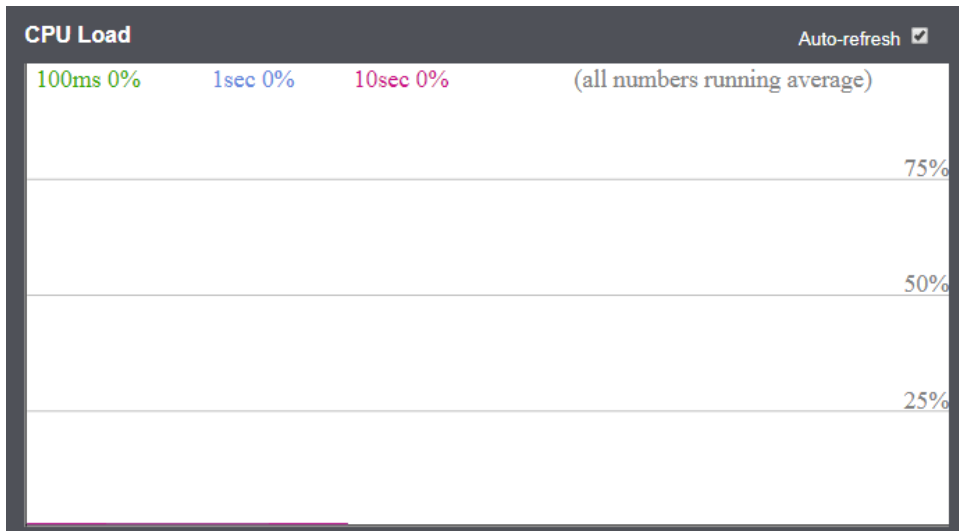
Items	Description
System	
Contact	The system contact configured in Configuration System Information System Contact.
Name	The system name configured in Configuration System Information System Name.
Location	The system location configured in Configuration System Information System Location.
Hardware	
MAC Address	The MAC Address of this switch.
Time	
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.

5.1.2 CPU Load

This page displays the CPU load, using an SVG graph.

The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well.



5.1.3 IP Status

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

IP Interfaces Auto-refresh Refresh

Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	::1/128	
OS:lo	IPv6	fe80:1::1/64	
VLAN1	LINK	00-01-c1-00-00-27	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.0.211/24	
VLAN1	IPv6	fe80:2::201:c1ff:fe00:27/64	
VLAN10	LINK	00-01-c1-00-00-27	<BROADCAST MULTICAST>
VLAN10	IPv4	192.168.10.211/24	
VLAN10	IPv6	fe80:3::201:c1ff:fe00:27/64	

IP Routes

Network	Gateway	Status
127.0.0.1/32	127.0.0.1	<UP HOST>
192.168.0.0/24	VLAN1	<UP HW_RT>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

Neighbour cache

IP Address	Link Address
192.168.0.30	VLAN1:60-a4-4c-07-1b-06
fe80:2::201:c1ff:fe00:27	VLAN1:00-01-c1-00-00-27
fe80:3::201:c1ff:fe00:27	VLAN10:00-01-c1-00-00-27

Items	Description
IP Interface	
Interfaces	The name of the interface.
Type	The address type of the entry. This may be LINK or IPv4.
Address	The current address of the interface (of the given type).
Status	The status flags of the interface (and/or address).
IP Routes	
Network	The destination IP network or host address of this route.
Gateway	The gateway address of this route.
Status	The status flags of the route.

Neighbour cache	
IP address	The IP address of the entry.
Link Address	The Link (MAC) address for which a binding to the IP address given exist.

5.1.4 Log

The switch system log information is provided here.

System Log Information

Auto-refresh Refresh Clear |<< << >> >>|

Level	All	▼
Clear Level	All	▼

The total number of entries is 2 for the given level.

Start from ID with entries per page.

ID	Level	Time	Message
1	Info	1970-01-01T00:00:01+00:00	Switch just made a cool boot.
2	Info	1970-01-01T00:00:06+00:00	Link up on port 15

Items	Description
ID	The ID (>= 1) of the system log entry.
Level	The level of the system log entry. The following level types are supported: Info: Information level of the system log. Warning: Warning level of the system log. Error: Error level of the system log. All: All levels.
Time	The time of the system log entry.
Message	The message of the system log entry.

5.1.5 Detailed Log

The switch system detailed log information is provided here

Detailed System Log Information

ID Refresh |<< << >> >>|

Message

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

Items	Description
ID	The ID (>= 1) of the system log entry.
Message	The message of the system log entry.

5.2 Green Ethernet

5.2.1 Port Power Savings

This page provides the current status for EEE.

Port Power Savings Status Auto-refresh Refresh

Port	Link	EEE	LP EEE Cap	EEE Savings	ActiPhy Savings	PerfectReach Savings
1	●	✘	✘	✘	✘	✘
2	●	✘	✘	✘	✘	✘
3	●	✘	✘	✘	✘	✘
4	●	✘	✘	✘	✘	✘
5	●	✘	✘	✘	✘	✘
6	●	✘	✘	✘	✘	✘
7	●	✘	✘	✘	✘	✘
8	●	✘	✘	✘	✘	✘
9	●	✘	✘	✘	✘	✘
10	●	✘	✘	✘	✘	✘
11	●	✘	✘	✘	✘	✘
12	●	✘	✘	✘	✘	✘
13	●	✘	✘	✘	✘	✘
14	●	✘	✘	✘	✘	✘
15	●	✘	✘	✘	✘	✘

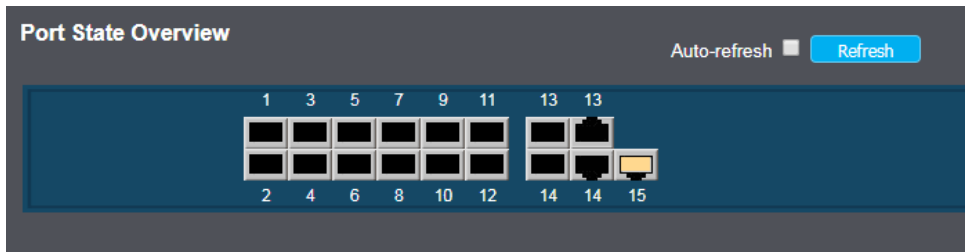
Items	Description
-------	-------------

Local Port	This is the logical port number for this row.
Link	Shows if the link is up for the port (green = link up, red = link down).
EEE	Shows if EEE is enabled for the port (reflects the settings at the Port Power Savings configuration page).
LP EEE cap	Shows if the link partner is EEE capable.
EEE Savings	Shows if the system is currently saving power due to EEE. When EEE is enabled, the system will powered down if no frame has been received or transmitted in 5 uSec.
ActiPhy Savings	Shows if the system is currently saving power due to ActiPhy.
Perfect Reach Savings	Shows if the system is currently saving power due to Perfect Reach.

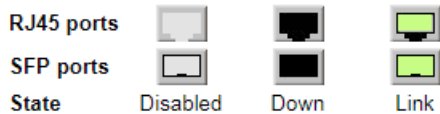
5.3 Ports

5.3.1 State

This page provides an overview of the current switch port states.



The port states are illustrated as follows:



5.3.2 Port Statistics Overview

This page provides an overview of general traffic statistics for all switch ports.

The displayed counters are:

The screenshot shows a 'Port Statistics Overview' interface with a table of traffic statistics for 15 ports. The table has columns for 'Port', 'Packets Received', 'Packets Transmitted', 'Bytes Received', 'Bytes Transmitted', 'Errors Received', 'Errors Transmitted', 'Drops Received', 'Drops Transmitted', and 'Filtered Received'. The data for port 15 is: 2986 packets received, 3212 packets transmitted, 399228 bytes received, 876989 bytes transmitted, 0 errors received, 0 errors transmitted, 0 drops received, 0 drops transmitted, and 573 filtered received. There are 'Auto-refresh', 'Refresh', and 'Clear' buttons in the top right corner.

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	2986	3212	399228	876989	0	0	0	0	573

5.3.3 QoS Statistics

This page provides statistics for the different queues for all switch ports.

The screenshot shows a 'Queuing Counters' interface with a table of QoS statistics for 15 ports. The table has columns for 'Port', 'Q0 Rx', 'Q0 Tx', 'Q1 Rx', 'Q1 Tx', 'Q2 Rx', 'Q2 Tx', 'Q3 Rx', 'Q3 Tx', 'Q4 Rx', 'Q4 Tx', 'Q5 Rx', 'Q5 Tx', 'Q6 Rx', 'Q6 Tx', 'Q7 Rx', and 'Q7 Tx'. The data for port 15 is: 3046 Q0 Rx, 0 Q0 Tx, 0 Q1 Rx, 0 Q1 Tx, 0 Q2 Rx, 0 Q2 Tx, 0 Q3 Rx, 0 Q3 Tx, 0 Q4 Rx, 0 Q4 Tx, 0 Q5 Rx, 0 Q5 Tx, 0 Q6 Rx, 0 Q6 Tx, 0 Q7 Rx, and 3300 Q7 Tx. There are 'Auto-refresh', 'Refresh', and 'Clear' buttons in the top right corner.

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	3046	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3300

Items	Description
Port	The logical port for the settings contained in the same row.
Qn	There are 8QoS queues per port. Q0 is the lowest priority queue.
Rx/Tx	The number of received and transmitted packets per queue.

5.3.4 QCL Status

This page shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.

QoS Control List Status Combined ▼ Auto-refresh Res Conflict Refresh

User	QCE	Port	Frame Type	CoS	Action	DPL	DSCP	Conflict
No entries								

Items	Description
User	Indicates the QCL user.
QCE#	Indicates the index of QCE.
Frame Type	Indicates the type of frame to look for incoming frames. Possible frame types are: Any: The QCE will match all frame type. Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. LLC: Only (LLC) frames are allowed. SNAP: Only (SNAP) frames are allowed. IPv4: The QCE will match only IPV4 frames. IPv6: The QCE will match only IPV6 frames.
Port	Indicates the list of ports configured with the QCE.
Action	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.
Conflict	Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

5.3.5 Detailed Port Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

Detailed Port Statistics Port 1 Port 1 ▼ Auto-refresh Refresh Clear

Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	0	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	0
Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

5.3.6 DDMI

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

SFP Digital Diagnostics Monitoring	
SFP Type	1000BASE_LX
SFP Vendor name	Hymax
SFP Vendor PN	HYM-P122-LID
SFP Vendor revision	V10
SFP Vendor Serial number	111140917911
SFP Vendor manufacturing date code	31 34 31 30 31 35 20 20 (2014.10.15)
SFP Laser wavelength	1310nm
SFP Fibre Channel Transmission Media	Single-Mode
SFP SFF-8472 Compliance	Rev 10.2
Temperature	
Value	44.750000C
High Warning Threshold	0.000000C
Low Warning Threshold	0.000000C
High Alarm Threshold	0.000000C
Low Alarm Threshold	0.000000C
Supply Voltage	
Value	3384300.000000uV
High Warning Threshold	0.000000uV
Low Warning Threshold	0.000000uV
High Alarm Threshold	0.000000uV
Low Alarm Threshold	0.000000uV

TX Bias Current	
Value	22014.000000uA
High Warning Threshold	0.000000uA
Low Warning Threshold	0.000000uA
High Alarm Threshold	0.000000uA
Low Alarm Threshold	0.000000uA
TX Output Power	
Value	273.699982uW(-5.627253dBm)
High Warning Threshold	0.000000uW(INFdBm)
Low Warning Threshold	0.000000uW(INFdBm)
High Alarm Threshold	0.000000uW(INFdBm)
Low Alarm Threshold	0.000000uW(INFdBm)
Received Power	
Value	0.000000uW(INFdBm), Low Warning, Low Alarm
High Warning Threshold	0.000000uW(INFdBm)
Low Warning Threshold	0.000000uW(INFdBm)
High Alarm Threshold	0.000000uW(INFdBm)
Low Alarm Threshold	0.000000uW(INFdBm)

5.4 Link OAM

5.4.1 Statistics

This page provides detailed OAM traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

The displayed counters represent the total number of OAM frames received and transmitted for the selected port. Discontinuities of these counter can occur at re-initialization of the management system.

Detailed Link OAM Statistics for Port 1 Port 1 Auto-refresh

Receive Total		Transmit Total	
Rx OAM Information PDU's	0	Tx OAM Information PDU's	0
Rx Unique Error Event Notification	0	Tx Unique Error Event Notification	0
Rx Duplicate Error Event Notification	0	Tx Duplicate Error Event Notification	0
Rx Loopback Control	0	Tx Loopback Control	0
Rx Variable Request	0	Tx Variable Request	0
Rx Variable Response	0	Tx Variable Response	0
Rx Org Specific PDU's	0	Tx Org Specific PDU's	0
Rx Unsupported Codes	0	Tx Unsupported Codes	0
Rx Link Fault PDU's	0	Tx Link Fault PDU's	0
Rx Dying Gasp	0	Tx Dying Gasp	0
Rx Critical Event PDU's	0	Tx Critical Event PDU's	0

5.4.2 Port status

This page provides Link OAM configuration operational status.

The displayed fields shows the active configuration status for the selected port.

Detailed Link OAM Status for Port 1 Port 1 Auto-refresh

PDU Permission	Receive only
Discovery State	Fault state
Peer MAC Address	-----

Local		Peer	
Mode	Passive	Mode	-----
Unidirectional Operation Support	Disabled	Unidirectional Operation Support	-----
Remote Loopback Support	Enabled	Remote Loopback Support	-----
Link Monitoring Support	Enabled	Link Monitoring Support	-----
MIB Retrieval Support	Enabled	MIB Retrieval Support	-----
MTU Size	1500	MTU Size	-----
Multiplexer State	Forwarding	Multiplexer State	-----
Parser State	Forwarding	Parser State	-----
Organizational Unique Identification	00-01-c1	Organizational Unique Identification	-----
PDU Revision	0	PDU Revision	-----

5.4.3 Event Status

This page allows the user to inspect the current Link OAM Link Event configurations, and change them as well.

The left pane displays the Event status for the Local OAM unit while the right pane displays the status for the Peer for the respective port.

Detailed Link OAM Link Status for Port 1 Port 1 Auto-refresh

Local Frame Error Status		Remote Frame Error Status	
Sequence Number	0	Frame Error Event Timestamp	0
Frame Error Event Timestamp	0	Frame error event window	0
Frame error event window	0	Frame error event threshold	0
Frame error event threshold	0	Frame errors	0
Frame errors	0	Total frame errors	0
Total frame errors	0	Total frame error events	0
Total frame error events	0		
Local Frame Period Status		Remote Frame Period Status	
Frame Period Error Event Timestamp	0	Frame Period Error Event Timestamp	0
Frame Period Error Event Window	0	Frame Period Error Event Window	0
Frame Period Error Event Threshold	0	Frame Period Error Event Threshold	0
Frame Period Errors	0	Frame Period Errors	0
Total frame period errors	0	Total frame period errors	0
Total frame period error events	0	Total frame period error events	0
Local Symbol Period Status		Remote Symbol Period Status	
Symbol Period Error Event Timestamp	0	Symbol Period Error Event Timestamp	0
Symbol Period Error Event Window	0	Symbol Period Error Event Window	0
Symbol Period Error Event Threshold	0	Symbol Period Error Event Threshold	0
Symbol Period Errors	0	Symbol Period Errors	0
Symbol frame period errors	0	Symbol frame period errors	0
Symbol frame period error events	0	Symbol frame period error events	0
Local Event Seconds Summary Status		Remote Event Seconds Summary Status	
Event Seconds Summary Time Stamp	0	Event Seconds Summary Time Stamp	0
Event Seconds Summary Window	0	Event Seconds Summary Window	0
Event Seconds Summary Threshold	0	Event Seconds Summary Threshold	0
Event Seconds Summary Events	0	Event Seconds Summary Events	0
Event Seconds Summary Error Total	0	Event Seconds Summary Error Total	0
Event Seconds Summary Event Total	0	Event Seconds Summary Event Total	0

5.5 Security

5.5.1 Access Management Statistics

This page provides statistics for access management.

Access Management Statistics Auto-refresh

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

5.5.2 Port Security - Switch

This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

The status page is divided into two sections - one with a legend of user modules and one with the actual port status.

Port Security Switch Status

User Module Legend

User Module Name	Abbr
Limit Control	L
802.1X	8
DHCP Snooping	D
Voice VLAN	V

Port Status

Port	Users	State	MAC Count	
			Current	Limit
1	----	Disabled	-	-
2	----	Disabled	-	-
3	----	Disabled	-	-
4	----	Disabled	-	-
5	----	Disabled	-	-
6	----	Disabled	-	-
7	----	Disabled	-	-
8	----	Disabled	-	-
9	----	Disabled	-	-
10	----	Disabled	-	-
11	----	Disabled	-	-
12	----	Disabled	-	-
13	----	Disabled	-	-
14	----	Disabled	-	-
15	----	Disabled	-	-

User Module Legend

The legend shows all user modules that may request Port Security services.

Items	Description
User Module Name	The full name of a module that may request Port Security services.
Abbr	A one-letter abbreviation of the user module. This is used in the Users column in the port status table.

Port Status

The table has one row for each port on the selected switch in the stack and a number of columns, which are:

Items	Description
Port	The port number for which the status applies. Click the port number to see the status for this particular port.
Users	Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.
State	Shows the current state of the port. It can take one of four values: Disabled: No user modules are currently using the Port Security service. Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive. Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in. Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.
MAC Count (Current, Limit)	The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.

If no user modules are enabled on the port, the Current column will show a dash (-).
 If the LimitControl user module is not enabled on the port, the Limit column will show a dash (-).
 Indicates the number of currently learned MAC addresses (forwarding as well as blocked) on the port. If no user modules are enabled on the port, a dash (-) will be shown.

5.5.3 Port Security - Port

This page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

Port Security Port Status Port 1 Port 1 Auto-refresh

MAC Address	VLAN ID	State	Time of Addition	Age/Hold
No MAC addresses attached				

Items	Description
MAC Address & VLAN ID	The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.
State	Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.
Time of Addition	Shows the date and time when this MAC address was first seen on the port.
Age/Hold	If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds)

expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin.

5.5.4 NAS - Switch

This page provides an overview of the current NAS port states.

Network Access Server Switch Status Auto-refresh

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled	-	-	-	-
2	Force Authorized	Globally Disabled	-	-	-	-
3	Force Authorized	Globally Disabled	-	-	-	-
4	Force Authorized	Globally Disabled	-	-	-	-
5	Force Authorized	Globally Disabled	-	-	-	-
6	Force Authorized	Globally Disabled	-	-	-	-
7	Force Authorized	Globally Disabled	-	-	-	-
8	Force Authorized	Globally Disabled	-	-	-	-
9	Force Authorized	Globally Disabled	-	-	-	-
10	Force Authorized	Globally Disabled	-	-	-	-
11	Force Authorized	Globally Disabled	-	-	-	-
12	Force Authorized	Globally Disabled	-	-	-	-
13	Force Authorized	Globally Disabled	-	-	-	-
14	Force Authorized	Globally Disabled	-	-	-	-
15	Force Authorized	Globally Disabled	-	-	-	-

Items	Description
Port	The switch port number. Click to navigate to detailed NAS statistics for this port.
Admin State	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
Port State	The current state of the port. Refer to NAS Port State for a description of the individual states.
Last Source	The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.
Last ID	The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the

	source MAC address from the most recently received frame from a new client for MAC-based authentication.
QoS Class	QoS Class assigned to the port by the RADIUS server if enabled.
Port VLAN ID	The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

5.5.5 NAS - Port

This page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics, only.

Use the port select box to select which port details to be displayed.

Items	Description
Admin State	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
Port State	The current state of the port. Refer to NAS Port State for a description of the individual states.
QoS Class	The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.
Port VLAN ID	The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.

	If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.
--	---

5.5.6 ACL Status

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 256 on each switch.

5.5.7 ARP inspection

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

5.5.8 IP Source Guard

Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.

5.5.9 AAA Radius

This page provides an overview of the status of the RADIUS servers configurable on the Authentication configuration page.

RADIUS Authentication Server Status Overview

#	IP Address	Status
1	0.0.0.0	Disabled
2	0.0.0.0	Disabled
3	0.0.0.0	Disabled
4	0.0.0.0	Disabled
5	0.0.0.0	Disabled

RADIUS Accounting Server Status Overview

#	IP Address	Status
1	0.0.0.0	Disabled
2	0.0.0.0	Disabled
3	0.0.0.0	Disabled
4	0.0.0.0	Disabled
5	0.0.0.0	Disabled

5.5.10 AAA Overview

This page provides detailed statistics for a particular RADIUS server.

RADIUS Authentication Statistics for Server #1

Server #1 ▾ Auto-refresh Refresh Clear

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		

Other Info

IP Address	0.0.0.0
State	Disabled
Round-Trip Time	0 ms

RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		

Other Info1111

IP Address	0.0.0.0
State	Disabled
Round-Trip Time	0 ms

5.5.11 ROM Statistics

This page provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.

The "Start from Control Index" allows the user to select the starting point in the Statistics table. Clicking the Refresh button will update the displayed table starting from that or the next closest Statistics table match.

The >> will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the << button to start over.

RMON Statistics Status Overview

Auto-refresh Refresh << >>

Start from Control Index 0 with 20 entries per page.

ID	Data Source (ifIndex)	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	128	256	512	1024	
No more entries														127	255	511	1023	1588

5.5.12 ROM History

This page provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table.

The "Start from History Index and Sample Index" allows the user to select the starting point in the History table. Clicking the Refresh button will update the displayed table starting from that or the next closest History table match.

The >> will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over

5.5.13 ROM Alarm

This page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table.

The "Start from Control Index" allows the user to select the starting point in the Alarm table. Clicking the Refresh button will update the displayed table starting from that or the next closest Alarm table match.

The >> will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

5.5.14 ROM Event

This page provides an overview of RMON Event table entries. Each page shows up to 99 entries from the Event table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table.

The "Start from Event Index and Log Index" allows the user to select the starting point in the Event table. Clicking the Refresh button will update the displayed table starting from that or the next closest Event table match.

The >> will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

5.6 LACP

5.6.1 System Status

This page provides a status overview for all LACP instances.

5.6.2 LACP Status

This page provides a status overview for LACP status for all ports.

LACP Status Auto-refresh [Refresh](#)

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	No	-	-	-	-	-
2	No	-	-	-	-	-
3	No	-	-	-	-	-
4	No	-	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-
7	No	-	-	-	-	-
8	No	-	-	-	-	-
9	No	-	-	-	-	-
10	No	-	-	-	-	-
11	No	-	-	-	-	-
12	No	-	-	-	-	-
13	No	-	-	-	-	-
14	No	-	-	-	-	-
15	No	-	-	-	-	-

5.6.3 LACP Statistics

This page provides an overview for LACP statistics for all ports.

LACP Statistics Auto-refresh [Refresh](#) [Clear](#)

Port	LACP		Discarded	
	Received	Transmitted	Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0

5.7 Loop Protection

This page displays the loop protection port status the ports of the switch.

Loop Protection Status Auto-refresh [Refresh](#)

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
No ports enabled						

5.8 Spanning Tree

5.8.1 Bridge Status

This page provides a status overview of all STP bridge instances.

STP Bridges Auto-refresh [Refresh](#)

MSTI	Bridge ID	Root ID	Port	Cost	Topology Flag	Topology Change Last
CIST	32768.00-01-C1-00-00-27	32768.00-01-C1-00-00-27	-	0	Steady	-

5.8.2 Port Status

This page displays the STP CIST port status for physical ports of the switch.

STP Port Status

Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	Disabled	Discarding	-
3	Disabled	Discarding	-
4	Disabled	Discarding	-
5	Disabled	Discarding	-
6	Disabled	Discarding	-
7	Disabled	Discarding	-
8	Disabled	Discarding	-
9	Disabled	Discarding	-
10	Disabled	Discarding	-
11	Disabled	Discarding	-
12	Disabled	Discarding	-
13	Disabled	Discarding	-
14	Disabled	Discarding	-
15	DesignatedPort	Forwarding	0d 16:07:23

5.8.3 Port Statistics

This page displays the STP port statistics counters of bridge ports in the switch.

STP Statistics Auto-refresh [Refresh](#) [Clear](#)

Port	MSTP	Transmitted			Received			Discarded		
		RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
15	29042	0	0	0	0	0	0	0	0	0

5.9 MVR

5.9.1 Statistics

This page provides MVR Statistics information

MVR Statistics Auto-refresh Refresh Clear

VLAN ID	IGMP/MLD Queries Received	IGMP/MLD Queries Transmitted	IGMPv1 Joins Received	IGMPv2/MLDv1 Reports Received	IGMPv3/MLDv2 Reports Received	IGMPv3/MLDv2 Reports Received
No more entries						

5.9.2 MVR Channel Groups

Entries in the MVR Channels (Groups) Information Table are shown on this page. The MVR Channels (Groups) Information Table is sorted first by VLAN ID, and then by group

MVR Channels (Groups) Information Auto-refresh Refresh << >>

Start from VLAN and Group Address with entries per page.

VLAN ID	Groups	Port Members													
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
No more entries															

5.9.3 MVR SFM Information

Entries in the MVR SFM Information Table are shown on this page. The MVR SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

MVR SFM Information Auto-refresh Refresh << >>

Start from VLAN and Group Address with entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

5.10 IPMC

5.10.1 IGMP Status

This page provides IGMP Snooping status.

IGMP Snooping Status Auto-refresh Refresh Clear

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received																																
Router Port																																									
<table border="1"> <thead> <tr> <th>Port</th> <th>Status</th> </tr> </thead> <tbody> <tr><td>1</td><td>-</td></tr> <tr><td>2</td><td>-</td></tr> <tr><td>3</td><td>-</td></tr> <tr><td>4</td><td>-</td></tr> <tr><td>5</td><td>-</td></tr> <tr><td>6</td><td>-</td></tr> <tr><td>7</td><td>-</td></tr> <tr><td>8</td><td>-</td></tr> <tr><td>9</td><td>-</td></tr> <tr><td>10</td><td>-</td></tr> <tr><td>11</td><td>-</td></tr> <tr><td>12</td><td>-</td></tr> <tr><td>13</td><td>-</td></tr> <tr><td>14</td><td>-</td></tr> <tr><td>15</td><td>-</td></tr> </tbody> </table>										Port	Status	1	-	2	-	3	-	4	-	5	-	6	-	7	-	8	-	9	-	10	-	11	-	12	-	13	-	14	-	15	-
Port	Status																																								
1	-																																								
2	-																																								
3	-																																								
4	-																																								
5	-																																								
6	-																																								
7	-																																								
8	-																																								
9	-																																								
10	-																																								
11	-																																								
12	-																																								
13	-																																								
14	-																																								
15	-																																								

5.10.2 IGMP Group Information

Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group.

IGMP Snooping Group Information Auto-refresh Refresh << >>

Start from VLAN and group address with entries per page.

VLAN ID	Groups	Port Members													
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
No more entries															

5.10.3 IGMP SFM Information

Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

IGMP SFM Information Auto-refresh Refresh << >>

Start from VLAN and Group with entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

5.10.4 MLD Status

This page provides MLD Snooping status.

MLD Snooping Status Auto-refresh Refresh Clear

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-
13	-
14	-
15	-

5.10.5 MLD group Information

Entries in the MLD Group Table are shown on this page. The MLD Group Table is sorted first by VLAN ID, and then by group.

MLD Snooping Group Information Auto-refresh Refresh << >>

Start from VLAN and group address with entries per page.

VLAN ID	Groups	Port Members
		1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

No more entries

5.10.6 MLD SFM Information

Entries in the MLD SFM Information Table are shown on this page. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

MLD SFM Information Auto-refresh Refresh << >>

Start from VLAN and Group with entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

5.11 LLDP

5.11.1 Neighbours

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

LLDP Neighbor Information Auto-refresh Refresh

Local Port	Chassis ID	Port ID	LLDP Remote Device Summary			Management Address
			Port Description	System Name	System Capabilities	
No neighbor information found						

5.11.2 LLDP-MED Neighbour Information

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

LLDP-MED Neighbor Information Auto-refresh Refresh

Local Port
No LLDP-MED neighbor information found

5.11.3 EEE

By using EEE power savings can be achieved at the expense of traffic latency. This latency occurs due to that the circuits EEE turn off to save power, need time to boot up before sending traffic over the link. This time is called "wakeup time". To achieve minimal latency, devices can use LLDP to exchange information about their respective tx and rx "wakeup time", as a way to agree upon the minimum wakeup time they need.

LLDP Neighbors EEE Information Auto-refresh Refresh

Local Port	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE in Sync
No LLDP EEE information found								

5.11.4 Port Statistics

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

LLDP Global Counters Auto-refresh Refresh Clear

Global Counters

Neighbor entries were last changed 1970-01-01T00:00:00+00:00 (60119 secs. ago)

Total Neighbors Entries Added	0
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	2004	0	0	0	0	0	0	0

5.12 Ethernet Services

5.12.1 EVC Statistics

This page provides NNI port traffic statistics for the selected EVC. It also shows counters for UNI ports of ECEs mapping to the EVC.

EVC Statistics Port 1 Auto-refresh Refresh Clear

Class	Green Frames		Yellow Frames		Red Frames	Discarded Frames	
	Rx	Tx	Rx	Tx	Rx	Green	Yellow
0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0

5.13 MAC Table

This function can show the dynamic Mac addresses learned by the G.SHDSL ROUTER.

MAC Address Table Auto-refresh Refresh Clear |<< >>

Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.

Type	VLAN	MAC Address	Port Members																
			CPU	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Dynamic	1	00-01-A2-B3-C4-E6																	✓
Static	1	00-01-C1-00-00-27	✓																
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-00-00-27	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dynamic	1	60-A4-4C-07-1B-06																	✓
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

5.14 VLANs

5.14.1 VLAN Membership

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

VLAN Membership Status for Combined users Combined Auto-refresh Refresh

Start from VLAN 1 with 20 entries per page. |<< >>

VLAN ID	Port Members														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
10	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼	▼

5.14.2 VLAN Port

This page provides VLAN Port Status.

VLAN Port Status for Combined users Combined Auto-refresh

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
2	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
3	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
4	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
5	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
6	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
7	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
8	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
9	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
10	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
11	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
12	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
13	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
14	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No
15	C-Port	<input checked="" type="checkbox"/>	All	1	Untag PVID		No

5.15 VCL

5.15.1 MAC-Based VLAN

This page shows MAC-based VLAN entries configured by various MAC-based VLAN users. Currently we support following VLAN User types:

CLI/Web/SNMP : These are referred to as static.

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

MAC-based VLAN Membership Status for User Static Static Auto-refresh

MAC Address	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
No data exists for the user																

5.16 sFlow

This page shows receiver and per-port sFlow statistics.

sFlow Statistics Auto-refresh

Receiver Statistics

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

Port Statistics

Port	Rx Flow Samples	Tx Flow Samples	Counter Samples
1	0	0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0
6	0	0	0
7	0	0	0
8	0	0	0
9	0	0	0
10	0	0	0
11	0	0	0
12	0	0	0
13	0	0	0
14	0	0	0
15	0	0	0

6. Diagnostics

6.1 Ping

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

ICMP Ping

IP Address	0.0.0.0
Ping Length	56
Ping Count	5
Ping Interval	1

After you press , 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

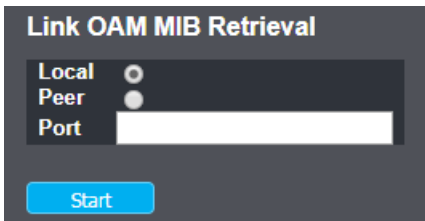
Sent 5 packets, received 5 OK, 0 bad

* Reference 4.5.3

6.2 Link OAM

6.2.1 MIB Retrieval

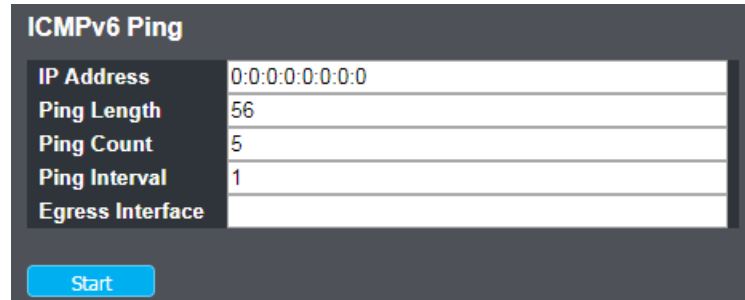
This page allows you to retrieve the local or remote OAM MIB variable data on a particular port.



Select the appropriate radio button and enter the port number of the switch to retrieve the content of interest. Click on to retrieve the content. Click on to retrieve another content of interest.

6.3 Ping6

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



After you press , 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:

Items	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>

Start Click to start transmitting ICMP packets.

New Ping Click to re-start diagnostics with PING.

6.4 VeriPHY

This page is used for running the VeriPHY Cable Diagnostics for 10/100 and 1G copper ports.

VeriPHY Cable Diagnostics

Port: All

Start

Port	Cable Status							
	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
13	—	—	—	—	—	—	—	—
14	—	—	—	—	—	—	—	—
15	—	—	—	—	—	—	—	—

Press **Start** to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 - 140 meters.

10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

Items	Description
Port	The port where you are requesting VeriPHY Cable Diagnostics.
Cable Status	<p>Port: Port number.</p> <p>Pair: The status of the cable pair.</p> <p>OK - Correctly terminated pair</p> <p>Open - Open pair</p> <p>Short - Shorted pair</p> <p>Short A - Cross-pair short to pair A</p> <p>Short B - Cross-pair short to pair B</p> <p>Short C - Cross-pair short to pair C</p> <p>Short D - Cross-pair short to pair D</p> <p>Cross A - Abnormal cross-pair coupling with pair A</p> <p>Cross B - Abnormal cross-pair coupling with pair B</p> <p>Cross C - Abnormal cross-pair coupling with pair C</p> <p>Cross D - Abnormal cross-pair coupling with pair D</p>

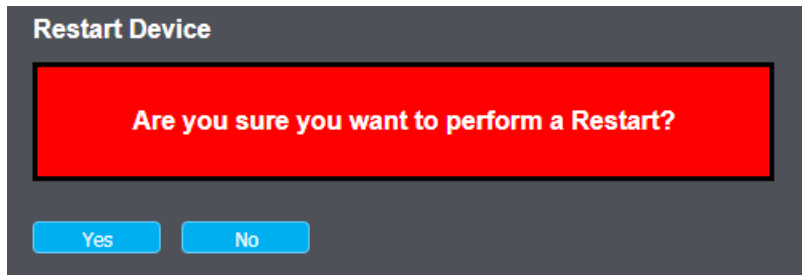
Length:

The length (in meters) of the cable pair. The resolution is 3 meters

7. Maintenance

The follow functions are used for system maintenance. They are Reboot Device, Factory Default, Save Configuration, Configuration File, Upgrade Firmware and ping functions.

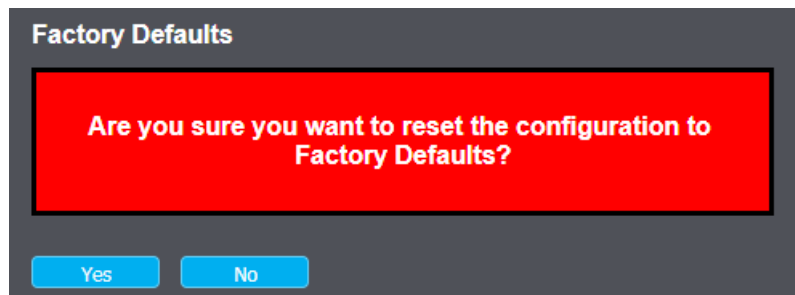
7.1 Restart Device



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

7.2 Factory Default

From Factory Default Menu, you'll get a dialog as following picture:

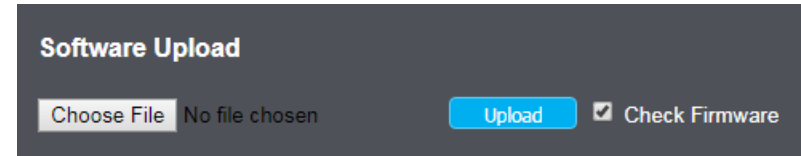


If you click "Yes" to re-load factory default, the device will reboot by itself.

7.3 Software

7.3.1 Upload

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



"Browse" to the location of a software image and click "Upload".

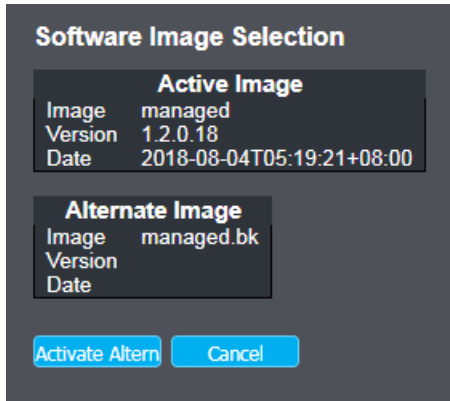
After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch restarts.

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

7.3.2 Image Select

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

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



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

Image Information

Items	Description
Image	The flash index name of the firmware image. The name of primary (preferred) image is image, the alternate image is named image.bk.
Version	The version of the firmware image.
Date	The date where the firmware was produced.

Activate Alternate Image

Click to use the alternate image. This button may be disabled depending on system state.

Reset

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

7.4 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.

There are three system files:

- **running-config:** A virtual file that represents the currently active configuration on the switch. This file is volatile.
- **startup-config:** The startup configuration for the switch, read at boot time.
- **default-config:** A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

It is also possible to store up to two other files and apply them to running-config, thereby switching configuration.

7.4.1 Save startup-config

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

Save Running Configuration to startup-config

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

Save Config

Click to save configuration.

7.4.2 Download

It is possible to download any of the files on the switch to the web browser. Select the file and click

Download Configuration

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

Download Configuration

Select configuration file to save.

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

File Name

- running-config
- default-config
- startup-config

Download

7.4.3 Upload

It is possible to upload a file from the web browser 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.

If the file system is full (i.e. contains the three system files mentioned above plus two other files), it is not possible to create new files, but an existing file must be overwritten or another deleted first.

Upload Configuration

File To Upload

選擇檔案 未選擇任何檔案

Destination File

File Name Parameters

- running-config Replace Merge
- startup-config
- Create new file

Upload

7.4.4 Activate

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

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

Activate Configuration

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

- default-config
- startup-config

Activate

7.4.5 Delete

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.

Delete Configuration File

Select configuration file to delete.

File Name

startup-config

Delete

Delete Configuration File

Click to delete configuration file.

Technical Specifications

Standards

- ITU-T G.8013/Y.1731
- IEEE 802.1ag
- IEEE 802.3ah
- IEEE 802.1d
- IEEE 802.1p
- IEEE 802.1Q
- IEEE 802.1s
- IEEE 802.1w
- IEEE 802.1X
- IEEE 802.1ab
- IEEE 802.1ad
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3x
- IEEE 802.3az (RJ-45 ports only)
- IEEE 802.3ab
- IEEE 802.1ax
- IEEE 802.3z

Device Interface

- 12 x SFP slots (100/1000Mbps)
- 2 x Shared Gigabit ports (RJ-45 or SFP slots)
- 1 x RJ-45 management port (in-band)
- 1 x RJ-45 console port (out-of-band)
- Ground point
- LED indicators
- Reset button

Data Transfer Rate

- Ethernet: 10Mbps (half duplex), 20Mbps (full duplex)

- Fast Ethernet: 100Mbps (half duplex), 200Mbps (full duplex)
- Gigabit Ethernet: 2000Mbps (full duplex)

Performance

- Switching capacity: 28Gbps
- RAM buffer: 128MB
- MAC address table: 8K entries
- Jumbo frames: 9.6KB (configurable per port)
- Forwarding mode: store and forward
- Forwarding rate: 20.8Mpps (64-byte packet size)

Management

- CLI (Console / Telnet / SSHv2)
- HTTP / HTTPS web based GUI
- SNMP v1, v2c, v3
- SNMP trap
- RMON groups 1/2/3/9
- LLDP/LLDP-MED with optional TLVs
- ICMPv4/ICMPv6
- IPv4/IPv6
- IPv6 neighbor discovery
- DNS proxy
- Network time protocol (NTP)
- Green Ethernet/EEE or 802.3az per port
- Dual image

Monitoring

- CPU load
- IP interfaces/routing table
- Internal system logging
- External syslog
- Port traffic statistics
- QoS queue counters

- QCL control list
- Port mirror (One to one, many to one)
- EVC (Ethernet Virtual Connection) statistics
- MAC address table
- Digital diagnostics monitoring (DDM) for SFP modules
- RFC2544 support
- sFlow statistics

MIB

- MIB II RFC 1213
- Bridge MIB IEEE8021-Q
- RMON (Group 1,2,3,9) RFC 2819
- Interface group MIB using SMiv2 RFC 2863
- Multicast group membership discovery MIB RFC 5519
- SNMP management frameworks RFC 3411
- User-based security model for SNMPv3 RFC 3414
- View-based access control model for SNMP RFC 3415
- Ethernet-like MIB RFC 3635
- 802.3 MAU MIB RFC 3636
- Entity MIB v3 RFC 4133
- Bridge MIB RFC 4188
- IP MIB RFC 4293
- RADIUS authentication client MIB RFC 4668
- RADIUS accounting MIB RFC 4670
- LLDP-MIB IEEE802.1AB
- PAE MIB IEEE802.1X

Spanning Tree

- Spanning tree protocol (STP)
- Rapid spanning tree protocol (RSTP)
- Multiple spanning tree protocol (MSTP)

Link Aggregation

- Static link aggregation and 802.3ad dynamic LACP (Up to 15 groups)

Quality of Service (QoS)

- Class of service (CoS)
- Set default drop precedence (DPL), priority code point (PCP), drop eligible indicator (DEI)
- Differentiated Services Code Point (DSCP) classification and translation
- Set egress port scheduler, port shaping, port tag marking
- Bandwidth control per port/rate limiting
- Queue scheduling: strict priority (SP), deficit weighted round robin (DWRR)

Storm Control

- Broadcast (Min. limit: 1pps)
- Multicast (Min. limit: 1pps)
- Unicast (Min. limit: 1pps)

VLAN

- 802.1Q tagged VLAN
- 802.1ad VLAN Q-in-Q
- MAC-based VLAN
- Protocol-based VLAN
- VLAN ID range 1-4095
- Private VLAN/port isolation
- Voice VLAN (16 user defined OUIs)
- VLAN port to group and VID translation

Carrier Ethernet / OAM

- IEEE 802.1ag Connectivity Fault Management (CFM)
- IEEE 802.3ah Link OAM
- Per port per queue dual leaky bucket service policers with PCP or DSCP marking per service point
- Statistics and tagging options per service point
- Y.1731 Fault Management (AIS, RDI, LCK)

- Y.1731 Performance Management (LM, DM)
- RFC2544 support
- Link OAM statistics, port status, event status
- Link state tracking
- Link OAM MIB Retrieval
- Maintenance entity point (MEP)

Link Protection

- ITU-T G.8032/Y.1344 Ethernet ring protection switching (ERPS)
- ITU-T G.8031/Y.1342 Ethernet linear protection switching

L3 Features

- IPv4 / IPv6 static routing
- IPv4 interfaces: Up to 8
- IPv6 interfaces: Up to 8
- Routing table entries: Up to 32 (IPv4 / IPv6)
- ARP table (up to 1024 entries)
- DHCP IPv4 server, relay, option 82
- Inter-VLAN routing

Multicast

- IGMP snooping v1, v2, v3
- IGMP fast leave
- Static multicast entries
- MLD Snooping v1, v2
- Multicast VLAN Registration (MVR)
- Up to 1K multicast groups

Access Control

- User account control with privilege level management
- Access management control
- Port Security/MAC address learning restriction (Up to 64 entries per port)
- 802.1X port-based/single/multiple or MAC-based authentication

- RADIUS (Up to 5 servers)
- TACACS+ (Up to 5 servers)
- RADIUS assigned QoS/VLAN/Guest VLAN
- Local dial in user authentication
- DHCP IPv4 snooping
- Loopback detection/prevention
- IP Source Guard
- Static/dynamic ARP inspection
- Create ACLs based on rate limit/EVC profile

Power

- Input: 100 – 240V AC, 50/60 Hz
- Max. Consumption: 36W

Fan/Acoustics

- Fanless design

MTBF

- 118,034 hours

Operating Temperature

- 0° – 50° C (32° – 122° F)

Operating Humidity

- Max. 95% non-condensing

Dimensions

- 280 x 185 x 44.45mm (11.02 x 7.28 x 1.75 in.)
- Rack mountable 1U height
- Wall mountable

Weight

- 1.6 kg (3.52 lbs.)

Certifications

- CE
- FCC
- UL

Troubleshooting

Q: I typed <http://192.168.10.200> in my Internet Browser Address Bar, but an error message says “The page cannot be displayed.” How can I access the switch management page?

Answer:

1. Check your hardware settings again. See “[Switch Installation](#)” on page 8.
2. Make sure the Power and port Link/Activity and WLAN lights are lit.
3. Make sure your network adapter TCP/IP settings are set to [Use the following IP address or Static IP](#) (see the steps below).
4. Make sure your computer is connected to one of the Ethernet switch ports.
5. Since the switch default IP address is 192.168.10.200, make sure there are no other network devices assigned an IP address of 192.168.10.200

Windows 7/8.1/10

- a. Go into the **Control Panel**, click **Network and Sharing Center**.
- b. Click **Change Adapter Settings**, right-click the **Local Area Connection** icon.
- c. Then click **Properties** and click **Internet Protocol Version 4 (TCP/IPv4)**.
- d. Then click **Use the following IP address**, and make sure to assign your network adapter an IP address in the subnet of 192.168.10.x. Click **OK**

Windows Vista

- a. Go into the **Control Panel**, click **Network and Internet**.
- b. Click **Manage Network Connections**, right-click the **Local Area Connection** icon and click **Properties**.
- c. Click **Internet Protocol Version (TCP/IPv4)** and then click **Properties**.
- d. Then click **Use the following IP address**, and make sure to assign your network adapter an IP address in the subnet of 192.168.10.x. Click **OK**

Windows XP/2000

- a. Go into the **Control Panel**, double-click the **Network Connections** icon
- b. Right-click the **Local Area Connection** icon and click **Properties**.
- c. Click **Internet Protocol (TCP/IP)** and click **Properties**.
- d. Then click **Use the following IP address**, and make sure to assign your network adapter an IP address in the subnet of 192.168.10.x. Click **OK**

Note: *If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.*

Q: If my switch IP address is different than my network's subnet, what should I do?

Answer:

You should still configure the switch first. After all the settings are applied, go to the switch configuration page, click on System, click IPv4 Setup and change the IP address of the switch to be within your network's IP subnet. Click Apply, then click OK. Then click Save Settings to Flash (menu) and click Save Settings to Flash to save the IP settings to the NV-RAM.

Q: I changed the IP address of the switch, but I forgot it. How do I reset my switch?

Answer:

Using a paper clip, push and hold the reset button on the front of the switch and release after 15 seconds.

The default IP address of the switch is 192.168.10.200. The default user name and password is “admin”.

Appendix

How to find your IP address?

Note: Please note that although the following procedures provided to follow for your operating system on configuring your network settings can be used as general guidelines, however, it is strongly recommended that you consult your computer or operating system manufacturer directly for assistance on the proper procedure for configuring network settings.

Command Prompt Method

Windows 2000/XP/Vista/7/8.1/10

1. On your keyboard, press **Windows Logo+R** keys simultaneously to bring up the Run dialog box.
2. In the dialog box, type **cmd** to bring up the command prompt.
3. In the command prompt, type **ipconfig /all** to display your IP address settings.

MAC OS X

1. Navigate to your **Applications** folder and open **Utilities**.
2. Double-click on **Terminal** to launch the command prompt.
3. In the command prompt, type **ipconfig getifaddr <en0 or en1>** to display the wired or wireless IP address settings.

Note: **en0** is typically the wired Ethernet and **en1** is typically the wireless Airport interface.

Graphical Method

MAC OS 10.6/10.5

1. From the Apple menu, select **System Preferences**.
2. In System Preferences, from the **View** menu, select **Network**.
3. In the Network preference window, click a network port (e.g., Ethernet, AirPort, modem). If you are connected, you'll see your IP address settings under "Status:"

MAC OS 10.4

1. From the Apple menu, select **Location**, and then **Network Preferences**.
2. In the Network Preference window, next to "Show:", select **Network Status**. You'll see your network status and your IP address settings displayed.

Note: If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.

How to configure your network settings to use a static IP address?

Note: Please note that although the following procedures provided to follow for your operating system on configuring your network settings can be used as general guidelines, however, it is strongly recommended that you consult your computer or operating system manufacturer directly for assistance on the proper procedure for configuring network settings.

Windows 7/8.1/10

- a. Go into the **Control Panel**, click **Network and Sharing Center**.
- b. Click **Change Adapter Settings**, right-click the **Local Area Connection** icon.
- c. Then click **Properties** and click **Internet Protocol Version 4 (TCP/IPv4)**.
- d. Then click **Use the following IP address**, and assign your network adapter a static IP address. Click **OK**

Windows Vista

- a. Go into the **Control Panel**, click **Network and Internet**.
- b. Click **Manage Network Connections**, right-click the **Local Area Connection** icon and click **Properties**.
- c. Click **Internet Protocol Version (TCP/IPv4)** and then click **Properties**.
- d. Then click **Use the following IP address**, and assign your network adapter a static IP address. Click **OK**

Windows XP/2000

- a. Go into the **Control Panel**, double-click the **Network Connections** icon
- b. Right-click the **Local Area Connection** icon and the click **Properties**.
- c. Click **Internet Protocol (TCP/IP)** and click **Properties**.
- d. Then click **Use the following IP address**, and assign your network adapter a static IP address. Click **OK**

MAC OS 10.4/10.5/10.6

- a. From the **Apple**, drop-down list, select **System Preferences**.
- b. Click the **Network** icon.
- c. From the **Location** drop-down list, select **Automatic**.
- d. Select and view your Ethernet connection.

In MAC OS 10.4, from the **Show** drop-down list, select **Built-in Ethernet** and select the **TCP/IP** tab.

In MAC OS 10.5/10.6, in the left column, select **Ethernet**.

e. Configure TCP/IP to use a static IP.

In MAC 10.4, from the **Configure IPv4**, drop-down list, select **Manually** and assign your network adapter a static IP address. Then click the **Apply Now** button.

In MAC 10.5/10.6, from the **Configure** drop-down list, select **Manually** and assign your network adapter a static IP address. Then click the **Apply** button.

f. Restart your computer.

Note: *If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.*

How to find your MAC address?

In Windows 2000/XP/Vista/7/8.1/10,

Your computer MAC addresses are also displayed in this window, however, you can type **getmac -v** to display the MAC addresses only.

In MAC OS 10.4,

1. **Apple Menu > System Preferences > Network**
2. From the **Show** menu, select **Built-in Ethernet**.
3. On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.

In MAC OS 10.5/10.6,

1. **Apple Menu > System Preferences > Network**
2. Select **Ethernet** from the list on the left.
3. Click the **Advanced** button.
3. On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.



IMPORTANT NOTE:

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Country Code selection feature to be disabled for products marketed to the US/CANADA

RoHS

This product is RoHS compliant.



Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 2004/108/EC and 2006/95/EC.

- EN 62368-1: 2014
- EN 55032: 2015: (Class A)
- EN 61000-3-2: 2014
- EN 61000-3-3: 2013
- EN 55035: 2017



Directives:

Low Voltage Directive 2014/35/EU

EMC Directive EN 2014/30/EU

WEEE Directive 2012/19/EU

Ecodesign Directive 2009/125/EC

RoHS Directive 2011/65/EU

REACH Regulation (EC) No. 1907/2006

CE Mark Warning

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

Limited Warranty

TRENDnet warrants only to the original purchaser of this product from a TRENDnet authorized reseller or distributor that this product will be free from defects in material and workmanship under normal use and service. This limited warranty is non-transferable and does not apply to any purchaser who bought the product from a reseller or distributor not authorized by TRENDnet, including but not limited to purchases from Internet auction sites.

Limited Warranty

TRENDnet warrants its products against defects in material and workmanship, under normal use and service. Specific warranty periods are listed on each of the respective product pages on the TRENDnet website.

- AC/DC Power Adapter, Cooling Fan, and Power Supply carry a one-year warranty.

Limited Lifetime Warranty

TRENDnet offers a limited lifetime warranty for all of its metal-enclosed network switches that have been purchased in the United States/Canada on or after 1/1/2015.

- Cooling fan and internal power supply carry a one-year warranty

To obtain an RMA, the ORIGINAL PURCHASER must show Proof of Purchase and return the unit to the address provided. The customer is responsible for any shipping-related costs that may occur. Replacement goods will be shipped back to the customer at TRENDnet's expense.

Upon receiving the RMA unit, TRENDnet may repair the unit using refurbished parts. In the event that the RMA unit needs to be replaced, TRENDnet may replace it with a refurbished product of the same or comparable model.

In the event that, after evaluation, TRENDnet cannot replace the defective product or there is no comparable model available, we will refund the depreciated value of the product.

If a product does not operate as warranted during the applicable warranty period, TRENDnet shall reserve the right, at its expense, to repair or replace the defective product or part and deliver an equivalent product or part to the customer. The repair/replacement unit's warranty continues from the original date of purchase. All products that are replaced become the property of TRENDnet. Replacement products may be new or reconditioned. TRENDnet does not issue refunds or credit. Please contact the point-of-purchase for their return policies.

TRENDnet shall not be responsible for any software, firmware, information, or memory data of customer contained in, stored on, or integrated with any products returned to TRENDnet pursuant to any warranty.

There are no user serviceable parts inside the product. Do not remove or attempt to service the product by any unauthorized service center. This warranty is voided if (i) the product has been modified or repaired by any unauthorized service center, (ii) the product was subject to accident, abuse, or improper use, or (iii) the product was subject to conditions more severe than those specified in the manual.

Warranty service may be obtained by contacting TRENDnet within the applicable warranty period and providing a copy of the dated proof of the purchase. Upon proper submission of required documentation, a Return Material Authorization (RMA) number will be issued. An RMA number is required in order to initiate warranty service support for all TRENDnet products. Products that are sent to TRENDnet for RMA service must have the RMA number marked on the outside of return packages and sent to TRENDnet prepaid, insured and packaged appropriately for safe shipment. International customers

shipping from outside of the USA and Canada are responsible for any return shipping and/or customs charges, including but not limited to, duty, tax, and other fees.

Refurbished product: Refurbished products carry a 90-day warranty after date of purchase. Please retain the dated sales receipt with purchase price clearly visible as evidence of the original purchaser's date of purchase. Replacement products may be refurbished or contain refurbished materials. If TRENDnet, by its sole determination, is unable to replace the defective product, we will offer a refund for the depreciated value of the product.

WARRANTIES EXCLUSIVE: IF THE TRENDNET PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDNET'S OPTION, REPAIR OR REPLACE. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. TRENDNET NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, OR USE OF TRENDNET'S PRODUCTS.

TRENDNET SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW, TRENDNET ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN

CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATE, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT TRENDNET'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Governing Law: This Limited Warranty shall be governed by the laws of the state of California.

Some TRENDnet products include software code written by third party developers. These codes are subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL").

Visit <http://www.trendnet.com/gpl> or the support section on <http://www.trendnet.com> and search for the desired TRENDnet product to access to the GPL Code or LGPL Code. These codes are distributed WITHOUT WARRANTY and are subject to the copyrights of the developers. TRENDnet does not provide technical support for these codes. Please visit <http://www.gnu.org/licenses/gpl.txt> or <http://www.gnu.org/licenses/lgpl.txt> for specific terms of each license.

PWP07172015v3

2022/11/10



Product Warranty Registration

Please take a moment to register your product online.
Go to TRENDnet's website at <http://www.trendnet.com/register>

TRENDnet
20675 Manhattan Place
Torrance, CA 90501. USA